



A MITEL
PRODUCT
GUIDE

OpenScape Xpressions V7

Server Administration

Administrator Documentation
08/2025

Notices

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

Trademarks

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

© Copyright 2025, Mitel Networks Corporation

All rights reserved

Contents

History of Changes	31
1 Introduction	41
1.1 General Information about OpenScape Xpressions V7	41
1.1.1 Server Characteristics	42
1.1.2 Communications Platforms	43
1.1.3 Languages	43
1.2 New Features with OpenScape Xpressions V7 V7R1.5	45
1.3 New Features with OpenScape Xpressions V7 V7R1.1	45
1.4 New Features with OpenScape Xpressions V7 V7R1	47
1.5 New Features with OpenScape Xpressions V7 V7R0	48
1.6 Document Conventions	53
1.7 Manual Structure	53
1.8 About the XPR Documentation	54
1.8.1 Installation and Administration	54
1.8.2 User Manual	55
1.8.3 Notes for the Service Technician	58
1.9 Data Protection and Data Security	59
2 Server Structure	61
2.1 XPR Structure	61
2.1.1 License Service	62
2.1.2 XPR Kernel Components	63
2.1.2.1 XPR Administrator	63
2.1.2.2 Message Transfer Agent	63
2.1.2.3 Information Store (Database)	64
2.1.2.4 Extended Message Reporter Service	64
2.1.2.5 Configuration Service	65
2.1.2.6 Name Locator	65
2.1.3 XPR Access Protocol Layer (APL)	66
2.1.4 Interface Tools	69
2.2 Component-Based Platform Architecture	70
2.3 XPR Process Structure	71
2.4 Staggered Administration	72
2.5 XPR Addressing	73
3 Starting and Stopping the Server	75
3.1 Installing and Starting individual Components	78
3.2 Stopping and Uninstalling individual Components	79
4 User Data Administration	81
4.1 Database Fields Significance	82
4.2 Users vs. Contacts	95
4.3 Voice Mail Server Fields	96
4.3.1 Announcement Directory	96
4.3.2 Access Security	97
4.3.3 Announcement and Name Recording	98
4.3.4 System Recordings	98
4.3.5 Deputy Numbers	98
4.3.6 Notification Numbers	99

Contents

4.3.7 Time Profiles	100
4.3.7.1 Simplified Time Profiles	103
4.3.8 Privileges	105
4.3.9 User Options	106
4.3.10 Specific Hicom PBX Fields	108
4.3.11 Login Information	108
4.3.12 Filter Rules	109
4.3.13 Message Folder	110
4.3.14 Sequence of Offered Messages	110
4.3.15 Trusted Phone Devices	111
4.3.16 Fax and Print Devices	111
4.4 The Mask Description Language MDL	112
4.4.1 Editing Masks	117
4.5 Privileges	118
4.5.1 Customer Specific Privileges	129
4.6 Assigning Voice Mail Settings group-specifically	130
4.7 PIN Handling in the XPR Server	132
4.7.1 Using personal User PINs	132
4.7.2 User PIN handling in the TUI and in the Web Assistant	133
4.7.2.1 Length defaults for PINs	134
4.7.2.2 Connection Abortion after wrong PIN Entries	134
4.7.2.3 Locking the Voice Box after wrong PIN Entries	134
4.7.2.4 Regular mandatory PIN Alteration	135
4.7.2.5 Warning before PIN Validity Expires	135
4.7.2.6 Default-PIN Definition	135
4.7.2.7 Trusted Numbers	136
4.7.2.8 PIN Check	137
4.7.2.9 Summary	139
4.8 Password Handling in the XPR Server	140
4.8.1 Authentication Mode in the XPR Server	140
4.8.2 Locking after several wrong Password Entries	141
4.8.3 Changing to the new Security Concept	141
4.8.4 Password Policies	142
4.8.4.1 OpenScape Xpressions V7 Authentication	142
4.8.4.2 Windows Authentication	143
5 XPR Service Provider (MSP)	151
5.1 Configuration	153
5.1.1 User Profiles	153
5.1.1.1 Editing a Profile	155
5.1.2 Server	156
5.1.3 Extended Settings	158
5.2 Configuring an Administrative User Profile	159
5.3 NAT Firewall Scenario	160
5.4 Client log-in via Windows User Account	162
5.4.1 Automatic Configuration	162
5.5 Client Log-in via Novell Network User Account	163
5.5.1 Automatic Configuration	163
5.6 Client Firewall	163
5.7 Automatic Client Update	164
6 XPR Monitor	167
6.1 Security	167

6.2	Configuration Lock	168
6.3	Operation	169
6.4	Creating a new Monitor Layout	170
6.4.1	Configuring a Logging Monitor	171
6.4.2	Configuring Line Monitors	173
6.4.3	Saving Monitor Layouts	174
6.5	Default-Layout Options	175
6.5.1	Modules	175
6.5.2	Line Window	175
6.5.3	Logging Monitor	176
6.5.4	OpenScope Voice Trace Manager (OSVTM)	177
6.6	Main Log File	177
6.7	Active Alert	178
6.8	Logging Profile	179
6.8.1	The Default Log Profile	179
6.9	Monitor Usage Examples	180
6.9.1	Line Monitor	180
6.9.2	Special Analysis Session	181
6.10	Local Installation	182
6.11	Remote Desktop Connection Specials	183
6.12	Access Overview of the Configuration Modules	183
7	Message Transfer Agent (MTA)	185
7.1	Configuration	185
7.1.1	Automatic Maintenance	185
7.1.1.1	Automatic Cleanup	186
7.1.1.2	System Monitoring	192
7.1.1.3	Active Alerts	193
7.1.2	Remote System Link	195
7.1.2.1	Properties	196
7.1.3	Routing Rules	200
7.1.4	Advanced	202
7.1.5	Global Journal	207
7.1.6	Logical Lines	209
7.1.7	Text-to-Speech	210
7.1.8	Fax Conversions	211
7.1.9	Session Monitoring	213
7.2	Maintenance Script	214
7.2.1	Actions	215
7.2.2	Variables	223
7.3	Backup	227
7.3.1	Syntax of the Backup Script	229
7.3.2	Recovery	230
7.3.3	Transactions	232
7.3.4	Backing up the PostgreSQL Database	233
7.4	XPR Server Rules	234
7.4.1	Rule Application within the Kernel	234
7.4.1.1	Application of the Routing Rules	235
7.4.2	First Rules Examples	236
7.4.2.1	Routing through Pattern Matching	236
7.4.2.2	Routing via Address Books	237
7.4.3	Rule Structure	238

Contents

7.4.3.1 Rule Element Address1 Structure	238
7.4.3.2 Rule Element Structure - Condition	238
7.4.3.3 Rule Element Address2 Structure	245
7.4.3.4 Rule Element Structure - Assignment	245
7.4.4 Extended Rule Syntax	248
7.4.4.1 Regular Expressions	248
7.4.5 Meta Rules	252
7.4.6 RouteLets	253
7.4.7 Examples and Uses	254
7.4.7.1 Routing Rules	254
7.4.7.2 Carbon Copy Rules (Send Copies)	258
7.4.7.3 Awake Rules	260
7.4.8 Automatic Report Transmission by Mail	262
7.4.8.1 Report Forms Installation	262
7.4.8.2 Report Forms Structure	263
7.4.8.3 Subject Customizing	265
7.4.8.4 Normal Report Suppression	265
7.4.9 Error Handling	266
7.4.10 Recursions	266
7.4.11 Tips for setting Rules	266
7.4.12 Testing new Rules	266
7.5 Watchdog Process	267
7.5.1 How the Watchdog functions	267
7.5.2 Watchdog Configuration	269
7.6 Heartbeat Monitor	270
7.7 Distributed XPR Server	272
7.7.1 Firewalls between Nodes of a distributed XPR Server	273
7.8 TCP/IP Ports used by the XPR Server	284
7.9 Message Waiting Indication (MWI)	287
7.9.1 Counter-based CIT	289
7.10 Simple Network Management Protocol (SNMP)	290
7.10.1 Translating Events into Traps	290
7.10.1.1 Modifying the SNMP Management System	295
7.10.1.2 Deleting the SNMP Management System	295
8 System Networking	299
8.1 General Structure of an SN Network	299
8.2 Administrative Network Access	301
8.3 The XPR Location Profile	302
8.3.1 Site Profile Information	303
8.3.2 Protocol Export	306
8.3.3 Site Profiles and PhoneMail Systems	307
8.3.4 Message Transmission String	308
8.3.4.1 Correcting the Message Transmission String	308
8.4 The XPR Network Profile	310
8.4.1 Network Profile Usage	310
8.4.2 Network Profiles and PhoneMail Systems	310
8.5 Configuration Management of the SN Network	311
8.5.1 Exchange of SN Node Configuration Modifications	312
8.5.2 Information Exchange	314
8.5.2.1 Profile Exchange via the 'Push' Mechanism	314
8.5.2.2 Profile Exchange via the 'Piggy-Back' Mechanism	315

8.5.2.3 Automatic Profile Exchange	315
8.5.3 Remote Access.	316
8.6 Configuration Management in PhoneMail Networks	318
8.6.1 Exchange of Configuration Modifications	318
8.6.2 Exchange of User and Distribution Lists.	319
8.6.3 Remote Access.	319
8.7 General Configuration of an SN Network.	320
8.7.1 Configuring the first Node of an SN Network	320
8.7.2 Adding a Node to an SN Network.	321
8.7.3 Restoring an SN Node	322
8.7.4 Integration of PhoneMail Networks.	323
8.8 User Addressing in an SN Network	324
8.8.1 Prefix Dialing.	324
8.8.2 Co-Location Dialing	325
8.8.3 Convenient Dialing	326
8.9 User-Message Exchange between SN Network Nodes.	326
8.10 Exchanging User Messages in PhoneMail Networks.	328
8.11 SMTP Routing via Relay Host	328
8.12 Security Mechanisms.	329
8.13 Adjusting the Maintenance Script	330
9 Number Conversion Object (NCO)	331
9.1 What is NCO?	332
9.2 Calling Number Handling in the XPR Server	333
9.3 Technological Concepts.	336
9.3.1 The general NCO Concept.	337
9.3.2 The NCO Elements.	337
9.3.2.1 <i>NCOAdmin</i> – The NCO Administration	339
9.3.2.2 Number Conversion Object (NCO)	340
9.3.2.3 Location.	340
9.3.2.4 Normalization Rule Set	341
9.3.2.5 Localization Rule Set.	341
9.3.2.6 Call Type Checker.	341
9.3.2.7 NCO Clients	342
9.3.2.8 Connect Points	343
9.3.2.9 Variables	343
9.3.3 The normalized NCO Phone Number Format	345
9.3.3.1 Format identifier	345
9.3.3.2 Phone number portion.	345
9.3.3.3 Phone Number Appendix	346
9.3.4 NCO Clients and Connect Points	347
9.3.5 Location, Phone Numbers and Prefixes	350
9.3.6 NCO Conditions	353
9.3.6.1 Batch Condition	354
9.3.6.2 Negating Condition	354
9.3.6.3 Number Range Condition	354
9.3.6.4 Number Length Condition	355
9.3.6.5 Regular Expression Condition.	355
9.3.6.6 Set of Conditions	356
9.3.6.7 Variable Condition	356
9.3.7 Localization and Normalization Rules.	357
9.3.7.1 Batch Rule.	360

Contents

9.3.7.2	Regular Expression Rule	363
9.3.7.3	Set of rules	365
9.3.7.4	Corporate Network Pre-Processing Rule	366
9.3.8	Batch and regular Expressions	367
9.3.9	Call Type Checker and Conditions	370
9.3.10	Administering NCO Variables – Name Areas	372
9.3.11	Export and Import of NCO Elements	375
9.3.12	Range Lists	376
9.3.12.1	What is a Range List?	376
9.3.12.2	Range List Structure	376
9.3.12.3	Check Directions for a Number Range List	377
9.3.12.4	Match Behavior using Common Codes	379
9.3.12.5	Assigning Variables during a Check-up	380
9.3.12.6	Definition of a Range List	380
9.3.12.7	The Condition of Type <i>Number Range</i>	382
9.3.13	Saving the NCO Configuration	383
9.3.14	Structure of the NCO Installation for a XPR Reinstallation	384
9.3.14.1	XPR Server Basic Settings	384
9.3.14.2	NCO Clients basic Settings	386
9.3.14.3	Further Settings	386
9.4	NCOAdmin Start – Access to NCO Configurations	387
9.4.1	Access to a local NCO Configuration	388
9.4.2	Access to a non-local NCO Configuration	388
9.4.2.1	Network Access to an NCO Configuration	389
9.4.2.2	NCOAdmin with Internet Access to an NCO Configuration	390
9.5	Configuring the NCO Elements	393
9.5.1	Defining a new NCO	394
9.5.2	Defining a new Location	396
9.5.3	Defining a new Variable	398
9.5.4	Defining a new Number Range List	400
9.5.4.1	Defining a Number Range List within a Location	400
9.5.4.2	Defining a Number Range List as Variable	402
9.5.5	Defining a new Condition	403
9.5.6	Defining a new Conversion Rule Set	404
9.6	Configuration Example of Number Conversion Objects (NCO)	405
9.6.1	Example Scenario	405
9.6.2	Example Configuration	406
9.7	NCO in a <i>Corporate Network</i> Environment	418
9.7.1	<i>Corporate Network</i>	418
9.7.2	<i>Corporate Network</i> Rules	420
9.7.2.1	Corporate Network Preprocessing Rule	420
9.7.2.2	Corporate Network Conversion Rule	421
9.7.3	Example of a Corporate Network Configuration	422
9.8	The <i>Number Conversion Prepare</i> Tool	432
9.8.1	How the Tool works	432
9.8.2	The Initialization File	432
9.8.3	Invoking the Tool	434
9.8.4	Using the Tool	434
9.9	Reference to the Number Conversion Administrator (NCOAdmin)	435
9.9.1	What is the NCOAdmin?	436
9.9.2	The <i>File</i> Menu	436
9.9.3	NCOs	438

9.9.3.1	Editing NCO	440
9.9.3.2	NCO Tester	441
9.9.4	NCO Clients	443
9.9.4.1	Editing NCO Clients	444
9.9.4.2	Editing Connect Points	446
9.9.5	NCO Locations	447
9.9.5.1	Editing Locations	449
9.9.5.2	Location Settings Corporate Network	451
9.9.5.3	Range List Editor of a Location	452
9.9.6	NCO Call Types	453
9.9.6.1	Editing the Call Type Checker	455
9.9.6.2	Editing the Conditions of a Call Type	457
9.9.7	Normalization Rule Sets	459
9.9.7.1	Rule Set Editing	461
9.9.8	Localization Rule Sets	462
9.9.9	Variables	463
9.9.9.1	Range List Editor of a Variable	465
9.9.10	Configuration	466
9.9.11	NCO Conditions	468
9.9.11.1	Number Length Condition	468
9.9.11.2	Number range Condition	469
9.9.11.3	Variable Check Condition	471
9.9.11.4	Batch Condition	472
9.9.11.5	Regular Expression Condition	474
9.9.11.6	Set of Conditions	475
9.9.11.7	Negating Condition	477
9.9.12	NCO Rules	478
9.9.12.1	Batch Rule – the <i>Condition Tab</i>	478
9.9.12.2	Batch Rule – the <i>Processing Instruction Tab</i>	479
9.9.12.3	Batch Rule – the <i>Result Tab</i>	481
9.9.12.4	Regular Expression Rule – the <i>Conditions Tab</i>	484
9.9.12.5	Regular Expression Rule – the <i>Processing Instruction Tab</i>	485
9.9.12.6	Regular Expression Rule – the <i>Result Tab</i>	486
9.9.12.7	Rule Set Rule – the <i>Condition Tab</i>	490
9.9.12.8	Rule Set Rule – the <i>Set of rules Tab</i>	491
9.9.12.9	Rule Set Rule – the <i>Result Tab</i>	493
9.9.13	NCO Variables Reference	495
9.9.13.1	Variables in the <i>Built-In Area</i>	496
9.9.13.2	Variables in the <i>Client specific Area</i>	498
9.9.13.3	Variables in the <i>Corporate Network Area</i>	508
9.9.13.4	Variables in the <i>Location Area</i>	516
9.9.13.5	Variables in the <i>Others Area</i>	520
10	Telematics APL	525
10.1	General Technological Concepts	526
10.1.1	Telematics Program Libraries	526
10.1.1.1	The Modules <i>TeleReg</i> and <i>TeleReg API</i>	526
10.1.1.2	The Modules <i>TeleCfg</i> and <i>TeleCfg API</i>	526
10.1.1.3	The Modules <i>TeleLib</i> and <i>TeleLib API</i>	527
10.1.2	Number Conversion Objects (NCO)	528
10.1.2.1	Normalized and localized Calling Number Format	528
10.1.2.2	The NCO Elements	529

Contents

10.1.3	Trusted Transfer Mode (TTM)	532
10.1.3.1	How the Trusted Transfer Mode operates	532
10.1.3.2	Calling Number Schema	534
10.1.3.3	Trusted Transfer Mode Specials	537
10.1.3.4	Activating the Trusted Transfer Mode	537
10.1.4	Voice Mail Networking	539
10.1.4.1	AMIS	540
10.1.4.2	VPIM	545
10.1.4.3	PhoneMail Connection (Hardware-PhoneMail)	548
10.1.5	Redirecting Numbers	551
10.1.5.1	What are Redirecting Numbers?	551
10.1.5.2	Cascaded Forwarding	552
10.1.5.3	Supporting Redirecting Numbers	553
10.1.5.4	Function Test for Redirecting Numbers	553
10.1.5.5	Known Problems with Redirecting Numbers in PBX Systems	554
10.1.6	Features of D-channel Protocols	555
10.1.6.1	Ergo	555
10.1.6.2	VMS	556
10.1.6.3	PhoneMail	557
10.1.7	Memory Requirements for Voice Messages	558
10.1.7.1	ISDN APL Memory Requirements	558
10.1.7.2	IP APL Memory Requirements	558
10.1.8	Call Attached Data (CAD)	559
10.2	Technological Concepts of the ISDN APL	560
10.2.1	ISDN APL Telematics Services	560
10.2.2	Supported ISDN Boards	560
10.2.3	CorNet-N Support	561
10.3	Technological Concepts of the IP APL	562
10.3.1	IP APL Usage Environment	563
10.3.2	IP APL Structure	564
10.3.3	TAPI-based Connection	566
10.3.4	H.323	567
10.3.5	CorNet IP	568
10.3.6	Session Initiation Protocol (SIP)	569
10.3.6.1	SIP Network Components	569
10.3.6.2	Addressing an SIP Subscriber	571
10.3.6.3	Interaction between logical SIP Components	572
10.3.6.4	SIP Support in the IP APL	575
10.3.7	Fax-over-IP (T.38)	576
10.3.7.1	T.38 Scenarios	577
10.3.7.2	Fax via T.38 or G.711?	577
10.3.7.3	T.38 Fax Support in the IP APL	578
10.3.7.4	Fax (G.711) Support in the IP APL	578
10.3.8	Transmitting DTMF Tones (RFC 2833)	579
10.3.8.1	Using the RFC 2833 in the IP APL	580
10.3.9	Quality of Service (QoS)	581
10.3.10	Public Key Infrastructure (PKI)	582
10.3.10.1	Reasons for Encryption	582
10.3.10.2	Asymmetric Encryption	582
10.3.10.3	Public-Key Exchange via Certificates	584
10.3.10.4	PKI Usage in the IP APL	584
10.3.11	Multimedia Internet Keying (MIKEY)	585

10.3.12	Encryption of the Signaling (TLS)	586
10.3.12.1	Transport Layer Security (TLS)	586
10.3.12.2	Using TLS in the XPR Server Environment	587
10.3.12.3	TLS Support in the IP APL	588
10.3.13	Encryption of the RTP Communication (SRTP)	588
10.3.13.1	Secure Realtime Transport Protocol (SRTP)	588
10.3.13.2	Using SRTP in the XPR Server Environment	589
10.3.13.3	SRTP Support in the IP APL	590
10.3.14	IP APL at a Layer 3 Cluster of OpenScape Voice	590
10.3.15	IP APL at an SIP Gateway Cluster	591
10.4	Protocols of the XPR Server	593
10.4.1	Evo	594
10.4.1.1	Installation of the EVO Protocol	595
10.4.1.2	Parameter Tab <i>General</i>	597
10.4.1.3	Parameter Tab <i>Options</i>	598
10.4.1.4	Parameter Tab <i>Menu</i>	599
10.4.1.5	Parameter Tab <i>Prompts</i>	600
10.4.1.6	Parameter Tab <i>Special</i>	602
10.4.1.7	Parameter Tab <i>Name Dialing</i>	605
10.4.1.8	Parameter Tab <i>Speech Recognition</i>	608
10.4.1.9	Parameter Tab <i>Customer</i>	612
10.4.1.10	Parameter Tab <i>Test</i>	615
10.4.1.11	Adjusting the XPR Routing Rules	616
10.4.2	Ergo	617
10.4.2.1	Parameter Tab <i>General</i>	618
10.4.2.2	Parameter Tab <i>Options</i>	620
10.4.2.3	Parameter Tab <i>Menu</i>	622
10.4.2.4	Parameter Tab <i>Prompts</i>	623
10.4.2.5	Parameter Tab <i>Special</i>	625
10.4.2.6	Parameter Tab <i>Customer</i>	628
10.4.2.7	Parameter Tab <i>OpenScape</i>	635
10.4.2.8	Parameter Tab <i>Test</i>	636
10.4.2.9	Adjusting the XPR Routing Rules	637
10.4.3	PhoneMail	638
10.4.3.1	Configuration Tab <i>General</i>	639
10.4.3.2	Configuration Tab <i>Identification</i>	639
10.4.3.3	Configuration Tab <i>Repeat Strategy</i>	639
10.4.3.4	Configuration Tab <i>Formats</i>	640
10.4.3.5	Configuration Tab <i>Attributes</i>	640
10.4.3.6	Configuration Tab <i>Private</i>	640
10.4.3.7	Configuration Tab <i>Script</i>	640
10.4.3.8	Parameter Tab <i>General</i>	641
10.4.3.9	Parameter Tab <i>Options</i>	645
10.4.3.10	Parameter Tab <i>Settings</i>	646
10.4.3.11	Parameter Tab <i>Addressing</i>	647
10.4.3.12	Parameter Tab <i>OpenScape</i>	649
10.4.3.13	Parameter Tab <i>Customer</i>	651
10.4.3.14	PhoneMail Language Settings	664
10.4.3.15	Company-specific Greetings	664
10.4.3.16	Company-specific Menu Adjustments	665
10.4.3.17	Connecting to a Message Originator with Hicom 150E Office	669
10.4.3.18	Repeat Strategy for User Outcall	669

Contents

10.4.3.19	Default Allocation for Shortcuts	669
10.4.3.20	Out-of-Office Greetings	673
10.4.3.21	Company-internal Messages	674
10.4.3.22	Guest Mailbox	675
10.4.4	Voicemail VMS	678
10.4.4.1	Configuration Tab <i>General</i>	679
10.4.4.2	Configuration Tab <i>Identification</i>	680
10.4.4.3	Configuration Tab <i>Repeat Strategy</i>	680
10.4.4.4	Configuration Tab <i>Formats</i>	680
10.4.4.5	Configuration Tab <i>Attributes</i>	680
10.4.4.6	Configuration Tab <i>Script</i>	681
10.4.4.7	Parameter Tab <i>General</i>	682
10.4.4.8	Parameter Tab <i>System</i>	684
10.4.4.9	Parameter Tab <i>Recording</i>	685
10.4.4.10	Parameter Tab <i>User prompts</i>	687
10.4.4.11	Parameter Tab <i>Addressing</i>	689
10.4.4.12	Parameter Tab <i>Customer</i>	691
10.4.4.13	Company-specific Greetings	696
10.4.4.14	VMS Language Settings	696
10.4.4.15	VMS Database Fields	697
10.4.4.16	Distribution Lists	697
10.4.4.17	Notification for User Outcall	698
10.4.5	Using the PhoneMail and VMS Protocols in parallel	699
10.4.5.1	Configuring Scripts	699
10.4.6	Fax G3	702
10.4.6.1	Configuration Tab <i>General</i>	704
10.4.6.2	Configuration Tab <i>Identification</i>	705
10.4.6.3	Configuration Tab <i>Fax G3</i>	706
10.4.6.4	Configuration Tab <i>Repeat Strategy</i>	707
10.4.6.5	Configuration Tab <i>Private</i>	708
10.4.6.6	Configuration Tab <i>Formats</i>	709
10.4.6.7	Configuration Tab <i>Attributes</i>	710
10.4.7	Fax G3 Post-Dialing	711
10.4.7.1	Configuration Tab <i>General</i>	713
10.4.7.2	Configuration Tab <i>Script</i>	714
10.4.7.3	Configuration Tab <i>Identification</i>	714
10.4.7.4	Configuration Tab <i>Repeat Strategy</i>	715
10.4.7.5	Configuration Tab <i>Formats</i>	715
10.4.7.6	Configuration Tab <i>Attributes</i>	715
10.4.7.7	Configuration Tab <i>Private</i>	715
10.4.8	Fax G3 Polling	715
10.4.9	Fax G4	716
10.4.9.1	Configuration Tab <i>Identification</i>	717
10.4.9.2	Configuration Tab <i>Fax G4</i>	717
10.4.9.3	Configuration Tab <i>Private</i>	718
10.4.10	Fax-on-Demand Server Script (Fax-on-Demand)	719
10.4.10.1	Direct Fax-on-Demand by Telephone (normal Mode)	720
10.4.10.2	Direct Fax-on-Demand via the Fax Device (normal Mode)	720
10.4.10.3	Fax-on-Demand by Telephone via DTMF (DTMF Mode)	721
10.4.10.4	Storing Fax-on-Demand Documents	722
10.4.10.5	Supervisor Mode for Administration	722
10.4.10.6	Configuration Tab <i>General</i>	725

10.4.10.7 Configuration Tab <i>Documents</i>	726
10.4.10.8 Configuration Tab <i>Supervisor</i>	727
10.4.10.9 Configuration Tab <i>Customer</i>	727
10.4.11 Fax-Fax Converter (Fax Forward)	728
10.4.11.1 Configuration Tab <i>Private</i>	730
10.4.12 Single Number	730
10.4.13 SMI	734
10.4.14 Voice	735
10.4.15 PlayWave	736
10.4.16 Hicom Message Waiting Indication (MWI)	738
10.4.16.1 Configuration Tab <i>Private</i>	738
10.4.17 Message Waiting Indication (MWI)	739
10.4.17.1 Configuration Tab <i>Private</i>	740
10.4.18 Pager	742
10.4.19 SMS (TAP or UCP Protocol)	748
10.4.19.1 Configuration Tab <i>Private</i>	749
10.4.20 AMIS	750
10.4.20.1 Configuration	751
10.4.21 CTI Computer Telephony Integration	757
10.4.22 CTI Light	759
10.4.23 Vogue	760
10.4.24 Caller Guide	763
10.4.24.1 Installation	764
10.4.24.2 Installation	765
10.4.24.3 Configuration	767
10.4.24.4 Defining the maximum Number of Search Hits	772
10.4.24.5 Tracking Phone Numbers and Personal Announcements	773
10.4.24.6 Defining Name Pronunciation	774
10.4.24.7 Excluding Users from the Caller Guide Search	776
10.4.25 Conversation Recorder	777
10.4.25.1 Technical Requirements	778
10.4.25.2 Permitting Conversation Recorder Protocol Usage	778
10.4.25.3 Installation	778
10.4.25.4 Configuration	778
10.4.25.5 Tips and Tricks	781
10.5 General Configuration of Telematics Services	782
10.5.1 Telematics Service Elements	782
10.5.1.1 Protocols	782
10.5.1.2 Location	783
10.5.1.3 Extensions	785
10.5.1.4 Devices	785
10.5.1.5 Trunk Groups	785
10.5.2 General Procedure for the Configuration of a Telematics Service	786
10.6 Telematics Service Configuration Example Scenarios	787
10.6.1 XPR Server via Tie Trunk without Trunk ID at a PBX	788
10.6.2 XPR Server via Tie Trunk <i>with</i> Trunk ID at a PBX	789
10.6.2.1 Trunk ID is Part of the XPR User Extension	789
10.6.2.2 Trunk ID is no Part of the XPR User Extension	791
10.6.3 XPR Server via internal S0-Bus at small PBX with MSNs	793
10.6.3.1 PBX with Point-to-Point Connection to the PSTN	793
10.6.3.2 PBX with Point-to-Multipoint Connection to the PSTN	794
10.6.4 XPR Server without PBX at the PSTN	795

Contents

10.6.4.1 XPR Server with Point-to-Point Connection to the PSTN	795
10.6.4.2 XPR Server with Point-to-Multipoint Connection to the PSTN	796
10.6.5 Remarks concerning the internal Phone Number Length	797
10.6.6 Remarks on Number Ranges	798
10.7 Specific Solutions with the Telematics APL	799
10.7.1 IP APL and the HiPath 3000	799
10.7.2 IP APL and the HiPath 5000	800
10.8 Creating a new SIP Certificate for the XPR Server.	801
10.9 Configuration Reference for ISDN Connections (ISDN APL)	804
10.9.1 Protocols	805
10.9.2 General Voicemail Settings (Voicemail)	811
10.9.2.1 <i>General Settings</i>	812
10.9.2.2 <i>Messaging Settings</i>	813
10.9.2.3 <i>Recording Settings</i>	815
10.9.2.4 <i>Security Settings</i>	816
10.9.2.5 <i>Call Transfer Settings</i>	819
10.9.2.6 <i>Prompt Settings</i>	821
10.9.2.7 <i>Customer Settings</i>	823
10.9.3 Extensions	824
10.9.4 Devices (Advanced Settings)	827
10.9.4.1 Device Properties	828
10.9.4.2 Trunk Group Properties	829
10.9.5 Locations	831
10.9.6 Resources (Advanced Settings)	832
10.9.7 Outbound (Advanced Settings)	834
10.10 Configuration Reference for Voice-over-IP Connections (IP APL)	837
10.10.1 Protocols	838
10.10.2 General Voicemail Settings (Voicemail).	841
10.10.3 Extensions	842
10.10.4 Devices (Advanced Settings).	842
10.10.4.1 Properties of H.323-based Devices	844
10.10.4.2 Properties of SIP-based Devices	858
10.10.4.3 Trunk Group Properties	873
10.10.5 Locations	873
10.10.6 Several IP APLs on one Server	874
10.10.6.1 Installation	874
10.11 Ending Telematics APLs “softly”	877
10.12 Supported Standards	878
11 Mail APL	879
11.1 Standard User Mailbox	879
11.2 Timed Copies	880
11.3 Broadcasts	881
11.4 Mailing Lists	883
11.5 Printer Embedded Codes	884
11.5.1 End-of-Job-Code	887
11.6 True Unified Messaging (TUM).	888
11.7 Distrib Protocol	889
11.8 The NIL Protocol	890
11.9 Address Book Consistency	891
11.10 Server CTI Journal	892
11.11 Vanity Number Support.	895

12 Internet Mail (SMTP APL)	897
12.1 Configuration	897
12.1.1 SMTP server	897
12.1.1.1 General Settings	898
12.1.1.2 E-Mail	899
12.1.2 Outgoing E-mail	903
12.1.3 POP3 Server	905
12.1.4 IMAP4 Server	907
12.1.5 Secure Sockets	909
12.1.6 Formats	911
12.1.7 POP3 Mail Import	912
12.1.7.1 New Database Fields	912
12.1.7.2 Authentication for sending	912
12.1.7.3 Active Schedules	913
12.2 SMTP (Simple Mail Transfer Protocol)	916
12.2.1 Authentication	916
12.2.1.1 SMTP after POP/IMAP	916
12.2.1.2 Authentication according to RFC 2554	916
12.2.2 Relay Authentication Strategy	917
12.2.3 Sending Mail via an SMTP Relay	918
12.2.4 Setting Reply-To Field	918
12.3 POP3 and IMAP4 Servers	919
12.3.1 Authentication	919
12.4 Standards	921
13 The XPR Webserver (Web APL)	923
13.1 Overview	923
13.2 Configuring the Web APL	924
13.2.1 HTTP Tab	924
13.2.2 CGI Tab	926
13.2.2.1 Configuring Single Sign-on (SSO)	927
13.2.2.2 Creating an HTML Forwarding Page	935
13.2.2.3 Using Web Protocols under Windows Server	935
13.2.2.4 Replication Trigger for LDAP	936
13.2.3 HTML Tab	937
13.2.4 SSL Tab	939
13.2.4.1 SSL Connection Problems	940
13.2.4.2 VeriSign Intermediate Certificate has expired	940
13.2.5 HTTP Client Tab	941
13.2.6 Firewall Tab	942
13.3 Standards	943
13.4 Enforcing SSL Accesses for the Web Assistant	943
13.5 Fax-printing Problems	944
13.6 Customizing the Web Assistant Interface	945
13.6.1 Data Transmission between Browser and XPR Server	945
13.6.2 Wildcard	946
13.6.3 Changing Web Assistant Default Settings	946
13.6.3.1 Appearance of the Interface Elements	947
13.6.3.2 New User and Groups	950
13.6.3.3 Authentication	952
13.6.3.4 Date and Time Formats	954
13.6.3.5 Default Language Settings	954

Contents

13.6.3.6	Filters for the User List in the User Administration	955
13.6.3.7	Message Settings	955
13.6.3.8	CTI Settings	956
13.6.3.9	Address Book Settings	956
13.6.3.10	Template Settings	958
13.6.3.11	Miscellaneous	961
13.6.4	Deactivating Web Assistant Features	963
13.6.4.1	Example: Hiding the <i>Notification</i> feature in the <code>Nav.html</code> file	964
13.6.5	Reference	966
13.6.5.1	show / hide	967
13.6.5.2	repeat	968
13.6.5.3	set	969
13.6.5.4	condition (<i>calculation</i>)	970
13.6.5.5	text	972
13.6.5.6	xp_if	973
13.6.5.7	xp_else	974
13.6.5.8	xp_elseif	975
13.6.5.9	xp_unless	976
13.6.5.10	xp_while	977
13.6.5.11	xp_until	978
13.6.5.12	xp_for	979
13.6.5.13	xp_switch	980
13.6.5.14	xp_case	981
13.6.5.15	xp_foreach	982
13.6.5.16	xp_set	983
13.6.5.17	xp_checkbox	984
13.6.5.18	xp_radio	985
13.6.5.19	xp_option	986
13.6.5.20	xp_block	987
13.6.5.21	xp_include	988
13.6.5.22	xp_compute	989
13.6.5.23	xp_hidden	990
13.6.5.24	xp_js_write	992
13.6.5.25	xp_no_space	993
13.6.5.26	xp_disp	994
13.6.6	Adjusting the Web Assistant Interface for different User Groups	995
13.7	Invoking XPR Functions from another Web Server	996
14	Short Message Service (SMS)	997
14.1	What is SMS?	997
14.2	SMS and XPR	997
14.2.1	SMS via ISDN: The Entry-level Solution	997
14.2.2	SMS via GSM Boxes	999
14.2.3	SMS via direct Provider Coupling	1000
14.3	Connection Type Comparison Overview	1004
14.4	Sending SMS Messages	1005
14.5	SMS Connector (SMSIPAPL)	1006
14.5.1	Installation	1006
14.5.2	Establishing and configuring a Connection	1006
14.5.2.1	Connections Tab	1007
14.5.2.2	Info & Statistics	1008
14.5.2.3	Establishing a new SMS Connection	1009

14.5.2.4 Configuring a new SMS Connection	1010
14.5.3 The Digest Algorithm	1021
14.5.4 Receiving SMS Messages	1024
14.5.4.1 Determining the Recipient	1024
14.5.5 Messages with Attachments	1024
14.5.6 Serial Adapters for GSM (COM Server)	1025
14.5.7 Automatic Monitoring of the SMS Device	1026
15 TCP/IP APL	1027
15.1 Ports and Encryption used	1027
15.2 Firewall Mechanism	1028
16 Notification APL	1033
16.1 General Overview	1033
16.2 Operating Requirements	1034
16.3 Notifications	1034
16.4 Configuration	1036
16.4.1 Formats	1036
16.4.2 Internal Settings	1038
16.4.3 Expert Settings	1040
16.5 Configuring Notifications	1042
16.6 MWI Fallback Strategy	1042
16.7 Web Message Access	1042
16.8 SMS/E-Mail Notifications	1044
16.9 Configuring a Repeat Strategy for User Outcall	1045
16.10 Examples of Routing Rule Adaption	1045
16.11 Problems with MWI via ISDN	1046
16.12 Problem with MWI LED	1046
17 CTI APL	1047
17.1 What is CTI?	1047
17.2 The CTI APL	1048
17.3 Technological Concepts for the CTI APL	1050
17.3.1 CTI Protocol Interfaces	1051
17.3.1.1 CSTA	1052
17.3.1.2 TSAPI	1052
17.3.1.3 TAPI	1053
17.3.2 CTI Transport Interfaces	1054
17.3.3 CTI Transactions	1054
17.3.4 CTI Features	1056
17.3.4.1 Set Monitor Points	1056
17.3.4.2 XPR Connection Model	1057
17.3.5 Device Profiles	1059
17.3.6 Multi PBX "AutoLearn" Mode	1065
17.3.7 Access Privileges	1069
17.3.7.1 Default Privileges	1069
17.3.7.2 Individual Privileges	1070
17.4 Example of a CTI Link Setup (CSTA)	1071
17.5 Connection to a HiPath 4000	1075
17.5.1 Installing the CA4000 Connector	1076
17.5.2 Configuring the CA4000 Connector	1077
17.5.3 CTI APL Configuration	1079
17.5.4 HiPath 4000 with E.164 Number Format	1080

Contents

17.6	Redundant Connection to OpenScape Voice with geographic Node Separation	1082
17.7	Configuration Reference	1083
17.7.1	CTI APL Settings	1084
17.7.2	Logging	1085
17.7.3	Assignment of Device Features	1087
17.7.3.1	New Device-Feature Assignment	1089
17.7.4	Terminal Device Features	1091
17.7.5	CSTA Settings	1093
17.7.5.1	Monitoring Parameters (CSTA)	1097
17.7.5.2	NCO Settings (CSTA)	1099
17.7.5.3	Trunk Lines (CSTA)	1101
17.7.5.4	Announcement Ports (CSTA)	1102
17.7.6	TSAPI/CSTA Link Properties (TSAPI)	1104
17.7.6.1	TSAPI/CSTA Advanced Settings (TSAPI)	1106
17.7.7	MS-TAPI Properties (TAPI)	1108
17.7.7.1	Select TAPI Lines (TAPI)	1111
17.8	Optimizing the CTI APL Starting Behavior	1112
17.9	PBXs in the CTI Environment	1114
17.10	Tips and Tricks	1114
17.10.1	Debug Filter Usage	1114
17.10.2	Error-Search Tools	1115
17.11	Standards supported in the CTI APL	1115
18	CSTA APL	1117
18.1	What is CSTA?	1117
18.2	CSTA APL Functionality	1117
18.3	CSTA APL Configuration	1119
18.3.1	Phone Numbers Tab	1119
18.3.2	Connectivity Tab	1120
19	The LDAP APL	1121
19.1	What is LDAP?	1121
19.2	LDAP and XPR	1122
19.3	The theoretic LDAP Structure	1123
19.4	The logical LDAP Model	1124
19.4.1	The LDAP Information Model	1124
19.4.1.1	Objects and Attributes	1124
19.4.1.2	Object Classes	1124
19.4.1.3	The Schema	1125
19.4.2	The LDAP Naming Model	1125
19.4.3	The LDAP Function Model	1127
19.4.4	The LDAP Security Model	1128
19.5	Directory Services	1129
19.5.1	Microsoft Active Directory	1130
19.5.2	Novell NDS eDirectory	1131
19.5.3	Further Directory Services	1131
19.6	Installing the LDAP APL	1132
19.6.1	LDAP APL Installation for Microsoft Exchange Server	1132
19.6.2	LDAP APL Installation for other Directory Services	1132
19.7	LDAP Settings	1134
19.7.1	The "Login" Tab	1136
19.7.2	The "Search" Tab	1138
19.7.3	The "Attributes" Tab	1144

19.7.3.1 Regular Expressions	1148
19.7.3.2 E-Script	1148
19.7.3.3 Extending XPR Attributes	1150
19.7.3.4 Attribute Settings for additional LDAP Servers	1151
19.7.3.5 Multivalue-Field Specials.	1151
19.7.3.6 Dial Number Replication Restrictions	1152
19.7.3.7 Excluding Fields from Replication	1152
19.7.3.8 Creating Fields with Default Values	1152
19.7.4 The “Global Settings” Tab.	1153
19.8 The “MySQL Settings” Tab	1154
19.8.1 Assigning Attributes	1155
19.9 LDAP and MWI	1157
19.10 Configuration in Connection with the Netscape Directory Server	1158
19.11 LDAP APL Configuration without Microsoft Exchange	1160
19.12 Monitoring the LDAP APL Activities.	1161
19.13 Secure LDAP Connection	1161
19.13.1 Prerequisites.	1161
19.13.1.1 General Prerequisites	1161
19.13.1.2 Domain Controller	1161
19.13.1.3 Xpressions.	1162
19.14 The RFCs.	1163
19.14.1 RFC 2251: Lightweight Directory Access Protocol (v3)	1163
19.14.2 RFC 2252: LDAP: Attribute Syntax Definitions.	1163
19.14.3 RFC 2253: LDAP: UTF-8 String Representation of Distinguished Names.	1163
19.14.4 RFC 2254: The String Representation of LDAP Search Filters	1164
19.14.5 RFC 2255: The LDAP URL Format	1164
19.14.6 RFC 2256: A Summary of the X.500 User Schema for use with LDAPv3	1164
20 HiPath User Management.	1169
20.1 The HiPath User Management	1169
20.2 Definition and Function of the HPM APL	1171
20.3 Configuration	1172
20.3.1 Element Manager	1172
20.3.2 Binding of Attributes	1173
20.3.3 URL to User Attributes	1174
20.3.4 Password	1175
20.4 Attributes	1175
20.5 The Connection of XPR Server and HPM-UM.	1176
20.5.1 Replication Directions.	1176
20.5.2 Transferring User Data from the XPR Server to the HPM-UM	1176
21 Presence APL	1187
21.1 Functions	1187
21.2 User Profile and Status Administration	1188
21.2.1 The Online Status.	1189
21.2.2 The Presence Profile	1191
21.2.3 Settings in Client Applications	1193
21.3 Data Replication.	1199
21.3.1 Settings in the XPR Monitor	1199
21.3.1.1 The TUM Calendar	1199
21.3.1.2 The Live Communications Server Tab	1200
21.4 Instant Messaging	1204
21.4.1 Transactions	1204

Contents

21.4.1.1	Invitation for Instant Messaging	1204
21.4.1.2	Leaving Instant Messaging	1205
21.4.1.3	Sending Instant Messaging Data	1205
21.4.1.4	Notification in Case of a joining Subscriber	1206
21.4.1.5	Notification when a Subscriber leaves the Instant Messaging Session	1206
21.5	Web Conferences	1208
21.5.1	Invitation for a Web Conference	1208
22	Print APL	1211
22.1	Printer Settings	1212
22.1.1	Supported File Formats	1214
22.1.2	Printer Properties	1214
22.2	Security Aspects	1216
23	Direct Print (LPR APL)	1217
23.1	Configuration	1217
23.2	Internal Database	1217
23.3	Structure of the Display in the XPR Monitor	1218
23.4	Structure of the Log Output	1218
23.5	Debug Transaction	1218
23.6	Example Scenario	1219
24	V.24 APL	1221
24.1	Identification	1222
24.2	Protocols	1223
24.3	Devices	1224
24.4	Bindings	1226
24.5	V.24 Dedicated Lines	1227
25	MWI to Alcatel 4400 (ABC APL)	1229
25.1	Telephone Display Support	1230
25.1.1	Waiting-Message Retrieval	1230
25.2	Several PBXs	1230
26	DB APL	1233
26.1	Introduction	1233
26.2	Requirements and Compatibility	1235
26.2.1	Requirements	1235
26.2.2	Compatibility	1235
26.3	Configuration	1236
26.3.1	DB APL Time-Out	1237
26.3.2	MS ODBC Time-Out	1238
26.3.3	Miscellaneous	1238
26.4	Configuring a Database for Testing Purposes	1239
27	Report APL and Report Schedule APL	1241
27.1	Preliminary Remarks	1241
27.1.1	How is this Chapter structured?	1241
27.1.2	The Databases	1242
27.1.3	Backup / Restore	1244
27.2	Introduction: What is Reporting?	1246
27.3	Functionality	1247
27.3.1	Report Generation	1247
27.3.2	Layouts	1251
27.4	Report APL Configuration	1254

27.4.1	Provider Tab	1256
27.4.2	Connection Tab	1257
27.4.3	Advanced Tab	1259
27.4.4	All Tab	1260
27.5	Report Schedule APL Configuration	1261
27.5.1	Reports Tab	1261
27.5.1.1	Times Tab	1263
27.5.1.2	Recipient Tab	1264
27.5.1.3	Export Tab	1265
27.5.1.4	Extensions Tab	1269
27.5.1.5	Information Tab	1271
27.5.2	Layouts Tab	1273
27.5.3	Parameters Tab	1278
27.6	Creating a Report	1279
27.6.1	Configuring the Report APL for Usage with an SQL Database	1280
27.6.2	Creating a Layout with Crystal Reports XI	1282
27.6.2.1	Layout Structure	1282
27.6.2.2	The Workspaces of a Layout	1283
27.6.2.3	The Crystal Reports XI Operating Interface	1285
27.6.2.4	Example of an available Layout	1286
27.6.2.5	Example of a Layout Creation	1288
27.6.3	Creating a Layout with BIRT	1304
27.6.3.1	Creating a new Layout	1305
27.6.3.2	The graphic Interface	1306
27.6.3.3	Connection to the Database Tables	1309
27.6.3.4	The Structure of Layout Files in BIRT	1312
27.6.3.5	The available Tools and Fields for creating and editing Layouts	1313
27.6.3.6	An Example: The Default Billing Report	1319
27.6.4	Selecting, activating and setting a Layout	1321
27.6.4.1	Step 1 - Introducing Layouts	1322
27.6.4.2	Step 2 - Adding a new Layout	1324
27.6.4.3	Step 3 - Setting an Execution Time	1325
27.6.4.4	Step 4 - Selecting a Recipient	1326
27.6.4.5	Step 5 - Selecting a Format	1327
27.6.4.6	Step 6 - Selecting a Folder	1328
27.6.4.7	Step 7 - Describing a Report	1329
27.6.4.8	Step 8 - Activating a Layout	1329
27.6.5	Creating a Report for the XPR Databases	1330
27.7	Structure of the XPR and Reporting Databases	1331
27.7.1	The CORREL.DBF Database	1332
27.7.2	The GEB.DBF Database	1334
27.7.3	The JOURNAL.DBF Database	1335
27.7.4	JobRecipient	1341
27.7.5	JobInfo	1341
27.8	Supplied Layout Files for Default Reports	1343
27.8.1	Demo Report	1345
27.8.2	Default Billing Report	1346
27.8.3	Fax Message Report	1347
27.8.4	Service-related Billing Report	1348
27.8.5	Subscriber-related Billing Report	1349
27.9	Available Telephone User Interface Reports (TUI) Reports	1350
27.9.1	Overview	1350

Contents

27.9.2 Reports about Systemwide Activity	1351
27.9.2.1 Systemwide Activity: Call Activity	1351
27.9.2.2 Systemwide Activity: Call Length	1353
27.9.2.3 Systemwide Activity: Board Load	1355
27.9.2.4 Systemwide Activity: Number of Accesses	1356
27.9.3 Subscriber Activity Reports	1357
27.9.3.1 Subscriber Activity: Subscriber Message Activity	1358
27.9.3.2 Subscriber Activity: Subscriber Message Inactivity	1359
27.9.3.3 Subscriber Activity: Subscriber Access Activity	1359
27.9.3.4 Subscriber Activity: Subscriber Access Inactivity	1360
27.9.3.5 Subscriber Activity: Billing Information	1361
27.9.3.6 Subscriber Activity: Outgoing Calls	1363
27.9.4 System Security Reports	1364
27.9.4.1 System Security: Invalid Access Attempts	1364
27.10 Basics on the Raw Data Database Tables	1365
27.10.1 Short Introduction to the Databases used	1365
27.10.1.1 CodeBase	1366
27.10.1.2 ADO	1367
27.10.2 Database Tables	1368
27.10.3 dBase and ADO Database Structure	1368
27.11 Database Tables: CTI Entries	1375
27.11.1 CtiCall	1375
27.11.2 CtiDevEvent	1376
27.11.3 CtiEvent	1377
27.12 Database Tables of the Telephone User Interfaces (TUI)	1379
27.12.1 Telematic – Call Processing Call	1379
27.12.2 Telematic – Physical Lines	1381
27.12.3 Telematic – Call	1382
27.12.4 Telematic – Message	1389
27.12.5 Telematic – Invalid Access	1391
27.12.6 Telematic – Event	1392
27.12.7 Telematic – Path Activity	1394
27.12.8 Telematic – Response Mailbox Activity	1395
27.13 Database Tables: User and Group Data as well as for NCO Location Information	1396
27.13.1 ExportMrsUsers	1396
27.13.1.1 The Structure of the Database Tables	1398
27.13.1.2 The Database Tables	1399
27.13.1.3 Adding User Attributes manually	1400
27.13.2 ExportNCOLocation	1401
27.13.2.1 The Structure of the Database Tables for NCO Location Information	1403
27.13.2.2 The Database Tables of the NCO Location Information	1404
27.14 Database Tables of the VOGUE Script	1407
27.14.1 Key Entries of the IVR Application	1409
27.14.2 Key Entries of the IVR Box	1411
27.14.2.1 Holiday Greetings Control	1412
27.14.2.2 ASR Expert Control	1413
27.14.2.3 ASR Menu Control	1414
27.14.2.4 End Control	1414
27.14.2.5 DB Read Control	1415
27.14.2.6 DB Write Control	1415
27.14.2.7 Definition Control	1415
27.14.2.8 Document Control	1415

27.14.2.9	DTMF Entry Control	1416
27.14.2.10	Questionnaire Control	1416
27.14.2.11	Contact Dialing Control	1417
27.14.2.12	DTMF Menu Control	1417
27.14.2.13	Name Dialing Control	1417
27.14.2.14	Language Control	1418
27.14.2.15	Script Control	1418
27.14.2.16	Compare Control	1418
27.14.2.17	Connect Control	1419
27.14.2.18	Prompt Control	1419
27.14.2.19	Time Profile Control	1420
28	General File Interface (FIAPL)	1421
28.1	Adding and removing Protocols	1422
28.2	The Protocol Properties	1423
28.2.1	Host -> FI APL	1423
28.2.2	File Interface APL to the Host	1425
28.3	Configuring Sites and Tenants via Import File	1427
28.3.1	Configuring the Configuration Script	1427
28.3.2	Creating a Configuration File	1428
28.3.3	Importing the Configuration File	1434
28.4	Copying Users from OpenScope UC Application	1435
28.4.1	Installing the XPR Import Script	1435
28.4.2	Configuring the XPR Import Script	1436
28.4.3	Creating an Import File	1437
28.4.4	Importing an Import File	1438
28.4.5	Password and PIN	1438
29	Web Services (XML APL)	1439
29.1	Functional Range of the XML APL	1439
29.2	XML APL Structure	1439
29.2.1	What is a Web Service?	1440
29.2.2	Announcing the Web Services	1440
29.2.3	Providing the Web Services	1441
29.2.4	Web Services of the XML APL	1442
29.3	Specific Connections via the XML APL	1444
29.3.1	Connection of SAP R/3 Systems	1444
29.3.2	Connecting OpenScope v2.3 Systems	1445
29.4	XML APL Configuration	1446
29.4.1	Configuration in the XPR Monitor	1446
29.4.2	The <code>Config.xml</code> configuration file	1447
29.5	Standards supported in the XML APL	1448
30	Connection APL	1449
30.1	Configuration	1451
30.1.1	Database	1451
30.1.1.1	Database Configuration	1452
30.1.1.2	Synchronization	1453
30.1.2	Media Server	1454
30.1.2.1	SIP Configuration	1454
30.1.2.2	Editing Listening Points for inbound SIP Communication	1457
30.1.2.3	Streaming Protocol (RTP)	1457
30.1.2.4	Managing Resource Bindings	1461

Contents

30.1.2.5	Configuring the OpenScape Voice Certificate in the Media Server	1462
30.1.3	Voice Conferences	1463
30.1.3.1	Conference Applet Configuration	1464
30.1.3.2	Server Settings	1466
30.1.3.3	Configuring a Notification Text	1467
30.1.3.4	Raw Data for Statistics	1470
30.1.3.5	Licenses	1471
30.1.4	Web Conferences	1472
30.1.5	OpenScape Web Client	1474
30.1.5.1	Configuring the Voicemail Function	1476
30.1.5.2	One-Number Service	1478
30.1.5.3	Team View	1479
30.1.5.4	DesktopIntegration	1480
30.1.5.5	Default Display Mode of the Work Area	1480
30.1.5.6	Providing a Key for SSL Operation	1480
30.1.5.7	Secure Sockets Layer Support (SSL)	1481
30.2	New UC WebClient and Fusion for Office Voice Mail Greeting feature (UCMODE)	1486
30.2.1	Feature prerequisites	1486
30.2.2	How to change the Greeting mode using Infotool	1486
30.2.2.1	UCMODE parameter	1487
30.2.2.2	UCMODE parameter usage	1489
30.2.2.3	How to change the user profile to 'Default system settings' for all mailbox users using SETVMSET parameter	1490
30.2.3	UC_MODE database entry using CMP and HpmApl	1491
30.2.4	Loop detection on IpApl	1491
31	Converting Voicemail into Text (VM2TXT APL)	1495
31.1	Proceedings	1496
31.2	Configuring the VM2TXT APL	1496
32	Tools	1499
32.1	CompactDB	1501
32.2	CtiTest	1503
32.2.1	Starting the Program	1503
32.2.2	CtiTest User Interface	1504
32.2.2.1	CTI Monitor	1504
32.2.2.2	Transaction Logging	1505
32.2.2.3	CTI Simulation	1505
32.2.3	Working with CtiTest	1506
32.2.3.1	Testing CTI Monitoring and CTI Control	1506
32.2.3.2	Testing without available PBX	1507
32.2.4	Tips and Tricks	1508
32.2.4.1	Displaying additional Locations in the CTI Monitor Window	1508
32.2.4.2	Displaying additional Locations in the CTI Simulation Window	1509
32.3	Database-Correl-Tool (DbTool)	1510
32.3.1	Introduction	1510
32.3.1.1	Function	1511
32.3.1.2	Start Requirements	1511
32.3.2	Start	1512
32.3.3	The Data Record Operations	1514
32.3.3.1	Operations by Means of the Toolbar	1514
32.3.3.2	Operations via the Edit Menu	1518
32.3.4	Importing and Exporting Data	1521

32.3.4.1 Import	1521
32.3.4.2 Export	1522
32.3.5 Tools	1522
32.3.5.1 Changing the Server Language	1522
32.3.5.2 Change User Settings	1523
32.3.5.3 Creating new Users	1524
32.3.5.4 Deleting Users	1526
32.3.5.5 Further Options	1528
32.4 InfoTool	1529
32.4.1 Deleting Correlation Data Records	1529
32.4.2 Deleting User Accounts	1531
32.5 LogTool	1532
32.5.1 Definition and Function	1532
32.5.2 Working with the LogTool	1532
32.5.2.1 The Toolbar	1532
32.5.2.2 Open Audit Logging Files	1533
32.5.2.3 Filtering Entries	1533
32.5.2.4 Hiding Entries	1535
32.5.3 Additional Editing Possibilities	1536
32.5.4 Display Settings	1537
32.6 MsgSize Tool	1539
32.7 Octel Migrator Tool	1540
32.7.1 Function	1540
32.7.2 Performance	1541
32.7.2.1 Step 1: General	1542
32.7.2.2 Step 2: Connection	1544
32.7.2.3 Step 3: User Properties	1545
32.7.2.4 Step 4: MRS Group Properties	1547
32.7.2.5 Step 5: Progress	1548
32.7.2.6 Step 6: Summary and Completion	1549
32.8 RangesNCO	1550
32.9 Syntax	1550
32.10 Proceedings	1551
32.11 Rename Server	1552
32.11.1 Satellite-inherent Specials	1553
32.11.2 Particularities of Systems with Connection APL and OpenScape Web Client	1554
32.12 SystemVersionInfo	1555
32.13 Time Zone Support	1556
32.13.1 Important Notes for the Usage of Time Zone Support	1556
32.13.2 Calling the Time Zone Support Tools	1556
32.13.3 Cluster with Microsoft Windows Server	1557
32.14 Logging Tool for Clients	1558
32.15 ZombiDetect	1560
32.16 SystemInfo	1561
32.17 XPRHFPackInstaller	1561
32.18 Xpressions Toolkit	1563
32.18.1 Installation	1563
32.18.2 Tool information	1565
32.18.3 XprToolkit features menu and usage	1565
32.18.3.1 Xpressions Toolkit' section	1565
32.18.3.2 Main Xpressions tools section	1566
32.18.3.3 Windows tools section	1567

Contents

32.18.3.4 'Xpr Server' menu	1567
32.18.3.5 'PP-COM registry' section	1568
32.18.3.6 'Open Folders' section	1569
32.18.3.7 e) 'Exit' command	1569
33 Component-spanning Features	1571
33.1 Fax Buffering When Busy	1571
33.2 Event Signaling	1573
34 Tips and Tricks	1575
34.1 Defining a proprietary TEMP Variable	1575
34.2 Adding a New User Data Field	1575
34.3 Copies of Received Messages	1577
34.4 Fax Delivery at favorable Tariffs	1577
34.5 Priority Control	1577
34.6 Line Control	1578
35 Behavior in Case of an Error (Trouble Shooting)	1581
35.1 Event Viewer	1581
35.2 XPR Monitor	1582
35.3 Overview of the installed Components	1583
35.4 Client Protocol	1583
A Document Formats	1585
A.1 Master Formats	1585
A.2 Text Formats	1585
A.3 Graphic Formats	1586
A.4 Audio Formats	1588
A.5 NVS Printer Formats	1588
A.6 Multi Document Format (PMF)	1589
A.7 Format Conversions	1590
A.7.1 Multi-format Documents	1591
A.8 Application Conversions	1592
A.8.1 Wrong Directory for temporary Files	1593
A.8.2 Windows Spooler Service	1593
A.8.3 Conversion Error in Case of MS Office 2003 SP2	1594
A.8.4 Switching the HTML Conversion to Microsoft Word	1594
A.8.5 Word and temporal Files	1595
A.8.6 Microsoft Error Reporting	1596
A.8.7 Switching the HTML conversion to Bersoft HTMLPrint	1596
B Xpressions Forms SMTP for Outlook 2007	1601
B.1 General Information about the Xpressions Forms SMTP for Outlook 2007	1601
B.2 Silent Setup	1603
B.3 Installation without Service Provider	1604
B.4 Upgrading	1605
B.5 Adding to another User Profile	1606
B.6 Remove Forms for a User Profile	1607
B.7 User-defined Installation	1608
B.7.1 Automatic Number Filtering	1608
B.7.2 Selecting Forms	1608
B.7.3 Changing the Telephone Number	1609
B.7.4 Fax Message Notifications	1610
B.7.5 SMS Notifications	1611
B.7.6 Keeping Area Code "0"	1611

B.7.7 Replacing the leading Plus Sign	1612
B.7.8 Maximum Number of Characters for SMS Messages	1612
B.7.9 Mailboxes in the POP3/IMAP Mode	1612
B.7.10 POP3 or IMAP	1613
B.7.11 No JPEG Fax Attachments	1613
B.7.12 Disable of Local Content search	1613
C Installation of the Xpressions Outlook Forms for Outlook 2010 and further versions (VSTO Forms) . .	1615
D Lear	1617
D.1 Definition and Function	1617
D.2 Configuration	1617
D.2.1 The Test Tab	1618
D.2.2 The Options Tab	1619
D.2.3 The Statistics Tab	1620
D.2.4 The Transactions Tab	1621
E Registry Reference	1623
E.1 Kernel Entries	1623
E.1.1 General Considerations	1623
E.1.2 Global Entries	1624
E.1.3 Converter	1635
E.1.4 Application Converter	1648
E.1.5 License Service	1650
E.1.5.1 CCF File	1650
E.1.6 Site Specific Entries	1652
E.1.7 The Router	1656
E.1.8 Automatic Database Import from the Registry	1674
E.1.9 Autoreporter	1675
E.1.10 CIT – Computer Integrated Telephony	1677
E.1.11 System Networking	1680
E.1.12 Line Cache	1683
E.1.13 Remote System Links	1684
E.1.14 Routing Rules	1688
E.1.15 Session Monitoring	1691
E.1.16 Services	1692
E.1.17 Database	1694
E.1.18 Important User Accounts	1696
E.1.19 Extended Message Reporter Service	1697
E.1.20 SNMP Agents	1704
E.1.20.1 Windows SNMP Service	1705
E.1.20.2 License Info SNMP Agent (CMP Usage Tracking)	1705
E.1.20.3 System Info SNMP Agent	1706
E.2 Entries of the ABC APL	1709
E.3 Entries of the Con APL	1711
E.4 CSTA APL Entries	1717
E.5 Entries of the CTI APL	1719
E.5.1 General Registry Keys	1720
E.5.2 Registry Keys for CTI Links	1728
E.5.3 Registry Values for the HiPath 4000	1758
E.6 Entries of the DB APL	1759
E.7 Entries of the FI APL	1761

Contents

E.7.1 Protocol Specific Settings	1761
E.8 HPM APL Entries	1765
E.8.1 Replication	1766
E.9 LDAP APL Entries	1767
E.9.1 Server Section	1768
E.10 Entries of the LEAR APL	1773
E.11 Entries of the LPR APL	1777
E.12 Entries of the Mail APL	1781
E.12.1 Printer Embedded Codes	1788
E.13 Notification APL Entries	1793
E.14 Entries of the Presence APL	1797
E.15 Entries of the Print APL	1799
E.15.1 Default Printer-Settings	1799
E.15.2 Individual Printer Settings	1801
E.16 Entries of the Report APL and Report Schedule APL	1803
E.16.1 General Entries	1803
E.16.2 Runtime Engine	1806
E.16.3 Manual Entries	1808
E.16.4 Database	1809
E.16.4.1 Storage of the Event Files	1810
E.16.4.2 Regular Database Maintenance	1811
E.16.4.3 Database Directory Statistics	1811
E.16.5 Job	1813
E.16.6 Configuration of the single Jobs	1814
E.16.7 Layouts	1820
E.16.8 Layout Configuration	1821
E.17 SMS-Connector Entries	1823
E.17.1 Global Values	1823
E.17.2 Connection-specific Values	1825
E.18 Entries of the SMTP APL	1837
E.18.1 POP3 Mail Import Time Schedules	1853
E.19 Entries of the TCP/IP APL	1855
E.19.1 Firewall	1855
E.19.2 Line	1855
E.19.3 Line Admin	1856
E.19.4 NwPlugTcp	1857
E.20 Registry Keys of the Telematics APLs	1859
E.20.1 Registry Keys of the TeleReg	1860
E.20.1.1 General Entries	1860
E.20.1.2 Blobs (Binary Large Objects)	1865
E.20.1.3 Devices	1866
E.20.1.4 Trunk Groups	1870
E.20.1.5 Extension number ranges	1874
E.20.1.6 Protocols	1878
E.20.2 ISDN APL Registry Keys	1889
E.20.2.1 General Entries	1889
E.20.2.2 Blobs (Binary Large Objects)	1919
E.20.2.3 Devices	1919
E.20.2.4 Trunk Groups	1923
E.20.2.5 Extension number ranges	1925
E.20.2.6 Protocols	1927
E.20.2.7 Voice and Fax-on-Demand Systems	1933

E.20.3 IP APL Registry Keys	1939
E.20.3.1 General Entries	1939
E.20.3.2 Blobs (Binary Large Objects)	1946
E.20.3.3 Devices	1946
E.20.3.4 Trunk Groups	1957
E.20.3.5 Extension number ranges	1959
E.20.3.6 FAX G3 Support	1960
E.20.3.7 Protocols	1966
E.20.3.8 Voice and Fax-on-Demand Systems	1969
E.21 Entries of the V.24 APL	1973
E.21.1 Device Settings	1975
E.21.2 Protocols	1977
E.21.3 Protocol Settings	1979
E.22 Entries of the VM2TXT APL	1981
E.23 Entries of the Web APL	1983
E.23.1 Protocols	1989
E.24 Entries of the XML APL	1991
E.25 Service Providers (MSP) Entries	1993
E.25.1 Applets	1993
E.25.2 Database	1993
E.25.3 Server	1994
E.25.4 Service Provider	1995
E.25.5 Transport	1998
E.25.6 TCP/IP-Transport	1999
E.25.7 User-dependent Entries	2000
F Open Source and other licensed Software	2003
F.1 Apache Geronimo	2007
F.2 Apache License	2018
F.3 cURLpp Copyright and Permission Notice	2022
F.4 Google Web Toolkit GWT 1.4.60	2022
F.5 GraphicsMagick	2023
F.6 iCal4j 1.0 beta3	2026
F.7 Jain Sip/Sdp implementation by NIST V 1.2	2027
F.8 K-XML 2.3	2027
F.9 libcurl Copyright and Permission Notice	2028
F.10 libTIFF Copyright and Permission Notice	2028
F.11 log4net Notice	2029
F.12 OpenSSL License	2029
F.13 PostgreSQL 8.2 & PostgreSQL 8.2 JDBC Drivers	2031
F.14 SNMP4J 1.7.5	2032
F.15 Sun XACML implementation 1.2	2032
F.16 Xerces-C	2033
Index	2035

History of Changes

Date	Changes	Reason
	The Caller Guide supports now the Multi Tenant feature.	RQ00032467
	New user group <i>Help Desk Group</i> , which has the new <i>Help Desk Privilege</i> . This privilege allows accessing some administrator features in the Web Assistant.	RQ00031656
	New user group <i>Tenant Supervisor Group</i> , which has the new <i>Tenant Supervisor Privilege</i> . This privilege allows accessing some administrator features in the Web Assistant, which are restricted to the tenant ID of the executing user.	RQ00027208
	You can create SNMP traps from log messages via the System Info SNMP Agent .	RQ00029163
	You can also use the 64-bit version of Microsoft Office 2010 for converting applications.	
	The Web Assistant includes the PIN forgotten link. You can configure this link via the parameters showpinforgotten , pinforgottenservice and KnownHostName .	RQ00031473
	Ergo supports the Trusted Transfer Mode to the voice portal of OpenScape UC Application.	RQ00031037
	The <i>Crystal Reports Viewer</i> is no longer shipped on the setup medium.	CQ00189369
	The <i>OpenScape Voice Trace Manager</i> is supported. After appropriate configuration, error messages and warnings of the IP APL are sent to this manager.	RQ00032376
	The XPR server checks the licenses used once a day. Exceedings are written in the log file as error with the respective licenses and exceedings being indicated. The error message is also written in the Windows event view parallel to the log file.	RQ00031516
	Single Sign-on (SSO) is supported for the Web Assistant under certain conditions. See Section 13.2.2.1, "Configuring Single Sign-on (SSO)", on page 927 .	RQ00032690
	New chapter for the VM2TXT APL. This APL serves for converting voicemails to text via an external service provider.	RQ00030528
	You can already start an associated web conference within the entrance grace period of a scheduled conference from the Outlook or Notes plug-in.	RQ00032125
	Added: New section about raw data for statistics files of the conference portal. See Section 30.1.3.4, "Raw Data for Statistics", on page 1470 .	RQ00032431
	New parameter WAITFIRSTLEGCOMPLETION in the registry value Private of the IP APL. You can activate this parameter for SIP if call transfer problems occur. This problem may in particular occur in the MMCC context.	CQ00192457
	New registry values FaxG3_CommetrexPath and FaxG3_ICLLogging of the IP APL	CQ00191897
	The path to the VM2TXT APL certificates is always <code><XPR Install>\res\certs</code> .	CQ00197426
2012-02-08	New registry value FaxG3_EchoSupression of the IP APL.	CQ00197583
2012-02-21	Under Windows Vista and Windows 7, <code>UnifiedLogTool.exe</code> must explicitly be started via the context menu option Run as Administrator.	CQ00198022
2012-03-02	Corrections to the VM2TXT APL.	CQ00200460
2012-03-02	The SystemInfo tool must first be activated in the Web APL before it can be used.	CQ00200371
2012-03-02	Collaboration of Smart Backup and PostgreSQL revised. See Section 7.3.4, "Backing up the PostgreSQL Database" .	CQ00199386 CQ00197239

History of Changes

Date	Changes	Reason
2012-03-13	The PIN forgotten functionality of the Web Assistant configurable via the parameter <code>showpinforgotten</code> , <code>pinforgottenservice</code> and <code>KnownHostName</code> is contained in the configuration file as comment. The end marking of the comment block must therefore be moved in front of this example if the example is to be used in adjusted form.	CQ00200725
2012-03-26	Modifications to the registry value UseOrigFax of the IP APL.	CQ00203816
2012-04-10	The IP APL does not support the Chaining of documents option of the FAX G3 protocol.	CQ00205135
2012-04-10	The behavior of the IsPINResetOld registry value of the Web APL has been changed.	CQ00204918
2012-04-11	New registry value GSPaperSize of the kernel.	CQ00206053
2012-04-11	Section about necessary additional manual steps when applying the <i>Rename Server</i> tool to XPR servers with Connection APL and OpenScape Web Client.	CQ00205184
2012-04-16	Changed OpenSSL references to the tool shipped with SDKTools.	CQ00206509
2012-04-16	Smart Backup also backs up the SQL database belonging to Web Collaboration via the UCC option. This requires the user to have write access to the <code>MRSFolders\$</code> share under which the SQL server operates.	CQ00203823
2012-04-27	The account of the user who wishes to log on to the XPR server via the XPR monitor must belong to the group of local administrators on the XPR server. The reason for this requirement is among other things that configuration changes may otherwise not be written in the registry.	CQ00206626
2012-04-27	The MWI Signal Active option of the CTI APL must not be set if OpenScape Voice is connected.	CQ00207747
2012-05-02	New PhoneMail parameter MaxVoiceMsg .	FRN 5542
2012-05-02	The number of simultaneously active monitor points of a user can be restricted. See registry value CheckMonitorLimit .	FRN 5405
2012-05-08	SAP Business byDesign integration and MMCC deleted.	FRN 5712
2012-05-08	Possible values of the SimplifiedMenuTree parameter of the Web APL changed to True/False.	CQ00208034
2012-05-09	New registry value CaseSensitiveSearch of the SMS IP APL.	CQ00209669
2012-05-10	VM2TXT APL configuration revised.	RQ00030528
2012-05-11	Added: Note for problems that occur with the automatic client update of the local Outlook forms.	CQ00208331
2012-06-04	Added: List of services allowed during a restoration.	CQ00213150
2012-06-13	New registry values ToAddressNPI , ToAddressTON , FromAddressNPI and FromAddressTON of the SMS IP APL.	CQ00214386
2012-06-13	As of V7R1 the Fax G3 protocol parameters UseFaxIdAsOAD , InsertMidHI and CheckPageNumbers are supported by the IP APL also.	FRN 4914
2012-06-13	As of V7R1 there is the new parameter tenant for the Vogue protocol. This protocol can thus also be used in a multi-tenant environment.	FRN 5258
2012-06-21	The Signal any change of box setting of the Notification APL must be set for the counter-based message display to work on OpenStage phones at an OpenScape Voice with active Voicemail feature.	CQ00215350
2012-06-29	The configuration of the Trusted Transfer Mode has been revised.	FRN 4930
2012-07-05	New registry value CheckMonitorTimer of the CTI APL.	CQ00211294
2012-07-09	The Trusted-Transfer mode always takes E.164 numbers as ANI. The maximum length of an OpenScape Voice number must not exceed 24 characters for this transfer.	CQ00218251

Date	Changes	Reason
2012-07-10	Default setting and possible values of the Hostname/IP Address parameter of the Media Server adjusted.	CQ00218430
2012-08-03	Note for licenses required on the customer side in case of application conversions with Microsoft products.	Review
2012-08-06	New note: <code>renservr</code> must be invoked from the <code><XPR Install></code> directory.	CQ00220212
2012-08-06	New registry value FaxG3_CheckNumberOfPages of the IP APL.	CQ00219890
2012-08-27	Using the FI APL configuration script <code>xprConfig.e</code> the location and tenant settings can be imported in the XPR server via a configuration file.	FRN 5259
2012-08-27	New instruction: How to install the certificates for configuring a secure LDAP connection.	CQ00223888
2012-09-19	New note: Dashes in the files for creating conference notifications may cause problems.	CQ00206216
2012-09-19	New parameter in the registry value Private for IP APL devices: SCRIPTFAXDETECTION	CQ00227047
2012-09-27	Port 5000 added to the port list for the web conference server.	CQ00229160
2012-10-10	The HTTP protocol is disabled by default for security reasons. To activate it, you need to switch it on via the registry value <code>HTTP_Enable</code> .	CQ00229990
2012-10-22	If a path is set for the VM2TXT APL in <code>libverbosemodedir</code> , it must exist since otherwise no log data will be written.	CQ00232387
2012-10-26	In case of a HiPath 4000 the MWIInterrogate feature must be disabled.	CQ00232849
2012-11-26	New registry value Compression Type of the MTA.	CQ00237431
2012-12-03	The <code>SimplifiedMenuTree</code> parameter of the Web APL must contain value true in small letters.	CQ00238378
2012-12-04	Additional information: You cannot normalize phone numbers for MSPTSP applications depending on the calling user.	NA10577796
2012-12-12	New note: Rename Server will prompt for a password when being executed.	CQ00239725
2013-01-07	Simplified configuration of tenants is valid for SIP-based protocols only.	CQ00240176
2013-01-14	New note for the Maximum caller number length parameter on the OpenScape tab of the PhoneMail protocol.	CQ00239428
2013-01-15	New registry value RefererCheck of the Web APL.	CQ00242553
2013-01-18	The file for importing tenant information via the FI APL must read <code>ipapl.xml</code> . Furthermore, the corresponding header sample must be adjusted.	CQ00242690
2013-02-05	New registry value UseAcidDnis of the CTI APL.	CQ00245501
2013-02-08	In case of Windows Server 2012 another printer must be used for configuring Printer Embedded Codes.	FRN 5992 CQ00246025
2013-02-15	The internal format for the calling number schema of the Trusted Transfer Mode inclusive examples added again.	CQ00239531
2013-02-21	Description of the CTI APL's registry value DontLocalize changed.	CQ00247315
2013-02-28	New section about configuring the CTI APL and HiPath 4000 as of V6R2 with E.164 number format.	CQ00248487
2013-03-05	PhoneMail as well as the Web Assistant can now be set to the Catalan language.	FRN 7057
2013-04-15	New registry value UseHttps of the HPM APL.	CQ00255513
2013-04-18	New option <code>NORMALIZE</code> in the routing rule assignment area.	CQ00254822
2013-04-23	New registry value FlushAfterWrite of the XMR service.	CQ00257342

History of Changes

Date	Changes	Reason
2013-05-08	New note in the Connection APL chapter: The configured numbers must match those transferred by the PBX. Pointed out: Automatic adjustment of the conference announcement language when users are recognized.	CQ00235684
2013-05-14	New registry value Send_DisableDsnCc of the SMTP APL.	CQ00260143
2013-05-21	New APL monitoring mechanism. See the corresponding section about the heartbeat monitor in chapter MTA.	CQ00259499
2013-06-10	New registry value ListenerTimeout of the Connection APL.	CQ00263708
2013-06-17	New registry value IgnoreSmtpCheck of the Web APL.	CQ00264174
2013-06-18	The unit for the START_DELAY parameter in the registry value ParamBlock is tenth of a second, not second.	CQ00264851
2013-07-30	PhoneMail supports a maximum of 180 days that can be specified for the Telephone password (PIN) expiration option.	CQ00269149
2013-08-14	New registry value FaxG3_StartTimestamp of the IP APL.	CQ00270390
2013-08-30	The IP APL now supports resuming an interrupted fax transmission.	FRN 6122CQ00271486
2013-09-04	Converting graphics formats to Fax requires installing the Desktop Experience feature under Windows Server 2008 R2.	CQ00270749
2013-10-23	New customer parameter "-IgnoreHP8KMaxLen" for PhoneMail.	CQ00239428
2013-10-24	New parameter in the registry value Private for protocols (Fax G3) of the ISDN APL: EvalNLCauseForSubject	CQ00276872
2013-11-29	The size of the carbon copy rules is restricted to 32kB.	CQ00279948
2013-12-02	New registry value SendSnapshot of the CSTA APL.	CQ00278914
2014-01-08	The XPRTEMP variable is not used by the Smart Backup.	CQ00283270
2014-01-10	The user ID characters that may be specified in the USER database field are no longer a recommendation but a restriction.	CQ00282831
2014-01-23	New registry value MaintenanceBackup Temp of the MTA.	CQ00285015
2014-01-24	The Check messages with McAfee Virus Scanner is obsolete.	Review
2014-02-17	Added: Instructions for importing a new Root certificate of the OpenScape Voice in the Media Server.	FRN 7703CQ00287797
2014-03-05	Registry key ...\\PostgreSQL\\Services\\pgsql-8.4 changed to current version 8.4.	CQ00289455
2014-03-07	Restriction on changing protocols with the IP APL obsolete.	CQ00290296
2014-03-14	Text on the registry values NetworkAliveCheck and NetworkTryReconnect revised.	CQ00290768
2014-04-03	Text on the One-Number Service revised.	CQ00278299
2014-04-03	You can export and import the filtering settings for the main log file.	CQ00290972
2014-05-30	Presetting of FaxG3_ForceConversion was wrong.	CQ00295210
2014-05-30	Using PhonemailUserDependantRouting and PMROUTPREFIX you can now furnish the PhoneMail user outcall with a prefix.	CQ00295335
2014-05-30	New registry value SendTimeout of the SMS APL.	CQ00301091
2014-05-30	Restriction of the user ID characters that may be specified in the USER database field extended to the LMACCOUNT database field.	CQ00295925
2014-05-30	New PhoneMail parameter ttmNormANI .	CQ00297418

Date	Changes	Reason
2014-05-30	Example added to the LDAP APL that illustrates how user replication can be restricted to a distribution list.	CQ00300371
2014-06-11	Workaround for the conversion from TIFF to Fax under Windows Server 2012 described.	CQ00302396
2014-06-25	Support of TLS 1.2.	FRN 8345
2014-07-21	An individual converter renders workarounds for the conversion from TIFF to Fax under Windows Server 2008 and 2012 obsolete.	CQ00300388
2014-07-23	If SIP is used by the IP APL as well as for Media Server conferences, two IP addresses must be configured and each of them must be used by the appropriate server component.	CQ00295982
2014-08-04	Description of the new tool compactdb for compressing database files.	CQ00300916
2014-08-04	New PhoneMail parameter -suppressLongANI .	CQ00309006
2014-08-12	Registry value ShortholdTime of the TCP/IP APL changed.	CQ00309848
2014-08-12	Description of the PhoneMail parameter MaxVoiceMsg extended.	CQ00308553
2014-09-19	The number of fax channels for T.38 has increased from 120 to 200.	CQ00314496
2014-09-30	Path to the licsvc changed.	CQ00315239
2014-10-24	You cannot change the number of conference participants during an ongoing conference.	CQ00317941
2014-12-09	minor corrections In section 4.1 for LMACCOUNT	CQ00321369
2014-12-09	in section 10.4.3.13 : add possible values for rw	CQ00320278
2014-12-09	in section 32.11 : add options i and r for rename server	CQ00319968
2014-12-09	in section 7.8 correct port	CQ00322181
2014-12-11	in section D17.2 add Unicode for GSM	CQ00322189
2014-12-22	In section D16.1 (CRDOTNET) correct default value and add short description	CQ00317172
2014-12-22	Add new Paragraph B7.12 for Disable of Local Content search (refer to CQ00317871)	CQ00322184
2014-12-24	Describe the InitialProcMode for NotAPI in more detail (refer to CQ00312711)	CQ00323342
2015-01-12	in section 10.4.3.13 : adapt rw parameter in accordance to CQ00320272	CQ00323785
2015-01-16	correction of some small typos	
2015-02-12	11 - in section 10.8 for openssl add the -config option	CQ00323721
2015-03-10	12 - Add new REG_DWORD for AllowDotInName in chapter D.1.2	CQ00327330
2015-04-06	13 - add a reference to section 6.4.1	CQ00329555 / CQ00329701
2015-04-06	13 - add information about Phonemail in section 10.4.3.20	CQ00310049
2015-05-08	14 - add in chapter 10.12 an entry for standard RFC 5746	CQ00330859
2015-05-11	14 - add new DWORD for MwiRepeatOnFailure in chapter D.1.2	CQ00330911
2015-05-14	14 - add new DWORDS for SSL_TLSv1_Enable and SSL_CBC_Enable	CC00331365
2015-05-22	15 - add new subchapter A.8.7 for Bersoft HTML Conversion	CQ00331697
2015-06-16	16 - add new DWORD for AllowHypherInName	CQ00332256
2015-06-16	16 - remove in section 10.8 certificate information	CQ00332788

Date	Changes	Reason
2015-07-13	17 - add entries CPU_POLLING_INTERVAL and CPU_LIMIT under ExUmApl (new subchapter D1.21)	CQ00333442
2015-07-15	17 - correction : Move SSL_TLSv1_enable and SSL_CBC_Enable from Section D1.2 to section D.23	CQ00331365
2015-09-01	18 - add parameter -nodispcalled in section 10.4.3.13	CQ00335569
2015-09-10	18 - remove in section 10.10.4.2 certificate information	CQ00336038
2015-09-10	18 - remove chapter D1.21 (CQ00335801) info should be in other document	CQ00335801
2015-09-30	19 - add key PinToProcessor to chapter D3	CQ00334561
2015-10-02	20 - make corrections for PinToProcessor in Chapter D3	CQ00334561
2015-12-01	21 - remove in section 10.10.4.2 part of certificate information left over from CQ00336038	UCBE-3180
2015-12-04	22 - adapt information for Outlook and differ between Outlook 2007 and Outlook 2010 / 2013	UCBE-3278
2015-12-11	23 - chapter 4.6, table 6: add also Phonemail for PMP_COMP_ANN (Company Announcement enabled).	UCBE-3501
2016-01-08	24 - chapter D20.2: add OutCallHoldAllowed	UCBE-4050
2016-01-11	24 - chapter 10.8 and 10.10.4.2 - remove info about default certificate	UCBE-4138
2016-01-27	25 - add info about fsi (chapter 10.4.3.13)	UCBE-4521
2016-01-27	25 - remove chapter 4.5 (Special User Database Adaptions) including also 4.5.1 (Bitmaps in Fax Stationary)	UCBE-4529
2016-02-02	26 - Chapter 10.10.6.1 use also example with names	UCBE-4040
2016-02-04	26 - revert changes for Jira UCBE-3278	
2016-03-15	27 - Chapter D20.3.1 and D20.3.6 add Registry keys - AdjustIncFaxLevel (D20.3.1) - AdjustOutFaxLevel (D20.3.1) - FaxG3_AltConfigActive (D20.3.6) - FaxG3_AltConfigValuesByCaller (D20.3.6) - FaxG3_AltConfigValuesByIP (D20.3.6)	UCBE-4644
2016-03-18	28 - Chapter D3, add Registry key XpressionsFolder	UCBE-3100
2016-04-07	29 - add new chapter (Annex C) for Outlook 2010 forms furthermore minor changes in Annex B	UCBE-3278
2016-06-02	30 - add Kernel Parameter LicSvcTimeout under General (Chapter E.1.2)	UCBE-6626
2016-06-03	30 - minor corrections of typos in 10.10.6.1 (for UCBE-4040)	
2016-06-21	31 - adapt changes in chapter C	UCBE-6657
2016-07-19	32 - Deleted chapters C.1- C.4	UCBE-6622
2016-08-29	Added note in chapter E.20.3.6 FAX G3 Support.	UCBE-7689
2016-09-19	Updated Section 13.2.2.1, "Configuring Single Sign-on (SSO)" .	UCBE-7917
2016-11-01	34 - Updated Section 32.11, "Rename Server"	UCBE-8477
2017-02-06	35 - Add Windows Firewall to Section 7.7.1 Firewalls between Nodes of a distributed XPR Server	UCBE-9357
2017-02-15	36 - replace link (for printer) in chapter 11.5 Printer Embedded Codes	UCBE-10010
2017-03-15	37 - Section E.20.3.6 FAX G3 Support add new registration key FaxG3_PartialReception	UCBE-10479

Date	Changes	Reason
2017-06-01	38 - Move Register Key MaintenanceBackupTemp from E1.2 (Global) to E.1.7 The Router	UCBE-11684
2017-06-27	39 - Section A.3 Graphic Formats Add info about other formats related to Imprint	UCBE-11975
2017-06-27	39 - Section 7.3 Backup Add note for files bigger than 4 GB.	UCBE-12000
2017-07-05	40 - Section 13.6.3 Changing Web Assistant Default Settings	UCBE-12151
2017-07-05	40 Section A.3 Graphic Formats Add info about other formats related to Imprint Corrections for UCBE-11975	UCBE-11975
2017-08-03	41 - Section A.8.7 Switching the HTLM conversion to Bersoft HTMLPrint Corrections for UCBE - 12542	UCBE-12542
2017-08-09	41 - Section E20.3.3 Correction for UCBE-12390	UCBE-12390
2017-08-17	41 - Section E.20.3.6 FAX G3 Support Default value for FaxG3_OutErrCorrMode [REG_DWORD] updated	UCBE-12524
2017-08-30	42 - Updated Table 8 in Chapter 5.7 Automatic Client Update	UCBE-12901
2017-10-05	43 - Updated Chapter 10.4.3.13 Parameter Tab Customer	UCBE-13446
2017-10-26	44 - Updated the following chapters: - Chapter 3 Starting and Stopping the Server - Chapter E.1.16 Services	UCBE-13819
2018-01-02	45 - Section E.23 Entries of the Web APL add SSL_TLSv1_1_Enable [REG_DWORD]	UCBE-14659
2018-01-05	46 - Section E.1.3 Converter add Tiff2Pdfa [REG_DWORD]	UCBE-14558
2018-01-24	47 - Section E.8 HPM APL Entries add EmailForOff365	UCBE-14925
2018-03-27	48 - Section E.17.2 Connection-specific Values add new parameter Truncate	UCBE-15472
2018-03-27	48 - Section 12.1.5 Secure Sockets	UCBE-15504
2018-04-11	49 - Chapter 32 Tools new Section 32.17 XPRHFPackInstaller	UCBE-15567
2018-05-18	50 - Section 32.4 Infotool new parameter EXPORT REC	UCBE-15966
2018-05-18	50 - New Section 1.3 New Features released on OpenScape Xpressions V7 R1.5 - updated Section 11.5 Printer Embedded Codes	UCBE-15941
2018-05-24	51 - Xchange Section 1.2 with 1.3 (change order)	UCBE-15941 (reopened)
2018-06-19	52 - the following sections have been updated: - section E.1.19 Extended Message Reporter Service - section E.1.20 SNMP Agents	UCBE-16210
2018-09-17	53 - the following sections have been updated - E.23 Entries of the Web APL - E.18 Entries of the SMTP APL - E.20.3.1 General Entries - E.1.2 Global Entries	UCBE-17176
2018-10-09	54 - E.17.1 Global Values add MaxLicenses	UCBE-17303

Date	Changes	Reason
2018-10-18	55 - Section 19.13 LDAP and SSL Encoding	UCBE-17565
2018-11-16	56 - Section 20.3.4 Password	UCBE-17739
2018-12-05	57 - Updated: - Appendix A.7 Format Conversions - Appendix A.8 Application Conversions - Appendix E.1.3 Entries of the Con APL	UCBE-18240
2019-02-13	58 - Updated: - Appendix E.3 Added StartDelay parameter - Appendix E.13 Added StartDelay parameter	UCBE-18652
2019-04-08	59 - Updated: - All references of Dialogic/Eicon changed to Sangoma Diva(R)	UCBE-19214
2019-04-18	60 - Updated: - Appendix E.1.16 Services - registry key: WatchdogActive	UCBE-19546
2019-04-24	61 - Updated: - Section 7.8 TCP/IP Ports used by the XPR Server	UCBE-19566
2019-05-21	62 - Updated: - Section 10.4.13 Parameter Tab Customer	UCBE-19633
2019-09-17	63 - Updated: - Section 4.3.14 Sequence of Offered Messages	UCBE-21058
2019-09-23	64 - Updated: - Section E.20.3.6 FAX G3 Support	UCBE-20709
2019-09-25	65 - Added: - Section 32.18 Xpressions Toolkit	UCBE-21101
2019-11-26	66 - Added: - Section A.8.8 Switching the PDF conversion to Foxit Reader	UCBE-21820
2020-03-10	67 - Updated: - Section E.20.3.3 Devices - Section 4.5 Privileges - Section 10.4.3.13 Parameter Tab Customer	UCBE-20352 UCBE-21224 UCBE-22107
2020-05-05	68 - Added: - Section 19.13.1 Prerequisites - Section 19.13.1.1 General Prerequisites - Section 19.13.1.2 Domain Controller - Section 19.13.1.3 Xpressions - Section 19.13.2 Setting up secure LDAP and SSL	UCBE-23216
2020-05-12	69 - Updated: - Section E.20.3 IP APL Registry Keys	UCBE-23337
2020-06-09	70 - Added: - Section New UC WebClient and Fusion for Office Voice Mail Greeting feature (UCMODE)	UCBE-23564
2020-07-27	71 - Updated: - Section 4.1 Database Fields Significance, Table 4 User database fields	UCBE-24097
2021-01-11	72 - Updated: Documentation of MgoSoft PDF/PS converter	UCBE-25280
2021-07-09	73 - Updated: - Section A.8.2 Windows Spooler Service	CBE-27398
2021-11-02	74 - Updated: - Section 7.4.8 Automatic Report Transmission by Mail	UCBE-28527
2021-11-24	75 - Removed: - All information regarding the use of Ghostscript and section A.8.8 Switching the PDF conversion to Foxit Reader	UCBE-27345

Date	Changes	Reason
2021-12-07	76 - Updated: - 7.8 TCP/IP Ports used by the XPR Server	UCBE-28858
2022-09-02	77 - Updated: - Chapter E Registry Reference E.17.2 Connection-specific values, page 1836	UCBE-30023
2022-10-11	78 - Updated - Chapter 32.11 Rename Server	UCBE-31225
2024-01-11	79 - Updated - Chapter A.8 Application Conversions	UCBE-33955
2025-03-06	80 - Updated - Chapter 1.2 New Features with OpenScape Xpressions V7 V7R1.5	DOCLOC-9419
2025-08-18	81 - Updated - Chapter E1.2 Global Entries with UseCAasOrig	UCBE-38347
2025-10-25	82 - Updated: - Chapter E.1.4 Application Converter - Chapter A.8 Application Conversions - Chapter A.8.3 Conversion Error in Case of MS Office - Chapter A.8.4 Switching the HTML Conversion to Microsoft Word	UCBE-38540

History of Changes

1 Introduction

1.1 General Information about OpenScape Xpressions V7

OpenScape Xpressions V7 adds multiple communication capabilities to the Windows server:

- Message routing for e-mail, fax, voice and SMS messages in store-and-forward mode.
- Realtime-switching device for dialog services, e.g. voice.
- Central information provider with access via a Windows client, Internet, telephone or fax terminal.
- Application server: Third party software can be integrated in the OpenScape Xpressions V7 server: virus checker, Microsoft Office packs (for document conversions on the OpenScape Xpressions V7 server used for fax transmission), speech recognition (ASR), text-to-speech, and much more.
- CTI applications
- Voice and web conferences

The OpenScape Xpressions V7 server can be configured for two different operating modes:

- The server as stand-alone solution,
- or the OpenScape Xpressions V7 server can be integrated within a communications server. Integration is possible with Microsoft Exchange 2003, 2007, 2010, and 2013, Lotus Notes 6.5, 7.x and 8.x as well as SAP R/3.

Both of the operating modes offer specific advantages. In the first case no foreign software and no existing communication infrastructure is assumed. OpenScape Xpressions V7 forms here a complete solution for advanced electronic communications. In the second case the OpenScape Xpressions V7 is integrated into an existing infrastructure. From the integrating communication server's view (Microsoft Exchange, Lotus Domino, SAP R/3), OpenScape Xpressions V7 acts as pure gateway. As such, it will be administered by the integrating system after the installation as far as possible.

Because of the symmetrical architecture of the server, communication is possible in all cases between two heterogeneous networks. OpenScape Xpressions V7 operates, thus, as a switch between different network types and communication architectures. All needed conversions, document formats, and addresses are automatically processed by the server. The required routing times are measured in fractions of seconds.

An incoming fax can, for example, be routed directly to a Microsoft Exchange user or an Internet e-mail could be made available via fax polling. Users can retrieve information selectively through either the client Communications, Internet, over the telephone or fax, or through via a third-party mail system.

The OpenScape Xpressions V7 server was implemented under Windows Server 2008/2012 and Windows 7. The high-level scalability of Windows and its broad range of application software increase the OpenScape Xpressions V7 application options.

The OpenScape Xpressions V7 server is a highly scalable unit. Several Windows servers can be interconnected in order to form one complete system (Distributed OpenScape Xpressions V7). To the outsider this system has the appearance of a singular OpenScape Xpressions V7 server. On the next scaling level, several OpenScape Xpressions V7 servers can be connected via "Remote System Links" respectively the newer System Networking to form a logical ensemble. Within a system configuration of this type, communication resources are at the disposition of all connected servers.

1.1.1 Server Characteristics

- Routing with symbolic address transcription (see [Section 7.1.3, "Routing Rules", on page 200](#)) and conversion. The converter has a broad range of text, image, voice and application formats at its disposal (see [Appendix A, "Document Formats"](#)).
- Scalability. Scalability is not only a characteristic of the complete system, but also of the internal architecture. Internally, scalability guarantees the transition from a single-node system to a multiple-node system; externally, OpenScape Xpressions V7 systems can operate as an entire system via remote system links.

OpenScape Xpressions V7 V7 offers the following functions simultaneously:

- E-mail server and gateway
(store-and-forward between e-mail and telematic services)
- Fax, voice, SMS, modems, ISDN, VoIP
- Voicemail server
- Voice and web conference server
- Fax-on-demand server
- Gateway between fax G3 and fax G4
(transition between analog fax and ISDN-G4 including format conversion)
- Gateway between the various text-based telematics services
(real-time and store-and-forward routing)

- Internet gateway
- Telematic gateway for external mail systems
- Unified Messaging
- Integrated Messaging with Lotus Notes and Microsoft Exchange
- True Unified Messaging with Lotus Notes and Microsoft Exchange

NOTE:

The services released in the scope of the product OpenScape Xpressions V7 can be obtained from the *OpenScape Xpressions V7 Release Notice*. Even if other services are mentioned in this manual for the sake of completeness, they are only available in the scope of a PSR with support by PSM.

1.1.2 Communications Platforms

OpenScape Xpressions V7 is connected via one (or several) S₀-, S₂ or IP tie trunk(s) to the PBX. Please see the *OpenScape Xpressions V7 Release Notice* for the supported communications systems.

1.1.3 Languages

OpenScape Xpressions V7 supports the languages listed in [Table 1](#) for the GUI of user applications. Administrator applications are supported in German and English only.

For Telephone User Interfaces (TUI) and Speech User Interfaces (SUI) see [Table 2](#).

	Communications optiClient OpenScape Web Client Notes Extensions Outlook Extensions Web Assistant	IP-Phone Assistant	XPR Monitor Application Builder
German	✓	✓	✓
English	✓	✓	✓
French	✓	✓	
Spanish	✓	✓	
Italian	✓	✓	
Dutch	✓	✓	

Table 1 Languages supported for GUI Applications

	Communications optiClient OpenScape Web Client Notes Extensions Outlook Extensions Web Assistant	IP-Phone Assistant	XPR Monitor Application Builder
Portuguese	✓	✓	
Brazilian	✓	✓	
Turkish	✓		
Russian	✓		
Catalan	✓*		

Table 1 Languages supported for GUI Applications

* Web Assistant and Outlook Extensions only.

	PhoneMail Ergo Conferencing	VMS	Evo Caller Guide	Text-to-Speech
German	✓	✓	✓	✓
English (US)	✓	✓	✓	✓
English (UK)	✓	✓	✓	✓
French (France)	✓	✓	✓	✓
French (Canada)	✓	✓		✓
Spanish	✓	✓		✓
Spanish (US)	✓	✓		✓
Italian	✓	✓		✓
Dutch	✓	✓		✓
Portuguese	✓	✓	✓	✓
Brazilian	✓	✓		✓
Turkish	✓	✓		
Russian	✓	✓		✓
Catalan	✓*			
Slovenian		✓		

Table 2 Languages supported for TUI and SUI Applications

* PhoneMail only.

IMPORTANT:

Ergo must not be installed parallel to PhoneMail and/or VMS in German, English (US) and English (UK).

1.2 New Features with OpenScape Xpressions V7 V7R1.5

Operating Systems

Windows Server 2016 is supported by the XPR server and Windows 10 is supported for some XPR Clients (see the OpenScape Xpressions Release Notice).

Virtualization

See the OpenScape Xpressions Release Notice for supported versions.

Newly supported web browsers versions

New versions of Microsoft Internet Explorer, Mozilla Firefox and Google Chrome are supported by the WebAssistant (see the OpenScape Xpressions Release Notice).

1.3 New Features with OpenScape Xpressions V7 V7R1.1

Operating systems

Windows Server 2012 and Windows 8 are supported by the XPR server (see the *OpenScape Xpressions V7 Release Notice*).

Exchange connection

- New option in the Exchange Fail-Safe Tool for skipping the transport directory test.
- New option in the Exchange Fail-Safe Tool for an advanced system property check with the following tests after setting up the connectors:
 - Checking which Exchange Server version is active in the system.
 - Checking whether a connection can be set up to this Exchange server.
 - Checking whether the core services such as System Attendant, Mail submission, RPC Client operate on the Exchange server.
 - Checking whether the registry entries are consistent after the ExUMApI installation.
 - Checking whether the registry entries are consistent after the E2k7ApI installation.
 - Checking the CAS Array and DAG AD configuration.
 - Checking whether the service account has a valid mailbox in case of a connection to Exchange Server 2010.
 - Result dialog displaying tips and hints concerning the XPR integration in an Exchange environment.

- E2k7Apl start/stop configurable independently from the current watchdog settings via registry value.
- Selecting the transport directories already during the E2k7Apl setup.
- Browse button for selecting the service account in the Exchange Fail-Safe Tool added.
- ExUmApl improvements with regard to detecting missing installation requirements to avoid login problems after the installation.

Catalan

PhoneMail, Web Assistant and Outlook Extensions can now be set to the language Catalan. The associated online help is in English language.

Smaller fix release package

You can create a setup medium for an upgrade to a fix release with help of an old setup medium and additional EXE files. This applies only for an upgrade to a fix release on a non-cluster system and for kernel computers (not for satellite computers). You perform the actual upgrade as usual.

Multi Tenant

New configuration field for configuring a tenant-specific welcome greeting.

Newly supported browsers

Internet Explorer 10 is supported by the Web Assistant and as of V7R1.3 also by the Web Client.

VMware configuration parameters

VMware configuration parameters for virtual computers have been specified (see the *OpenScape Xpressions V7 Release Notice*).

OpenScape UC Application

As of OpenScape UC Application V7R1.2, PhoneMail can be connected to the OpenScape UC Application voice portal with several systems. This also refers to displaying voicemails in the journal of the clients of OpenScape UC Application. The corresponding configuration is described in the *OpenScape UC Application V7 Configuration and Administration*.

1.4 New Features with OpenScape Xpressions V7 V7R1

Application Builder

The Name Dialing control of the Application Builder can use a filter (\$AAFILTER). As a result, the Automated Attendant may e.g. search a company's subsidiary for names and not the entire company.

IP APL

The Fax G3 protocol parameters **UseFaxIdAsOAD**, **InsertMidHI** and **CheckPageNumbers** are supported by the IP APL also.

Multi Tenant

- Voice Guide (Vogue) support

If a user deploys the Voice Guide on an XPR server with several tenants, only users of the same tenant are returned with the corresponding configuration. This setting applies for an SIP connection only.

- You can perform site and tenant settings of the XPR server using the FI APL and a configuration file. For this purpose, the `XprConfig.e` configuration script, which can process the corresponding configuration files, is shipped for the FI APL. These settings apply for an SIP connection only.

PhoneMail/Ergo

The configuration of the Trusted Transfer Mode has been revised.

Configuring Sites and Tenants via Import File

You can perform site and tenant settings of the XPR server using the FI APL and a configuration file. For this purpose, the `XprConfig.e` configuration script, which can process the corresponding configuration files, is shipped for the FI APL. These settings apply for an SIP connection only.

Web APL

The HTTP protocol is disabled by default. This affects the IP Phone Assistant and the SNMP Agent. Both require this protocol. If you require these applications, you need to reactivate the protocol.

Web Assistant

You can configure the Web Assistant to make it impossible for users to play voicemails on the PC.

Web Client

The journal also displays entries of unavailable phones, for example of a softphone on a switched-off computer.

Supported browser

Internet Explorer 9 and Firefox to 3.6

1.5 New Features with OpenScape Xpressions V7 V7R0

OpenScape Xpressions V7 comprises the following new or revised features:

Supported operating systems

Only 64-bit operating systems are supported for the XPR server. Windows 7 Professional is supported for the XPR server with restrictions.

Upgrading from MRS V8 to OpenScape Xpressions V7 V7

You can upgrade MRS V8 of the Cycos AG to OpenScape Xpressions V7 V7. You can use the clients as MRS clients until the next upgrade when the branding will be changed to OpenScape Xpressions.

Installation

A USB stick replaces DVDs as setup medium.

Connecting PBXs

The following connections are supported:

- HiPath 4000 V6 R1 via CorNet-IP or SIP

PCI slots with ISDN cards have been sold for newer HiPath 4000 installations up to version V6 R0. You can upgrade this hardware to a hardware for HiPath V6 R1 by adding a DSCXL-V2 card.

If you have entirely new hardware for HiPath 4000 V6 R1, a purely server-based solution is on hand (VoIP-Switch). This V6 R1 hardware does not contain any ISDN cards and has been sold as of HiPath 4000 V6 R1. **This hardware does not support any CorNet-IP and SIP-Q but SIP only.**

- OpenScape Voice V6
- Cisco Unified Communications Manager 8.6
- Alcatel OmniPCX Enterprise (OXE) R9.1

TTS and ASR

TTS is executed by Nuance Vocalizer for Networks 5 and ASR by Nuance Recognizer 9.

VM2TXT APL

This new APL enables converting a voicemail to written text and further processing it.

Microsoft SQL Server

Microsoft SQL Server 2008 and SQL Server 2008 R2 are supported for the Report APL in the following editions:

- Datacenter Edition
- Enterprise Edition
- Standard Edition
- Workgroup Edition
- Web Edition
- Developer Edition
- Express Edition

Microsoft Exchange Server

- Support of multi-connector operation for Exchange Server 2003, 2007 and 2010
- Client-Access-Server-Array support for setting up the connectors for Exchange Server 2010
- Database-Availability-Group support for setting up the connectors for Exchange Server 2010

Ergo

Using the Trusted Transfer Mode, you can connect the XPR server Ergo to the voice portal of the OpenScape UC Application. This expands Ergo by the corresponding OpenScape UC Application features.

Multi Tenant

- Caller Guide support

If a user deploys the Caller Guide on an XPR server with several tenants, only users of the same tenant are returned.

- Tenant management

The **Tenant Supervisor Group** user group has been introduced. Users of this group can administer users within a tenant and have the following privileges:

- Access to the Web Assistant's **Server settings > User administration** menu except for creating a new user group
- Creating a user
- Assigning a user to a tenant
- Assigning a user to a tenant supervisor group

New user group Help Desk Group

The **Help Desk Group** user group has been introduced with the following privileges:

- Creating a user
- Assigning a user to the Help Desk Group
- No access to the XPR server configuration
- Restricted access to the Web Assistant's **Server settings > User administration** menu:
 - Unlocking a user
 - Deleting the MWI status
 - Updating the MWI status
 - Resetting the PIN
 - Resetting the password
 - Resetting notification settings
 - Resetting voicemail settings
 - Acting on behalf of a user

Client Applications

Support of the Outlook extensions for Microsoft Outlook 2010 64-bit in the 32-bit mode

Java-JRE

The SUN-JRE was replaced with the IBM-JRE.

Web Assistant

- Requesting a new PIN can be configured.
- All existing user licenses and those being deployed are displayed.
- True Single Sign On (SSO)

A user of the same domain like the XPR server is authenticated after logging in to the domain and need not re-enter the password.

This applies for using the browsers Internet Explorer 6 or later or Firefox 4 or later on the client side and for using Microsoft Windows Server 2003 or 2008 as domain controller. If you use other domain controllers, a special configuration may be required for activating the Kerberos authentication protocol.

SNMP traps for errors and warnings

From now on, XPR uses SNMP (Simple Network Management Protocol) traps not only for sending system information but also for transmitting error messages and warnings to the management center.

Error messages about missing licenses

In case of a license violation a warning used to be written in the XPR log. This is now an error. In addition, an entry is made in the Microsoft event log. If SNMP is used, an SNMP trap is sent also.

Installing LocalFormsSmtplib without Outlook profile

Setting up LocalFormsSmtplib (OpenScape Xpressions optiClient Extensions) does not require the Outlook profile of the installing user anymore. This does not apply for publishing LocalFormsSmtplib.

Supporting the OpenScape Voice Trace Manager

XPR can send logging information to the OpenScape Voice Trace Manager (OSVTM), which collects this information centrally.

Conferences

- Web conferences can be accessed from the Outlook or Lotus Notes plug-in within a specific period (entrance grace period) prior to the scheduled web conference start.
- If participants are still in a web conference at a specific time (termination grace period) before the web conference ends, the web conference is prolonged by 30 minutes if the required resources can be reserved. If no participants are in the web conference at this time, it ends as scheduled.
- Statistics raw data of conferences can be used for reporting as in the OpenScape UC Application V6 R0. Such statistics raw data comprise among other things a conference's creation and start date and the times at which participants joined or left a voice or web conference.

Resetting a PIN

You can reset a PIN by mail from Lotus Notes, Microsoft Exchange or by SMTP. The user clicks on **PIN forgotten** and receives a message that he/she needs to confirm. He/she then receives a second mail with the new, arbitrary PIN. The user logs on with this PIN and changes it then.

Crystal Report Runtime Engine

This runtime engine is available on the setup medium (USB stick) and is installed in the scope of a Report Schedule APL setup.

XPR version in the program list

The list of programs installed on the Windows computer displays the XPR version.

Security checklist

The new documentation called *OpenScape Xpressions Security Checklist* serves as basis for defining the security settings when you expand systems, put them into operation or update their software. The checklist supports the service in the direct and indirect channel when making arrangements with the customer and for documenting decisions taken.

1.6 Document Conventions

The product name OpenScape Xpressions V7 is abbreviated by **XPR** in this manual.

The following conventions are used in the manual to clearly distinguish the various types of information.

1. The single operating instruction steps are numbered.
- Enumerations are indicated with dots.

NOTE:

A note is inserted in the text to draw your attention to a feature or to provide information that facilitates working with the program.

IMPORTANT:

Text indicated in this way signals high priority information. The corresponding details must be heeded to avoid damages to the system or loss of data.

Indications of operating controls, such as buttons and window captions, are emphasized in boldface, for example, **Login Options**.

1.7 Manual Structure

This manual is written for the XPR server administrator. First of all, a short overview of the server will be presented.

Next, the administration of the database will be discussed along with all associated tasks. These tasks include the installation and configuration of new users, security, and various other administrative duties that occur within the daily operation.

After this, an overview will be presented of the various XPR components with particular attention to the XPR monitor as a central surveillance and configuration tool. In the single XPR components context also the supported protocols and their options are explained.

In the Appendix you find an overview of the possible document formats and an overview of the registry settings. Experienced administrators use registry settings for further configurations.

1.8 About the XPR Documentation

This section informs you about the technical documentation available for XPR.

As a matter of rule, manuals in printed format are only available on special request. All documents are provided on the setup medium as PDF version. Updated document editions are published via the E-Doku Portal or SEBA.

The documents mentioned display all entry dialogs important for the installation, configuration and operation. Depending on the operating system, the screen resolution and the PC configuration, the dialog representations may slightly vary. The following documents are available with XPR:

1.8.1 Installation and Administration

Release Notice, A31003-S2370-S100-*-20

This manual describes the released features and XPR server restrictions.

Server Installation, A31003-S2370-J100-*-31

The installation manual describes the linear installation of the XPR system as well as the subsequent installation of additional features and program components. Beyond that you are comprehensively informed about the installation and configuration of the communication hardware used. A corresponding guide supports a possible hardware conversion.

Cluster Installation, A31003-S2370-J101-*-31

Installation of the XPR server on a Microsoft cluster system with Microsoft Windows Server 2008.

Upgrade Instructions, A31003-S2370-J102-*-31

Here you find the description of how to upgrade an existing XPR server to the current version.

Client Installations, A31003-S2370-J103-*-31

The installation of the client applications is described here.

Cisco UC Manager, A31003-S2370-J104-*-31

This manual addresses the installer and administrator of the XPR server connection to a Cisco UC Manager PBX.

optiClient & MS Dynamics CRM, A31003-S2370-J105-*-31

This manual address system administrators who integrate optiClient in Microsoft Dynamics CRM 3.0 or 4.0 via its MS CRM integration.

Server Administration, A31003-S2370-M100-81-76A9

This manual, which you are currently reading, addresses the XPR system administrator and describes the product on its maximum extension level. It informs you about the structure of the overall system and describes the system configuration.

Microsoft Exchange Gateway, A31003-S2370-M101-*-A9

This manual addresses the installer and the administrator of an XPR system with a gateway to Microsoft Exchange. It informs you about the structure of the overall system and describes the system installation and configuration.

Lotus Notes Gateway, A31003-S2370-M102-*-A9

This manual addresses the installer and the administrator of an XPR system with a gateway to Lotus Notes. It informs you about the structure of the overall system and describes the system installation and configuration.

SAP R/3 Gateway, A31003-S2370-M103-*-A9

This manual addresses the installer and administrator of an XPR-system with a gateway to SAP R/3. It informs you about the structure of the entire system and describes the system installation and configuration.

Multi Tenancy, A31003-S2370-M104-*-A9

Configuration and administration of multi-tenant scenarios.

optiClient, A31003-S2370-M106-*-A9

Configuration and Administration of the optiClient client.

Application Builder, A31003-S2370-U119-*-19

This manual describes the operation of the Application Builder. Via this builder you can create individual IVR systems, which serve e.g. as automated attendant.

1.8.2 User Manual

Client Applications, A31003-S2370-U100-*-19

This manual provides an overview of all clients used with XPR and refers, if required, to the respective user manual.

Web Assistant, A31003-S2370-U101-*-19

This manual describes the administrator as well as the user functions. The former are, for example, the creation and modification of user accounts. The latter are, for example, the creation of notifications for new messages or access to the own mailbox.

Web Assistant, A31003-S2370-U122-*-19

Quick guide through the Web Assistant.

Microsoft Outlook Extensions, A31003-S2370-U102-*-19

This manual describes the operation of the extensions for Microsoft Outlook. These consist of the Outlook Forms and the conference extension, which are components of the *optiClient Extensions*. You can operate the Outlook forms with a Microsoft Exchange server as well as install them in a version where the XPR server operates as IMAP server that is directly connected by Microsoft Outlook.

Microsoft Outlook Extensions, A31003-S2370-U123-*-19

Quick guide through the Microsoft Outlook extensions.

Lotus Notes Extensions, A31003-S2370-U103-*-19

This manual describes the operation of the extensions for Lotus Notes. These consist of the Lotus Notes Templates and the conference extension, which are components of the *optiClient Extensions*.

optiClient, A31003-S2370-U104-*-19

The optiClient Extensions comprise the CTI client described here and the Outlook forms respectively the Lotus Notes templates. You use the CTI client optiClient to control you office phone, to optionally configure it as SIP softphone, to write short messages by Integrated Messaging and to access web conferences. You find the operating instructions on the Outlook forms in the Microsoft Outlook Extensions manual. How to operate the Lotus Notes templates is described in the Lotus Notes Extensions manual.

optiClient, A31003-S2370-U124-*-19

Quick guide through the optiClient.

OpenScape Web Client, A31003-S2370-U105-*-19

This manual describes the operation of the *OpenScape Web Client*. This client offers CTI controlling of the individual telephone via the intranet, access to individual voicemails and conference management.

PhoneMail, A31003-S2370-U106-*-19

This manual describes the operation of PhoneMail. PhoneMail is the Telephone User Interface (TUI) predominantly used in the US. The PhoneMail Telephone User Interface (TUI) was originally realized in hardware. XPR PhoneMail is a replica of this TUI, extended by Unified Messaging functionality.

PhoneMail Function Tree, A31003-S2370-U108-*-19

Function tree.

PhoneMail Function Tree Simplified Mode, A31003-S2370-U109-*-19

Function tree for the simplified mode.

PhoneMail Function Tree Octel-like-Menu, A31003-S2370-U126-*-19

Function tree adjusted to the Octel menu.

VMS, A31003-S2370-U110-*-19

This manual describes the operation of VMS. The VMS Telephone User Interface (TUI) was originally realized for the Hicom 300 PBXs in hardware. XPR VMS is a replica of this TUI.

VMS Function Tree, A31003-S2370-U110-*-19

Function tree.

Evo, A31003-S2370-U113-*-19

This manual describes how to use Evo. The Telephone User Interface (TUI) Evo offers voice-controlled operation, but it can also be conventionally operated via telephone keys in addition.

Ergo, A31003-S2370-U114-*-19

This manual describes the operation of Ergo. The Ergo Telephone User Interface (TUI) has been specially designed with regards to Unified Messaging functionality. At the same time, many advanced features can only be configured via the Web Assistant, since they would have led to a rather complex operation by phone.

Ergo, A31003-S2370-U115-*-19

Quick guide through Ergo.

Ergo Function Tree, A31003-S2370-U116-*-19

Function tree.

Conferencing, A31003-S2370-U117-*-19

Quick guide, which describes configuring and operating voice conferences from the view of Microsoft Outlook, Lotus Notes and Web Client users.

Communications, A31003-S2370-U118-*-19

The Communications client can be used by the administrator as well as by the end user. The administrator can e.g. create new user groups and user accounts. The user is e.g. enabled to access his/her messages.

IP-Phone Assistant, A31003-S2370-U120-*-19

The *IP-Phone Assistant* is an extension for OpenStage 60/80 telephones. With the *IP Phone Assistant* you can retrieve respectively play text messages, voicemails and greetings, record new greetings, and send SMS messages.

OpenScape Web Collaboration, A31003-S2410-U100-*-19

OpenScape Xpressions V7 uses the product *OpenScape Web Collaboration* in the configuration *OpenScape Web Collaboration Embedded*. This is the operation guide.

OpenScape Web Collaboration, A31003-S2410-U101-*-19

OpenScape Xpressions V7 uses the product *OpenScape Web Collaboration* in the configuration *OpenScape Web Collaboration Embedded*. This is the corresponding quick guide.

1.8.3 Notes for the Service Technician

Besides the user documentation and the administrator manual please also take note of the XPR release information found on the product data carrier. Here you are provided with current product notes that may not have been considered for the documentation. You find the file under `XpressionsInstall\ReleaseNotes.rtf`.

1.9 Data Protection and Data Security

This system also processes and uses personal data for purposes such as billing, displays, and customer data acquisition.

In Germany, the processing and use of such personal data is subject to various regulations, including the regulations of the Federal Data Protection Law (Bundesdatenschutzgesetz = BDSG). For other countries, please follow the appropriate national laws.

The aim of data protection is to protect the rights of individuals being affected by use of their personal data.

In addition, the aim of data protection is to prevent the misuse of data when it is processed and to ensure that one's own interests and the interests of other parties which need to be protected are not affected.

IMPORTANT:

The customer is responsible for ensuring that the system is installed, operated and maintained in accordance with all applicable labor laws and regulations and all laws and regulations relating to data protection, privacy and safe labor environment.

Employees of Unify Software and Solutions GmbH & Co. KG are bound to safeguard trade secrets and personal data under the terms of the company's work rules.

In order to ensure that the statutory requirements during service – whether during “on-site service” or during “remote service” – are consistently met, you should always observe the following rules. You will not only maintain the interests of your and our customers, you will also avoid personal consequences.

A conscientious and responsible approach helps protect data and ensure privacy:

- Ensure that only appropriately authorized persons have access to customer data.
- Take full advantage of password assignment options; do not allow unauthorized persons to gain access to passwords by writing them down on a piece of paper or via other means.
- Ensure that no unauthorized person is able to process (store, modify, transmit, disable, delete) or use customer data in any way.
- Prevent unauthorized persons from gaining access to data media such as backup disks or printed reports. This applies to service calls as well as to storage and transport.

- Ensure that data media which are no longer required are completely destroyed. Ensure that no papers remain generally available.

Work closely with your customer contact; this promotes trust and reduces your workload.

2 Server Structure

2.1 XPR Structure

The XPR software consists of

- several Windows services, which implement the server functionality,
- some GUI applications (Graphical User Interface) and other tools, which enable the operation and administration,
- as well as TUI applications (Telephone User Interface) for the terminal user.

The Windows services can then be split into four groups:

- License service
- XPR kernel components,
- XPR APLs (Access Protocol Layers),
- External components.

The XPR kernel is based on the five kernel components *Message Transfer Agent* (MTA), *Database*(InfoStor), *Extended Message Reporter Service* (XMRSvc), *Configuration Service* (CfgSvc) and *Name Locator* (NameLoc). Access to the kernel is provided by various access protocol layers (APL) which integrate external protocols, e.g. ISDN, SMTP, Exchange Gateway and TCP/IP. The Access Protocol Layers thus allow access to the server over various communication mediums. In principle, access protocol layers are optional components. Their purpose and configuration will be described later.

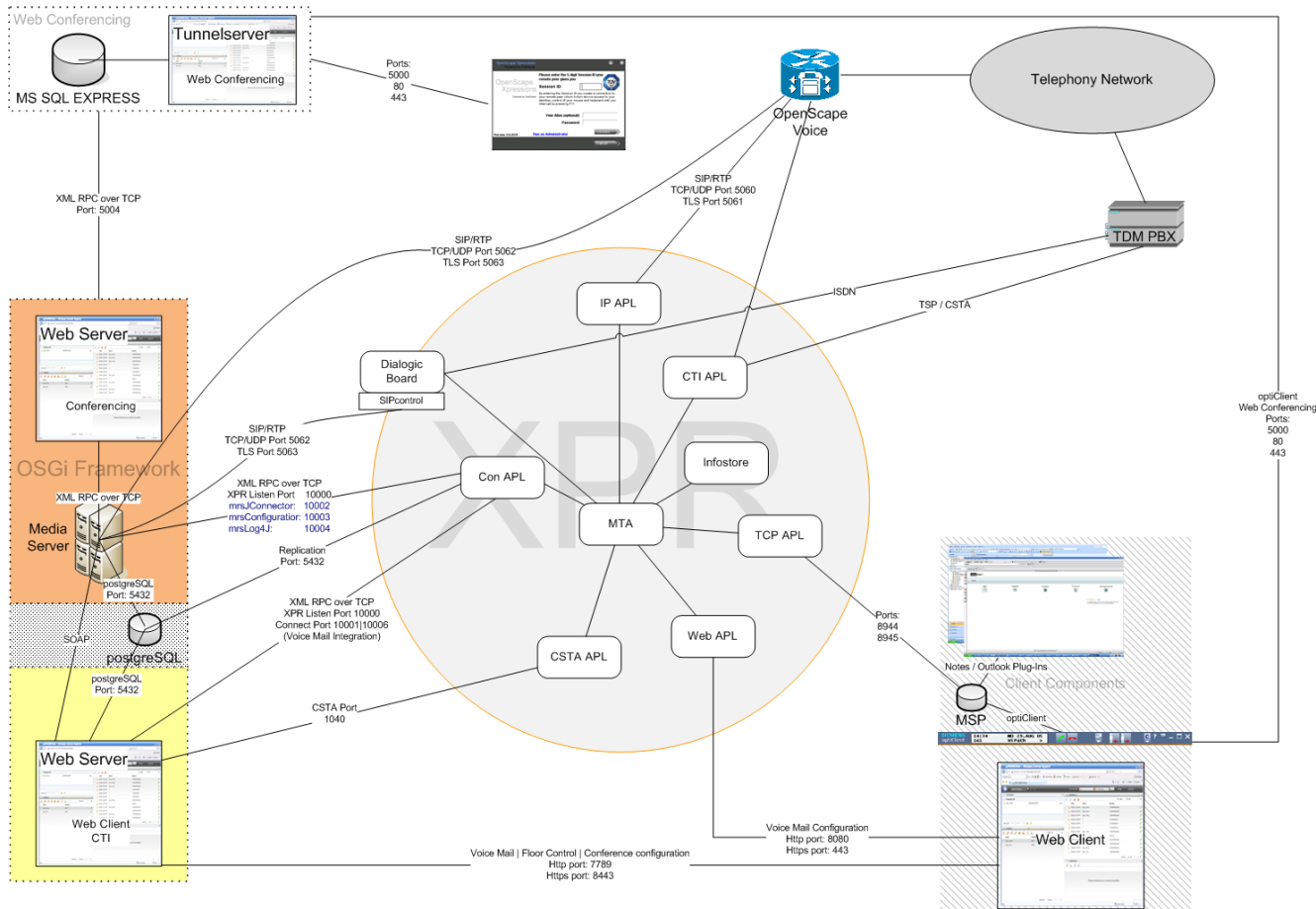
With the exception of the Name Locator (organizes the communication in a distributed system), all other components can be seen in the XPR Monitor.

NOTE:

A maximum of 60 APLs may connect to a kernel. All kernel services must jointly run on one computer. The APLs can be connected via satellite systems.

External components that cannot be verified as APL are managed and controlled via the Connection APL (ConAPL). Such components are e.g. the conference server for voice and web conferences and the web server for *OpenScape Web Client* as web-based CTI client.

Server Structure



2.1.1 License Service

The license service serves for communicating with the HiPath License Management. See [LicSvcAddress \[REG_SZ\]](#).

NOTE:

The XPR server checks the licenses used once a day. Exceedings are written in the log file as error with the respective licenses and exceedings being indicated. Parallel to the log file, the error message is also written in the Windows event view as error with source MTA.

2.1.2 XPR Kernel Components

2.1.2.1 XPR Administrator

The XPR Administrator controls the starting and stopping of the XPR Server. The Administrator is the only service that has the start option “automatic” in the Service Control Manager. As soon as the Windows server is started, the XPR Administrator is also started since it controls the starting of the kernel and subsequently the starting of the APL's.

The XPR will refuse to start when the system date is less than 1995 or greater than 2038. This is done to prevent database corruption through invalid system dates.

2.1.2.2 Message Transfer Agent

The Message Transfer Agent (MTA) assumes the function of document routing and the establishment of connections. As soon as a document is received by an Access Protocol Layer (APL), it is then routed to the MTA. The MTA uses the address book and any applying rules to convert and forward the document to the target APL. “Routing Rules” govern the behavior of the router.

Distribution lists and conversions are executed within the MTA.

The MTA performs large amounts of work simultaneously. All jobs that can be executed independently of each other are processed simultaneously in separate threads. Only jobs whose chronological order is critical are processed sequentially.

Simultaneously processed tasks are:

- Routing of documents and dialogs,
- Conversions,
- Definition of distribution lists.

Simultaneously processed tasks are:

- Report assignment,
- Line states,
- Database accesses.

The router which otherwise represents a bottle neck for conventional routing techniques, is perfectly scalable due to this technology. In case of a multi-processor system, routing processes can be distributed among different CPUs.

2.1.2.3 Information Store (Database)

The InfoStor is based on the database cTree. Journals, user, and charge information are managed by InfoStor. The database is designed to support address book synchronization with other databases such as the Active Directory by Microsoft.

Dialing number display is standardized in the XPR server. If, for example, you want to send a fax to +49-1234-567890, this address is mapped under XPR as NVS : FAXG3/+491234567890. No outside dialing information is contained in the address since addresses are managed by the appropriate APL.

Before the setup, the server can be set to the use of a Russian or Turkish codepage via **Control Panel > Regional and Language Options > Advanced > Language for non-Unicode programs**. By means of this setting, the XPR database is initialized in the respective codepage during the installation. This enables the use of Cyrillic or Turkish characters in many areas. For these two languages the database is written in the codepage 1251 with Russian respectively 1254 with Turkish. Please note that with setting a client to another language some special characters may not be properly represented if they are not available in this codepage. As regards the user ID, special characters such as Cyrillic characters may still not be used.

IMPORTANT:

This setting can only be performed in case of a new installation. A simple upgrade is not given!

The condition is that the server as well as the client must be set to Russian respectively Turkish to ensure a correct representation of anything to be displayed from the database. A client set to Turkish at a Russian server or vice versa is not possible. Likewise, a client set to Russian does not receive correct Cyrillic characters from a server not installed in Russian.

For all other languages, codepage 1252 is still used for the output.

In case of System Networking, only servers may be used that have the same codepage. You find more information on this in [Chapter 8, "System Networking"](#).

2.1.2.4 Extended Message Reporter Service

This centralized service gathers all Log information from the various XPR components. Monitor processes distributed over the network, can be logged-in with the XMR service giving various and dissimilar system reports.

Special surveillance terminals, for example, can be configured very easily in this way. On one Monitor security information could be displayed while on another Monitor fax information is shown etc.

The Extended Message Reporter Service is a highly optimized router between two monitors and the XPR services. Basically, information is only generated for active XPR Monitors. Information is gathered by the Extended Message Reporter Service from throughout the Windows network. This information can then be viewed by specially configured Monitors within the network.

The Extended Message Reporter Service is much more efficient than the Windows Event Viewer.

2.1.2.5 Configuration Service

The Configuration Service sees to the configuration data being read from a Windows registry or being written into it.

2.1.2.6 Name Locator

The Name Locator frees the Intertask-Communication from having to know which task is being performed on which computer. Name Locator runs in the background on every XPR node and supplies the names of the XPR components running on this node to all other XPR nodes in the network.

2.1.3 XPR Access Protocol Layer (APL)

Component	Description
ABC-A APL (ABCAPL)	MWI at an Alcatel 4400 PBX via ABC-A protocol. For the administration see Chapter 25 .
Computer Telephony Integration APL (CTIAPL)	Connection of telephone exchanges for CTI functionality. For the administration see Chapter 17 .
Connection APL (CONAPL)	The Connection APL serves two purposes. On the one hand it is a middleware to provide Java programs with the XPR server transactions. On the other hand it manages all components that are not available as normal APL. For more information see Chapter 30 .
CSTA APL (CSTAAPL)	Abstraction layer for CSTA. Allows CSTA client applications to cooperate with all PBXs supported by the XPR server. For more information see Chapter 18 .
Database APL (DBAPL)	Connection to external databases. Data can be retrieved by other APL's via transactions. For the administration see Chapter 26 .
Directory Service APL (DIRSVC)	The Directory Service is an XPR service that enables other XPR components to perform address queries. It is installed as part of the kernel setup and used by the Web APL to display the real name (display name) associated to an e-mail address.
Microsoft Exchange APL (E2KAPL)	Gateway to Microsoft Exchange. For the administration see <i>Microsoft Exchange Gateway</i> manual.
Microsoft Exchange True Unified Messaging APL (EXUMAPL)	Additional connector that allows True Unified Messaging with a Microsoft Exchange connection. For the administration see <i>Microsoft Exchange Gateway</i> manual.
File Interface APL (FIAPL)	General File Interface. Any file exchange formats can be defined via a script language. For the administration see Chapter 28 .
HiPath Management APL (HPMAPL)	Administering user data via HiPath User Management. For the administration see Chapter 20 .
Integrated Services Digital Network APL (ISDNAPL)	This APL implements the ISDN protocols Voice, Fax G3, Fax-on-demand and Fax G4. The Sangoma Diva(R) hardware is addressed via those protocols. The CorNet-N/NQ protocol of the telephone systems from Unify GmbH & Co. KG (Hicom and HiPath) is also supported. For the administration see Chapter 10 . A virtual machine is integrated into the ISDN APL which uses a Script language to implement customized applications. Fax-on-demand systems or complex voice mail systems can be implemented by means of these scripts.

Component	Description
Internet Protocol (IPAPL)	VoIP interface for connecting XPR to Cisco Callmanager, HiPath and OpenScape systems and other IP-based PBXs for voicemail. Components used in the IP APL context are: • Voice mail systems • Fax over IP (FoIP, T.38) • HiPath H.323 Service Provider For the administration see Chapter 10 .
Lightweight Directory Access Protocol APL (LDAPAPL)	This APL implements the interface to a directory service such as Active Directory, DirX Directory, Netscape Directory with a gateway functionality to respectively integration in Microsoft Exchange via the LDAP protocol. For the administration see Chapter 19 and the <i>Microsoft Exchange Gateway</i> manual.
Lotus Notes APL (LNAPL)	Gateway to Lotus Notes 6.x, 7.x and 8.x. For the administration see <i>Lotus Notes Gateway</i> manual.
Lotus Notes True Unified Messaging APL (LNUMAPL)	Additional connector that allows True Unified Messaging in a Lotus Notes connection. For the administration see <i>Lotus Notes Gateway</i> manual.
Direct Print APL (LPRAPL)	Addressing of printers via the LPR protocol. For the administration see Chapter 23 .
Mailbox APL (MAILAPL)	The Mailbox APL implements the XPR e-mail protocol. It provides a mailbox for every user's messages. The mailbox can use so-called "Awake Rules" to deliver APL documents that have not been read within a set time to a responsible party. Automatic subscriber lists (LIST server) can be created with the Mailbox APL. Further features are the CTI Journal and Printer Embedded Codes. For the administration see Chapter 11 .
Notification Module (NOTAPL)	The Notification APL is used to send server-generated notifications about newly incoming messages (e-mails, fax or voice mails) to terminal devices. Notification can be via MWI, SMS or a TUI call (User Outcall). The settings are performed by the users via the Web Assistant ; the administrator may set useful defaults. For the administration see Chapter 16 .
Presence (PRESENCEAPL)	Presence status and Instant Messaging Provider. Is also required for web conferences. For the administration see Chapter 21 .
Print APL (PRINTAPL)	Automatic printing of in and outbound documents can be configured through use of the <i>Carbon Copy Rules</i> . The (tele)phone user interface can be used to print out documents using network printers. For the administration see Chapter 22 .

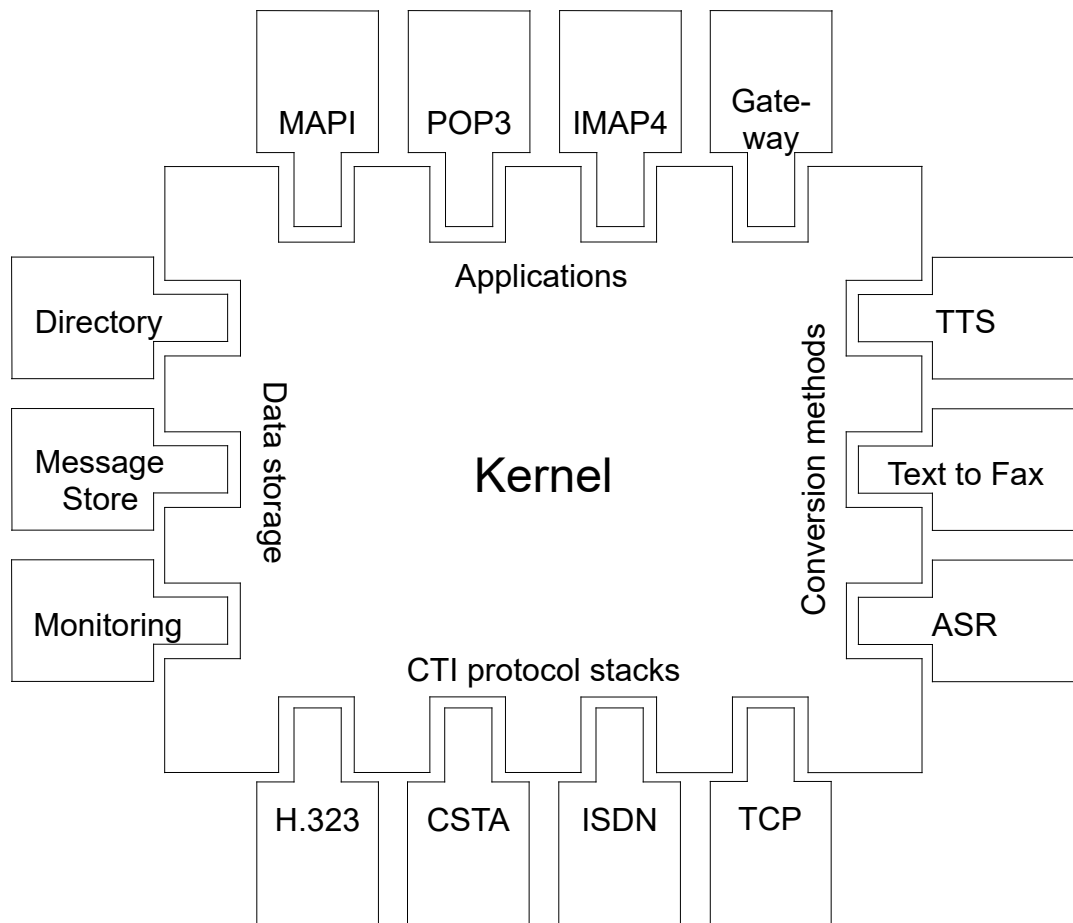
Component	Description
Report APL (REPAPL)	Generates databases from the statistical raw data of the XPR components. For the administration see Chapter 27 .
Report Schedule APL (REPSCHEDULEAPL)	Generates various statistics from the databases created by the Report APL. For the administration see Chapter 27 .
SAP R/3 APL (SAPAPL)	Gateway to SAP R/3 using the SAPconnect interface. For the administration see <i>SAP R/3 Gateway</i> manual.
SAPphone APL (SAPPHONEAPL)	CTI functions for SAP R/3 via the SAPphone interface. For the administration see <i>SAP R/3 Gateway</i> manual.
SMS Connector (SMSIPAPL)	Sending and receiving SMS messages via GSM adapters or a direct provider coupling. For the administration see Section 14.5, "SMS Connector (SMSIPAPL)" .
Internet Mail APL (SMTPAPL)	Gateway to the Internet. Messages can be sent and received via the SMTP protocol. POP3 and IMAP4 clients can log on to the XPR server and receive inbound documents. User mail can be retrieved from other mail servers via POP3. Voice mail servers can be networked using the VPIM protocol. For the administration see Chapter 12 .
TCP/IP Transport APL (TCPAPL)	This Network APL enables the client/server communication via the network protocol TCP/IP. For administration see Chapter 15 .
V.24 APL (V24APL)	The V.24 APL enables the use of fax with fax class 2 modems. You can use the script language to create any V.24 protocols to deliver and receive documents. The protocols implemented are, for example, analog Message Waiting Indication for Hicom systems. For the administration see Chapter 24 .
Web Server APL (WEBAPL)	The XPR Web Server can respond to normal HTTP 1.1 queries and insert various XPR functionalities in transmitted HTML pages via E-Scripts. This enables e.g. accessing the own messages via a regular Web browser, or the administration of the own mailbox via a Web-based application such as the Web Assistant. Furthermore, besides the server functionality, an HTTP client is included, which can be controlled by other APL's via transactions. Thus HTML pages can automatically be called and information can be extracted from these pages per E-script and forwarded to the querying APL. For the administration see Chapter 13 .
Web Services APL (XMLAPL)	The XML APL serves as an interface via which the XPR server functions are provided as Web service. For the administration see Chapter 29 .

2.1.4 Interface Tools

The interfaces for the administration and operation of XPR consist of

- XPR Monitor (see [Chapter 6, “XPR Monitor”](#)),
- Web Assistant, a web-based application for mailbox administration for the users as well as tool for the administration of the XPR system or the administrator (see manual *Web Assistant*).
- XPR Administration and Mail Client (see the *Communications* manual),
- A range of helpful support tools, partly used on the command line level (see [Chapter 32, “Tools”](#)),
- Telephone User Interfaces (see manuals *PhoneMail*, *VMS*, *Ergo* and *Evo*).
- Client extensions for integration in foreign systems such as Microsoft Outlook or Lotus Notes (see *Microsoft Outlook Extensions* and *Lotus Notes Extensions* manuals).
- Application Builder for creating Automated Attendant applications (see the *Application Builder* manual).
- Internet integration (POP3, IMAP4), Caller Guide, cyViewer, TAPI via MSP, Conversation Recorder (see *Client Applications* manual).
- CTI: Control of the individual telephone. See the *optiClient* manual.

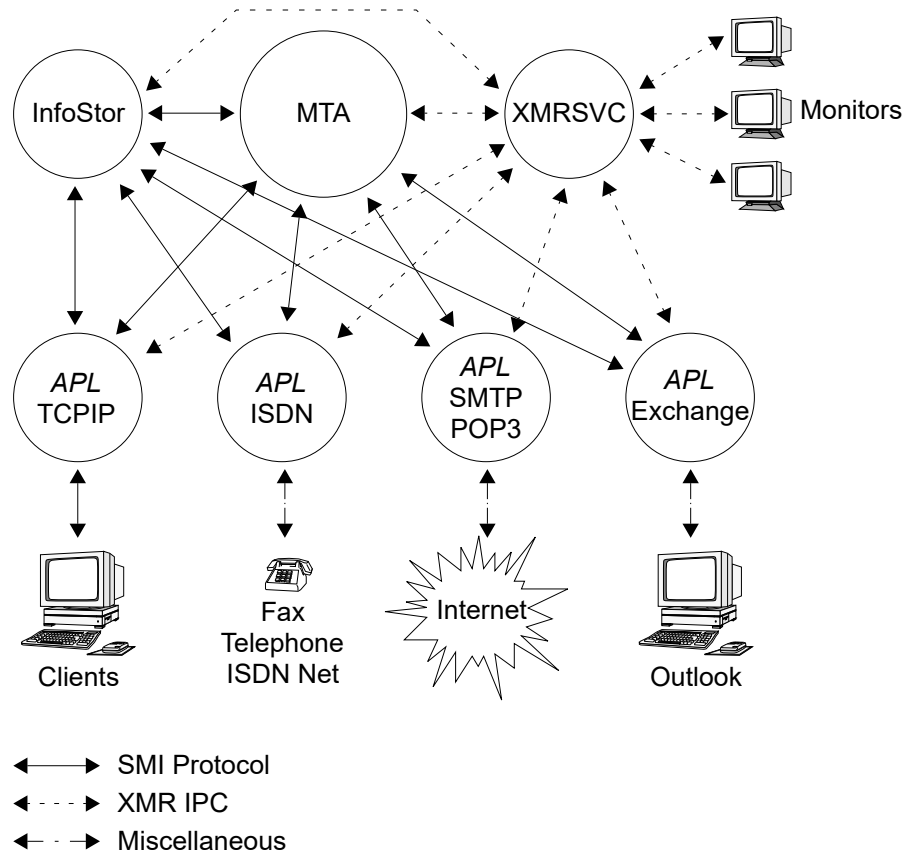
2.2 Component-Based Platform Architecture



The flexibility and modularity of the XPR configuration option allow the customization of a service installation and configuration to suit your precise requirements.

2.3 XPR Process Structure

The following diagram provides an overview of the XPR process structure.



2.4 Staggered Administration

A staggered access privilege is available for the administration, which is split up as follows:

- Engineering level: tools such as DBTool, InfoTool, NCOAdmin, ZombiDetect etc. require for write operations a special password, which is only disclosed in the corresponding trainings for this group of persons.
- Service level: network administrator. Is required to set up System Networking. See [Chapter 8, "System Networking"](#).
- Default admin: *Supervisor privilege* - Default administrator access for service technicians or specially trained customer administrators. Access to the XPR monitor with all configuration options. May edit users and user groups in the Web Assistant or Communications without restriction.
- Service admin: *Service privilege*: Customer administrator with access to the XPR monitor. Not all configuration pages respectively options are displayed. Debug level for logging in the XPR monitor cannot be activated. It must not change the group membership or privileges of a user with *supervisor privilege* in the Web Assistant or Communications. Users with *supervisor privilege* cannot be created either. Routing rules cannot be edited. No messages can be forwarded or viewed in the global MTA journal. The following features are possible in particular:
 - Editing user and contact data
 - Editing distribution lists
 - Editing user groups without changing the *supervisor privilege*
 - Editing global and company greetings
 - Editing local, spoken location name in case of system networking
 - Editing IVR applications with the Application Builder
 - Editing voicemail profiles
 - Restricted editing of NCO from a telematics APL
 - Using the XPR monitor for monitoring
 - Using the XPR monitor for simple, uncritical configuration modifications
 - Viewing global log files
 - Viewing the server status

2.5 XPR Addressing

Irrespective of the protocol and structure of the target system, the XPR server always uses the following form of address for addressing:

`NVS:NODE.CLASS/USER`

or

`NVS:NODE/USER`

The first address section (`NVS:`) is a constant and non-changeable, as it characterizes the syntax as well as the address type. In this way it is later possible to insert new address types. This part of the address can thus be omitted at present. Based on this address type we also speak of a NVS address.

The target network is described via `NODE`. Typical nodes are `FAXG3`, `SMS`, `TCPIP`, `SMTP`, `LN` etc.

Examples:

`NVS:FAXG3/+491234567890`

Fax G3 subscriber +49-1234-567890.

`NVS:EXCH/MAYER`

Microsoft Exchange user Miller.

`NVS:SMTP/info@domain.com`

TCP/IP e-mail via SMTP protocol to TCP/IP user, Info, in the domain domain.com.

A distinction can be made between the various similar accesses to the same `NODE` network with the optional `CLASS` entry. If a server is connected via seven logical fax lines to the network, these seven logical fax lines can be told apart by specifying the `CLASS`. If the option `CLASS` is not used (e.g. `NVS:NODE/USER`), then the router decides which access is to be used to the net `NODE` based on internal evaluation tables. The entry `USER` is an address expressed in local syntax within the network. In the case of a fax this is the fax number in a standardized form.

Examples:

`NVS:FAXG3.1/+491234567890`

Fax G3 subscriber +49-1234-567890 via logical line (`CLASS`) 1.

`NVS:FAXG3.2/+491234567890`

Fax G3 subscriber +49-1234-567890 via logical line (`CLASS`) 2.

NVS addresses always define a logical access from and to the XPR system. Access Protocol Layers define the individual structure of a physical point of access to the network.

3 Starting and Stopping the Server

There are various methods of starting and stopping the XPR server. In most cases the user sees none of this, since the server starts automatically without any logged-in users and therefore requires no display output.

NOTE:

The server and tools require administrative privileges. Therefore, select *Run as administrator* in the context menu.

But the status of the server start can be monitored at any time via a previously started XPR monitor. The following methods are also available and will be described in more detail below:

- Start/stop by starting or shutting down the Windows server
- Start/stop through installed program icons or selection of these programs from the Start menu
- Start/stop via the Windows *Service Control Manager*
- Start/stop locally from the command line
- Start/stop locally and remotely via the command line with the utility **sc** (part of the Windows NT Resource Kit).

First, the program icons **Start XPR Server** and **Stop XPR Server** created during the installation deserve a mention. They can be reached via the Start menu.

Second, the Service Control Manager. It can be reached via **Start > Settings > Control Panel > Administrative Tools > Services**. Now you can see all installed services and their states.

The service **XPR Administrator (MRS)** starts the complete XPR server. A service is stopped by selecting the service from the list and subsequently selecting the **Stop** button. Through this action the XPR server is shut down. This way, it is also possible to end and restart single server components by selecting the respective setting.

In most cases, the startup mode for the **XPR Administrator (MRS)** service is **Automatic**. With this setting the XPR server is automatically started when the computer is started. If this is not desired, you can change the startup type to **Manual**. Subsequently, you need to start the XPR server manually after each computer reboot.

Every XPR server component can be started or stopped via the command line. To do this, enter the component name (in parentheses after the descriptive name in the *Service Control Manager*) along with the **Start** or **Stop** command. The directory `<XPR Install>\bin` must have been added to the environment variable `PATH`. To start or stop the XPR server, the commands `MRS Start` or `MRS Stop`

are entered in the command line. Locally, this is possible via the `NET` command, which does not require an extension of the `PATH` variable. Simply enter `net start <Service>` or `net stop <Service>`.

All the methods mentioned thus far function only on the local computer (computer where the XPR server is installed). Starting and stopping the XPR server is also possible from other computers within the network. The `sc` utility is provided for this purpose. This utility is not part of the standard Windows package, but comes with the Windows NT Resource Kit. The acquisition of the Windows NT Resource Kit is suggested not only for this utility, but also for the useful knowledge contained within for the execution of the system administrator's duties.

This utility allows users to control and query services on the local computer as well as other computers within the network via the command line. The call for starting and stopping the XPR server is as follows:

```
sc \\<Server Name> start mrs
sc \\<Server Name> stop mrs
```

The server name is the name of the computer in the Windows network, and is not required when this utility is executed for services on the local computer.

A range of XPR APLs can also be restarted via the XPR monitor. These also support remote operation.

Live processing may not be terminated correctly as a result of a Windows error when shutting down and rebooting Windows. This also affects XPR and can in extreme cases lead to database inconsistency. This is signaled when the XPR monitor is restarted and the database is automatically repaired. However, this leads to delayed XPR software startup. The server must not be shut down and the MRS service must not be stopped while the automatic repair is in progress, as this can otherwise lead to a permanent database inconsistency. If this happens, the only solution is to reload a database backup. Backups are automatically created every day at midnight as standard and saved in the server's backup directory. Any documents entered after the last backup are generally lost.

We thus strongly recommend that you always stop XPR before shutting down Windows and only restart (or shutdown) Windows when the initial task has been completed correctly.

Also use this Registry key:

```
Registry key
HKLM\SOFTWARE\Wow6432Node\PP-COM\MRS\Services\
AplDelay - REG_MULTI_SZ
```

Set this registry key order to delay any Xpressions service initialization when starting up Xpressions.

This is used specially on Failover Cluster installations.

In case of a failover scenario NotApl and ConApl should be started only after the voicemail is reestablished for the users.

with syntax:
apl name,delay in minutes

Example:

ConApl,5

NotApl,10

3.1 Installing and Starting individual Components

Almost all components can be installed at a later time using the setup program. This is not possible for certain modules that were not included as part of the setup program delivered. Installation instructions for these modules by using the Commandline Interpreter is as follows:

You can install any APL or kernel component from the `<XPR Install>\bin` directory with

```
Name install -branding=XPR
```

from the command line. An attempt is made to incorporate meaningful default values, but a complete configuration of the component should be subsequently performed from the XPR monitor. Components installed in this way, for example without taking possible security settings into consideration, are put into service in the server with the result that necessary access rights may be missing. Some components, such as the Exchange Gateway, are more complicated to install and therefore should only be installed via the setup program.

Example:

```
tcpapl install -branding=XPR
```

The following command must be given in the Commandline Interpreter, so that these components are also started:

```
Name start
```

or in the *Service Control Manager* by selecting the component and then clicking **Start**. The “Manual” startup mode is usually entered during the component installation.

Since components installed in this way are not started automatically by the XPR Administrator service, they must be started manually. If you prefer an automatic start, you need to add the component in the registry under the key `HKLM\Software\Wow6432Node\PP-COM\MRS\Services` in value [Access Protocol Layers \[REG_MULTI_SZ\]](#).

It should be noted, furthermore, that components installed in this manner do not demonstrate any awareness of the security mechanisms set and operate by default in the system account.

Applying this method, you can install an APL on the same XPR server several times. This can be useful, for example, in case of the IP APL if you wish to instantiate it several times. See [Section 10.10.6, “Several IP APLs on one Server”, on page 874](#).

Install the corresponding APL from the command line another time:

```
Name install -branding=XPR -name=<RegName>
```

For each further registration the parameter `-name=<RegName>` is adapted. Via the `<RegName>` parameter the registry key for this entity of the *Name* APL is adjusted and the name determined, under which the APL is displayed in the XPR monitor for configuring it.

3.2 Stopping and Uninstalling individual Components

In a likewise manner to that of the installation, individual components can also be uninstalled from the Commandline Interpreter through the use of

Name remove

in the command line. Before doing this, all live components should be shut down in the *Service Control Manager* by selecting the component and then clicking **Stop** or by selecting

Name stop

in the command line.

4 User Data Administration

The user database contains important administration data required to coordinate and validate the access of individual users to the services of the XPR Server. The database contains files that allow the XPR server to route incoming documents and reports to a user. The database also includes the passwords used to check privileges.

The user data are administered via the Windows client Communications or via the web-based application Web Assistant. For this purpose you need to log in with the administrator account created during the setup. You find a detailed description in the Communications or Web Assistant manuals.

User groups are basically definitions of privileges that can subsequently be assigned to new XPR users. It is thus not necessary to assign privileges individually to each new account. Instead, all necessary privileges can be assigned in one go by means of user group privilege inheritance.

ID	Description	Associating User Accounts
SUPERVISOR	Administrator group	Administrator
TENANTSUPER	Tenant Supervisor Group	
SERVICE	Service group	
HELP_DESK	Help Desk Group	
ADVANCED	Privileged user group	
USER	User group	POSTMASTER
GUEST_GROUP	Guest group	SYSTEM, COMPANY

Table 3 *User groups*

All administrators should belong to the `SUPERVISOR` group since this group has all privileges.

The `TENANTSUPER` group has all privileges of a normal user and the privileges *Tenant Supervisor Privilege*, *Global Alias Editor* and *Global Distribution List Editor* in addition.

Compared to normal users, `SERVICE` has further privileges to partly take on administrator tasks. In particular, these users can log in to the XPR monitor.

The `HELP_DESK` group has all privileges of a normal user and the *Help Desk Privilege* in addition.

All normal users belong to the `USER` group. For example, the `POSTMASTER` account defined with the installation can be found in this group.

`ADVANCED` is an extension of the `USER` group with users from this group being given extended configuration options in client applications. This is currently not used.

The `GUEST_GROUP` has only been established for the special accounts `SYSTEM` and `COMPANY`, which are required for special TUI configurations. The private user greetings `SYSTEM` are, for example, used as default greetings for the TUI.

NOTE:

Please note that any one user can only be included in one group since in there the user's privileges are defined. You can manually assign further privileges to a user, though, or withdraw privileges that he/she has inherited from the group.

You find an overview of all privileges that can be assigned to a user group and of the privileges that are assigned to these groups by default in [Section 4.5, "Privileges"](#), on page 118.

4.1 Database Fields Significance

In the following table all user database fields available in the standard distribution are explained. The table is sorted according to the internal field names. In the Web Assistant you can toggle between the representation of this internal field name and a description. In Communications only the description is displayed, if available in the database. In the following table an available description is indicated *italicized* as first part of the database field significance.

Depending on the definition of the fields in the mask definitions (see [Section 4.4.1, "Editing Masks"](#), on page 117), the fields are only to be edited with the *SUPERVISOR privilege* or the *SERVICE privilege*.

The *SUPERVISOR privilege* is particularly required for the fields `GROUP`, `PASSWORD`, `PIN` and `PRIVILEGES`, since the access privilege to the server can be modified via these fields.

Field Name	Meaning
ADDR1	<i>Address 1</i> Line 1 for the postal address. Can optionally be copied for fax stationery.
ADDR2	<i>Address 2</i> Line 2 for the postal address. Can optionally be copied for fax stationery.
CIT	<i>Message waiting signal</i> A Message Waiting Indicator (MWI) is sent to the address entered here. The applicable protocol must be made available by an APL. Administering possible notifications has been handled via the Notification APL for a while. Every user can perform the corresponding configuration via the Web Assistant. For Notification APL information see Chapter 16 . If no Notification APL is installed, see Section 7.9, "Message Waiting Indication (MWI)" , on page 287.
CITFILE	<i>File for CIT</i> Reference to individual notification file. See Section 16.8, "SMS/E-Mail Notifications" , on page 1044.

Table 4 User database fields

Field Name	Meaning
CITY	<i>Location</i> Address information. Can optionally be copied for fax stationery.
COMPANY	<i>Organization</i> Address information. Can optionally be copied for fax stationery.
CONTACT-ID	<i>Contact person</i> Is managed in a Multi Tenant scenario. See the description in the <i>Multi Tenancy</i> manual on this. In this field you enter the ID of the XPR user who is to have read access to the data of this tenant.
CONSRV	For integration with OpenScape UC Application. Contains the name of the corresponding OpenScape UC Application server. Is automatically set when importing the corresponding user data.
CONUSER	For integration with OpenScape UC Application. Contains a <user ID> automatically set during the import.
COSTINFO	<i>Cost info (*)</i> Number from COSTINFO# normalized by the server using NCO. This number can be used by the XPR server for inbound routing. Direct entries via a client such as Web Assistant is not possible. On the format see Section 9.3.3, "The normalized NCO Phone Number Format" , on page 345.
COSTINFO#	<i>Cost info</i> User information used for billing purposes by the PBX. This information is combined in the extension number through special sequences so that billing can be assigned by the PBX to a user or cost center. Default is a conversion via NCO into the normalized phone number in the COSTINFO field. This field is then transferred to the PBX. If you require special sequences, you should remove the DNO attribute from the COSTINFO field, so that you can enter the sequence for booking the costs in the COSTINFO field directly. The COSTINFO# field should then be removed from the mask.
COUNTRY	<i>Country</i> Address information. Can optionally be copied for fax stationery.
CTIJOURNAL	<i>CTI journal</i> Via this switch the CTI journal for this user is activated. This is a basic requirement for CTI features to be offered in clients.
DENY_PRIVILEGES	<i>Privileges</i> The privileges fields are modified via a privilege editor. This field maps the column of prohibited privileges. All the fields that are activated in this column will not be assigned to this user. The assignment is particularly useful for groups. More information on single privileges is found in Section 4.5, "Privileges" , on page 118.
DIVISION	<i>Department</i> Address information. Can optionally be copied for fax stationery.
E_LOGIN_WEB	<i>Date of last failed login</i> For access via the Web Assistant a number of failed login attempts can be defaulted, after which this access is blocked. This blocking is effected by the entry of a corresponding time stamp in this database field. Besides the complete user blocking, a temporal blocking based on this time stamp as well can also be configured. In order to manually enable the blocked user access again, the administrator has to delete the content of this database field for the corresponding user. Access is once again granted after this deletion.

Table 4 User database fields

Field Name	Meaning
EXCH	<i>Microsoft Exchange</i> User Microsoft Exchange address. A reference to this entry in the field <code>PREFERRED</code> routes all incoming messages to the Exchange Gateway.
FAX-ACT-QUOTA	<i>Fax quota used up so far</i> Is managed in a Multi Tenant scenario. See the description in the <i>Multi Tenancy</i> manual on this. This field displays the fax quota of this tenant used up so far.
FAX-MAX-PAGES	<i>Maximum number of fax pages</i> Is managed in a Multi Tenant scenario. See the description in the <i>Multi Tenancy</i> manual on this. Enter here the number of pages that each fax message to be sent must not exceed. The XPR server will not send fax messages with more pages.
FAX-QUOTA	<i>Fax quota</i> Is managed in a Multi Tenant scenario. See the description in the <i>Multi Tenancy</i> manual on this. Enter here the total number of fax messages that the XPR server is to send for the users of this tenant at the most. This specification refers to the period of one calendar month. When the total number of sent fax messages approaches this quota, the XPR system administrator and the XPR user defined under Contact person will be informed. Via the Alert threshold you can specify the number of messages from which this information occurs. When the Fax quota has been reached, the XPR server will not send any more faxes for this tenant. In this case, a sending party receives an error message with a corresponding information.
FAXG3	Business fax G3 (*) Number from <code>FAXG3#</code> normalized by the server using NCO. This number is used by the XPR server for inbound routing. Direct entries via a client such as Web Assistant is not possible. On the format see Section 9.3.3, "The normalized NCO Phone Number Format" , on page 345.
FAXG3#	Business Fax G3 Fax number of the user for inbound fax G3 documents. In clients (e.g. Web Assistant, Communications) this field displays the number from <code>FAXG3</code> localized by NCO. In the database, however, the entered number is stored from which the <code>FAXG3</code> field is written in normalized format by NCO. This occurs for the following reason: The server inbound routing always requires the normalized number to directly assign incoming fax documents to a user. This normalized number is always generated by the server using NCO. This is why for each field with a normalized dialing number there is one field that stores the original entry. From this field the normalized number is formed once by NCO. A # character is attached to the field name of the normalized dialing number for this purpose. The administrator wants a readable user entry as far as possible. Therefore not the normalized number or the original entry is displayed to him/her, but a representation localized by NCO. Via the configuration of this NCO he/she can default a uniform format for all displayed dialing numbers.
FAXG3-HEADLINE	<i>Fax G3 header</i> Default Fax G3 user header. This entry appears in the header of all outbound fax G3 documents. If this field is empty, the server takes the default header of the APL used. With ISDN, up to 50 characters are permitted. <i>Example:</i> Mister AG/Germany

Table 4 User database fields

Field Name	Meaning										
FAXG3-ID	<i>Fax G3 ID</i> User fax ID. This ID is found in the header of all outbound fax messages. If this field is empty, the default ID of the APL would be inserted. Example: +49 2404 98765432										
FAXG4	<i>Business fax G4 (*)</i> Number from FAXG4# normalized by the server using NCO. This number is used by the XPR server for inbound routing. Direct entries via a client such as Web Assistant is not possible. On the format see Section 9.3.3, “The normalized NCO Phone Number Format”, on page 345.										
FaxG4#	<i>Business fax G4</i> Displayed Fax G4 user number for inbound fax documents. Besides FaxG4# the FaxG4 field is also available. See the corresponding explanation with FAXG3#.										
FAXG4-ID	<i>Fax G4 ID</i> Fax G4 user ID in accordance with F.200 standards. This ID is found in the header of all outbound fax documents. If this field is empty, the default ID would be inserted. Example: +49-240498765432=MISTER										
FAXSTATIONARY	<i>Fax stationery</i> This field is normally filled in automatically by the assignment in Communications. If you add it to the mask for filling it e.g. by LDAP replication, it must be furnished with the UPPER attribute. The following entry can be used when a default form is set for all users in WebAssistant > Server Settings > Fax Forms on Administrator mode . <table><tr><td>DOMAIN</td><td>CLASSNAME</td><td>CLASS</td><td>KEYNAME</td><td>KEY</td></tr><tr><td><Server></td><td>USER</td><td>DEFAULTFAXFORM</td><td>FAXSTATIONARY</td><td><Fax Form Name></td></tr></table>	DOMAIN	CLASSNAME	CLASS	KEYNAME	KEY	<Server>	USER	DEFAULTFAXFORM	FAXSTATIONARY	<Fax Form Name>
DOMAIN	CLASSNAME	CLASS	KEYNAME	KEY							
<Server>	USER	DEFAULTFAXFORM	FAXSTATIONARY	<Fax Form Name>							
FAXROUTPREFIX	<i>Fax routing prefix</i> So that fax messages can be sent via different gateways depending on the sending user, you can write a dial prefix in the FAXROUTPREFIX database field. So that this prefix is used, the feature must be activated in UserDependantRouting [REG_DWORD] for the IP APL used.										
GROUP	<i>User group</i> The group in which the user is included. A user group is defined by allocating the USER, Name, Privileges database fields and the IsGroup entry. The box USER contains the group name, Name contains a description of the group and Privileges contains the privileges assigned to the group. Via the ISGROUP switch this entry is considered a user group in the Web Assistant and in Communications. By inclusion in a group, a user thus receives all group-related privileges, in addition to those explicitly defined in this privileges box. Beyond that, some defaults for voice mail systems can be set. See the Web Assistant documentation on this. Please note that any one user can only be included in one group.										
GSM	<i>Mobile phone (*)</i> Number from GSM# normalized by the server using NCO. This number is used by the XPR server for inbound routing. Direct entries via a client such as Web Assistant is not possible. On the format see Section 9.3.3, “The normalized NCO Phone Number Format”, on page 345.										

Table 4 User database fields

Field Name	Meaning
GSM#	<i>Mobile phone</i> Displayed private cell phone number of the user. Can be offered as option if you want to call this user from a CTI client. Besides <code>GSM#</code> the <code>GSM</code> field is also available. See the corresponding explanation with <code>FAXG3#</code>.
HPMRES	<i>Resources for HiPath User Management</i> Assignment to the <i>HiPath User Management</i> mailboxes. A manual modification should remain undone. See Chapter 20, "HiPath User Management".
ISDN-CLASS	<i>Trunk groups</i> Is managed in a Multi Tenant scenario. See the description in the <i>Multi Tenancy</i> manual on this. You can reserve an ISDN trunk group for a tenant's communication. For this purpose, enter here the class name for the relevant trunk group. The class name is a portion of an NVS address and arises in the following way: <code>NVS:NODE.CLASS/USER</code>
KEYWORD	<i>Keyword</i> Field that can be freely used for entering a self-defined keyword.
LANGUAGE_ID	<i>Language ID</i> The language set by the user in the Web Assistant. This language is also used, for example, by the TUI.
LMACCOUNT	<i>Windows user account</i> If the domain\account of a Windows user has been entered in a Windows domain, the Windows account can be used for logging in at the XPR server per option to be set in the MSP profile for this user. Under Windows, a validation is automatically performed via the logged in user account. See Section 5.4, "Client log-in via Windows User Account", on page 162. At the same time, this allows logging on to the <i>Web Assistant</i> by entering either domain\account or account@domain as user before authenticating yourself with your Windows password. Please note that logging on in the more recent UPN format account@domain is possible, but the format domain\account is always expected here in this database field. You can assign several Windows user accounts to an XPR user account. This requires this field getting furnished with the <code>MULTI</code> attribute for assigning the user accounts. If only one domain is used on the customer side, you can set the DefaultDomain parameter in the param.xml of the Web APL. In this case you need not specify the domain. The first logon attempt is then made via the Windows account. If this attempt fails, another one is made with the XPR user ID and password. Please note that although the maximum entry length is 63 characters, this allocation must never be fully used since the maximum length of an NVS address is also 63 characters and some non-addressable users would be generated in the event that e.g. the <code>NVS:MAILBOX/</code>, required to form the address, could not be prefixed owing to the lack of space then. A user ID must therefore comprise fewer than 26 characters. Hint: Spaces are not allowed for the user name when Windows Login is used for WebClient.
LN	<i>Lotus Notes</i> User Lotus Notes address. A reference to this entry in the field <code>PREFERRED</code> routes all incoming messages to the Lotus Notes Gateway. Example: <code>Joe User/SAMPLE</code>
MAILBOX	<i>Internal mailbox</i> A unique mailbox name. Normally, the user's log-in name is used since it is also unique. Incoming messages are collected in this mailbox until the user collects them.

Table 4 User database fields

Field Name	Meaning
MAX_MONITOR	Maximum number of simultaneously active monitor points of a user. All requests for further monitor points that go beyond this limit are rejected with error code <code>ACCESSDENIED</code> . This function must be activated via CheckMonitorLimit [REG_DWORD] .
MAX_VOICE_MSG	If the PhoneMail parameter <code>MaxVoiceMsg</code> was activated, you can set the maximum number of messages a user can receive via this field. This requires the system to be Voice-only, so that voicemails are exclusively managed via the Mail APL internally. In case of handing voicemails over to an external system such as Microsoft Exchange this restriction is not possible. The number of voicemails is counted by PhoneMail in the <code>VM_MSG_COUNT</code> database field.
NAME	<i>Name</i> Full name of the user. If <i>Communications</i> is used as mail client, these names must be unique.
NCO_GUI_CONN_PT	<i>NCO Connect Point for GUI users</i> Definition of this GUI user's dial rules. If no specification has been made for a user, this field is looked for in the user group. If no definition has been entered there either, the system default is used. These dial rules can be selected from the defined NCO dial rules. See Section 9.3.4, "NCO Clients and Connect Points" , on page 347.
NCO_GUI_PREFIX	<i>GUI user dials with external prefix</i> Definition whether this GUI user dials with external prefix. If no specification has been made for a user, this field is looked for in the user group. If no definition has been entered there either, the system default is used. See Section 9.3.5, "Location, Phone Numbers and Prefixes" , on page 350.
NCO_LOCATION	<i>NCO location</i> Location definition for this user. If no specification has been made for a user, this field is looked for in the user group. If no definition has been entered there either, the system default is used. This location can be selected from the defined NCO locations. See Section 9.3.5, "Location, Phone Numbers and Prefixes" , on page 350.
NCO_TUI_CONN_PT	<i>NCO Connect Point for TUI users</i> Definition of this TUI user's dial rules. If no specification has been made for a user, this field is looked for in the user group. If no definition has been entered there either, the system default is used. These dial rules can be selected from the defined NCO dial rules. See Section 9.3.4, "NCO Clients and Connect Points" , on page 347.
NCO_TUI_PREFIX	<i>TUI user dials with external prefix</i> Definition whether this TUI user dials with external prefix. If no specification has been made for a user, this field is looked for in the user group. If no definition has been entered there either, the system default is used. See Section 9.3.5, "Location, Phone Numbers and Prefixes" , on page 350.
NO_REPLICATION	<i>No replication to other sites</i> In the scope of the system networking (see Chapter 8, "System Networking") the local administrator can stop the replication of single users to other locations via this switch.
OS_SPEECHENABLE	<i>Activating voice portal</i> Activates the <i>OpenScope Media Server for Xpressions</i> . This is an access from OpenScope before version 3 to the user's Lotus Notes mailbox.
PAGER_01	<i>Pager number/address 1</i> With the pager protocol users can be defined with pagers via the configuration in the XPR monitor. See Section 10.4.18, "Pager" , on page 742.

Table 4 User database fields

Field Name	Meaning
PAGER_02	<i>Pager number/address 2</i> See PAGER_01 .
PAGER_03	<i>Pager number/address 3</i> See PAGER_01 .
PAGER_04	<i>Pager number/address 4</i> See PAGER_01 .
PAGERSET_01	<i>Used pager set for pager 1</i> See PAGER_01 .
PAGERSET_02	<i>Used pager set for pager 2</i> See PAGER_01 .
PAGERSET_03	<i>Used pager set for pager 3</i> See PAGER_01 .
PAGERSET_04	<i>Used pager set for pager 4</i> See PAGER_01 .
PASSWORD	<i>Password</i> User's password. Passwords are not displayed in plaintext, but represented by asterisks. Passwords are additionally protected in the database by one-way encoding, so that they cannot be read there. Attention: The XPR server does not differentiate between capital and small letters with passwords. There is no default password. Thus, a password must be entered, since the XPR server allows <i>no</i> access via blank passwords. Users should be reminded to choose passwords which are not identifiable by simple methods, such as trying all the words in a dictionary.
PHONE	<i>Business phone (*)</i> Number from PHONE# normalized by the server using NCO. This field is required by CTI applications for establishing connections between the user's telephone and other subscribers or connections. This number is still used by the XPR Server for the CTI journal when logging user information. Since a unique number is required by all users on the XPR Server, an extension number may not be assigned to more than one user. Direct entries via a client such as Web Assistant is not possible. On the format see Section 9.3.3, "The normalized NCO Phone Number Format", on page 345 .
PHONE#	<i>Business phone</i> Users' telephone extension number, usually found at their workplace. Besides PHONE# the PHONE field is also available. See the corresponding explanation with FAXG3#.
PIN	<i>PIN</i> Personal Identification Number. This number is required for remote inquiries of the voice mailbox via a Telephone User Interface (TUI). Passwords are <i>not</i> displayed in plaintext, but represented by asterisks. PINs are additionally protected in the database by one-way encoding, so that they cannot be read there. There is <i>no</i> PIN defaulted by the system. PIN presettings can be configured each for the various TUIs. You find further information on PINs in Section 4.7, "PIN Handling in the XPR Server", on page 132 .
PMI-HOSTNAME	<i>Server for pop mail import</i> See Section 12.1.7, "POP3 Mail Import", on page 912 .

Table 4 User database fields

Field Name	Meaning
PMI-PASSWORD	<i>Password for pop mail import</i> See Section 12.1.7, "POP3 Mail Import" , on page 912.
PMI-SCHEDULE	<i>Schedule for pop mail import</i> See Section 12.1.7, "POP3 Mail Import" , on page 912.
PMI-USERNAME	<i>User name for pop mail import</i> See Section 12.1.7, "POP3 Mail Import" , on page 912.
POPFORMATS	<i>E-mail formats</i> See Section 12.1.6, "Formats" , on page 911.
POP3_Timeout	See Section 12.1.3, "POP3 Server" , on page 905.
PMROUTPREFIX	<i>Voice routing prefix</i> So that PhoneMail user outcalls can be sent via different gateways depending on the user, you can write a dial prefix in this database field. Using this prefix requires activating the feature in PhonemailUserDependantRouting [REG_DWORD] for the IP APL used. Each script with the PHONEMAIL string in its name will then use this feature.
PREFERRED	<i>Preferred Address</i> The preferred mode of routing for incoming messages. Another database box, containing the actual address, must be referenced as entry. If there is no <i>active routing</i> and True Unified Messaging (TUM) is not used, mailbox is the referenced database box. In this case, the system waits until the user calls up incoming messages himself, which is normally when he/she logs in for the first time. Thus, there is no automatic routing of new incoming messages. The user himself must ask the Server whether new documents have arrived since he/she last logged in. All other addresses are actively delivered when the user is logged in at the server. The SMI transport <code>TCPIP</code> must be specified for this purpose. The database field <code>TCPIP</code> then contains the address to which the XPR server should route the message. Since the user's current log-in status is known, each new incoming message is routed on if the user is logged in. If not, messages are routed to his/her mailbox until he/she logs in again. With TUM usage the database field of the respective foreign system (<code>Exch</code> or <code>LN</code>) is specified. A TUI, accessing a mailbox per TUM, uses this entry to reach the data via the correct True Unified Messaging Provider. This field is also used in the case of contacts, for example, to select the required telematic service. Care should be taken that with telematic services not the readable field suffixed with the # is used but the internal one without #, which contains a normalized form of the telematic number. See also the explanation with FAXG3# .
PRINTER	<i>Printer</i> Here you can specify a printer entered with the Print APL. On this printer incoming fax messages are automatically put out for this user according to routing rules.
PRIVFAX	<i>Private fax (*)</i> Number from <code>PRIVFAX#</code> normalized by the server using NCO. This number is displayed by clients as possible contact fax numbers. Direct entries via a client such as Web Assistant is not possible. On the format see Section 9.3.3, "The normalized NCO Phone Number Format" , on page 345.
PRIVFAX#	<i>Private fax</i> Displayed private fax number of the user. Besides <code>PRIVFAX#</code> the <code>PRIVFAX</code> field is also available. See the corresponding explanation with FAXG3# .

Table 4 User database fields

Field Name	Meaning
PRIVILEGES	<i>Privileges</i> The privileges fields are modified via a privilege editor. This field maps the column of permitted privileges. All active fields in this column are assigned to this user, if this field has not been set in the <code>DENY_PRIVILEGES</code> of the group or user. More information on single privileges is found in Section 4.5, "Privileges", on page 118. All privileges permanently assigned via group membership can be withdrawn from the user by setting the respective privilege to prohibited. More information on single privileges is found in Section 4.5, "Privileges", on page 118.
PRIVTEL	<i>Private number (*)</i> Number from <code>PRIVTEL#</code> normalized by the server using NCO. Can be offered as option if you want to call this user from a CTI client. Direct entries via a client such as Web Assistant is not possible. On the format see Section 9.3.3, "The normalized NCO Phone Number Format", on page 345.
PRIVTEL#	<i>Private number</i> Displayed private phone number of the user. Besides <code>PRIVTEL#</code> the <code>PRIVTEL</code> field is also available. See the corresponding explanation with <code>FAXG3#</code>.
QUOTA	<i>Quota</i> Harddisk capacity to be allocated for a maximum of one user. See Section 7.1.4, "User Quotas", on page 205.
QUOTAUSED	<i>Quota used</i> Harddisk capacity currently allocated for a user. See Section 7.1.4, "User Quotas", on page 205.
REMARK	<i>Remark</i> Freely usable field in which remarks or comments may be entered.
SAPSMTP	SAP address of an SAP user connected by SMTP APL. See <i>SAP R/3 Gateway manual</i> .
SEC_LANGUAGE_ID	<i>Language ID 2</i> Second set language. This language is used by Ergo if the welcome greeting is played in two languages in succession via the <code>-bga</code> parameter.
SMS	<i>SMS number (*)</i> Number from <code>SMS#</code> normalized by the server using NCO. This number is used by the XPR server for inbound routing. It can also be offered as option with a CTI client. Direct entries via a client such as Web Assistant is not possible. On the format see Section 9.3.3, "The normalized NCO Phone Number Format", on page 345.
SMS#	<i>SMS number</i> Displayed GSM mobile telephone of the user to which SMS messages may be sent. Besides <code>SMS#</code> the <code>SMS</code> field is also available. See the corresponding explanation with <code>FAXG3#</code>.
SMS-ACT-QUOTA	<i>SMS quota used up so far</i> Is used in a multi-tenant scenario. See the <i>Microsoft Exchange Gateway manual</i> on this. This field displays the SMS quota of this tenant used up so far.

Table 4 User database fields

Field Name	Meaning
SMS-QUOTA	SMS quota Is used in a multi-tenant scenario. See the description in the <i>Multi Tenancy</i> manual on this. Enter here the total number of short messages that the XPR server is to send for the users of this tenant at the most. This specification refers to the period of one calendar month. When the total number of sent short messages approaches this quota, the XPR system administrator and the XPR user defined under Contact person will be informed. Via the Alert threshold you can specify the number of messages from which this information occurs. When the SMS quota has been reached, the XPR server will not send any more short messages for this tenant. In this case, a sending party receives an error message with a corresponding information.
SMTP	E-mail User SMTP address (Internet e-mail standard). This entry must be present if the user is to receive messages through the Internet. A reference to this entry in the <code>PREFERRED</code> field routes all incoming messages to the e-mail address. Example: <code>ju@sample.com</code>
STAND-IN	Mailbox diversion A user to whom all incoming documents should be routed, e.g. in case of absence through illness or holiday. <code>Stand-in</code> must be entered in the <code>Preferred</code> field as soon as the delegation is to become active. Note: With this type of delegation the stand-in only receives original messages and no copies. Application examples: • If an employee leaves a company, it is possible to transfer messages originally addressed to him/her to his/her successor for editing. • Another frequent application is redirecting via an SMTP address after a change of location within a company.
STATE	State Additional information on <code>COUNTRY</code>. Particularly in the USA specification of the state as address information is desired.
TCPIP	TCP/IP address TCP/IP address of the user's computer. Either a name that can be resolved by the DNS server or a direct entry such as <code>222.222.222.106</code> can be given. This entry occurs automatically via Communications when the TCP/IP transport is used and active delivery is activated.
TIMEZONE	Time zone User time zone. This database field can also be default set for the users of a user group. The time zone support requires activating via the corresponding command line tool. See Section 32.13, "Time Zone Support", on page 1556.

Table 4 User database fields

Field Name	Meaning
TZ	Java time zone of the user. This database field can also be default set for the users of a user group. The Connection APL assigns a time zone for Java applications such as <i>OpenScape Web Client</i> from the list of time zones possible under Java from the set Windows time zone. This assignment is not unique, so that the summer time (Daylight Saving Time) may not be considered. As a result, the times are entered in the <i>OpenScape Web Client</i> incorrectly by one hour. In this case, you can enter an appropriate Java time zone in this field. For Northern Ireland this would be e.g. "Europe/Dublin". If you look for "Java Timezone ID" in the internet, you quickly find a list of possible entries for this field. If TZ is set, it is used instead of TIMEZONE in the Connection APL.
USE_LAST_REDIR	<i>Use last redirected number</i> Use of the first or last redirected number in case of cascaded forwardings. For this purpose, this field must be added for a user (mask <code>USER</code>) or for a user group (mask <code>GROUP</code>) as CHAR with at least two ##. See Section 4.4, "The Mask Description Language MDL", on page 112. In this way it is displayed in the Web Assistant as selection field with the options "On", "Off" and "Default". It allows to control which redirected number shall be used by Ergo. Without this field or in case of the "Default" setting the first redirected number is used. If "On" is set for the user group, Ergo will use the last redirected number. But this can be individually changed for each user again if required.
USER	<i>User name</i> Login name also used for addressing with XPR e-mail. This name must be unique and contain the characters A–Z and 0–9 only to avoid problems with addressing via gateways. Please note that although the maximum entry length is 63 characters, this allocation must never be fully used since the maximum length of an NVS address is also 63 characters and some non-addressable users would be generated in the event that e.g. the <code>NVS:MAILBOX/</code>, required to form the address, could not be prefixed owing to the lack of space then. A user ID must therefore comprise fewer than 26 characters. In countries where the characters "A-Z" are unknown, entries must be restricted to the characters "0-9". As user ID the telephone number may then be used, which is normally also the mailbox number.
VM_ANNOUNCE_01	<i>Greeting 1</i> See Section 4.3.3, "Announcement and Name Recording", on page 98.
VM_ANNOUNCE_02	<i>Greeting 2</i> See VM_ANNOUNCE_01.
VM_ANNOUNCE_03	<i>Greeting 3</i> See VM_ANNOUNCE_01.
VM_ANNOUNCE_04	<i>Greeting 4</i> See VM_ANNOUNCE_01.
VM_ANNOUNCE_05	<i>Greeting 5</i> See VM_ANNOUNCE_01.
VM_ANNOUNCE_06	<i>Greeting 6</i> See VM_ANNOUNCE_01.
VM_ANNOUNCE_07	<i>Greeting 7</i> See VM_ANNOUNCE_01.
VM_ANNOUNCE_08	<i>Greeting 8</i> See VM_ANNOUNCE_01.

Table 4 User database fields

Field Name	Meaning
VM_ANNOUNCE_09	<i>Greeting 9</i> See VM_ANNOUNCE_01 .
VM_AUTH_CODES	<i>Authorization codes</i> See Section 4.3.8, "Privileges" , on page 105.
VM_DN_00	<i>Deputy number 0</i> See Section 4.3.5, "Deputy Numbers" , on page 98.
VM_DN_01	<i>Deputy number 1</i> See VM_DN_00 .
VM_DN_02	<i>Deputy number 2</i> See VM_DN_00 .
VM_DN_03	<i>Deputy number 3</i> See VM_DN_00 .
VM_DN_04	<i>Deputy number 4</i> See VM_DN_00 .
VM_DN_05	<i>Deputy number 5</i> See VM_DN_00 .
VM_DN_06	<i>Deputy number 6</i> See VM_DN_00 .
VM_DN_07	<i>Deputy number 7</i> See VM_DN_00 .
VM_DN_08	<i>Deputy number 8</i> See VM_DN_00 .
VM_DN_09	<i>Deputy number 9</i> See VM_DN_00 .
VM_FAX_EXT	<i>Number of external fax</i> See Section 4.3.16, "Fax and Print Devices" , on page 111.
VM_FAX_INT	<i>Number of internal default fax</i> See Section 4.3.16, "Fax and Print Devices" , on page 111.
VM_HI_DSP_NAM	<i>Hicom display name</i> See Section 4.3.10, "Specific Hicom PBX Fields" , on page 108.
VM_HI_PIN	<i>Hicom PIN</i> See Section 4.3.10, "Specific Hicom PBX Fields" , on page 108.
VM_LAST_LOGIN	<i>Date of last login</i> See Section 4.3.11, "Login Information" , on page 108.
VM_LOCK_SET	<i>Voicemailbox lock</i> See Section 4.3.11, "Login Information" , on page 108.
VM_LOGIN_FAILED	<i>Number of failed logins</i> See Section 4.3.11, "Login Information" , on page 108.
VM_MSG_COUNT	See MAX_VOICE_MSG .
VM_NAME	<i>File name of name recording</i> See Section 4.3.3, "Announcement and Name Recording" , on page 98.

Table 4 User database fields

Field Name	Meaning
VM_OUT_ANN_T	<i>Out of office greeting expires on</i> You can use PhoneMail to record a greeting for out of office times. After its configuration it is valid until the date specified here and played instead of all other greetings.
VM_PIN_UPDATED	<i>Date of last PIN change</i> See Section 4.3.2, "Access Security" , on page 97.
VM_PRINTER	<i>Name of default printer</i> See Section 4.3.16, "Fax and Print Devices" , on page 111.
VM_PROTOCOL	<i>Voicemail system</i> See Section 4.3.1, "Announcement Directory" , on page 96.
VM_TIMEPROFILE	<i>Time profile</i> See Section 4.3.7, "Time Profiles" , on page 100.
VM_USER_OPTIONS	<i>User options for voice mail system</i> See Section 4.3.9, "User Options" , on page 106.
VOICE	<i>Voice mail (*)</i> Number from VOICE# normalized by the server using NCO. This number is used by the XPR server for inbound routing. Direct entries via a client such as Web Assistant is not possible. On the format see Section 9.3.3, "The normalized NCO Phone Number Format" , on page 345.
VOICE#	<i>Voicemail</i> Displayed user voice mail number. Since an internal fax tone recognition is implemented in the TUI, the same number can be used for Fax G3 and Voice. This number can also be used for Fax G4 since here a differentiation can be made by the ISDN Service Indicator. Several numbers can be assigned to a user, so that for all these numbers only one mailbox must be queried. This might be the case if e.g. several phones are available and these are forwarded to the voice mail system by redirecting number. In this case the fields VOICE and VOICE# must be additionally flagged with MULTI. You find more information on this flag in Table 5 on page 113 . Besides VOICE# the VOICE field is also available. See the corresponding explanation with FAXG3#.
VPIM	<i>VPIM</i> The originator address of a voicemail sent by VPIM is created from the originator's mailbox number and the host name configured for the individual location. The mailbox number is the number localized from VOICE respectively PHONE by NCO, if the former is empty. If the VPIM field of the user database is added, you can configure for the user a number for VPIM messages to replace the mailbox number in the originator address. See also Section 10.1.4, "Voice Mail Networking" , on page 539.
WARNING-LEVEL	<i>Alert threshold</i> Is managed in a Multi Tenant scenario. See the description in the <i>Multi Tenancy</i> manual on this. In this field you specify a percentage threshold value used in combination with the fields Fax quota and SMS quota . If the sent fax or sent short message/associated quota ratio reaches this percentage value, the XPR system administrator and the XPR user defined under Contact person will be informed.

Table 4 User database fields

Field Name	Meaning
WEB_STARTPAGE	<i>Start page after login</i> This field is used in the Web Assistant to determine the start page after login. The user can then immediately either edit settings or his/her mail. Depending on the privileges he/she can also toggle between the two areas via menu.
ZIP	<i>Zip code</i> Address information. Can optionally be copied for fax stationery.

Table 4 User database fields

4.2 Users vs. Contacts

The main difference between a user and a contact lies in the user's potential to log on to the system. Once a day, the MTA determines the number of users available in the system. Therefore, all Correlation database entries that have one of the following database fields are counted:

- PASSWORD
- PIN
- LMACCOUNT
- HICOMPIN
- LNIBXREPL

In this process, database entries that have the ISGROUP field and the associated user name of which is not ADMINISTRATOR, ACDSUSER, SYSTEM, COMPANY or POSTMASTER are ignored.

To perform the actual login, the user must have appropriate privileges in addition. In case of replicating contacts from 3rd-party systems verify that the above database fields are not used. They are otherwise counted as users and consequently require appropriate licenses.

4.3 Voice Mail Server Fields

All current voice mail servers support the common database layout given below. These are Ergo, Evo, PhoneMail, and VMS, for example.

4.3.1 Announcement Directory

All announcements recorded by a user or system announcements recorded by an administrator are filed in a subdirectory in the `\\<XPR Install>\MrsUserdata$` structure. Different voice mail systems can thus use a common or an individual directory each. Via the following entry in the correlation database the setting:

DOMAIN	CLASSNAME	CLASS	KEYNAME	KEY
<Server>/\$SYSTEM	VM_FOLDERS	USER_DATA_SUB_FOLDER	<Protocol Name>	<Folder>

<Protocol Name> corresponds to the name of the voice mail server used and <Folder> corresponds to the subdirectory related to `\\<XPR Install>\MrsUserdata$`.

Through use of the protocol name instead of the script name a script could even be installed several times with a different protocol name and individual directories for recording could be assigned each. The default folder for all voice mail systems can be allocated via the following entry:

DOMAIN	CLASSNAME	CLASS	KEYNAME	KEY
<Server>/\$SYSTEM	VM_FOLDERS	USER_DATA_SUB_FOLDER	#DEFAULT	<Folder>

If this entry is not present, voice mail servers without individual directory should use the `vmdata` default directory.

So that administrative software, such as the Web Assistant, files a user's recording in the correct directory, the user needs to be assigned to a specific voice mail system. Likewise, the voice-controlled Evo must be able to forward to a DTMF-controlled voice mail server if no speech recognition licenses are free any more. This is done via the following entry that offers the installed TUI protocols as list fields in the interface:

DOMAIN	CLASSNAME	CLASS	KEYNAME	KEY
<Server>	USER	<User ID>	VM_PROTOCOL	<Protocol Name>

If you have installed several protocols in parallel, there is a particularity in the Forward/Callback Access. The call is forwarded to the protocol set here even if another protocol has accepted the call.

Consequently you can configure Ergo, Evo, PhoneMail, and VMS for example and assign extensions to only one of these protocols for the Forward/Callback Access. Each user reroutes their phone to this number and depending on the voicemail system set here the call is forwarded to the other Telephone User

Interface if required. In case of Evo, the automatic forwarding must be activated for the respective user by the `R` option in the `VM_USER_OPTIONS` database field. For PhoneMail and VMS this feature is automatically active.

4.3.2 Access Security

The PIN database field serves as default. Further options can be released here as well. They require for example regular PIN modification or save several PINs already used so that these cannot be immediately used again.

To activate checking older PINs already used, the following database entry must be present:

DOMAIN	CLASSNAME	CLASS	KEYNAME	KEY
<Server>/\$SYSTEM	VM_PIN_UPDATE	<Protocol Name>	VM_STORE_PINS	<Number of PINs>

<Number of PINs> corresponds to the number of PINs previously used and to be saved. If this value is 0, the function is inactive. This corresponds simultaneously to the default of this value.

If a value <Number of PINs> were greater than 0, database entries `VM_PIN_01` to `VM_PIN_<Number of PINs>` would be generated for each user for encoded saving of PINs previously used. If a newly entered PIN were identical with one of the PINs used, it would not be accepted.

The date of the last modification to a user's PIN database entry is set down in the following value:

DOMAIN	CLASSNAME	CLASS	KEYNAME	KEY
<Server>	USER	<User ID>	VM_PIN_UPDATED	<Date>

<Date> corresponds to date and time in the format `YYYY-MM-DD-HH-MM`.

So that this entry is evaluated and a PIN expires after a certain number of days, the following database entry must be present:

DOMAIN	CLASSNAME	CLASS	KEYNAME	KEY
<Server>/\$SYSTEM	VM_PIN_EXPIRE	<Protocol Name>	VM_EXPIRE_DAYS	<Number of Days>

<Number of Days> corresponds to the number of days after which a PIN becomes invalid. With a value greater than 0 a PIN is considered invalid when the current date has exceeded the date entered for `VM_PIN_UPDATED` by <Number of Days>. If `VM_EXPIRE_DAYS` is 0 or not entered in the database, a PIN never expires.

Note that older clients do not know this mechanism, thus the PIN could be modified without updating the list of previous PINs and without updating the modification date.

4.3.3 Announcement and Name Recording

In the following database entries the greetings recorded by users are stored in the file specified in the `KEY` database field:

DOMAIN	CLASSNAME	CLASS	KEYNAME	KEY
<Server>	USER	<User ID>	VM_ANNOUNCE_<XX>	<User ID>_ANN_<XX>_<Y>.pcm

No statement about the use of the respective `VM_ANNOUNCE_<XX>` (example: `VM_ANNOUNCE_01`) is given since the context (example: info, greeting) is exclusively defaulted by the respective voice mail system.

The `<Y>` in the file name is required for re-recording an old announcement and replacing a current one while it is still played to callers of the voice mail system. The procedure within a voice mail system should be the following:

1. Current recording be `MARKUS_ANN_01_7.pcm`.
2. Determine the current value for `<Y>`, here thus 7, from the database.
3. Record new announcements in a temporal file and simultaneously enhance `<Y>` by 1.
4. Rename the temporal recording in `MARKUS_ANN_01_8.pcm` and file the corresponding store directory underneath of `\\userdata`.
5. Try to delete all older announcement versions probably available with the file names `MARKUS_ANN_01_<n>.pcm` except for `MARKUS_ANN_01_8.pcm`.

With name recordings proceed in the same way with the exception that the file name for the recording is stored in the following database field:

DOMAIN	CLASSNAME	CLASS	KEYNAME	KEY
<Server>	USER	<User ID>	VM_NAME	<User ID>_NAME_<Y>.pcm

4.3.4 System Recordings

If a set of recordings/announcements is to be commonly used for all users, a virtual user with ID `SYSTEM` is used. If this user account does not exist it is automatically generated by the voice mail system.

4.3.5 Deputy Numbers

A deputy number is a telephone number that can be specified by the voice mail system user. This number may serve as individual operator, thus can be for example a deputy within the same department. An announcement of the type "I'm

currently not in the office, press ** to talk to my deputy.” would inform and enable the caller to connect to the deputy. Depending on e.g. time profiles, various deputy numbers could be set for different periods.

DOMAIN	CLASSNAME	CLASS	KEYNAME	KEY
<Server>	USER	<User ID>	VM_DN_<XX>	<Number>

4.3.6 Notification Numbers

A notification number can be configured by the voice mail user, so that he/she is called by the voice mail system when a new message has arrived. The voice mail system must have a corresponding feature (“User Outcall”) for this purpose.

DOMAIN	CLASSNAME	CLASS	KEYNAME	KEY
<Server>	USER	<User ID>	VM_NN_<XX>	<Number>

Do not confuse this feature with [Section 7.9, “Message Waiting Indication \(MWI\)”](#), on page 287.

4.3.7 Time Profiles

Time profiles can be defined user-based so that for each user different settings can be performed. Several time profiles can be defined per user. The name of the currently active time profile is filed in the `VM_TIMEPROFILE` database field.

DOMAIN	CLASSNAME	CLASS	KEYNAME	KEY
<Server>	USER	<User ID>	VM_TIMEPROFILE	<Profile Name>

The <Profile Name> is freely selectable with the exception that it must not begin with the # character. Names beginning with this character are reserved for day profiles (see below).

Time profile structure

Time profiles define for each entity a status from date and time. For example, a company could have a time profile in which from Monday to Friday the working hours stretch from 9:00 a.m. to 5:00 p.m. each. At all other times the company is closed. Thus Tuesdays at 10:00 a.m. the status would be `WORKING`, and during the whole Sunday for example `NONWORKING`.

The XPR server differentiates two types of time profiles, **Day Profiles** for single days and **Calendar Profiles** that reference exactly one day profile for each day.

Day Profiles for voice mail systems are filed in the correlation database in the following manner:

DOMAIN	CLASSNAME	CLASS	KEYNAME	KEY
<Server>/<VM>/<User ID>	VM_TIMEPROFILE	#<Day Profile>	<From>-<To>	<State>
<Server>/<VM>/<User ID>	VM_TIMEPROFILE	#<Day Profile>	OTHERWISE	<State>

<Day Profile> is the name of the time profile that must begin with the # character.

<From>-<To> are start and end time in the format `hhmm` each.

<State> is a string which states the valid voice mail system behavior for this time interval. The behavior contains among other things: active announcement for internal and external callers as well as whether recording is possible at the time being or whether only an informal announcement is played.

The following <State> definitions are presently possible, each with <Token>=<Definition>. Several settings are separated by the | character:

Token	Definition/Description
AA	<Alternative Announcement>IUS Number for an alternative announcement with the additional, optional flags infobox (I), non-interruptable announcement (U) or system announcement (S). The number corresponds to the <XX> as occurs with announcement entries, see Section 4.3.3, "Announcement and Name Recording", on page 98.

Token	Definition/Description
BA	<Busy Announcement> ^{IUS} Announcement number when the telephone was busy, with the additional, optional flags infobox (I), non-interruptable announcement (U) or system announcement (S).
IA	<Intern Announcement> ^{IUS} Announcement number for internal callers with the additional, optional flags infobox (I), non-interruptable announcement (U) or system announcement (S).
EA	<Extern Announcement> ^{IUS} Announcement number for external callers with the additional, optional flags infobox (I), non-interruptable announcement (U) or system announcement (S).
	If flag S were set, the corresponding announcement of the user account SYSTEM would be taken, otherwise the user's individual one. If flag I is not set, a voice mail can be recorded after an announcement. If flag U is not set, announcement playback can be interrupted by a caller. This is only considered useful when flag I is not set either. Priority: The announcement types are implicit in the sequence of their priority. AA before BA before IA/EA. This means that if AA is defined, this announcement is always used, independent from the type of caller or whether he/she has received a busy tone. Otherwise BA, IA or EA is used depending on the situation.
NN	<Notification number> Index number of the database field which is to be used for a call when new messages come in (User Outcall). See Section 4.3.6, "Notification Numbers", on page 99 .
DN	<Number of Deputy> Index number of the database field which is used for forwarding to a deputy or individual operator. See Section 4.3.5, "Deputy Numbers", on page 98 .

Time profiles can overlap each other with the later one being preferred. Intervals must never transgress midnight or completely contain another interval. Thus the intervals 0000–0900 and 0900–2359 would be legal with the minute from 9:00 to 9:01 belonging to the second interval, The intervals 0000–2359 and 0900–1000 are however not allowed. Using 2400 for the end of a day is legal but not recommended.

If the current time is not contained in one of the defined day profiles, the *<State>* given in the OTHERWISE entry applies. If this entry does not exist, an empty *<State>* definition applies for all times outside the defined intervals.

Calendar Profiles are filed in the correlation database in the following manner:

DOMAIN	CLASSNAME	CLASS	KEYNAME	KEY
<Server>/<VM>/<User ID>	VM_TIMEPROFILE	<Profile Name>	<Day>	<Day Profile>

<Profile Name> is the time profile name, *<Day>* is the definition of the day(s) for which this entry applies and *<Day Profile>* is the name of the day profile that is to be used for these days.

<Day>, sorted according to the precedence sequence, can be

- a single date, such as 20010225 for 25 February 2001.

- one day of the year, such as 0225 for 25 February of every year.
- the same day in each month, such as D25 for the 25th of each month.
- one day of a week, abbreviated by the first two letters, thus for example SU for Sunday.
- OTHERWISE for all days not defined by another entry.

Thus the database entries might appear as follows:

DOMAIN	CLASSNAME	CLASS	KEYNAME	KEY
COMPANY/\$VM/JOE	VM_TIMEPROFILE	#NWDAY	0000-2359	IA=0I EA=11I
COMPANY/\$VM/JOE	VM_TIMEPROFILE	#WDAY	0000-0900	IA=0IU EA=0I
COMPANY/\$VM/JOE	VM_TIMEPROFILE	#WDAY	0901-1230	IA=1 EA=0 NT=B DN=1
COMPANY/\$VM/JOE	VM_TIMEPROFILE	#WDAY	1231-1300	IA=1I EA=2I
COMPANY/\$VM/JOE	VM_TIMEPROFILE	#WDAY	1301-1700	IA=0 EA=11 NT=B DN=1
COMPANY/\$VM/JOE	VM_TIMEPROFILE	#WDAY	1701-2359	IA=0I EA=11I
COMPANY/\$VM/JOE	VM_TIMEPROFILE	JOES PROFILE	SA	NWDAY
COMPANY/\$VM/JOE	VM_TIMEPROFILE	JOES PROFILE	SU	NWDAY
COMPANY/\$VM/JOE	VM_TIMEPROFILE	JOES PROFILE	OTHERWISE	WDAY

The name of the time profile to be used is in this example JOES PROFILE.

4.3.7.1 Simplified Time Profiles

The simplified time profiles are only used by PhoneMail for a simplified greeting mode. Only five recordings are possible here. One each for the following greeting types: alternate, busy, internal, external and after-hours. The simplified time profiles allow only one entry for the business hours, thus for example Mondays to Fridays, 08:00 – 17:00. It is not possible to specify different business hours for each day.

For the simplified greeting mode, eight additional database fields are available:

1. Definition of working days:

DOMAIN	CLASSNAME	CLASS	KEYNAME	KEY
<Server>	USER	<User ID>	VM_TPS_B_DAY	mo=1 tu=1 we=1 th=1 fr=1 sa=0 su=0

1 means working day, 0 means no working day. The days are abbreviated as only the first two letters appear.

2. Definition of business hours:

DOMAIN	CLASSNAME	CLASS	KEYNAME	KEY
<Server>	USER	<User ID>	VM_TPS_B_HOURS	0800-1700

The business hours are specified in the key.

3. The field stating which greetings are stored:

DOMAIN	CLASSNAME	CLASS	KEYNAME	KEY
<Server>	USER	<User ID>	VM_SIMPLE_ANN	saa=0 sia=0 sea=0 sba=0 sah=0

The tokens represent the following greeting types:

saa=<Simple alternate announcement>
sia=<Simple internal announcement>
sea=<Simple external announcement>
sba=<Simple busy announcement>
sah=<Simple after-hours announcement>

The possible values are:

0 – No greeting assigned
P – Private greeting recorded
S – Use system greeting

4. The files associated to the greetings are referenced in the following fields:

DOMAIN	CLASSNAME	CLASS	KEYNAME	KEY
<Server>	USER	<User ID>	VM_S_ANN_ALT	<User ID>_SAA_<Y>.pcm
<Server>	USER	<User ID>	VM_S_ANN_INT	<User ID>_SIA_<Y>.pcm
<Server>	USER	<User ID>	VM_S_ANN_EXT	<User ID>_SEA_<Y>.pcm
<Server>	USER	<User ID>	VM_S_ANN_BUSY	<User ID>_SBA_<Y>.pcm
<Server>	USER	<User ID>	VM_S_ANN_AAH	<User ID>_SAH_<Y>.pcm

<Y> is a consecutive number, which allows exchanging greetings in live operation. See also [Section 4.3.3, “Announcement and Name Recording”](#), on page 98.

4.3.8 Privileges

For some voice mail systems specific privileges were required that could not be handled via the XPR default privileges. These are represented in a *<String>* via capital letters.

DOMAIN	CLASSNAME	CLASS	KEYNAME	KEY
<i><Server></i>	USER	<i><User ID></i>	VM_AUTH_CODES	<i><String></i>

Common users should not be permitted to modify this value but only those with supervisor privilege or with a privilege code to be correspondingly defined. At present this feature is used by the conversion recorder (letter R).

4.3.9 User Options

For some voice mail systems specific options can be set on user level. These are represented in a *<String>* via capital letters.

DOMAIN	CLASSNAME	CLASS	KEYNAME	KEY
<i><Server></i>	USER	<i><User ID></i>	VM_USER_OPTIONS	<i><String></i>

The following letters are presently allocated and used by the voice mail system specified:

Letter	Description	Voicemail system
A	Activate short greetings	PhoneMail
B	Deactivate automatic fax tone recognition	PhoneMail VMS
C	Activate extended system mode	Ergo
D	Activate personal-mailbox sorting	Ergo
E	Activate personal-mailbox filtering	Ergo
F	Enable confidential flag for other users	Ergo
H	Activate automatic new message playback	Ergo
I	Do not flag message as read before it ends	Ergo
J	Do not query before deleting messages	Ergo
K	Do not play message subject	VMS
L	Activate automatic speech recognition	(None)
M	Activate mobility number support	PhoneMail
N	Activate message wizard for mailbox	Ergo
O	Play extra hint at message end	Ergo
P	No option to connect to switchboard in forward access	VMS
Q	Activate referral extension	VMS
R	Activate possible protocol change in the Forward Access. Please note that this option need not be explicitly activated for PhoneMail and VMS. Consequently, the option cannot be deactivated there either.	Ergo Evo
S	Uses TTY/TDD devices (hearing impaired). If this user employs the PhoneMail TUI with American prompts, he/she will hear the special TDD prompts. These TDD prompts generate a text output on the American TDD terminals.	PhoneMail
T	Activate extended greeting menu	PhoneMail
T	Activate simplified greeting configuration. The user can create a simplified time profile in the Web Assistant.	Ergo
U	Activate simplified Web access	Web Assistant

Letter	Description	Voicemail system
@	Forbid other users to flag as urgent	Ergo Evo PhoneMail VMS Web Assistant

4.3.10 Specific Hicom PBX Fields

The fields described here are only considered useful in an environment with Hicom PBXs:

DOMAIN	CLASSNAME	CLASS	KEYNAME	KEY
<Server>	USER	<User ID>	VM_HI_PIN	<Hicom PIN>
<Server>	USER	<User ID>	VM_HI_DSP_NAM	<Display Name>

The <Hicom PIN> is a string stored in uncoded format and used e.g. by the VMS voice mail system.

The <Display Name> is used alternatively to the NAME field for filing and representing a name on the Hicom telephones' display that is contracted according to the short display.

4.3.11 Login Information

These entries in the user database can be used to check whether a mailbox is still active. Inactive mailboxes could then be deleted after a certain period.

DOMAIN	CLASSNAME	CLASS	KEYNAME	KEY
<Server>	USER	<User ID>	VM_LAST_LOGIN	<Date>
<Server>	USER	<User ID>	VM_LOGIN_FAILED	<Count>
<Server>	USER	<User ID>	VM_LOCK_SET	<Locked?>

For this purpose, the date of the last login at the voice mail server is stored in <Date>, so that a script or the maintenance task can evaluate it. The maintenance task could perform an automatic deletion with this information. The format is YYYY-MM-DD-HH-MM.

In <Count> the number of failed attempts during the last login are recorded. This field can be used to block access to the voice mail server after reaching a fixed maximum number of attempts. A voice mail server should issue a corresponding error message or warning when a user reaches the maximum number.

As soon as in VM_LOGIN_FAILED the maximum number of logon attempts via a TUI has been reached, access to the TUI is locked via VM_LOCK_SET. When the administrator assigns a new PIN via the Web Assistant, this field is automatically deleted. This unlocks the mailbox again. You can also delete the content of this field. But this is only useful if the user has not caused the failed attempts himself/herself.

4.3.12 Filter Rules

Via these rules that each user can configure for themselves, messages offered per TUI via the voice mail system can be restricted. Since the XPR database allows a maximum number of 63 characters in KEY, the rule from VM_FILTER_01 is continued in VM_FILTER_02, etc. The final rule results from the complex rule consisting of all VM_FILTER_<XX> user commands:

DOMAIN	CLASSNAME	CLASS	KEYNAME	KEY
<Server>	USER	<User ID>	VM_FILTER_<XX>	<Filter Rule>

The single rules are logically linked by || (Or) respectively && (And) whereby the And-link is evaluated before the Or-link. The following filter rules are currently defined:

Rule	Operations	Possible Values
SERVICE	==, !=	NATIVE, SMTP, SMS, VOICE, FAXG3, FAXG4
IMPORTANCE	<, <=, ==, !=, >=, >	LOW, NORMAL, HIGH
FORMAT	==, !=	Bitmask
READ	==, !=	0 or 1 (read)
FLAGGED	==, !=	0 or 1 (flagged)
RECEIVE_DATE	<, <=, ==, !=, >=, >	<Date/time> (format: YYYYMMDDHHMMSS)
SEND_DATE	<, <=, ==, !=, >=, >	<Date/time> (format: YYYYMMDDHHMMSS)
FROM_ADDR	==	<NVS address>
REPLY_ADDR	==	<NVS address>
TO_ADDR	==	<NVS address>

Example

```
VM_FILTER_01="SERVICE!=VOICE&&SERVICE!=FAXG3&&READ==0 || SERVICE==VOICE"
```

All voice messages and new (unread) e-mails are offered to this user via the TUI.

4.3.13 Message Folder

If users use folders and only specific folders with messages are to be offered via the TUI, these folders can be defined here:

DOMAIN	CLASSNAME	CLASS	KEYNAME	KEY
<Server>	USER	<User ID>	VM_FOLDER_COUNT	<Number of Folders>
<Server>	USER	<User ID>	VM_FOLDER_<XX>	<Folder Name>

In *<Number of Folders>* the number of folders supported by the TUI is stored. In *VM_FOLDER_01* etc. the name of each folder is stored. If no message folders have been configured, only the *INBOX* folder is offered in each case. If other folders are to be offered as well, do not forget to configure the *INBOX* folder, too.

Example

```
VM_FOLDER_01=INBOX
VM_FOLDER_02=MyXpressions
VM_FOLDER_COUNT=2
```

The folders *INBOX* and *MyXpressions* are offered by TUI.

4.3.14 Sequence of Offered Messages

A user can set the sequence in which messages are offered per TUI via the rule specified here. The corresponding Web Assistant function must be used.

DOMAIN	CLASSNAME	CLASS	KEYNAME	KEY
<Server>	USER	<User ID>	VM_SORT_ORDER	<Sort Order Rule>

- On Phonemail you can set the messaging sort order only via TUI or Webassistant.
- On ERGO there are more settings and they can also be managed via TUI or Webassistant.
- On VMS it is not possible to configure those settings.

See also the following sections on the *OpenScape Xpressions V7 Web Assistant, User Guide*:

- 3.3.2.1 *Phonemail and VMS - Set message sort order*
- 3.3.2.2 *ERGO - Set message sort order*

4.3.15 Trusted Phone Devices

If the voice mail server is called in control mode via one of the numbers set here (not more than 3), the PIN is not queried. The user may configure those numbers by himself/herself. Each configured number must be unique and thus a check must be performed as to whether it is already present before a trusted number is entered in the database.

DOMAIN	CLASSNAME	CLASS	KEYNAME	KEY
<Server>	USER	<User ID>	VM_TN_01	<Phone Number>
<Server>	USER	<User ID>	VM_TN_02	<Phone Number>
<Server>	USER	<User ID>	VM_TN_03	<Phone Number>

<Phone Number> is a normalized telephone number. This feature is supported by Ergo, Evo, and PhoneMail.

4.3.16 Fax and Print Devices

If a voice mail system supports e-mails and fax messages, an output device for such messages is required as well. Therefore the following database fields are intended for an internal fax device, an external fax device and a printer:

DOMAIN	CLASSNAME	CLASS	KEYNAME	KEY
<Server>	USER	<User ID>	VM_FAX_INT	<NVS address>
<Server>	USER	<User ID>	VM_FAX_EXT	<NVS address>
<Server>	USER	<User ID>	VM_PRINTER	<NVS address>

Example

```
VM_FAX_INT = NVS:FAXG3/+49123498765
VM_FAX_EXT = NVS:FAXG3/+49432156789
VM_PRINTER = NVS:PRINTER/QMS
```


4.4 The Mask Description Language MDL

Via the Mask Description Language MDL you can define the layout of the entry masks for user or contact data in the Web Assistant. Communications reads the fields to be displayed out of these masks but does not copy the representation described here as well. You can specify attributes for each field for defining the content more precisely. When they are displayed, some of the internal field names are overwritten by readable descriptions in the language set. If this is the case, the corresponding assignment of field names to descriptions is noted in the documentation of the respective program.

All data are always stored in the correlation database. The masks defined here are thus always only a different representation of these data. For example from the other user's point of view, a user is always a contact, too.

XPR uses the following masks:

- **USER**
Displaying and editing user data.
- **SHORT**
Displaying and editing contact data.
- **PROFILE**
Display of the Communications settings to be modified or seen by the user him/herself. See the menu option **Tools > My Database Settings...** there.
- **WEBADMIN**
Display of the Web Assistant settings to be modified or seen by the user him/herself.
- **GROUP**
Displaying and editing user groups in the Web Assistant. The fields considered useful for user groups are already part of the mask definition. Other individually added fields may lead to client malfunctions. Therefore this mask should not be modified.
- **SOFT**
Internal mask. Must not be modified.

A mask description in the correlation database consists of two parts:

- `$mask`, which defines the mask layout and
- `$attrib`, which defines the field attributes.

In the first part (`$mask`) the mask layout is "painted". No tabulator characters may be used. The only rule is: a field name must always be followed by a wildcard of `#` characters for data entry or display in the same line. If required, the **USER** field is always displayed as the first field and must never be directly defined in the mask.

In the second portion (\$attrib) an attribute is declared for each field. The possible attributes are itemized in the following table.

Attribute	Meaning
CHAR	All characters are allowed (default). A field with a length of 1 and this attribute is a check box. No characters are entered in this field, but it can be checked, whereby an x is inserted. If this field is nonexistent or empty in a user's database, it will be displayed as unchecked.
CIPH	This field is encrypted. The encryption can be reversed and is used e.g. for POP3 passwords. These fields are unreadable in the database but when required, can be transferred to the POP3 server in a non-encrypted form.
CRYPT_SEC	The entry is made as hash value with additional time stamp. SHA-256 is used as algorithm for the hash value generation.
DNO	This field contains a dialing number normalized by NCO. See Section 9.3.3, "The normalized NCO Phone Number Format", on page 345 . This number is only displayed in the client (e.g. Web Assistant, Communications) and cannot be modified. For an alteration the associated field with the DNOREAD attribute must be modified. Convention: the field with DNOREAD attribute has the same name as the field with DNO attribute with a suffixed #.
DNOREAD	Within the clients a dialing number is entered in the fields with this attribute and then specified in the associated field with the DNO attribute normalized by means of NCO. The number transmitted to the field with DNO attribute is only displayed to the administrator in the client (e.g. Web Assistant, Communications), though. Display of the field with DNOREAD attribute in a client such as the <i>Web Assistant</i> may deviate from your own entry, since the format localized by NCO from the field with DNO attribute is displayed instead of the database content. In the database the original entry and thus also a faulty normalization or localization by NCO can be tracked via DB tool or an export.
HIDE	Additional to PUSER, PSERV or PSUPER. Only users with the same or higher privilege may see this field.
KRYPT	The contents in this field are encrypted.
LOWER	Lowercase characters only.
MULTI	Several contents may be available for this field to be entered via the Web Assistant or Communications. Application examples: – Several user SMTP addresses. – One mailbox for several calling numbers. Note that with calling number fields the entry is made in the field with the DNOREAD attribute each. The number is stored in the associated field with the DNO attribute in normalized format, though. Both fields should thus receive the MULTI attribute. With outgoing messages the primary field is entered as originator. Please also note that by deleting the primary field all associated fields are deleted as well. If you do not want this, move the contents of one of the secondary fields into the primary field.

Table 5 User database field attributes

Attribute	Meaning
PSERV	Only a user with <i>Service, Help Desk, Tenant Supervisor</i> or <i>Supervisor Privilege</i> may modify the field.
PSUPER	Only a user with <i>Supervisor Privilege</i> may modify the field.
PUSER	Only a user with <i>USER, Service</i> or <i>Supervisor Privilege</i> may modify the field.
UNIQUE	The contents of this field must be declared in the database. No two data records exist with the same entry for this field.
UPPER	Only uppercase characters.

Table 5 *User database field attributes*

Example

```
$mask USER
NAME #####
PASSWORD ##### PIN #####
PRIVILEGES ##### GROUP #####

PREFERRED #####
MAILBOX #####
STAND-IN #####
CIT #####

FAXG3# ##### FAXG3-ID #####
VOICE# ##### FAXG3-HEADLINE #####
FAXG4# ##### FAXG4-ID #####

SMS# ##### COSTINFO #####

SMTP #####
EXCH #####
LN #####

ZIP ##### CITY #####
COUNTRY #####
STATE #####
COMPANY #####
DIVISION #####
ADDR1 #####
ADDR2 #####
REMARK #####
PRIVTEL# ##### PRIVFAX# #####
GSM# ##### KEYWORD #####

TCPIP #####
PRINTER #####

PHONE# #####

PMI-SCHEDULE #####
PMI-HOSTNAME #####
PMI-USERNAME #####
PMI-PASSWORD #####

FAXG3 #####
FAXG4 #####
PHONE #####
VOICE #####
SMS #####
GSM #####
PRIVTEL #####
```

```

PRIVFAX #####
CITFILE #####
LANGUAGE_ID #####
QUOTA #####
QUOTAUSED #####
LMACCOUNT #####
PAGER_01 #####
PAGER_02 #####
PAGER_03 #####
PAGER_04 #####
PAGERSET_01 ###
PAGERSET_02 ###
PAGERSET_03 ###
PAGERSET_04 ###
VM_PROTOCOL #####
VM_AUTH_CODES #####
VM_FAX_EXT #####
VM_FAX_INT #####
VM_HI_DSP_NAM #####
VM_HI_PIN #####
VM_LAST_LOGIN #####
VM_LOGIN_FAILED #####
VM_PIN_UPDATED #####
VM_PRINTER #####
VM_TIMEPROFILE #####
VM_USER_OPTIONS #####
VM_NAME #####
VM_ANNOUNCE_01 #####
VM_ANNOUNCE_02 #####
VM_ANNOUNCE_03 #####
VM_ANNOUNCE_04 #####
VM_ANNOUNCE_05 #####
VM_ANNOUNCE_06 #####
VM_ANNOUNCE_07 #####
VM_ANNOUNCE_08 #####
VM_ANNOUNCE_09 #####
VM_DN_00 #####
VM_DN_01 #####
VM_DN_02 #####
VM_DN_03 #####
VM_DN_04 #####
VM_DN_05 #####
VM_DN_06 #####
VM_DN_07 #####
VM_DN_08 #####
VM_DN_09 #####
E_LOGIN_WEB #####
CTIJOURNAL #

$attrib
ADDR1 CHAR
ADDR2 CHAR
CIT CHAR
CITFILE CHAR,PSUPER
CITY CHAR
COMPANY CHAR
COSTINFO CHAR
COUNTRY CHAR
CTIJOURNAL CHAR
DIVISION CHAR
EXCH CHAR,UNIQUE,UPPER
E_LOGIN_WEB PSUPER,HIDE,CHAR

```

```

FAXG3 DNO, PSUPER, HIDE, CHAR, UNIQUE
FAXG3# DNOREAD, CHAR, UNIQUE
FAXG3-HEADLINE CHAR
FAXG3-ID CHAR
FAXG4 DNO, PSUPER, HIDE, CHAR, UNIQUE
FAXG4# DNOREAD, CHAR, UNIQUE
FAXG4-ID CHAR
GROUP CHAR, UPPER, PSUPER
GSM DNO, PSUPER, HIDE, CHAR, UNIQUE
GSM# DNOREAD, CHAR
KEYWORD CHAR
LANGUAGE_ID CHAR
LMACCOUNT UNIQUE, CHAR, PSUPER, UPPER
LN CHAR, UNIQUE, UPPER
MAILBOX CHAR, UPPER, UNIQUE
NAME CHAR
PAGERSET_01 PSUPER, CHAR
PAGERSET_02 PSUPER, CHAR
PAGERSET_03 PSUPER, CHAR
PAGERSET_04 PSUPER, CHAR
PAGER_01 PSUPER, CHAR
PAGER_02 PSUPER, CHAR
PAGER_03 PSUPER, CHAR
PAGER_04 PSUPER, CHAR
PASSWORD CHAR, UPPER, KRYPE, UPPER, PSUPER, HIDE
PHONE DNO, PSUPER, HIDE, CHAR, UNIQUE
PHONE# DNOREAD, CHAR
PIN CHAR, UPPER, KRYPT, PSUPER, HIDE
PMI-HOSTNAME LOWER, CHAR
PMI-PASSWORD CIPH, CHAR
PMI-SCHEDULE CHAR
PMI-USERNAME CHAR
PREFERRED CHAR, UPPER
PRINTER CHAR
PRIVFAX DNO, PSUPER, HIDE, CHAR, UNIQUE
PRIVFAX# DNOREAD, CHAR
PRIVILEGES CHAR, UPPER, PSUPER, HIDE
PRIVTEL DNO, PSUPER, HIDE, CHAR, UNIQUE
PRIVTEL# DNOREAD, CHAR
QUOTA PSUPER, CHAR
QUOTAUSED PSUPER, CHAR
REMARK CHAR
SMS DNO, PSUPER, HIDE, CHAR, UNIQUE
SMS# DNOREAD, CHAR
SMTP CHAR, LOWER, UNIQUE
STAND-IN CHAR, UPPER
STATE CHAR
TCPIP CHAR, UNIQUE
VM_ANNOUNCE_01 CHAR
VM_ANNOUNCE_02 CHAR
VM_ANNOUNCE_03 CHAR
VM_ANNOUNCE_04 CHAR
VM_ANNOUNCE_05 CHAR
VM_ANNOUNCE_06 CHAR
VM_ANNOUNCE_07 CHAR
VM_ANNOUNCE_08 CHAR
VM_ANNOUNCE_09 CHAR
VM_AUTH_CODES UPPER, CHAR
VM_DN_00 CHAR
VM_DN_01 CHAR
VM_DN_02 CHAR
VM_DN_03 CHAR

```

```

VM_DN_04  CHAR
VM_DN_05  CHAR
VM_DN_06  CHAR
VM_DN_07  CHAR
VM_DN_08  CHAR
VM_DN_09  CHAR
VM_FAX_EXT CHAR
VM_FAX_INT CHAR
VM_HI_DSP_NAM CHAR, UNIQUE
VM_HI_PIN CHAR, UNIQUE, PSUPER, HIDE
VM_LAST_LOGIN CHAR
VM_LOGIN_FAILED PSUPER, CHAR
VM_NAME CHAR
VM_PIN_UPDATED CHAR
VM_PRINTER CHAR
VM_PROTOCOL CHAR
VM_TIMEPROFILE CHAR
VM_USER_OPTIONS UPPER, CHAR
VOICE DNO, PSUPER, HIDE, CHAR, UNIQUE
VOICE# CHAR, DNOREAD, UNIQUE
ZIP CHAR
$end

```

4.4.1 Editing Masks

First we export the user database mask via the

```
Infotool Maskexport File=user.mdl
```

command to the `user.mdl` file. The Infotool program is part of the SDK utilities and found in the `<XPR Install>\SDKUtils` folder after the installation. With a text editor such as Notepad we supplement the desired mask with the fields to be complemented and “paint” the layout.

Next we will furnish these fields with the desired attributes in the associated attributes portion.

With the `Infotool Maskimport File=user.mdl` command we reimport the extended mask definition to the correlation database.

NOTE:

You can also edit the masks with the *Web Assistant*.

4.5 Privileges

A user's authority depends on the assigned privileges. A user bequeaths the privileges already assigned to the user groups. His/her actual privileges thus conform with the user group he/she belongs to as well as with individual privileges additionally assigned by the administrator. In this connection keep in mind that when assigning a privilege via Communications or the Web Assistant to a user or user group, this assignment can be **allowed** and also be **refused**. The **Effective** column indicates whether a privilege is valid for the displayed user or group. An entry under **Deny** always leads to a user group or user not having this privilege. You can thus withdraw a privilege from a user that he/she inherited from a group by denying it.

IMPORTANT:

The *supervisor privilege* always includes all privileges. Therefore, **refusing** does not affect other privileges if the user has this privilege!

A privilege is required for almost every transaction. You find the available default privileges and their significance in the following table. Individual privileges can also be defined if additional restrictions are required. The necessary steps for defining privileges will be discussed at the end of this section. Privileges always appear in English. The internal privilege name is specified in brackets. The name is required, for example, with creating a rule file for user administration via the HiPath 4000 Manager. Furthermore, the privileges are displayed in alphabetic order based on this internal name.

NOTE:

In [Table 6](#) the currently valid privileges are described. After an update privileges of previous versions may still be available but the XPR server does not use these any more and they are thus not listed here.

To edit privileges use a client application such as the Web Assistant, which offers the English privilege name for selection.

Privilege	Meaning	Use	User group			
			GUEST_GROUP	USER	ADVANCED	SERVICE
Receive Dictates Privilege (DICTATE_RECEIVE)	The user may receive dictations in VMS.	VMS			x	
e-Mail dialog (DLG_EMAIL)	Obsolete.	None			x	x
Telex dialog (DLG_TLX)	Obsolete.	None			x	x

Table 6 Privileges

Privilege	Meaning	Use	User group			
			GUEST_GROUP	USER	ADVANCED	SERVICE
Voice dialog (DLG_VOICE)	Obsolete.	None	x		x	x
Internal Fax Privilege (FAX_INTRNL)	Internal fax forwarding is allowed in the TUI.	PhoneMail, VMS		x	x	x
International Fax Privilege (FAX_INTRNT)	World-wide fax forwarding is allowed in the TUI.	PhoneMail, VMS			x	x
Local Fax Privilege (FAX_LOCAL)	Local fax forwarding is allowed in the TUI.	PhoneMail, VMS		x	x	x
National Fax Privilege (FAX_NATL)	Fax forwarding within a country is allowed in the TUI.	PhoneMail, VMS		x	x	x
Hide Voice Conference (HIDE_VOICECONF)	When this privilege is set, the user cannot schedule any voice conferences via Lotus Notes or Microsoft Outlook any more.	Notes Conferencing Plugin, Outlook Conferencing Plugin				
Hide Web Conference (HIDE_WEBCONF)	When this privilege is set, the user cannot schedule any web conferences via Lotus Notes or Microsoft Outlook any more.	Notes Conferencing Plugin, Outlook Conferencing Plugin				
Answering Options Menu Privilege (MENU_ANSW_OPTS)	In PhoneMail the user is enabled to modify their answering options, e.g. welcome greetings, via key 8.	PhoneMail		x	x	x
Automatic Playback Menu Privilege (MENU_AUT_PB)	In PhoneMail, the user is enabled to set the automatic playback via the key sequence 9, 5 and 7. In addition, this depends on the privileges <i>Mailbox Options Menu Privilege</i> and <i>Playback Options Menu Privilege</i> , via which option 9 or 5 can be deactivated.	PhoneMail		x		
Call Forwarding Menu Privilege (MENU_CALL_FWD)	In PhoneMail, the user is enabled to set a call rerouting via the key sequence 8 and 7. In addition, this depends on the privilege <i>Answering Options Menu Privilege</i> , via which option 8 can be deactivated.	PhoneMail		x		

Table 6 Privileges

User Data Administration

Privilege	Meaning	Use	User group			
			GUEST_GROUP	USER	ADVANCED	SERVICE
Cell Phone Number Menu Privilege (MENU_CELL_NR)	In PhoneMail, the user is enabled to change his/her mobility number via the key sequence 8 and 5. In addition, this depends on the privilege <i>Answering Options Menu Privilege</i> , via which option 8 can be deactivated. It also allows/deny transfer to the mobile phone via Forward Access menu and <i>Mobility number</i> options in the <i>WebAssistant Personal settings\Voice mail system</i> user page.	PhoneMail		x		
Change Language Menu Privilege (MENU_CHNG_LANG)	In PhoneMail, the user is enabled to set the voice prompts language via the key sequence 9 and 7. In addition, this depends on the privilege <i>Mailbox Options Menu Privilege</i> , via which option 9 can be deactivated.	PhoneMail		x		
Change Password Menu Privilege (MENU_CHNG_PWD)	In PhoneMail, the user is enabled to change his/her PIN via the key sequence 9 and 3. In addition, this depends on the privilege <i>Mailbox Options Menu Privilege</i> , via which option 9 can be deactivated.	PhoneMail		x		
Distribution List Menu Privilege (MENU_D_LIST)	In PhoneMail, the user is enabled to change or create distribution lists via the key sequence 9 and 1. In addition, this depends on the privilege <i>Mailbox Options Menu Privilege</i> , via which option 9 can be deactivated.	PhoneMail		x		
Faxtone Recognition Menu Privilege (MENU_FAXRECOG)	In PhoneMail, the user is enabled to set the fax tone recognition via the key sequence 9 and 6. In addition, this depends on the privilege <i>Mailbox Options Menu Privilege</i> , via which option 9 can be deactivated.	PhoneMail		x		
Guest Mailbox Privilege (MENU_GUEST_MB)	In PhoneMail, the user is enabled to configure a mailbox for guests.	PhoneMail				
Mailbox Options Menu Privilege (MENU_MBX_OPTS)	In PhoneMail the user is enabled to modify their mailbox options, such as modifying their PIN via key 9.	PhoneMail		x	x	x
Mailbox Stand-In Menu Privilege (MENU_MBX_STDIN)	In PhoneMail, the user is enabled to set a mailbox rerouting via the key sequence 8 and 6. In addition, this depends on the privilege <i>Answering Options Menu Privilege</i> , via which option 8 can be deactivated.	PhoneMail		x		

Table 6 Privileges

Privilege	Meaning	Use	User group			
			GUEST_GROUP	USER	ADVANCED	SERVICE
Message type Menu Privilege (MENU_MEDIATYPE)	In PhoneMail, the user is enabled to set the retrievable message types via the key sequence 9 and 8. In addition, this depends on the privilege <i>Mailbox Options Menu Privilege</i> , via which option 9 can be deactivated.	PhoneMail		x		
Playback Options Menu Privilege (MENU_PB_OPTS)	In PhoneMail, the user is enabled to set the playback options via the key sequence 9 and 6. In addition, this depends on the privilege <i>Mailbox Options Menu Privilege</i> , via which option 9 can be deactivated.	PhoneMail		x		
Prompt Level Menu Privilege (MENU_PMP_LEVEL)	In PhoneMail, the user is enabled to toggle between detailed or short menu prompts via the key sequence 9 and 2. In addition, this depends on the privilege <i>Mailbox Options Menu Privilege</i> , via which option 9 can be deactivated.	PhoneMail		x		
Recording Menu Privilege (MENU_REC)	In PhoneMail the user is enabled to record messages via key 1.	PhoneMail		x	x	x
Change Referral Extension Menu Privilege (MENU_REF_EXT)	In PhoneMail, the user is enabled to change his/her referral extension via the key sequence 8 and 3. In addition, this depends on the privilege <i>Answering Options Menu Privilege</i> , via which option 8 can be deactivated.	PhoneMail		x	x	x
Sequence Menu Privilege (MENU_SEQ)	In PhoneMail, the user is enabled to set the output sequence via the key sequence 9, 5 and 3. In addition, this depends on the privileges <i>Mailbox Options Menu Privilege</i> and <i>Playback Options Menu Privilege</i> , via which option 9 or 5 can be deactivated.	PhoneMail		x		
Set Notifications Menu Privilege (MENU_S_NOT)	In PhoneMail, the user is enabled to set his/her notification options via the key sequence 9 and 4. In addition, this depends on the privilege <i>Mailbox Options Menu Privilege</i> , via which option 9 can be deactivated.	PhoneMail		x		
Transfer Menu Privilege (MENU_TRANSFER)	In PhoneMail, the user is enabled to be connected to a subscriber via key 7.	PhoneMail		x		
Trusted Transfer Mode (MENU_TTM)	Activates the Trusted Transfer Mode via which you can invoke <i>OpenScape UC Application</i> voice portal features from PhoneMail or Ergo.	Ergo, PhoneMail				

Table 6 Privileges

User Data Administration

Privilege	Meaning	Use	User group			
			GUEST_GROUP	USER	ADVANCED	SERVICE
Use Programmable Short Cuts Menu Privilege (MENU_USE_S_CUTS)	In Ergo you can activate programmable short cuts, which perform a key sequence defaulted by the Web Assistant. The corresponding configuration dialog in the Web Assistant and with installed Ergo is only displayed, if this privilege has been set.	Ergo, Web Assistant				
Volume Menu Privilege (MENU_VOL)	In PhoneMail, the user is enabled to set the playback volume via the key sequence 9, 5 and 5. In addition, this depends on the privileges <i>Mailbox Options Menu Privilege</i> and <i>Playback Options Menu Privilege</i> , via which option 9 or 5 can be deactivated.	PhoneMail		x		
Xpressions Folder Menu Privilege (MENU_XPR_FLD)	In PhoneMail, the user is enabled to set the Xpressions folder playback via the key sequence 9, 5 and 1. In addition, this depends on the privileges <i>Mailbox Options Menu Privilege</i> and <i>Playback Options Menu Privilege</i> , via which option 9 or 5 can be deactivated.	PhoneMail		x		
No obligation to record name after first login (NO_OBLIG_NAME)	The user is not obliged to record their name in the TUI after the initial login.	PhoneMail, VMS	x		x	x
No obligation to change password after first login (NO_OBLIG_PWD)	The user is not obliged to change his/her PIN in the TUI after the initial login. When using VMS, a PIN may be enabled for the user by means of a customer parameter. This is particularly useful when the user has already identified him/herself by his/her Hicom-PIN. Users who do not yet have a PIN and have not been assigned this privilege are prompted to assign an individual PIN the first time they log on with the default PIN 000000. This default PIN only applies to the default TUI configuration profile! If the user or administrator have already defined a PIN via the Web Assistant, this PIN is used without the user being compelled to assign a new one. In the Web Assistant the user may keep a default password or PIN assigned by the administrator and is not prompted to change it at the initial log-in.	PhoneMail, VMS, Web Assistant	x			x
ConnectToInfoboxOf User is prompted (PMP_CIU)	Special privilege for VMS. The announcement "You are connected with the mailbox of..." is played for this user.	VMS		x		

Table 6 Privileges

Privilege	Meaning	Use	User group			
			GUEST_GROUP	USER	ADVANCED	SERVICE
Company announcement file enabled (PMP_COMP_ANN)	Special privilege for VMS and Phonemail. The specific company announcement is played for this user.	VMS, Phonemail			x	
Long prompts available (PMP_LONG)	Special privilege for PhoneMail. The user may choose between long and short voice prompts.	PhoneMail		x	x	x
VoiceMailSystem is prompted (PMP_VMS)	Special privilege for VMS. For this user the greeting "This is the voice mail system" is played.	VMS		x		
Receive broadcast privilege (RCV_BROADCAST)	Messages sent via the broadcast service are delivered to the user's mailbox.	MTA		x	x	x
Additional Recording Info Privilege (REC_INFO)	Special privilege for VMS. For recordings, additional information is included in the announcement.	VMS		x	x	
Short Recording Start Info Privilege (REC_SHORT)	Special privilege for VMS. The caller only hears "Please speak after the tone" without indication of the maximum recording time.	VMS		x		
File Group Access (SFT_GROUP)	This privilege is not a user privilege but an access privilege for files and folders in the virtual file system of the XPR server. If it is set, only users sharing the same user group as the generator/owner of a file or folder may access these. Direct assignment to a user is pointless.	MTA				
File Owner Access (SFT_OWNER)	This privilege is not a user privilege but an access privilege for files and folders in the virtual file system of the XPR server. If it is set, only the generator/owner of a file or folder may access these. Direct assignment to a user is pointless.	MTA				
AMIS/VPIM Privilege (SND_AMIS)	External voice mail servers may be addressed via AMIS or VPIM protocol.	MTA, PhoneMail, VMS			x	x
Send broadcast privilege (SND_BROADCAST)	This user may use the broadcast service. If send jobs were created where the user lacks the privilege, they would be executed just the same.	Communications, PhoneMail, VMS				
Send dictates privilege (SND_DICTATE)	This user may record dictations. In contrast to a normal voicemail these may become rather long and require the corresponding space.	VMS			x	
e-Mail Privilege (SND_EMAIL)	Internal mail may be sent. This is for example a voice mail or e-mail that a XPR server user sends to another user.	MTA		x	x	x

Table 6

Privileges

User Data Administration

Privilege	Meaning	Use	User group			
			GUEST_GROUP	USER	ADVANCED	SERVICE
Send enterprise broadcast message privilege (SND_ENTERPRISE)	This user may deploy the broadcast service for company-internal messages. These messages cannot be forwarded.	PhoneMail				
FAX G3 Privilege (SND_FAXG3)	Fax G3 may be transmitted	MTA, PhoneMail, VMS		x	x	x
FAX G3 Poll Privilege (SND_FAXG3REV)	Fax documents may be polled from a fax-on-demand server.	Communications; MTA		x	x	x
FAX G4 Privilege (SND_FAXG4)	Fax G4 may be transmitted.	MTA			x	x
Send network wide broadcast privilege (SND_N_BROADCAST)	This user may send messages via the broadcast service and also to global distribution lists via XPR servers connected by system networking. If send jobs were created where the user lacks the privilege, they would be executed just the same. In the Web Assistant this privilege is queried for generating network-wide distribution lists.	PhoneMail, VMS, Web Assistant				
Paging Privilege (SND_PAGER)	The pager service may be used.	MTA, PhoneMail, VMS		x	x	x
Short Message Privilege (SND_SMS)	Short messages (SMS) to cellular phones may be transmitted.	MTA, PhoneMail, VMS		x	x	x
Internet Mail Privilege (SND_SMTP)	Internet mail may be sent.	MTA		x	x	x
Telex Privilege (SND_TLX)	Obsolete.	None			x	x
Voice Privilege (SND_VOICE)	Voice mails may be put out via telephone.	MTA, PhoneMail, VMS		x	x	x
ACD Monitor Privilege (SYS_ACDMONITOR)	Obsolete.	None				
Restricted ACD Supervisor Privilege (SYS_ACDRESTRICT)	Obsolete.	None				
ACD Supervisor Privilege (SYS_ACDSUPER)	Obsolete.	None				

Table 6 Privileges

Privilege	Meaning	Use	User group			
			GUEST_GROUP	USER	ADVANCED	SERVICE
Trusted Domain Privilege (SYS_ACTASDOMAIN)	This privilege can be used for services and gateways. Through the configuration of the pseudo users FAX G3 or XPRNAME, privileges assigned to the pseudo user are also assigned to all incoming FAX G3 documents or documents coming in over the remote system XPRNAME. This is used, for example, when further costs are accumulated by a routing where the originator does not have the necessary authority. This privilege is required for the validation of Remote System Links.	MTA				
Advanced USER (SYS_ADVUSER)	Obsolete.	None			x	
Local Call Privilege (SYS_AMT)	Telematic services can be locally used within the individual area code range. If required, this privilege is checked with Notification APL jobs as well.	Ergo, MTA, PhoneMail, VMS		x	x	x
External Archive Query (SYS_ARCHIVRECH)	Obsolete.	None				x
Client Beta Tester (SYS_BETATESTER)	Obsolete.	None				
Pickup call (SYS_CALLPICKUP)	You can answer calls on telephones monitored in the team bar. The SYS_VIEWPHONENR privilege needs to be assigned as precondition. This is no default privilege! Therefore, it must first be added to the XPR server. See also Section 4.5.1, "Customer Specific Privileges", on page 129 . If this privilege is not contained in the database, then all users may take the calls.	optiClient				
Fax Logo- and Coverpage-Editor (SYS_EDITLOGO)	Fax stationery may be created, modified or deleted with Communications.	Communications			x	x

Table 6 Privileges

User Data Administration

Privilege	Meaning	Use	User group			
			GUEST_GROUP	USER	ADVANCED	SERVICE
Help Desk Privilege (SYS_HELP_DESK)	You can view and edit all database fields flagged with PSERV. Furthermore, you can access the section Server settings > User administration in the Web Assistant. In there you can click on Execute to trigger the following actions: - Unlocking a user - Resetting the MWI status - Updating the MWI status - Resetting the PIN - Resetting the password - Resetting notification settings - Resetting voicemail settings - Acting on behalf of another user	Web Assistant				
Internal Call Privilege (SYS_INTERNAL)	With a TUI the user is permitted to recouple. The user may thus connect to an internal extension from within PhoneMail. In addition, a <i>User Outcall</i> can be configured as notification for an internal extension.	Ergo PhoneMail, VMS	x	x	x	x
International Call Privilege (SYS_INTERNAT)	Telematic services can be used worldwide. If required, this privilege is checked with Notification APL jobs as well.	Ergo, MTA, PhoneMail, VMS			x	x
Local File Access (SYS_LOCALFILE)	Allows access to Explorer Folders > My Computer in Communications.	Communications		x	x	x
National Call Privilege (SYS_NATIONAL)	Telematic services can be used within the individual country. If required, this privilege is checked with Notification APL jobs as well.	Ergo, MTA, PhoneMail, VMS		x	x	x
Private Query (SYS_PRIVRECH)	Obsolete.	None		x	x	x
Login via Phone possible with PIN from all devices (SYS_PWD_LOGIN)	Obsolete.	None		x	x	
Server Query (SYS_RECH)	You can perform a global research in the Web Assistant.	Web Assistant				x
Global Distribution List Editor (SYS_REEDIT)	Global distribution lists can be created, modified or deleted with the client's editor.	Communications, Web Assistant				x
ISDN Service Remote Access (SYS_REMACC)	Obsolete.	None				x

Table 6 Privileges

Privilege	Meaning	Use	User group			
			GUEST_GROUP	USER	ADVANCED	SERVICE
Global Distribution List Send Privilege (SYS_RSEND)	Messages may be sent to global distribution lists.	Communications, Ergo, PhoneMail, VMS, Web Assistant		x	x	x
Global Alias Editor (SYS_SEDIT)	The global contact information can be created, modified or deleted with the client's editor. Local or private contacts are always permitted. With a remote system link this privilege is required for the user account via which the remote MRS server is validated if user data synchronization is to occur. In this case the remote server users are defined on the local XPR server as contacts so that they are addressable.	Communications, MTA				x
Server File Access (SYS_SERVERFILE)	Access to the virtual file system of the XPR server via the server file manager of the client (Explorer Folders > Server).	Communications, MTA				x
SERVICE Privilege (SYS_SERVICE)	Database fields can be so created that this privilege is required to make modifications. Furthermore, it authorizes the restricted use of the user data editor and the XPR monitor via which the XPR server is configured. You find more information about this under Section 2.4, "Staggered Administration", on page 72 and Section 6.12, "Access Overview of the Configuration Modules", on page 183 . Furthermore, logging on and unrestricted operation of the <i>Application Builder</i> are permitted.	Application Builder, Communications, XPR Monitor, Web Assistant				x
Special Delivery Options Privilege (SYS_SPECIAL_DEL)	Special privilege for PhoneMail and VMS. With the privilege set, the user is queried for special options such as acknowledgement of receipt, private flag, urgent flag, and future delivery.	PhoneMail, VMS	x	x	x	x
SUPERVISOR Privilege (SYS_SUPERVISOR)	Database fields can be so created that this privilege is required to make modifications. Furthermore, it authorizes the restricted use of the user data editor and the XPR monitor via which the XPR server is configured. Attention: With this privilege all rights are implicitly assigned even if some of the following privileges have not been assigned to the corresponding user. Therefore, refusing does not affect other privileges if the user has this privilege!	All modules				

Table 6 Privileges

User Data Administration

Privilege	Meaning	Use	User group			
			GUEST_GROUP	USER	ADVANCED	SERVICE
Tenant Supervisor Privilege (SYS_TENANTSUPER)	Each of the following actions is restricted to users with the same tenant ID that the executing tenant supervisor has assigned. You can view and edit all database fields flagged with PSERV. Furthermore, you can access the section Server settings > User administration in the Web Assistant. In there you can click on Execute to trigger all actions except for creating a new user group.	Web Assistant				
Document Chain Query (SYS_TREE)	Document routing and response tracking may be viewed.			x	x	x
TTS Capabilities Privilege (SYS_TTS)	The user is permitted to play back messages via a TUI per Text-to-Speech.	Ergo PhoneMail, VMS		x	x	x
USER Privilege (SYS_USER)	This privilege is mandatory for server access. Entries in the correlation database without this privilege are contacts, thus no users!	All modules	x	x	x	x
View other users' remote phone numbers (SYS_VIEWPHONENR)	If a user is assigned this privilege, they may see with their monitored telephones the current status (engaged, free) and the telephone number respectively the associated name of a caller/callee in optiClient.	optiClient				
Query Result Document View (SYS_VIEWRECHDOC)	Documents given by a research of server, routing or reply tracking may be viewed. Without this privilege you only see the header information of the documents.					x
VMS Administrator Privilege (SYS_VMS_ADMIN)	Special administrator privilege for VMS.	VMS				
Voicemail transcript (VM_TRANSCRIPT)	Allows converting voicemails in written text by an external service provider using the VM2TXT APL.	MTA				
Web Assistant Access (WEB_ASSISTANT)	In the Web Assistant, access to the available configuration options is enabled.	Web Assistant		x	x	x
Web Mail Access (WEB_MAILCLIENT)	In the Web Assistant, message access is enabled.	Web Assistant		x	x	x

Table 6 Privileges

4.5.1 Customer Specific Privileges

Privileges are defined by a correlation data record. Customer specific privileges can be defined and inserted anytime. These new privileges are entered in the condition format in the registry value [Privileges \[REG_MULTI_SZ\]](#) under the key `HKLM\SOFTWARE\Wow6432Node\PP-COM\MRS\MTA\RULES`. This occurs through the entry of the privilege and it's address separated by a comma. Further entries would be individually entered as lines in `REG_MULTI_SZ`. Addresses that conform to the listed wildcards require the corresponding privilege. For this purpose, pattern matching for the given service and number is used. For example, you can poll information by fax via relatively expensive service numbers that begin in Germany with the area code 0900. A privilege could be assumed for persons to have access to this information.

Example: `FAXG3REV_0190,NVS:FAXG3REV/+49900*`

To add this privilege to the database, take a free number from the range 0xE0 to 0xF7 reserved for this purpose. Now a text file, for example `x.txt`, can be created with the following contents:

CLASSNAME	CLASS	KEYNAME	KEY
PRIVILEGES	FAXG3REV_0900	0xE0	Fax Poll 0900

Exactly one TAB must be inserted as a separator between the individual parts! The privilege number in the above example is 0xE0 (hexadecimal). On the XPR server command line you can now import this definition into the database with the following command:

```
infotool CLASSIMPORT FILE=x.txt CLASS=PRIVILEGES
```

You can also write the data directly with DBTool. The XPR server must be restarted before this new privilege comes into effect. Subsequently, this privilege is required for each fax polling with a 0900-number.

There are also privileges such as `SYS_CALLPICKUP` that have a permanently specified significance but do not belong to the standard delivery. If you want to use such a privilege, take a free number from the range 0xE0 to 0xF7 and write the privilege in the database in the same manner. The step via the [Privileges \[REG_MULTI_SZ\]](#) registry value is then omitted. The definition for `SYS_CALLPICKUP` might then look like this:

CLASSNAME	CLASS	KEYNAME	KEY
PRIVILEGES	SYS_CALLPICKUP	0xF7	Pickup call

4.6 Assigning Voice Mail Settings group-specifically

The global voice mail settings defaulted in the telematics APLs and valid for all users by default, can be adapted user-specifically. When this happens, the global settings are overwritten by the group-specific settings. Furthermore, additional database fields can be assigned via the group. These are in the database mask `GROUP`. We strongly advise not to try individual mask extensions.

The definition of these group-specific voice mail parameters is done by changing the group definition in the Web Assistant.

The following parameters can be customized for the selected group:

Field	Description
Maximum Voice Mail Duration (s)	The time available to callers to record their message. The caller receives a warning shortly before the set time expires.
Maximum Voice Mail Duration (s)	The time available to group members to record their own announcements.
Max. duration of company greeting (in sec):	The time available to record the company greeting. Annotation: This setting is only useful for the group containing the "Company" user via which the company greeting is activated.
Maximum duration of name recording (in sec)	The time available to group members to record their own names.
Minimum number of digits for valid PINs	The value entered here determines of how many digits a new group member PIN must at least consist. The longer the PIN, the greater the security it provides. On the other hand they are hard to remember so that a useful compromise should be found.
Validity period of the PIN	The number of days after which the PIN is considered invalid for group members and the user is prompted to enter a new PIN. This function can be deactivated by entering 0.
The number of warning days before the PIN expires	The number of days a warning should be output before the telephone password expires is set here for the users of the selected group. The warning is then always displayed when the user logs on. Example: the validity period of the PIN shall be set to 30 days and the number of warning days to three. After 27 days when you log in you will be informed for the first time that the PIN will expire in three days.

Field	Description
Number of failed login attempts before mailbox is locked	The entered value is used to specify for the group members the number of incorrect logon attempts (PIN input) after which the TUI access to the mailbox is locked. It must then either be unlocked again by the administrator. This occurs automatically when a new PIN is assigned via the Web Assistant or after expiration of the time set in the voicemail profile under Time (in minutes) until locked users are granted access again . You can perform this setting only via the <i>Web Assistant</i> . You can also delete the content of the database fields <code>VM_LOGIN_FAILED</code> and <code>VM_LOCK_SET</code> as alternative.
Maximum number of private distribution lists	Number of distribution lists that a group member can generate.
User ID for the operator of this group	A call to a member of this user group is forwarded on request to the subscriber whose user ID is entered here.
GUI user dials with external prefix	See description of database field <code>NCO_GUI_PREFIX</code> .
TUI user dials with external prefix	See description of database field <code>NCO_TUI_PREFIX</code> .
NCO Connect Point for GUI users	See description of database field <code>NCO_GUI_CONN_PT</code> .
NCO Connect Point for TUI users	See description of database field <code>NCO_TUI_CONN_PT</code> .
NCO location	See description of database field <code>NCO_LOCATION</code> .
User must enter project code	If this button is set, a code is demanded in PhoneMail before a callback. This code will be transferred to the PBX.
Language ID 2	Use of a second language for the Ergo welcome greeting. See description of database field <code>SEC_LANGUAGE_ID</code> .
Use last redirected number	Use of the first or last redirected number in case of cascaded forwardings in Ergo. See description of database field <code>USE_LAST_REDIR</code> .
Voicemail system	See description of database field <code>VM_PROTOCOL</code> .
Time zone	See description of database field <code>TIMEZONE</code> .

4.7 PIN Handling in the XPR Server

This chapter describes the PIN handling within the XPR server.

IMPORTANT:

If the features described here are incorrectly configured or not at all, serious XPR server security violations may be the result. In case you are unsure about the effects of the (non-)configuration of one of the described features, please contact your system integrator.

4.7.1 Using personal User PINs

Each user that has been assigned a voice box may alter the associated personal PIN. This alteration can be performed in different ways:

- Via the TUI
- About the Web Assistant

This section provides an overview of the mechanisms that are or can be applied with PIN handling.

4.7.2 User PIN handling in the TUI and in the Web Assistant

The TUI and the Web Assistant of the XPR server currently provide the following PIN handling mechanisms. They are configured via the voice mail settings (VM-s) of the telematics APL used or via the Web Assistant (WA). The settings performed in this way are centrally stored in the Correlation Database and are thus available in the entire system.

- Length defaults for PINs
- Connection abortion after a defined number of wrong PIN entries
- Voice box locking after a defined number of wrong PIN entries
- Regular mandatory PIN alteration
- Warning before PIN validity expires
- Default-PIN definition
- Trusted numbers
- PIN check for invalid characters
- PIN check for mailbox number
- PIN check for identical digits
- PIN check for ascending or descending numerical sequences
- PIN check for vanity dialing of the user ID
- PIN check for PIN history
- PIN check for default PIN

The following sections will consider these XPR server features in detail.

You find further information on the configuration of the mechanisms described here in the *Web Assistant* manual or in [Chapter 10, “Telematics APL”](#).

4.7.2.1 Length defaults for PINs

In the XPR server you can define the minimum length of the PINs to be used. In this way mailbox users are prevented from softening their mailbox access security by a too short PIN.

The longer the PIN, the greater the security it provides. On the other hand, users can often remember passwords that are much too long only with the help of undesired notes. This again contradicts the idea of security. Therefore a default minimum PIN length will always be a compromise between security requirements and usability.

The minimum PIN length can be defined by the system administrator for the entire system and/or per user group. The maximum PIN length is 24 digits.

4.7.2.2 Connection Abortion after wrong PIN Entries

To make sure that unauthorized persons cannot guess the current PIN of a mailbox by making numerous entries, an automatic connection abortion can be activated in the XPR server. When this mechanism is active and a defined number of wrong PIN entries has been made in the attempt to dial in into a mailbox, the connection is aborted.

The number of wrong PIN entries leading to a connection abortion can be defined by the system administrator for the entire system.

4.7.2.3 Locking the Voice Box after wrong PIN Entries

Under conditions equal to aborting a connection (cf. [Section 4.7.2.2, “Connection Abortion after wrong PIN Entries”, on page 134](#)), locking a mailbox can be set as well.

This setting can be performed by the system administrator for the entire system and/or per user group. It is thus possible to lock a mailbox in security-critical user areas and to set the simple connection abortion for all other users.

IMPORTANT:

Mailbox locking after a defined number of wrong PIN entries is always active for the Ergo and Evo voicemail systems.

By assigning a new PIN in the Web Assistant the administrator can automatically unlock the mailbox. The mailbox is also automatically unlocked after the time set in the voicemail profile under **Time (in minutes) until locked users are granted access again** has expired. You can perform this setting only via the *Web*

Assistant. If you do not want to have the mailbox unlocked automatically, you can enter a value like $5 \times 365 \times 86400 = 157680000$ seconds = 5 years, which is high enough to prevent this. This corresponds practically to a permanent locking.

4.7.2.4 Regular mandatory PIN Alteration

To impede unauthorized access to foreign mailboxes, mailbox users can be compelled to change their PIN in regular intervals. On the one hand this shortens the time in which unauthorized persons might find out a current PIN. On the other hand mailbox security is restored after the next timely PIN alteration if the current PIN has become known.

The mandatory PIN alteration can be defined by the system administrator for the entire system and/or per user group.

IMPORTANT:

The regular mandatory PIN alteration is not supported by the Ergo and Evo voicemail systems.

4.7.2.5 Warning before PIN Validity Expires

So that users can react in time to the validity expiration of their PIN in case of mandatory PIN alteration, a corresponding prewarning can be activated in the XPR server. Such a warning informs a mailbox user concerned that his/her PIN will become invalid within a defined period. In this way a user is enabled to define a new PIN before the current one expires.

This feature can be defined by the system administrator for the entire system and/or per user group.

4.7.2.6 Default-PIN Definition

Upon the definition of a new mailbox user the system administrator can assign an individual initial PIN. Under this PIN the respective user can subsequently log in at the voice mail system.

To optimize the specification of new mailbox users, a default PIN can be defined in addition. This default PIN is automatically assigned to the newly defined mailboxes that do not receive an individual PIN by the system administrator. The default PIN serves solely for the initial login at the voice mail system and must then immediately be changed.

A default PIN can be defined by the system administrator for the entire system. It need not meet the general PIN requirements (see [Section 4.7.2.8, “PIN Check”, on page 137](#)).

4.7.2.7 Trusted Numbers

IMPORTANT:

The improper configuration of trusted numbers may lead to serious security violations concerning the XPR server and the data stored on it. Therefore we recommend to exclusively use such phone numbers as trusted numbers that are under **permanent personal control of the respective mailbox user**.

So that accessing the private mailbox is simplified, each mailbox user can define up to three trusted numbers. If the respective user then dials in into the voice mail system from one of the phone connections thus defined, the XPR server does not demand entry of the configured PIN.

IMPORTANT:

Trusted numbers usage is not supported by the VMS voicemail system.

IMPORTANT:

Trusted number usage is always active for the Ergo and Evo voicemail systems.

4.7.2.8 PIN Check

If a user changes his/her PIN, the new one must meet various requirements. The fulfillment of these qualifications is secured by different TUI or Web Assistant checks.

New PINs are currently checked in the following manner.

Invalid characters

A PIN must exclusively consist of a combination of the digits 0 to 9. The precise number of digits results from the length defaults by the system administrator (cf. [Section 4.7.2.1, “Length defaults for PINs”, on page 134](#)).

A newly defined PIN is checked as to whether it contains characters different from the permitted digits. If this is the case, the new entry is rejected as invalid.

Mailbox number

A newly defined PIN is checked as to whether it corresponds to the number of the respective mailbox or contains the mailbox number. If this is the case, the new entry is rejected as invalid.

Example:

The mailbox number is 789321.

The entries 789321 or 04 **789321** 05 for a new PIN are invalid and not accepted by the TUI or the Web Assistant.

Identical digits

A newly defined PIN is checked as to whether it merely consists of a string of identical digits. If this is the case, the new entry is rejected as invalid.

Example:

The entries 111111 or 6666666666 for a new PIN are invalid and not accepted by the TUI or the Web Assistant.

Ascending and descending numerical sequences

A newly defined PIN is checked as to whether it merely consists of a sequence of ascending or descending digits. If this is the case, the new entry is rejected as invalid.

Example:

The entries 345678 or 32109876 for a new PIN are invalid and not accepted by the TUI or the Web Assistant.

Vanity dialing of the user ID

Each mailbox user has an internal user ID within the XPR server.

A newly defined PIN is checked as to whether it merely consists of the vanity dialing of this user ID. If this is the case, the new entry is rejected as invalid.

Example:

A user has the ID *SCHILLER*.

The entry 72445537¹ for a new PIN is invalid and not accepted by the TUI or the Web Assistant.

PIN history

A specific number of PINs used last can be stored for each mailbox as PIN history. The administrator can define for the entire system how far this history may stretch back.

A newly defined PIN is checked as to whether it has already been used in the stored PIN history. If this is the case, the new entry is rejected as invalid.

IMPORTANT:

PIN checking based on a PIN history is not supported by the Ergo and Evo voicemail systems.

Default PIN

The system administrator can define a default PIN for configuring new mailboxes (cf. [Section 4.7.2.6, “Default-PIN Definition”, on page 135](#)).

A newly defined PIN is checked as to whether it corresponds to the currently defined default PIN. If this is the case, the new entry is rejected as invalid.

1. Vanity dialing via the telephone keypad: 7 =S, 2 =C, 4 =H, 4 =I, 5 =L, 5 =L, 3 =E, 7 =R

4.7.2.9 Summary

Attribute	Available	Default	Configurable	Configuration
Minimum PIN length	Yes	6	Yes	VM [*] ; in the WA ^{**} configurable per user group
Maximum PIN length	Yes	24	No	–
Connection abortion after wrong PIN entries	Yes	3	Yes	VM [*] , WA ^{**}
Voice box locking after a defined number of wrong entries	Yes	Off ^{***}	Yes ^{***}	VM [*] ; in the WA ^{**} configurable per user group
Regular mandatory PIN alteration	Yes ^{****}	Off	In days	VM [*] ; in the WA ^{**} configurable per user group
Warning before PIN validity expires	Yes	Off	In days	In the WA ^{**} configurable per user group
Default-PIN definition	Yes	000000	Yes	VM [*] ; WA ^{**}
Trusted numbers	Yes ^{****}	Off ^{***}	3 numbers per user	Configurable in the WA. Activation in the VMs [*] .
PIN check for invalid characters	Yes	On	No	–
PIN check for mailbox number	Yes	On	No	–
PIN check for identical digits	Yes	On	No	–
PIN check for ascending or descending numerical sequences	Yes	On	No	–
PIN check for vanity dialing of the user ID	Yes	On	No	–
PIN check for PIN history	Yes ^{****}	On	PIN history length	VM [*] ; WA ^{**}
PIN check for default PIN	Yes	On	No	–

Table 7 Security Criteria for PINs

* VM = Voice mail settings of the Telematic APL.

** WA = Web Assistant.

*** Depending on the voice mail script used.

****Is not supported by all voice mail systems.

Via the voice mail settings of the Telematic APL you can set global defaults for the respective TUI. With the Web Assistant you can partly override such global defaults for single user groups. A possible direct setting at or by a user may override the user group settings as well as the global defaults.

4.8 Password Handling in the XPR Server

This section describes the password handling in the XPR server. With XPR 5, a new security concept for user passwords has been introduced. The innovations comprise basically the following points:

Introduction of an SHA-256 encryption

A hash algorithm with SHA-256 encryption is used. In this context, hash algorithms have two essential advantages:

1. The recovery of the original character string from the hash value is virtually impossible.
2. In addition to the password to be encoded, further character strings can be added to the hash value, for example a time stamp or a user ID.

Encoding is exclusively valid for the `PASSWORD` database field.

System-wide password policies

Policies as regards the lifespan and complexity of a password can be specified via an administrative interface in the Web Assistant for the entire system. Such policies determine the following password parameters:

- Minimum length
- Validity period
- Number of old, to be considered passwords
- Whether and which special characters are to be contained

4.8.1 Authentication Mode in the XPR Server

The authentication mode is set by an administrator in the Web Assistant for the entire system. The following authentication alternatives are available:

Windows Authentication

With the Windows authentication, all authentication functions in the XPR server are deactivated. The authentication mechanisms of the operating system are then used.

IMPORTANT:

For technical reasons the XPR monitor always requires an OpenScape Xpressions V7 authentication.

OpenScape Xpressions V7 Authentication

If the OpenScape Xpressions V7 authentication is used, all passwords are encoded by means of the above hash algorithm. An administrator must define the password policies to be valid for the entire system.

We recommend the Windows authentication as default. This setting can be modified during the XPR server setup.

NOTE:

The authentication is configured via the Web Assistant. Please read the corresponding chapter in the *Web Assistant* manual on this.

4.8.2 Locking after several wrong Password Entries

If a user tries to log on with an incorrect password five times, the account will be automatically locked. The user then needs to consult an administrator who can unlock the account.

A period can be set after the expiration of which the account is automatically released again.

4.8.3 Changing to the new Security Concept

Besides the new security concept, the XPR server from version 5 still supports the old functionality to ensure downward compatibility and upgrading. Activating the new security concept requires the following steps:

1. All clients must have been upgraded to version 5 or later.
2. No cross-effects with old systems may exist, such as a connection to a commonly used Active Directory.
3. The MASK attributes of the PASSWORD field are to be changed in all masks from KRYPT, UPPER to CRYPT_SEC.
4. Adjusting the value HKLM\Software\Cycos AG\MSP\SecurePassword (REG_DWORD) to 1. A 0 in this value represents the old security concept.

NOTE:

On a 64-bit operating system this is value

HKLM\Software\Wow6432Node\Cycos AG\MSP\SecurePassword.

5. After this adjustment you need to re-enter the password for all stored profiles, so that it is encrypted with the new procedure and saved again.

When a user logs on, the system first checks whether the associated hash value was generated with the old algorithm. If yes, the already existing password and the user ID are encoded with the new algorithm to a new hash value and stored in the database.

If the existing password does not conform to the policies specified, the user is prompted to define a new password that is, along with the user ID, also encoded with the new algorithm and stored in the database.

4.8.4 Password Policies

Password policies are defined using the Web Assistant. An administrator determines the parameters to be considered.

As soon as a user changes his/her password, the new password must conform to these policies, since only then will the system accept the entered character string.

4.8.4.1 OpenScape Xpressions V7 Authentication

For the OpenScape Xpressions V7 authentication, the password policies can be set in the following categories:

Valid characters

Character categories can be specified that must be contained in password. The following character categories are available:

- upper case letters A-Z
- lower case letters a-z
- numerics 0-9
- special characters: ! " # \$ % & ' () * + , - _ . : ; < = > ? @ [] { } \ | ~

NOTE:

Umlauts such as Ä, ä, Ö, ö, Ü, or ü are considered special characters.

Minimum length

The minimum number of characters that a password must comprise can be set.

Validity period

A period of validity can be set for passwords. After expiration of this validity period a user is automatically prompted to enter a new password at his/her next login. The maximum period of validity is set in days.

Password history

To stop users from selecting always the same passwords in turn, the number of new passwords that must be defined before an old one is accepted again can be set.

4.8.4.2 Windows Authentication

The following policies apply for the Windows operating systems Windows XP and Windows Server 2003:

NOTE:

Please obtain the precise policies (e.g. thresholds, default settings and recommendations) from the documentation of your operating system. We only provide a short overview here. Please check the policies in particular for operating systems not listed here.

Password history

To stop users from selecting always the same passwords in turn, the number of new passwords that must be defined before an old one is accepted again can be set.

Validity period

A validity period can be specified in days, after which the user must enter a new password.

Minimum age

A minimum period for a password to be valid before a user may define a new one can be set in days.

Minimum length

A password minimum length can be set.

Complexity

A password complexity check can be activated. The following password properties are checked:

- length of a least 6 characters
- contains characters of at least three of the following five categories:
 - upper case letters A-Z
 - lower case letters a-z
 - numerics 0-9

- non-alphanumeric characters (e.g. !, \$, # or %)
- does not contain three or more characters that are also contained in the user name

5 XPR Service Provider (MSP)

The XPR Service Provider serves as global substructure for all client applications that want to use XPR server services. Such clients are, for example, optiClient Extensions and Communications. While several client applications can run on one computer simultaneously, only one entity of the XPR Service Provider is available at a time.

According to requirements the MSP is automatically implemented upon the installation of an XPR client component. When the installation is completed you will find the file `MSP.INSTALL.LOG` in the TEMP directory of the installing user, helping to detect errors if problems should occur. If problems arise during operation, you can use the UnifiedLogTool to receive debug outputs. See [Section 32.14, “Logging Tool for Clients”, on page 1558](#).

The MSP is installed as service. The service runs in the system context. During the installation, the option for enabling the service to interact with the desktop is set. This is required in special situations to enable the MSP displaying error messages or warnings on the desktop as service. In case of terminal server operation, interaction is not possible because the service cannot know on which desktop the message is to be displayed. This is why the Windows Event 7030 brings this to attention as warning in the log during the setup on a terminal server. The service works just the same. To be on the safe side, you can simply disable the interaction with the desktop in the configuration of the service.

IMPORTANT:

Users may open Wave files, for example in Communications, to play them via telephone. The MSP must be able to read these files for this purpose. If the MSP is installed as service, it must be assigned a corresponding user account.

The XPR Service Provider is started by the first client application requiring it. Such an application is the XPR Service Provider configuration module in the control panel.

The following XPR services are provided:

Local database (cache)

Every client application does not have to keep its own database up to date. If required, the XPR Service Provider synchronizes its local database with the database of the XPR server. Thereby the contents of the local database is made available to all client applications so that fast access is enabled anytime.

Store & forward interface

Client applications can send documents to or receive them from an XPR server. This refers to classic communication per fax, e-mail etc. The XPR CTI journal of the Message Routing System operates via this interface as well.

Transactions interface

Client applications can communicate with APLs of the XPR server that support transactions. Via this interface normally realtime information or jobs are sent. An example are status information to the own telephone device.

5.1 Configuration

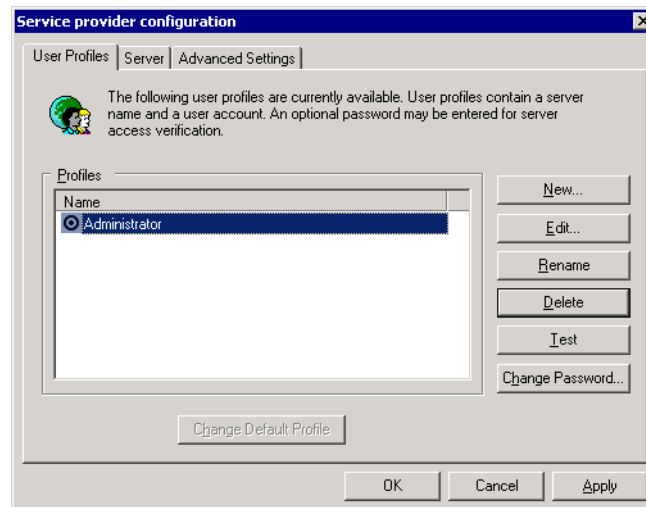
Configuration of the XPR Service Provider  is accessed with a double-click on **Start > Settings > Control Panel > MRS Service Provider**. Here XPR servers can be added and a new profile be created for new users or an existing one be modified. You need a user profile with administrative privileges, for example, for configuring the XPR user and groups. See [Section 5.2, “Configuring an Administrative User Profile”, on page 159](#).

The communication between client and server can be encrypted by means of SSL. For the configuration see [Section 15.1, “Ports and Encryption used”, on page 1027](#).

NOTE:

Using SSL V2 and V3 is always disabled in the XPR server. TLS V1, V1.1 or V1.2 is always used.

5.1.1 User Profiles



To connect a client application with an XPR server, a **User Profile** is required. For that purpose, several options are available:

- A profile containing the name of an XPR server, a user account on this server and optionally the account's password.
- A profile with the name of an XPR server. For logging on, the logged-in Windows user account is used. See also section [Section 5.4, “Client log-in via Windows User Account”, on page 162](#).

- A profile with the name of an XPR server. For logging on, the logged-in Novell Network user account is used. See also section [Section 5.5, “Client Log-in via Novell Network User Account”](#), on page 163.

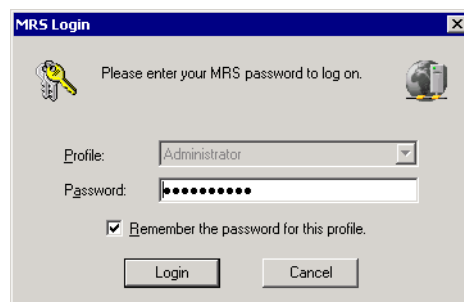
Click on **New** to generate a new profile. The name of the currently logged in user is suggested as **User Name** which should be altered to the XPR User Name. Depending on the network environment, the Service Provider may not automatically detect all available XPR servers. In this case switch to the **Server** tab and configure the missing server manually. See [Section 5.1.2, “Server”](#), on page 156.

Edit... displays the selected user profile so that you can perform modifications. See [Section 5.1.1.1, “Editing a Profile”](#), on page 155.

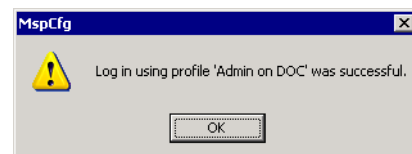
Rename enables a change of the selected profile name.

Delete removes the selected user profile.

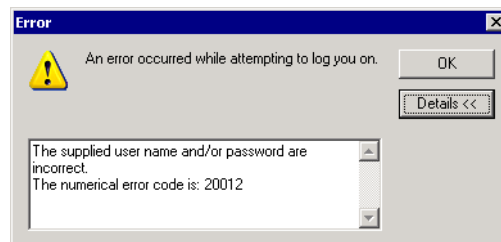
Next validate the configurations made with an attempt to log in to the XPR server via **Test**.



This process either results in a message of success



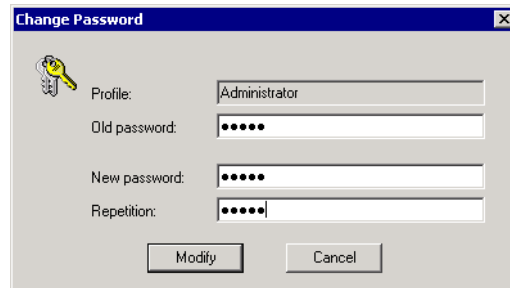
or, in case of failure, a possible reason for the error is given.



In the event that several profiles are available, one of the existing user profiles can be selected via the **Toggle Default** button for permanent use. The default profile is indicated by a dot which appears in the circle preceding the user name. If you click on this button when a user entry with default profile has been selected, the default profile setting for this user is canceled. In this case the applications

using the MSP always provide a Log-in form in which the desired profile has to be selected. Otherwise log-in would be performed directly without query. However, this again requires entering the password that associates the user account.

In the **Change Password** dialog you can modify a profile password. Enter the old password and specify the new one twice. Since the new password is not displayed while you enter it, the confirmation makes sure that no typing errors occur.

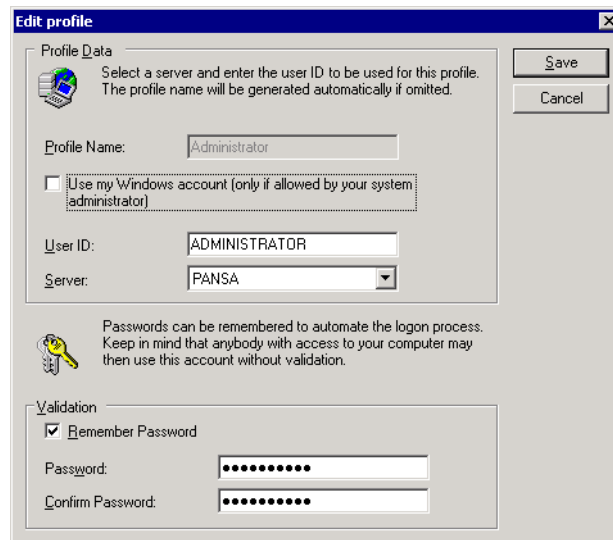


The **Change Password** dialog box has a title bar with a close button. It contains a key icon and the following fields:

- Profile:** A text box containing "Administrator".
- Old password:** A password field with six dots.
- New password:** A password field with six dots.
- Repetition:** A password field with six dots.

 At the bottom are two buttons: **Modify** and **Cancel**.

5.1.1.1 Editing a Profile



The **Edit profile** dialog box has a title bar with a close button. It is divided into two main sections:

- Profile Data:** Contains a globe icon and instructions: "Select a server and enter the user ID to be used for this profile. The profile name will be generated automatically if omitted." Below this are:
 - Profile Name:** A text box containing "Administrator".
 - ☐ **Use my Windows account** (only if allowed by your system: administrator)
 - User ID:** A text box containing "ADMINISTRATOR".
 - Server:** A dropdown menu showing "PANSA".
- Validation:** Contains a key icon and instructions: "Passwords can be remembered to automate the logon process. Keep in mind that anybody with access to your computer may then use this account without validation." Below this are:
 - ☒ **Remember Password**
 - Password:** A password field with ten dots.
 - Confirm Password:** A password field with ten dots.

 On the right side of the dialog are two buttons: **Save** and **Cancel**.

The **Profile Name** is a descriptive entry displayed for selecting different profiles later on.

If no profile name is entered with the creation of a new user profile, an entry consisting of the specified **User Name** and the **Server** is automatically generated.

In the event that only one server is available it is preset and cannot be modified. For information on the configuration of XPR servers and how to look them up see the description further below.

The log-in process is performed automatically when the **Remember Password** option is activated and a **Password** is subsequently entered. The password is not displayed while you enter it! To avoid subsequent input errors, the password must be entered twice.

NOTE:

Please note that the passwords used in XPR are not case sensitive.

IMPORTANT:

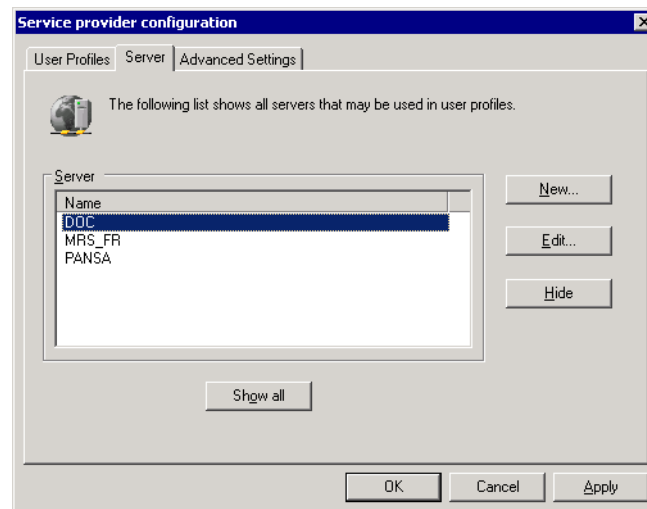
Please note that when you activate this option, this profile can be used without any further validation and thus also this XPR user account. Therefore, you should **lock your workstation**¹ before leaving it.

With editing an existing profile the same options can be set, however, the name of the profile cannot be altered any more.

A click on **Save** stores the user profile just generated or modified.

The **Use my Windows account** option carries out a validation of the logged in Windows user via the XPR server. The corresponding Windows user account must be entered in the XPR user account so that the XPR server can perform the corresponding assignment. See also section [Section 5.4, "Client log-in via Windows User Account"](#), on page 162.

5.1.2 Server



-
1. Under Windows, push the keys **[Ctrl]**, **[Alt]** and **[Delete]** simultaneously and select the "Lock Computer" option in the menu then available.

Here all XPR servers found in the network environment are displayed and can thus be selected for user profiles.

Depending on the network environment it may happen that the XPR service provider does not automatically find all existing XPR servers.

In this case these XPR servers can manually be added via **New**. First, you need to enter the network address of the missing XPR server. The network address is protocol specific, so the hostname (e.g. mail.cycos.com) or the IP address (e.g. 10.1.14.128).

Then click on **Lookup**. The MSP now searches for an XPR server with operating TCP/IP APL under the specified network address. If the MSP finds a server, it enters the server's name in the **Server Name** field. In the event that the MSP could not address an XPR server, a corresponding message is issued.

A click on **Save** appends the XPR server to the server list. In user profiles only servers included in this list can be used.

A displayed XPR server can be hidden with **Hide**. Since the XPR server is, with reference to the network environment, a globally available resource (similar to a Windows NT Server in the Server Manager), it cannot be “deleted” or “removed” because the MSP stores the information about this server for a longer period.

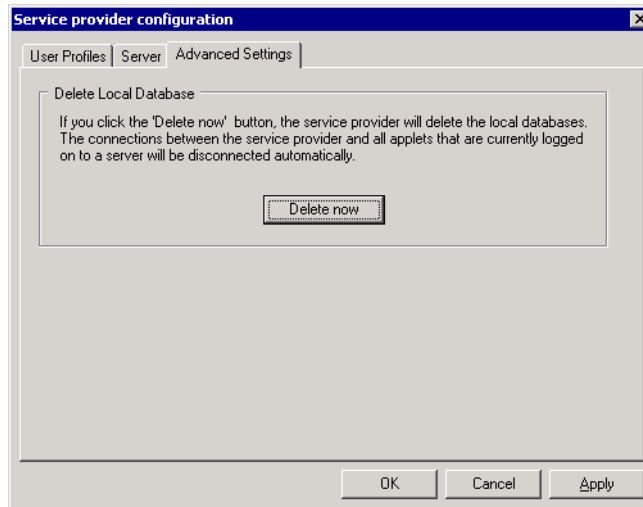
So if a displayed server is not to be used in your user profiles, it can be “hidden”, that is marked, so that it does no longer appear in the server list. However, this selection only applies to the user currently logged in, whereas another one would see the complete XPR server list again.

In case a hidden server is to be displayed again later, click on **Show all** so that all XPR servers known to the MSP are listed again.

An XPR server used in an individual profile cannot be hidden.

Alternatively you can enter a * as **Address** and subsequently click on **Lookup**. Now the MSP starts a new attempt to find an XPR server among all addresses reported by the network router and displays the first one found. In the **Server** configuration tab also all newly found XPR servers are displayed now; the button **Show all** probably needs to be clicked here again.

5.1.3 Extended Settings



If you notice discrepancies between the XPR server database and local databases administered by the Service Provider, you can delete the databases so that the XPR server polls all data anew. This is normally only required when the server was reinstalled with the same name and thus the server database was reinitialized as well. In practice this scenario only occurs in test labs.

NOTE:

If a client login attempt fails at the XPR server, please check the service provider profile settings. If you are unable to locate the problem here, it may be caused by a damaged local database. Via the **Delete now** button the local database could be used in this case. The local database is automatically reconstructed at the next logon of a client application that uses the service provider.

5.2 Configuring an Administrative User Profile

First of all, you must set up a user profile with administrative rights with the XPR service provider.

1. To do this, start the Service Provider by selecting **Start > Settings > Control Panel > Service Provider**.
2. Open the following mask by clicking **New**.

For the User ID, enter a user account with administrative rights. This could be the default setting for the installation, in other words the user account **ADMINISTRATOR**.

If there is only one XPR server in the network, this is already selected by default. Specify the name of the user profile in the **Profile Name** field, e.g. "Admin on DOC".

3. Then click the **Add** button.

The user profile has been defined.

NOTE:

Please note that the passwords used in XPR are not case sensitive.

Testing profiles

A newly configured profile and its settings can be immediately validated by attempting to log on to the server.

- Click **Test**.

This results either in a success message or in the event of failure, an advisory about the possible cause of the fault.

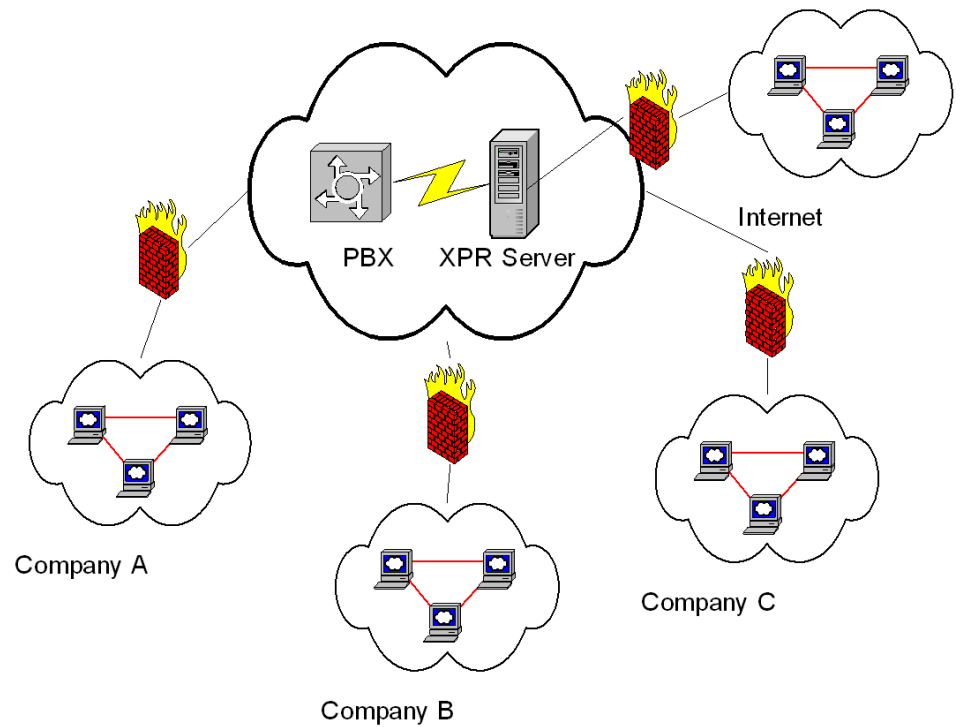
Deleting the default profile setting if required

If more than one profile has been configured, one of these profiles can be defined as default. In this way this profile is always used at logging in. If an individual user profile has been defined besides the administrative one, no profile should be defined as default. In this way the profile to be used is queried with each client application start.

- Select the current default profile and click the **Set as Default** button. The dot in the circle preceding the default profile disappears and no default profile is configured anymore.
4. Click **Save** to save the newly created administrative user profile.

5.3 NAT Firewall Scenario

This scenario is a kind of campus scenario. A Service Provider makes available the PBX infrastructure with XPR server to several companies. The companies are separated from the PBX and the XPR server via a firewall. This firewall outwardly converts the private IP addresses of the company into unique public addresses (NAT). The company networks have no connection amongst each other. From the view of the single companies the PBX and the XPR server are in a so-called Demilitarized Zone (DMZ). A DMZ is not considered absolutely safe. Optionally, the XPR server might be connected to the internet, e.g. to handle sending and receiving of e-mails.



In order to enable answers to the monitor transactions made by the XPR server to the respective clients (Communications, Lotus Notes Extensions, Outlook Extensions etc.), the XPR server does not need to know the private IP address but the public IP address assigned by the NAT firewall. Since the clients do not know this address and hence cannot enter it as the reply address, you need to proceed as follows:

If required, create the registry value `NatClient [REG_DWORD]` for each agent and set it to 1.

Thus the MSP returns the string `###.###.###.###` to the client applications as the local IP address. If this period is smaller than the time-out set here, the Web Assistant will continuously request data and thus reset this time-out. This local address is solely used by the client applications for the CTI monitor request at the XPR server. Because of this identification the TCP/IP APL recognizes that it is a matter of a client behind a firewall. So it replaces this string with the client's public IP address that has been assigned by the NAT firewall. This IP address must be unique. At the same time, the TCP/IP APL switches off the shorthand for this client line.

5.4 Client log-in via Windows User Account

Instead of a user profile with XPR user account and password you can also assign the Windows user account to an XPR user account. Therefore, in a scenario with an Exchange connection, the administrator need not maintain individual XPR user profiles on the respective client computer. For the required login, for example of the Outlook Forms, the logged-in user account is simply used.

In the [LMACCOUNT](#) database field a user's Windows domain and account must be entered. Example: the entry for user `MK` in the `TEST` domain would be `TEST\MK`. Subsequently, the corresponding option for the MSP profile needs to be activated and, as of Microsoft Windows 2000, logging on occurs automatically via validation at the domain server.

To perform this type of login, an XPR user must not have a `\` in his/her `USER` field. He/she can then also log in, for example, at the Web Assistant or via POP3/IMAP4 with the Windows domain and the Windows user account having to be entered here as login name either as described above or in the form `user@domain`. There is, however, the security gap that for access via HTML, POP3 or IMAP4 the Windows password would be transmitted in plain text. This restriction exists in the same way with addressing the Exchange server via POP3/IMAP4. This can be evaded by using the SSL connection for these accesses each.

The [LMACCOUNT](#) field is automatically correctly filled in with usage of the LDAP APL and an Exchange 2003/2008 Server connection and maintaining the user data in the Active Directory. Furthermore, you can always configure a default profile for the logged-in Windows Account via a registry entry in the MSP. This avoids further work for configuring an MSP profile on the client computers. If logging in with the Windows account via this standard profile fails, you are prompted to install a corresponding MSP profile. For this reason the [LMACCOUNT](#) field should always be updated before the automatic distribution of client applications to the respective client computer.

The MSPTSP application cannot be logged in via the Windows user account since this application runs in the system context and thus does not know the logged-in Windows user. Thus a corresponding MSP profile must be specified there at any rate. For the same reason, you cannot normalize phone numbers for MSPTSP applications depending on the calling user. You find further information about the MSPTSP in the *Client Applications* manual.

5.4.1 Automatic Configuration

During the installation you can have the default user profile "My Windows Account" automatically configured for all users. Simply generate the registry value [UserProfiles \[REG_MULTI_SZ\]](#) with the following content:

```
"My Windows Account on <Server>, , <Server>, 0"
```

<Server> is here the XPR server name.

As long as the user does not create his/her own user profile, this default profile is used.

5.5 Client Log-in via Novell Netware User Account

Instead of a user profile with XPR user account and password you can also assign the Novell Netware user account to a XPR user account.

Firstly, the XPR user ID must correspond to the user's Netware user ID for this purpose. Secondly, the registry value [NetwareLoginOnly \[REG_DWORD\]](#) must be set to 1 for the user. You can also set the registry value [NetwareLoginOnly \[REG_DWORD\]](#) to 1 for all users of this computer.

The MSPTSP application cannot be logged in via the Netware user account since this application runs in the system context and thus does not know the logged-in Netware user. Thus a corresponding MSP profile must be specified there at any rate. You find further information about the MSPTSP in the *Client Applications* manual.

5.5.1 Automatic Configuration

During the installation you can have the default user profile "My Netware Account" automatically configured for all users. Simply generate the registry value [UserProfiles \[REG_MULTI_SZ\]](#) with the following content:

```
"My Netware Account on <Server>, , <Server>, 0"
```

<Server> is here the XPR server name.

Subsequently, set the registry value [NetwareLoginOnly \[REG_DWORD\]](#) to 1.

As long as the user does not create his/her own user profile, this default profile is used.

5.6 Client Firewall

In case of an active firewall you need to give the MSP outgoing access to the XPR server. For this purpose the `MSPSVC.EXE` and `STUNNEL.EXE` programs must be added to the exception list of the firewall. The programs are installed on an English operating system in the directory

```
C:\Program Files\Common Files\Cycos\Service Provider\.
```

Depending on the operating system language the path may vary. In this case look for one of the above programs and determine the setup directory.

`MSPSVC.EXE` is the Service Provider. `STUNNEL.EXE` is used for encrypted communication with the XPR server. See [Section 15.1, “Ports and Encryption used”](#), on page 1027.

5.7 Automatic Client Update

The mechanism for automatically updating the clients is based on the MSP. For this purpose, the setup packages must have been selected during the server installation, thus being available. The administrator can check this in the *Web Assistant*. The clients are displayed there with version number, so that the administrator can install or update the clients from there also manually.

Upon start, the MSP AutoUpdate Client (`MSPAuClnt`) checks whether at least one XPR server is configured in the MSP. If so, then the first XPR server found is used as update server. If not, then the MSP configuration dialog is started, so that you can specify an XPR server. The XPR server used in key

`HKCU\SOFTWARE\CYCOS AG\AutoUpdate` is stored in value `Server`:

Server [REG_SZ]

Default:	–
Possible values:	XPR server name

The XPR server used for client updates. If several XPR servers are configured on the MSP, then the first one found is entered here and used. If the client setup packages are to be taken from another XPR server, you can change this here.

The *AutoUpdate* application starts automatically when the user logs on. For this purpose it is entered in the registry value

`HKLM\Software\Microsoft\Windows\CurrentVersion\Run`. Checking for new clients starts after approximately 1 to 2.5 hours. Thereafter, the checking interval is approximately three hours. If a new version for an installed client is found, then you receive this information via a speech balloon in the notification area of the task bar. Depending on individual privileges the user can either install the current clients or is only informed and needs to contact his/her administrator.

You can set the functionality via the registry values [AutoUpdate \[REG_DWORD\]](#), [AutoUpdateNoAdmin \[REG_DWORD\]](#) and [AutoUpdateNotification \[REG_DWORD\]](#).

[Table 8](#) shows the clients supported by this function. Other clients such as *optiClient* or *Communications* have implemented automatisms, which come to bear when you log on to these clients. Many of the clients listed here are not logged on to the XPR server. For them, the external update option was created.

Client	Folder
Fax-MAPI	FaxMapi
Lotus Notes Conference Plugin	LnConfPlugin
Lotus Notes Fax Extension	LnFax
Lotus Notes ActiveX Extension	LnActiveX
Local Outlook Forms *	LocalForms
Outlook Conference Plugin	OIConfPlugin
Server based Forms Client Components for Outlook	SBFCC

Table 8 *Supported Clients of the AutoUpdate Feature*

* The local Outlook forms require another step. To this, `FormRegister` is automatically started at the next login with the parameters S (Silent) and U (Auto Update).

IMPORTANT: If Microsoft Outlook is started automatically, the local Outlook forms cannot be automatically updated at the next login. The invocation of `Formregister` also attempts to start Outlook and closes the already started Outlook in this process.

The only remedy here is to remove the registry value **Formregister.exe** (REG_SZ) under HKCU\Software\Microsoft\Windows\CurrentVersion\Run. However, this also disables the automatic update of the local Outlook forms.

6 XPR Monitor

The XPR monitor is used for displaying status, performance, diagnostic, etc. messages for the complete XPR system. The configuration of individual XPR components is also done through the use of the monitor.

The monitor can be started from any Windows XP/7/2003/2008 computer within the network, so that the XPR server can be comfortably administered. With the XPR server installation a share is implemented from which you can start the monitor when you do not operate the XPR server itself.

Remote maintenance can also be performed by trained personnel without having to be onsite using the Remote Access Service (RAS) from Windows.

6.1 Security

Working with the XPR monitor requires logging in at the XPR server. Via the log-in options you can specify whether this logging in is to be permanent for a session or is to become automatically invalid after a configurable period. The last option is considered useful, for example, to prevent unauthorized users from accessing the XPR server via this XPR monitor after an authorized person has logged in at the XPR server by accessing the computer with the started monitor.

Accessing the XPR server requires at least the *Service Privilege*. This privilege offers only restricted options since specific configuration alternatives or registers are not displayed or are deactivated. In section [Section 6.12, “Access Overview of the Configuration Modules”](#), on page 183 you find an overview of the configuration tabs you can edit with the *service privilege*.

The account of the user who wishes to log on to the XPR server via the XPR monitor must belong to the group of local administrators on the XPR server. The reason for this requirement is among other things that configuration changes may otherwise not be written in the registry.

Configuration is unrestricted when you log on with the *supervisor privilege*.

6.2 Configuration Lock

If a configuration module has already been opened in a running XPR monitor entity, you will receive a note in every further entity upon the attempt to open this configuration module as well. This note contains the user and computer on which the configuration module has already been opened. To avoid inconsistencies caused by parallel processing, the configuration module will not be loaded on further entities in such a case.

If you have the *Supervisor Privilege*, you will, however, be enabled to lift this lock. In this case the configuration module will be loaded and the connection from the XPR server to the first XPR monitor entity closed. This causes the configuration module to shut down there with an error report.

Unfortunately, the configuration module cannot differentiate between a possibly collapsed network connection to the XPR server or somebody having lifted the configuration lock.

6.3 Operation

After its installation, the XPR monitor displays by default data of the local XPR server running on the local computer. This information is provided in the monitor windows **Modules of <server>**, **Lines**, and **Default Logging**.

All components installed within the XPR server are displayed in the **Modules of <server>** window. A topic area is assigned to each component where log information can be displayed. If a log report is generated that has no topic area, this report would appear in the general *without topic* section. In the logging window all general information, error, and warning reports are displayed. If you want to add a component or have special debugging information for error analysis at a later date, the desired topic can be seized with the left mousebutton kept pressed and dropped in a **logging monitor**. A dialog is then opened in which the filter for the selected topic can be configured.

All components that administer lines are displayed under Lines. As with the logging information, lines can also be moved to a **line monitor** per drag&drop and displayed there. The line monitor displays all lines. When a connection is set up on a line, you can see this in the line window. In there you can see the corresponding information such as the called fax number.

The last entry found in the **Modules of <server>** window is the *Settings* option. Configurable components can be configured here.

The **Toolbar** and **Status Bar** can be switched on or off under the menu entry **View**.

Fast access to many of the monitor's functions can be found by clicking on the icons within the toolbar. A short description of the icon's function appears (QuickInfo), when the mouse pointer is positioned over the icon.

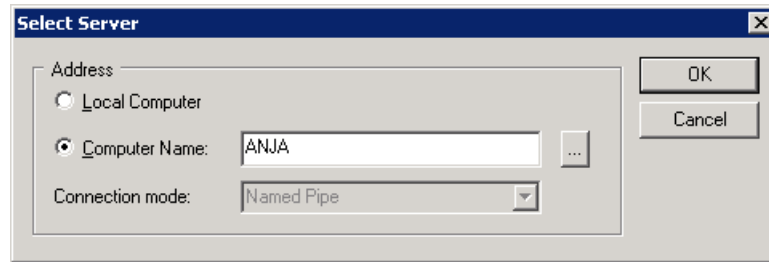
Current date and time are always displayed in the status bar.

Following this general introduction of the XPR monitor features, a review of all monitor possibilities will be presented. This will be accomplished by creating a complete monitor-layout. Any of the delivered monitor layout examples may also be used.

6.4 Creating a new Monitor Layout

In the following a new monitor layout for an XPR server will be created. Throughout the monitor setup, important concepts and various configuration possibilities of the XPR monitor will be demonstrated.

First, we create a new monitor layout and select the computer where an XPR server is running. In the example, the computer named *Anja* has been selected on which an XPR server named *Anja* is running.



A window now opens in which all components of the server are contained. A component consists of:

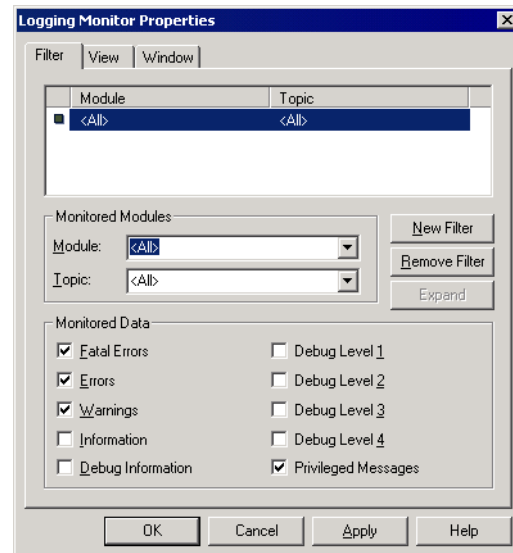
- Topics, which categorize the logging outputs of the component
- Lines, which represent the physical and logical connections.
- Settings, with which components configurations can be viewed and modified.

At the top of the list is the name of the XPR server and the connection status. Individual monitor windows can be created for lines and topics. The individual monitor windows can either be confined within the monitor, or placed independently within the user interface. The last-mentioned (floating monitors) are visible even when the XPR monitor is minimized.

6.4.1 Configuring a Logging Monitor

Next, we define a logging monitor in which error reports, warning messages, and general information of all modules will be displayed.

Select **View** followed by the **Logging Monitor** entry. After the appearance of the new monitor, click with the right mouse button to invoke the pop-up menu and select the **Properties** dialog.



On the **Filter** tab, select the **New Filter** button for all components and topics. In the **Monitored Data** section check the entries Fatal errors, Errors, Warnings and Privileged messages. The last-named are selected messages additionally flagged. The developer can add this flag to any sort of message. In this way it is possible to see important info messages even if the info messages as such have been deactivated.

If you want to install a logging monitor for specific APL topics, you can also select a module and click on **Expand**. For each topic of this APL an individual filter entry is generated then. Those not needed can be deleted. With several APL topics required this procedure is normally less time-consuming than defining each of these filters separately.

In the **View** tab of the logging monitor properties window a file name may be entered so that all protocol information is simultaneously logged for evaluation at a later date.

If several logging monitors are to be created, a unique name must be entered for each monitor for the log file! A font as well as various font colors may be used to separate the various types of **Monitored Data**. In this manner, error reports could appear in red to enhance their visibility.

In the **Window** tab of the properties dialog a title can be assigned to the monitor describing its function. This name is then displayed in the window's title bar. By checking the **Show Caption** entry, the monitor title is displayed in the title bar of

the monitor thus reducing possible confusion when numerous monitors are in use.

Please refer also to Installation Guide

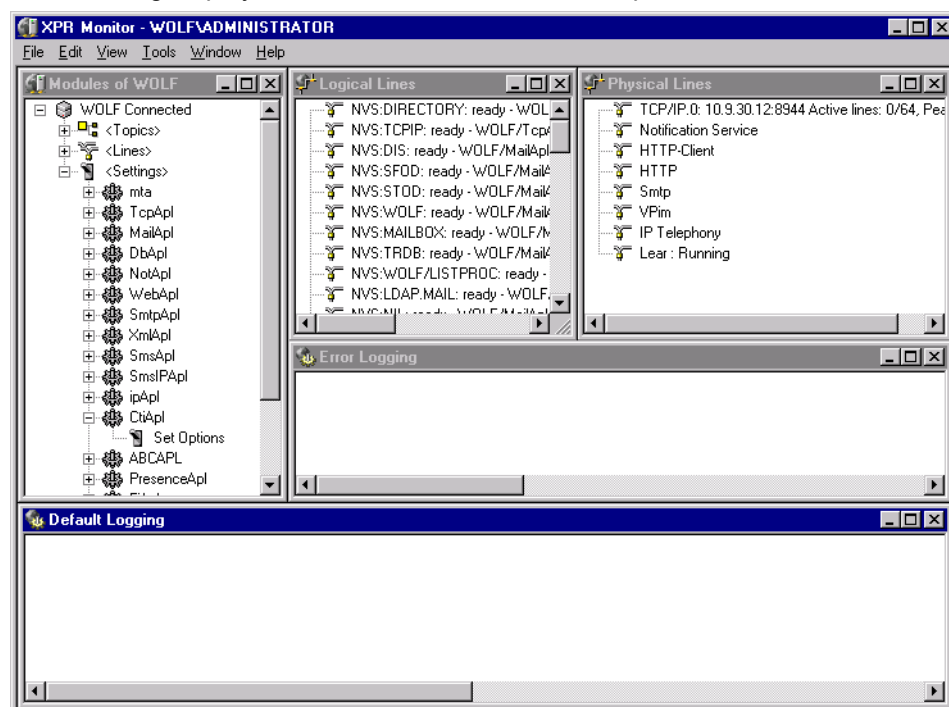
section 6.4 Local Status Dispatcher Server on Satellite Computers.

6.4.2 Configuring Line Monitors

The Access Protocol Layer converts physical lines into logical lines. A physical line is defined and provided by an external network. It is represented by a port (network hardware). A logical line is independent from the external network and is determined by the network type and protocol. They are represented through `NODE` and `CLASS` of an NVS address. With the exception of the Access Protocol Layers, the complete XPR server works exclusively with logical lines. If the network has the appropriate protocols, then a physical line can be composed of many logical lines.

Two monitors will now be configured for displaying physical and logical lines. The MTA (Message Transfer Agent) module administers all logical lines. Therefore, we can simply create a new **line monitor** and drag the MTA lines from the module window into this new window by drag&drop. The other modules administer only physical lines, if any at all. The creation of a new line monitor for physical lines is the same as for logical lines with the exception that the MTA module is excluded from the filter settings.

The resulting display of the XPR server is here as depicted:



6.4.3 Saving Monitor Layouts

The monitor layout can be stored and later loaded for use on another computer through use of the menu entry **File > Save As Template**. The XPR server name can be changed for further applications with the layout. For example, if you created the layout for the local computer, it can also be reused again for another computer in the network.

If, in contrast, you save with **File > Save As...**, the set XPR server will be saved as well. Loading this file immediately opens the view on the set XPR server.

If you want to immediately start the XPR monitor with a selected or generated layout on your computer with each log-in, create a shortcut with the `MrsMon.exe` file in the autostart directory and specify the layout that you have saved as parameter.

6.5 Default-Layout Options

Every new window is assigned the default settings as specified under **Tools > Options**. These settings may be changed at a later time for each individual window, as described above for the monitor windows.

6.5.1 Modules

This portion of the monitor is used to configure the default appearance of the Module window. In the **Display automatically** section, sub-trees are selected, which are to be displayed in the expansion. Furthermore, we can toggle the sorted by modules and sorted by type (topics, lines and settings) display on the right hand side. For both arrangements you can default set a configuration.

The type of sorting used for the creation of a new module window depends on the entry in the menu option **Sort**.

When sorted by type, all topics, lines and settings are sorted into three groups and displayed. When sorted by modules, topics, lines, and settings are displayed under their various modules.

Various reports from the modules are found under Topics. General reports without specifically assigned topics are filed under *Without topic*. Further topics are provided by the modules for special topic areas, in which targeted report selection is possible. All lines administered by the modules are physical lines with the exception of the MTA (logical lines only). Component configuration and validation is performed under Settings.

When **Drag&Drop** is activated, the properties are automatically displayed. Now when a new monitor is created and a topic inserted with the drag&drop method, the properties dialog automatically appears for immediate configuration and individual adaptation of the monitor window.

6.5.2 Line Window

For lines, two configuration tabs, **Window** and **Filter**, are available. The Window tab allows the assignment of a name or caption to a new line monitor as switching on or off the caption bar. These configurations can be individually adapted for other line monitors.

In the **Filter** configuration tab, the entry **Display sub-lines automatically** determines whether sub-lines are automatically shown for the displayed lines.

Connections are defined through the displayed data in the **Data to be displayed** section. Various parameters can be selected for defining the connection: Line State Information, Remote/Local Address, Cost, Baud Rate, Error Rate, Incoming/Outgoing Bytes, Total Bytes to Send, Incoming/Outgoing Pages, Total Pages to Send.

Not every line provides all this information, as e.g. the Baudrate is not available in case of a local connection in the network. This information would be of interest, though, with a modem connection.

6.5.3 Logging Monitor

For the configuration of logging monitors three configuration tabs, **Filter**, **View**, and **Window** are used. In the Window configuration tab you can default set the caption for a new logging monitor and switch on or off the caption bar. These configurations can be individually adapted for other line monitors.

The displayed information that assigns a new logging window by default can be selected in the **Logging Filters** tab. The following options are available:

- *Fatal Errors*, which normally lead to module termination.
- *Errors*, which are non-critical. In most cases the module can put itself back into a functioning state.
- *Warnings*, which find fault with e.g. configurations that are inconsistent and must be corrected by the module.
- *Information*, which report about normal module operation.
- Various levels of *Debug Information* used by developers and service personnel for diagnostic purposes. For the average user these reports are meaningless.

NOTE:

To show *debug information* you need the *Supervisor Privilege*.

The choice of default topics is *All topics* and *Without topic*. In most cases the entry <All> should be selected since each module has special topics defined for its output and a categorical distribution is then possible.

The actual appearance of a logging monitor is set in the **Logging Display** settings dialog.

Fonts can be selected as well as font color assignment for the various report types (F - fatal error, E - error, W - warning, I - informational, debug info, debug levels (1-4)). Through the use of the various colors the gravity of a report can be recognized at a glance.

The background color of the logging monitor can be changed using the **Background Color...** button.

Selection of the **Reset** button returns all values to the preset defaults. This is different to the properties dialog of a specific logging monitor in which **Reset** resets the settings to the values set here.

A specialty is the **RotoLogger** option which can be selected to limit the size of log files and simultaneously to specify the number of log files to be stored. Especially when looking for a very rare error or for one that occurs after many hours of extreme server load, the debug log file would become exceptionally large. Of interest is, however, only the last detailed information delivered by the occurrence of the error sought-after. Therefore, the log files are overwritten by the RotoLogger using the Round-Robin method, so that the maximum size entered for all log files will not be exceeded. You can have created up to 5 GB in up to 500 log files. We recommend to set the parameters in a way that a single log file does not exceed the size of 10 MB. To activate the RotoLogger you must enable the **Log into File** option for the corresponding log window.

6.5.4 OpenScape Voice Trace Manager (OSVTM)

The OSVTM collects the log data of different applications centralized. The XPR server can send its log data to OSVTM. This requires configuring the following parameters under **Settings > Options > OSVTM**:

Server Address, Element Name, Node ID, Path, User and Password. You receive all of these parameters from the OSVTM. As soon as you have made the respective entries, the XPR server sends the log data of the IP APL with the categories *Fatal errors, Error, Warnings* and *Privileged messages* every five minutes. The last-named are selected messages additionally flagged. The developer can add this flag to any sort of message. In this way it is possible to see important info messages even if the info messages as such have been deactivated.

You can set the intervals via [DiagPeriod \[REG_DWORD\]](#) and the filter via [DiagFilter \[REG_MULTI_SZ\]](#).

6.6 Main Log File

Filter settings for the main log file are configured in this dialog. This log information is always included with the main log file. You can export and import the filtering settings for the main log file. You need the *Supervisor Privilege* to edit the main log file filter.

6.7 Active Alert

Filter settings for Active Alert reports generated by the MTA. For this function no debug reports are selectable, though. See [Section 7.1.1.3, “Active Alerts”, on page 193](#). All of the log reports listed in this dialog can be used for active alerts. Active alerts could be used, for example, to report an error to an administrator or the accountable service hotline.

IMPORTANT:

Activation of the **Information** filter setting generates a high load. We recommend not to use this setting in an active system.

6.8 Logging Profile

With logging profiles the service can write appropriate log settings in a file when problems occur. A customer administrator only needs to open this file, so that an analysis of the occurring problem can be written in an appropriate log file.

Invoke the **File > Logging Profile > Create** menu option for the creation. A **free logging monitor** is created and the dialog for setting the filter properties opens. In this dialog you need to perform all necessary settings. In particular, you can already set a path and file name for the log file. In the event that this path does not exist or the logged-in user does not have write privileges when the logging profile is opened at a later date, a new path and file name will be queried. As soon as you close the properties dialog with **OK**, you need to save the created logging profile.

IMPORTANT:

You cannot modify the created logging profile. Logging profiles must always be completely created anew in one step.

You can open a logging profile via the **File > Logging Profile > Open** menu option. The profile opens with the defined properties as free logging monitor. If a log file has been defined in the properties, logging starts in this file immediately. In case the set path does not exist or the logged-in user does not have write privileges there, a new path and file name will be queried.

If required, open the **Properties** via the context menu of the free logging monitor and see on the **View** tab in which log file entries are made.

6.8.1 The Default Log Profile

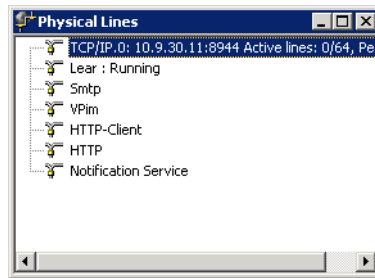
Store a log profile on your desktop under the name `PLogDefinition.mlp`. You can now use the **pLog** button in the toolbar to activate/deactivate this log profile. If required, activate the toolbar via **View > Toolbar**.

The output is automatically stored in a file on the desktop. The file name follows the pattern `PLogYYYYMMDDhhmmss.log`.

6.9 Monitor Usage Examples

6.9.1 Line Monitor

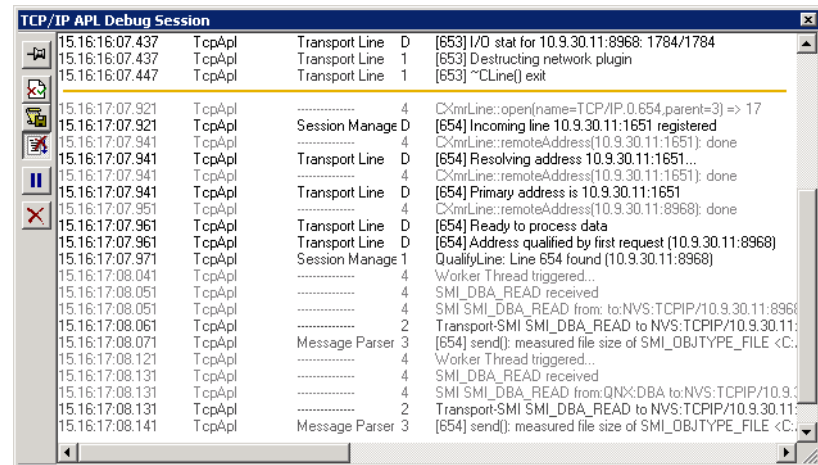
The XPR monitor can be used in a number of different situations. It can, for example, be applied as a type of activity monitor in which only the activity of the physical lines is displayed in a small window. For this purpose generate, as above, a new monitor layout with a server view. Subsequently, create a floating line monitor (**View > Floating Line Monitor**) in which all physical connections are displayed, and minimize the XPR monitor. Even when the monitor is minimized, the floating monitor remains open and is not minimized.



All floating line and logging monitors can have their own toolbars. These **toolbars** are activated by a click with the right mousebutton within the window, and subsequent selection of this option.

6.9.2 Special Analysis Session

If a specific module is to be under close examination, you create an individual log window for this module. You channel all possible module outputs into this log window, thus you activate all possible output filters for this component.



In the above free logging monitor, this has been done for the TCP/IP APL. Press the spacebar to insert a line in the logging window as a visual separation for the easy identification of test phases. Thus you can quickly find the beginning of the test later on.

6.10 Local Installation

On each computer where XPR server modules are installed, a share MrsMonitor to the configuration DLLs of these components is automatically installed as well. On the kernel computer you then also find in this directory the actual XPR monitor.

We recommend to configure a link to the `MrsMon.exe` file in the MrsMonitor share of the kernel computer. The XPR monitor will thus always be started by the server. In this way you automatically receive the correct version with an XPR server update.

In addition to the files that can be reached via the share, a Xerces-DLL is required on the local computer. The XPR server must copy this DLL from the `<Windows Install>\System32` directory to the corresponding directory on the local computer. Please note that several versions of this DLL may be available. If required, copy all DLLs that you find under `Xerces*.dll`. During an update you need to copy these files again, as a newer version might then be used.

The XPR monitor always loads a required configuration DLL from the computer where the APL to be configured or the kernel component runs. For this purpose it is loaded from the corresponding share on this computer. Consequently, version conflicts are avoided when you have e.g. a local, deviating version of this configuration DLL. This case might occur when you administer several XPR servers of a different version status with one XPR monitor.

NOTE:

If required, the packet `vcruntimeinst.exe` from the `XpressionsInstall\Prerequisites` folder of the product data carrier must be installed previously.

If you want to install the XPR monitor on a local computer (not recommended), copy the files `MrsMon.exe`, `MrsRsrc.dll` from the monitor share of a kernel computer and for the online user assistance all files with suffix `chm`. The above Xerces-DLL must be copied to the local computer. During an update these files must be copied again.

6.11 Remote Desktop Connection Specials

If you access the server via a remote desktop connection, always set **Remote computer sound** to **Leave at remote computer** on the **Local Resources** configuration page.

Especially in case of the IP APL, which works with different TAPI service providers, this will otherwise lead to malfunctions.

6.12 Access Overview of the Configuration Modules

The following table provides an overview of the configuration modules that definitely require the *supervisor privilege* and of the respective configuration module tabs that are offered to a service administrator (see [Section 2.4](#), “[Staggered Administration](#)”, on page 72) with *service privilege*.

Component	Description
ABC-A APL (ABCAPL)	<i>Service privilege</i> required.
Computer Telephony Integration APL (CTIAPL)	<i>Supervisor privilege</i> required.
Database APL (DBAPL)	<i>Service privilege</i> required.
Microsoft Exchange 2003 APL (E2KAPL)	With the <i>service privilege</i> only the General and Normalization tabs can be edited.
Microsoft Exchange 2007 APL (E2K7APL)	<i>Supervisor privilege</i> required.
File Interface APL (FIAPL)	<i>Supervisor privilege</i> required.
HiPath Management APL (HPMAPL)	<i>Service privilege</i> required.
Integrated Services Digital Network APL (ISDNAPL)	With the <i>service privilege</i> only the Protocols , Voicemail , Extensions , Device , Locations and Outbound tabs can be edited. Via the Device tab you can access the restricted NCO Administration .
Internet Protocol (IPAPL)	With the <i>service privilege</i> only the Protocols , Voicemail , Extensions , Device and Locations tabs can be edited. Via the Device tab you can access the restricted NCO Administration .
Lightweight Directory Access Protocol APL (LDAPAPL)	With the <i>service privilege</i> only the Properties of an existing connection can be invoked. Only the Login and Search tabs of this connection can be edited.
Lotus Notes APL (LNAPL)	<i>Service privilege</i> required.
Mailbox APL (MAILAPL)	With the <i>service privilege</i> only the Printer Embedded Codes and Advanced tabs can be edited.
Notification Module (NOTAPL)	With the <i>service privilege</i> only the Format and Internal Settings tabs can be edited.

Component	Description
Presence (PRESENCEAPL)	<i>Service privilege</i> required.
Print APL (PRINTAPL)	<i>Service privilege</i> required.
Report APL (REPAPL)	<i>Service privilege</i> required.
Report Schedule APL (REPSCHEDULEAPL)	<i>Service privilege</i> required.
SAP R/3 APL (SAPAPL)	<i>Service privilege</i> required.
SAPphone APL (SAPPHONEAPL)	<i>Service privilege</i> required.
SAP Business Routing APL (SAPROUTEAPL)	<i>Service privilege</i> required.
SMS Connector (SMSIPAPL)	<i>Service privilege</i> required.
Internet Mail APL (SMTPAPL)	With the <i>service privilege</i> only the SMTP Server , Outbound Mail , POP3 Server , IMAP4 Server and Secure Sockets tabs can be edited. The SMTP Server tab only makes available the Advanced option.
TCP/IP Transport APL (TCPAPL)	<i>Service privilege</i> required.
V.24 APL (V24APL)	<i>Service privilege</i> required.
Virtual Machine APL (VMAPL)	<i>Service privilege</i> required.
Wall Display APL (WALLAPL)	<i>Service privilege</i> required.
Web Server APL (WEBAPL)	With the <i>service privilege</i> only the CGI , SSL and Firewall tabs can be edited.
Web Services APL (XMLAPL)	<i>Service privilege</i> required.

7 Message Transfer Agent (MTA)

The MTA is the central router, through which all messages in the XPR system must pass. The default configuration of the server is sufficient for most applications. If any modifications to the system must be made, these should only be implemented by an individual that is extremely familiar with the system. This is particularly applicable to *Routing Rules* modifications.

7.1 Configuration

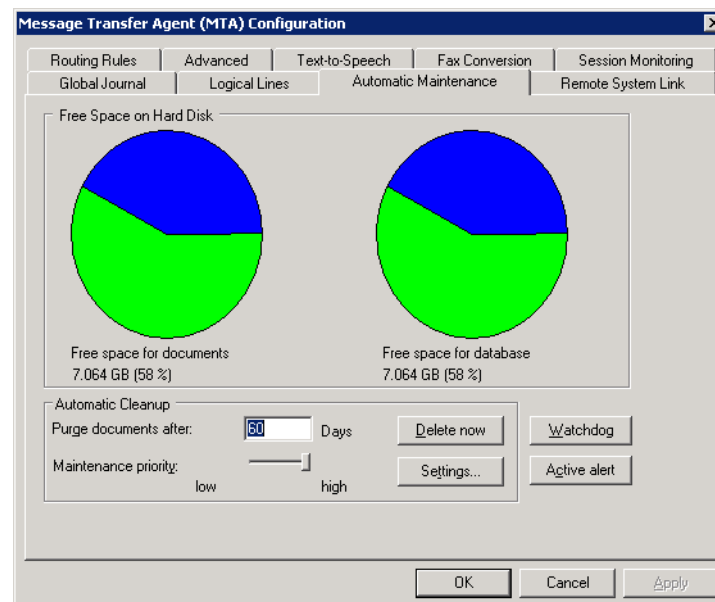
The configuration is performed from the XPR monitor as usual. The configuration dialog is started by double clicking on the **Set Options** entry in the Modules window under **<MTA/Settings>**.

NOTE:

An administrator with *service privilege* only sees the **Automatic Maintenance**, **Global Journal**, **Logical Lines**, **Text-to-Speech** and **Fax Conversion** tabs. On the **Global Journal** tab the **View** and **Forward** features are not available to him/her.

7.1.1 Automatic Maintenance

The circles display the amount of available free storage space for documents and the database.



7.1.1.1 Automatic Cleanup

This option allows the server to remove any documents which exceeded the specified time limit. Through use of the **Purge now** button an immediate setting modification can be triggered as well. This is especially useful with acute shortage of storage space. Otherwise a modification would not take effect until the next performance of the corresponding maintenance script job.

NOTE:

The MWI signal will not be reset if unread documents are deleted via this mechanism. To reset the MWI signal just the same, adjust in the **Settings** further below the value **Purge unread documents after ... days** to a smaller value than the deletion time specified here.

With the **Maintenance priority** option these purge operations and all other routine maintenance jobs are executed with the set priority. If computation bound processes such as simultaneous voicemail user service occur along with the maintenance script, a low priority should be chosen.

Further maintenance options are available for the maintenance script through selection of the **Settings** button. These options greatly influence the amount of free storage space on the server.

Maintenance Cleanup Options

Remove Database Entries and Documents

- ☐ Remove MWI indication after days.
Script variable: \$(LifeTimeService)
- ☐ Remove pass-through documents after days.
Script: \$(LifeTimePassthrough)
- ☐ User defined parameter days.
Script: \$(LifeTimeUserdefined)

Compression

- ☐ Representation and voice compression after days.
Script: \$(LifeTimeCompress)
- ☒ Do Not Compress (DNC-Driver) 8000 Hz Mono

Remove Documents

- ☐ Purge e-mail after days.
Script: \$(LifeTimeEmail)
- ☐ Purge outbound documents after days.
Script: \$(LifeTimeOutbound)
- ☐ Purge inbound documents after days.
Script: \$(LifeTimeInbound)
- ☐ Purge read documents after days.
Script: \$(LifeTimeRead)
- ☐ Purge unread documents after days.
Script: \$(LifeTimeUnread)
- ☐ Purge documents flagged as deleted after days.
Script: \$(LifeTimeDeleted)

NOTE:

The descriptions of the setting options available on the **Maintenance Cleanup Options** tab refer to their use in the unchanged maintenance script. As soon as the maintenance script is modified and the variables are used in other applications, their meaning changes immediately.

NOTE:

Adapted to the following options, “purging” means that the actual document will be replaced with a short administrative note. The transaction process in the journal database, however, is maintained, so that, for example, the charge information can be further evaluated or the MWI signal reset. In the event that the document as well as the journal entry are purged directly, you will be explicitly informed.

Remove Database Entries and Documents

- **Remove MWI indication after ... days**

Each MWI notification of a new message corresponds under XPR to a send job. Consequently, a document is also stored on the server with setting an LED on the telephone. This option deletes the document as well as any corresponding database entries. The corresponding rule in the maintenance script reads:

```
Delldb record=Journal age=$(LifeTimeService) recipient=NVS:CIT
Delldb record=Journal age=$(LifeTimeService) recipient=NVS:MWI
```

- **Remove pass-through documents after... days**

This option deletes all documents transmitted from one non-interactive service to another non-interactive service. All non-interactive services are defined in the registry value [NonInteractiveServices \[REG_SZ\]](#). From the XPR server point of view a non-interactive service is a service with which the flag `DELREC` (Deleted by Recipient) is never set. This is e.g. the case for fax G3. Here the server will never receive a status report about the recipient purging the document.

So if a document arrived at the server via the fax G3 service and this document was then sent to another fax number via the fax G3 service after application of the routing rules, it would be a “pass-through” document. The corresponding document will consequently be purged after the number of set days.

The corresponding rule in the maintenance script reads:

```
Delldb record=Journal age=$(LifeTimePassthrough)
originator=$NonInteractive recipient=$NonInteractive
options=FILEONLY
```

- **User defined parameter**

This option sets the \$(LifeTimeUserdefined) variable, which can then be used in customized delete commands in the maintenance script.

Compression

The **Representation and voice compression** option removes after the set number of days the conversions created for representation on clients or for transmission. Only the original document is kept on the server. The audio codec set under **Codec** is used to compress voicemails. In this way voicemails can later still be played with a possibly inferior quality. They need, however, much less space on the server harddisk. The XPR server always uses 8 kHz/Mono. Therefore, only audio codecs are offered for selection as they meet this requirement. We recommend MS-ADPCM (factor 1.95), TrueSpeech (tm) (factor 7.5) or the MPEG Layer-3 Codec (factor 4 to 8), since these codecs are supplied with the current Windows operating systems.

NOTE:

This voicemail compression only affects the XPR message store. It works, for example, in a voice-only scenario. In an integrated-messaging scenario the messages would be compressed in the XPR message store, but not transmitted to the foreign system (Microsoft Exchange or Lotus Domino). The uncompressed voicemail is thus maintained there. In a True Unified Messaging scenario the messages are stored in the foreign system only. A compression is not possible at a later date.

NOTE:

Besides the later compression the codecs setting is also responsible for direct compression. Direct compression is available for Integrated as well as for Unified Messaging and applies with the arrival of a message. It is used for all voicemails transmitted by the XPR MTA, i.e. all voicemails recorded by Forward and Guest Access. Direct compression cannot be used with messages directly generated in foreign systems (Microsoft Exchange or Lotus Domino) by True Unified Messaging. These are all messages recorded in Direct Access. With the Exchange Gateway direct compression is set in the **Formats** tab as audio format by exclusive selection of the **WAV compressed** format. With the Lotus Notes Gateway only **Windows Wave compressed** is set as audio format in the **File Formats** tab.

Removing documents

- **Purge e-mail after ... days**

All documents the status of which has been set to purge by the originator as well as by the recipient are purged. These could be for example, documents sent from one mail gateway to another. The corresponding rule in the maintenance script reads:

```
Delldb record=Journal age=$(LifeTimeEmail)
recipient=$Interactive originator=$Interactive
flags=DELOG,DELREC options=FILEONLY
```

- **Purge outbound documents after ... days**

All documents sent by the XPR server to a non-interactive service are purged. All non-interactive services are defined in the registry value [NonInteractiveServices \[REG_SZ\]](#). The corresponding rule in the maintenance script reads:

```
Delldb record=Journal age=$(LifeTimeOutbound)
recipient=$NonInteractive flags=DELOG options=FILEONLY
```

- **Purge inbound documents after ... days**

All documents that have reached the XPR server via a non-interactive service are purged. All non-interactive services are defined in the registry value [NonInteractiveServices \[REG_SZ\]](#). The corresponding rule in the maintenance script reads:

```
Delldb record=Journal age=$(LifeTimeInbound)
originator=$NonInteractive flags=DELREC options=FILEONLY
```

- **Purge read documents after ... days**

Documents the user has read are deleted. The corresponding rule in the maintenance script reads:

```
Delldb record=Journal age=$(LifeTimeRead) flags=READ
options=DELETESOFT
```

- **Purge unread documents after ... days**

Unread documents are also deleted. This is useful especially in networked systems in which messages are forwarded via a central distributor to the other systems. The messages would not be read by a central distributor or could be deleted after being forwarded to the target system. Furthermore, the MWI signal is not reset if an unread documents is deleted completely. Therefore, adjust this value to a smaller one than the time set for **Purge documents after** if possible. An unread document is then replaced with a short administrative note after the time set here. This resets the MWI signal. Subsequently, the document can be removed completely. The corresponding rule in the maintenance script reads:

```
Delldb record=Journal age=$(LifeTimeUnread) flags=!READ
options=DELETESOFT
```

NOTE:

In PhoneMail you can configure that users are warned a few days beforehand, if messages they have not yet listened to are to be deleted. See parameters "mwtd" in [Section 10.4.3.13, "Parameter Tab Customer"](#), on page 651.

- **Purge documents flagged as deleted after ... days**

Deviating from the above note, journal information is purged as well when this option is activated. The documents deleted by the recipient will be purged.

The corresponding rule in the maintenance script reads:

```
Delddb record=Journal age=$(LifeTimeDeleted) flags=DELREC
```

Improvements in a TUM environment

The task group *RemoveOldAndCompress* can be improved in an Exchange-TUM environment in the following:

Insert the middle of the following lines as shown here:

```
Delddb record=Journal age=$(LifeTimeService) recipient=NVS:MWI  
Delddb record=Journal age=3 finalrecipient=NVS:EXCH  
Delddb record=Journal age=$(LifeTimeInbound)  
originator=$NonInteractive flags=DELREC options=FILEONLY
```

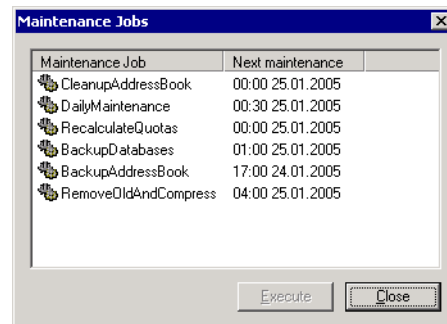
With this modification all messages successfully delivered to Exchange are removed from the XPR server after three days. Consequently, this modification relieves memory in an Exchange-TUM environment. This rule can also be used in a multiline environment as specified here.

If the message is still in the send queue, it will not be deleted.

This modification can be performed analog for Lotus Notes.

Jobs

Jobs defined in the maintenance script are displayed in this dialog along with their upcoming execution time.



An immediate execution of the job is possible through selection of the job and subsequent selection of the **Execute** button.

Selection of the **Close** button returns the user to the Maintenance Clean-up Options dialog.

Stop jobs

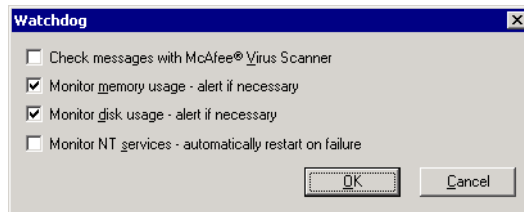
Via this button you can terminate all currently running maintenance script jobs.

Load script

If you have modified the maintenance script, press this button to reload it so that the modifications are copied. Note that with an XPR server update a modified script would be overwritten again by the script default version. To avoid this, save the modified version under a different name in the *<XPR Install>\res\maint* directory. This new name with the complete path specification should then be entered in the registry value [MaintenanceScript \[REG_SZ\]](#) in key `HKLM\SOFTWARE\Wow6432Node\PP-COM\MRS\MTA`.

[Section 7.2, “Maintenance Script”, on page 214](#) lists all maintenance script options.

7.1.1.2 System Monitoring



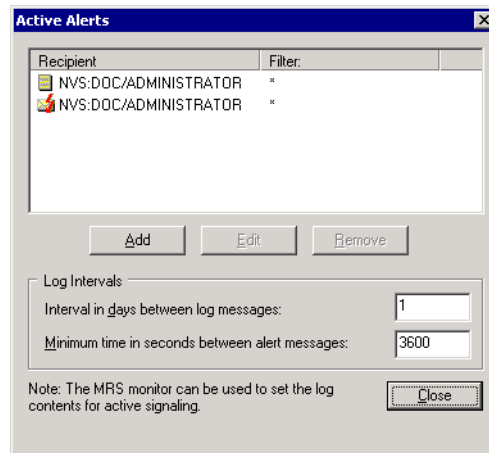
Several surveillance functions can be set here.

On the one hand you can monitor memory usage (RAM) and hard disk capacity. When the available memory/hard disk capacity is depleted to a critical point, a warning/error message is issued.

XPR services can also be monitored on process level, and restarted in the event of a crash. This may take some manually adjusting the Windows Registry, though. See [Section 7.5, "Watchdog Process"](#), on page 267.

The **Check messages with McAfee Virus Scanner** is obsolete.

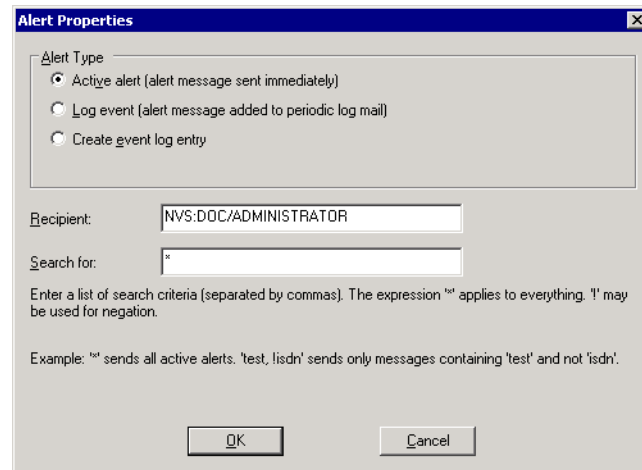
7.1.1.3 Active Alerts



Through the use of active alerts, the surveillance of all log messages to the XPR monitor is possible. By applying various search criteria to the messages, warnings can be sent, routine status reports containing all error messages can be sent, or a notification can be written in the Windows event log.

Before active alerts can be used, the global filter in the XPR monitor must be configured for their use. This is performed much in the same manner as with the global log files. Messages will only be generated when one of the filter conditions specified here has been satisfied. Under Log Intervals, the Interval in days between log messages is entered. Minimum time in seconds between alert messages is also defined in this portion of the dialog. This entry prevents reoccurring reports from being continuously sent.

Alert Properties

The image shows a Windows-style dialog box titled "Alert Properties". It has a tab labeled "Alert Type". Inside the tab, there are three radio buttons: "Active alert (alert message sent immediately)" which is selected, "Log event (alert message added to periodic log mail)", and "Create event log entry". Below the radio buttons, there is a "Recipient:" label followed by a text box containing "NVS:DOC/ADMINISTRATOR". Below that is a "Search for:" label followed by a text box containing an asterisk (*). Underneath the search box, there is a small text block explaining search criteria: "Enter a list of search criteria (separated by commas). The expression '*' applies to everything. '!' may be used for negation." and an example: "Example: '*' sends all active alerts. 'test, !isdn' sends only messages containing 'test' and not 'isdn'." At the bottom of the dialog are "OK" and "Cancel" buttons.

If the **Alert Type** for a recipient/filter setting combination is set to **Active alert...**, a message is sent immediately when a log message of this kind occurs.

Log events are compiled and sent at regular intervals.

For **event log entries** no recipient can be defined since the entry is generated in the Windows event log. This alert type is suitable e.g. for further editing by an SNMP management tool. You find more information on this subject in [Section 7.10, "Simple Network Management Protocol \(SNMP\)", on page 290](#).

NOTE:

A recipient that had already been entered before you changed to the **event log** will later be displayed in the list. The corresponding entry is created in the event log just the same.

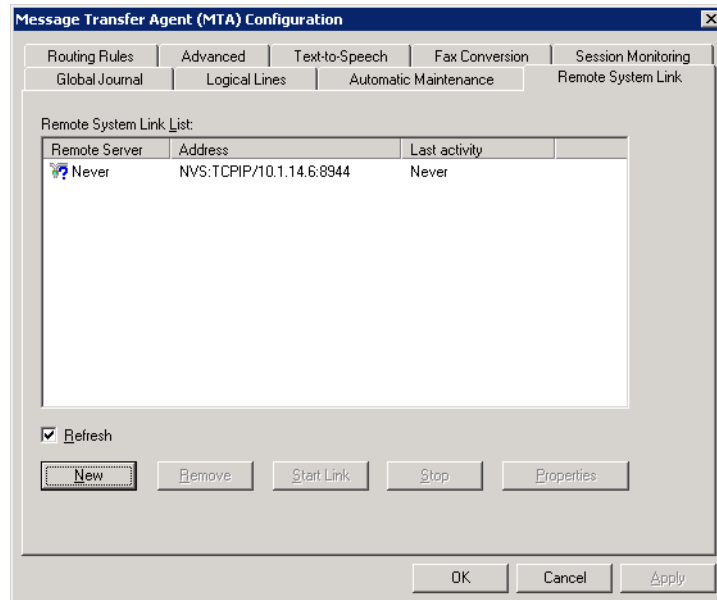
Any NVS address can be used as **Recipient** for a notification.

In the **Search for** field search criteria are defined that must be present in the log messages before the message is transmitted. The * character corresponds to all messages set in the XPR monitor for Active Alerts. An exclamation mark (!) that prefixes an expression means all messages that do not contain this expression. Numerous search criteria may be entered when separated by a comma.

7.1.2 Remote System Link

Connections to other XPR servers can be configured or removed via this dialog. Under the dialog entry **Last activity** the functionality of a connection can be checked anytime. Selected connections can be dynamically stopped or started when the server is live with the **Start Link** and **Stop** buttons.

It should be noted that lines imported over a remote system link from another XPR server are unidirectional. A bidirectional link between two XPR servers is only possible when a Remote System Link is executed by both servers to the other.



The option box **Refresh** ensures that the data displayed in the window is always current.

New connections are inserted in the dialog through use of the **New** button. Configuration of the new link is described in the following paragraphs. Existing links can be removed by selecting the link and subsequent selection of the **Remove** button.

7.1.2.1 Properties

The most important entry to mention in the **Remote System Link Properties** dialog is the **Address** of the other server. The NVS address of another XPR server is specified here. The service of this address must be an SMI transport. The TCP/IP APL, for example, provides such a SMI transport. See [Chapter 15](#), “TCP/IP APL”.

In the **Protocols** entry field you can either import all protocols from the remote server (empty field) or specific ones. All logical lines (protocols) of the remote MTA not having the *Local* attribute can be imported. More than one protocol may be entered when separated by a comma.

If the validation for remote connections has been activated on the **Advanced** MTA configuration tab, a password must be specified for each connection. This password must also be entered on the remote server. For this purpose, a pseudo user account must be created on the remote system with the name of this XPR server as user ID. The password assigned to this user account is entered here. Assign the following privileges to this user account:

- **Trusted Domain Privilege**
All jobs from the foreign system receive the privileges of this user account. Additional rights besides this privilege must be assigned so that a fax can be sent via the remote system, for example. This is easiest accomplished by assigning a user group to the user account.
- **Global Alias Editor**
This privilege is required for correlation data exchange (see further below). Thus remote system users on the individual XPR server can, for example, be automatically defined as contacts.

After validation of the connection there are in addition two options to grant privileges to the remote system users:

1. Users are entered in the database of both systems. In the database of the remote system an additional data field is configured for the name of the remote XPR server. For each remote system user an entry with the user's account name is created. This account name is also written in the newly created database field. The server now recognizes the user, and will correspondingly route messages in accordance with assigned authorities.

Example scenario:

Two XPR servers (`BRUSSELS` and `AACHEN`) are connected by Remote System Link. The user database from `BRUSSELS` is extended to include the data field `AACHEN`, and the `AACHEN` field is extended to include the `BRUSSELS` field.

If user `HUGO` in the `AACHEN` system wants to send a message to a user in the `BRUSSELS` system, this message is routed to the recipient by the `BRUSSELS` system since it knows user `HUGO` based on the following database entry and has the message transmission privilege via group assignment.

Database field	Content
USER	HUGO
Group	USER
Aachen	HUGO

The disadvantage to such a method is that user data in both systems must be maintained parallel to one another.

2. The second method is through the use of pseudo user accounts on both systems which receive the "Trusted Domain Privilege" each. The pseudo user is again assigned the name of the relevant remote system and should be granted the same privileges as the user on the remote system in addition to the "Trusted Domain" privilege.

Scenario: two systems (BRUSSELS and AACHEN) are connected via Remote System Link.

A user is configured on the BRUSSELS system:

Database field	Content
USER	AACHEN
Group	USER

Likewise, the system in AACHEN has the user:

Database field	Content
USER	BRUSSELS
Group	USER

In addition to the authorities of the group USER, both users are assigned the “Trusted Domain” privilege, so that authority of these users is inherited by all incoming documents of the remote system.

Assignment of a password is only necessary if validation is to occur via this password. If no connection validation is set, the password can be omitted. The advantage is that XPR does not allow users to log in at the server without password, so that the pseudo users generated in this way cannot be used as real accounts.

In the dialog entry **Poll rate**, the time interval is given in seconds. A value of 60 denotes that a connection will be attempted every 60 seconds. If no connection is established during the time interval indicated in **Time**, the next attempt is started after **rate** seconds. **Retries** is the number of times an attempt is made before a remote system link is deactivated.

If the option **Synchronize local server clock with remote server** is activated, the clock of the server making the remote connection will be set to that of the remote system. This could be of interest when establishing a remote system link to a server equipped with an atomic clock (DCF-77).

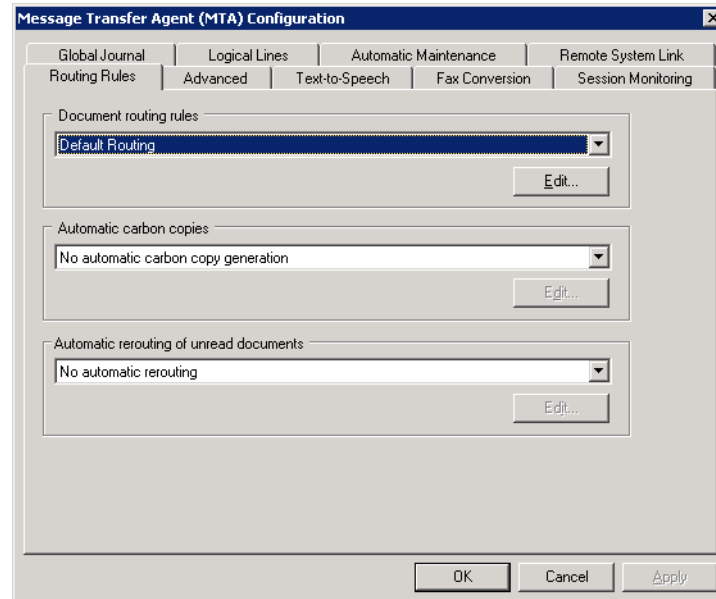
The correlation data can be replicated by the remote server. In this way the local information is overwritten by the information of the remote system, so that the entire user administration of both systems occurs on the remote system. You can specify the replication scope in the option fields in the lower portion of the dialog. Here you can select **User data**, **Distribution lists**, **System masks** and **CTI Journals**.

Please note that with the **Only users with SYNC<Node>** option only user accounts for which a corresponding switch has been set are replicated. This switch must first be inserted in the user database mask each. A database field of the CHAR type with length 1 (switch) must be created on the remote server for this purpose. Using this option the XPR server name may only consist of a maximum of 11 characters instead of 15. If the individual server was named DOC, a database field called SYNCDOC had to be installed on the remote server. Since a

remote system link is unidirectional, the settings must be performed on both XPR servers. This option is only active, if the user data replication is generally activated.

7.1.3 Routing Rules

The **Routing Rules** tab is essential for determining the MTA routing behavior. In the following you find a description of various presettings. If you want to customize the respective rules via the **Edit** button, make yourself familiar with the routing rules explanations in [Section 7.4, “XPR Server Rules”, on page 234](#).



Document routing strategy

In most cases, documents are routed over the XPR address book (**default routing rules**). To do this, you must provide it with the appropriate information. See [Chapter 4, “User Data Administration”](#).

The **fax server inbound routing** is different from the **default routing rules** insofar as a special rule for networking voicemail servers is omitted.

The **SAP inbound routing** forwards all messages to an SAP R/3 system. This system takes care of the inbound routing by assigning the corresponding information such as fax numbers to the users. Please note that **SAP inbound routing** must at any rate be adapted since the routing rules must also contain the individual token of the connection to the SAP R/3 system, which cannot be added automatically. See the *SAP R/3 Gateway* manual.

If the routing strategy is to be customized, routing rules can be adapted after a click on **Edit** by means of the integrated editor. In this case the **user-defined routing** is displayed. Please note that no blank lines are allowed within the rules.

Automatic carbon copies

Each incoming fax document can be routed to a printer as an automatic copy. The only requirements for this procedure is an installed Print APL and a printer connected to the system.

Through use of the option **Incoming fax documents are copied to the default printer**, all incoming fax documents are copied to the default printer of the Print APL.

With the option **Incoming fax messages are copied to a user-defined printer**, incoming fax documents are only printed if the recipient specifies a printer of the print APL in the user database field `PRINTER`.

Via **Custom carbon copy rules** you can default-set individual rules. Selecting the **Edit** button invokes the built-in editor for creating custom rules. Please note that no blank lines are allowed within the rules.

By means of **No automatic carbon copy generation** this function is deactivated.

Automatic rerouting of unread documents

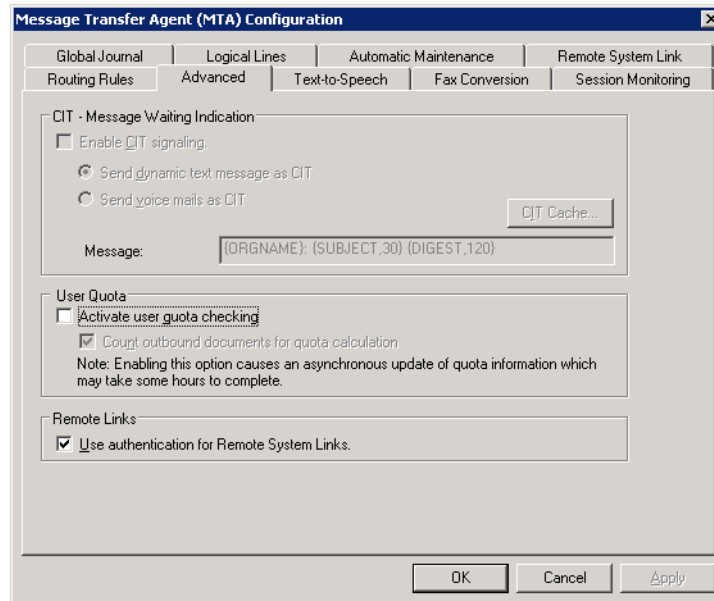
Incoming documents not read by the recipient within a specified time limit can be rerouted to another user. The **Incoming documents are rerouted to a postmaster if not read** option takes care of that after 10 days for fax documents and voicemails. The recipient is the (`POSTMASTER`) defined during the installation.

The option **Custom rescheduling rules** enables administrators to define their own rules for the rerouting of unread documents. Selecting the **Edit** button calls up the built-in editor for modifying the awake rules. Please note that no blank lines are allowed within the rules.

By means of **No automatic rerouting** this function is deactivated. In lieu of data protection prescription, this option should remain active.

7.1.4 Advanced

You can set certain options on the **Advanced** tab.



CIT – Message Waiting Indication

See also [Section 7.9, “Message Waiting Indication \(MWI\)”](#), on page 287.

IMPORTANT:

If you use the Notification APL for message waiting indication, the CTI signalization must be deactivated here! This is done automatically with the Notification APL installation. If the Notification APL is installed, the CIT range would be completely deactivated here and could not be activated. If you would like to activate the CTI area, you must first uninstall the Notification APL.

Here you can **enable CIT signalization** via the kernel and select the type of signalization.

Send dynamic text message as CIT allows transmission of a configurable text message over a text-compatible protocol such as SMS. The text is entered in the **Message** field and may contain the following variables:

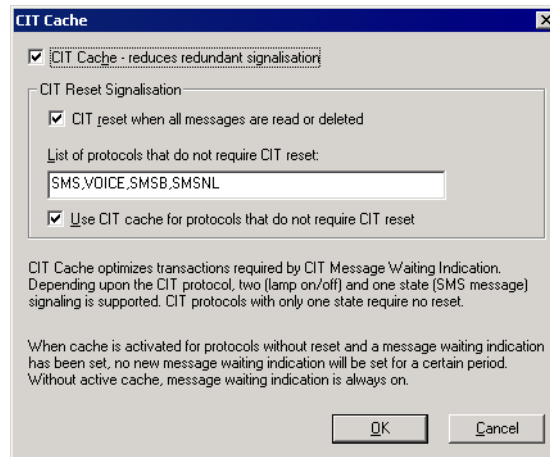
Variable	Meaning
{ DATE }	Date.
{ DIGEST [, <Max>] }	A portion of the text message is embedded in the CIT notification. The maximum length can be defined through the optional entry <Max>. The algorithm used for building the Digest attempts to retrieve the text without a loss of information. Example: Empty lines, greetings, ...
{ FORMAT }	Inbound message format (e.g. voice, fax, or e-mail) independent of the inbound service used.
{ ORGNAME [, <Max>] }	Readable form of the originator address. If information about the fax originator is contained in the Alias database, this could appear as a name instead of a fax number. The maximum length can be defined through the optional entry <Max>.
{ ORGNODE }	Incoming service.
{ ORGUSER }	Originator address.
{ RECNAME [, <Max>] }	Readable form of the recipient address. The maximum length can be defined through the optional entry <Max>.
{ RECNODE }	Target service.
{ RECUSER }	Recipient address.
{ SUBJECT [, <Max>] }	Message subject. The maximum length can be defined through the optional entry <Max>. If the subject field is longer, it will be truncated and '...' appended.
{ TIME }	Time

The option **Send voice as CIT message** enables the transmission of voice files over the ISDN voice protocol. This protocol is also used for setting and resetting indicator lamps on telephones connected to an Integral PBX from Bosch-Telecom. After selecting this option the path to the PCM voice file is entered that is to be used for notifications.

Protocols used for setting and resetting indicator lamps (e.g. CIT over the Hicom PBX from the V.24 APL) should be of the type text since no actual message is being sent. For the kernel the transmission job acts as a trigger for setting or resetting the indicator lamps.

Such specifications are also possible user-dependently. You have to enter for each user the file including its individual text or voice file in the database field **CITFILE**. Text files must be suffixed with **TXT** for this purpose. The files are stored in the XPR server's **UserData** directory tree and files are thus entered in relation to this directory. This feature enables among other things various language versions of the CIT notification.

If you want to use user-independent CIT files, the [CitUserBasedMessage \[REG_DWORD\]](#) value must be set to 1 in the registry.



The number of transaction required for signaling can be optimized via the **CIT Cache** button.

Depending on the CIT protocol, two (lamp on/off) and one state (SMS message) signaling is supported. For the **protocols that do not require a signaling reset**, no new notification is sent with active CIT cache and set flag for a while.

A counter-based CIT is activated when the option **CIT reset when all messages are read or deleted** is selected. The counter-based CIT differs largely in one aspect: XPR registers in the `NEWMSG` database field the number of new, unread messages. The CIT signal will not be reset until this counter reaches 0. The option CIT Cache should not be activated with counter-based CIT.

NOTE:

If you wish to reset the Message Waiting Indication (MWI) even if a user has entered `MAILBOX` in the `PREFERRED` field but reads the message e. g. under Exchange (inbox replication with Integrated Messaging), via TUI over the TUM interface of the Mail APL or with the Web APL, the following registry key must be set to 1: `HKLM\SOFTWARE\Wow6432Node\PP-COM\MRS\MailApl\ResetCITonRead`

The correct setting for connecting the XPR to Hicom via CorNet-N/NQ is:

- Enable CIT signalization
- Send dynamic text message as CIT
- CIT Cache **not** active
- CIT reset when all messages are read or deleted

The MWI (Message Waiting Indication) protocol must be correctly configured for this and the appropriate reference must be set in the user data's CIT field.

The following is preset in the system language as the default text for incoming message notification:

```
New{ORGNODE} message for{RECUSER} from +{ORGUSER} {DATE} -
Poll under ...
```

The callback access number should be entered here (in place of the three dots) in international format with leading plus symbols so that in the case of notification via SMS the recipient can call back the relevant number at the push of a button to play back the message.

This dynamic text is language-dependent. If a mailbox user set a language other than the system language for communication with the server, then the text displayed in the MTA administration is not used, but rather a text file from the user data directory. These text files should be modified in the same way as the MTA message type. A separate file named SMS_<language ID>_<tui>.txt is thus provided in each supported language for the TUI PhoneMail and VMS.

User Quotas

User quotas are usually employed to limit the resources (disk space) used by the user. Access to resources are denied when the user attempts to use resources in excess of those allotted. There are, however, conceptual differences between quotas used on a file server and those of a mail server.

Users on a mail server have only a limited control of how resources allotted to them can be used. The actions of the user (transmit message) as well as those actions of other users (receive messages), influence the users allotted resources. It is therefore possible that a user may not be able to send a message while either several large messages, or simply too many messages have been received. Receiving messages is always possible even with exceeded user quota.

NOTE:

If the messages are accessed via the TUM interface, the corresponding function of Microsoft Exchange or Lotus Notes should be used. Calculation of the quotas used occurs only based on the messages locally available on the XPR server.

With TUM via Microsoft Exchange or Lotus Notes the messages are only available on the foreign system, so that the quota settings of the XPR server never come to bear in practical terms.

How do quotas work?

Two database fields are used; `QUOTA` and `QUOTAUSED`. The allocated amount of resources is given in the field `QUOTA`. An entry of zero indicates an unrestricted amount of resources. The field `QUOTAUSED` contains the amount of resources currently in use. When transmission attempt is made the sum of the message size and the amount in the field `QUOTAUSED` are compared with the amount in `QUOTA`. If this is not the case, the send job is rejected. As soon as the user decreases the disc space he uses by actively deleting already sent or received documents, sending documents is possible again. New message receiving is possible any time and not restricted by this option!

NOTE:

If a user deleted a sufficient number of documents by TUI, he/she must hang up and dial in again. Only then he/she may record and send new messages.

When quotas are activated, you can decide whether the outgoing documents are also to belong to the contingent.

The current disk space occupied by a user is determined asynchronously during a maintenance task job (generally once a day). Consequently, new inbound documents are only entered in the summary information following the next maintenance task job. Documents deleted by the user, however, are immediately reflected in the summary information.

In addition, a warning threshold can be set in the PhoneMail and VMS telephone applications to inform the user about depleting resources. See on this topic the corresponding voicemail settings in [Section 10.9.2.2, "Messaging Settings", on page 813](#).

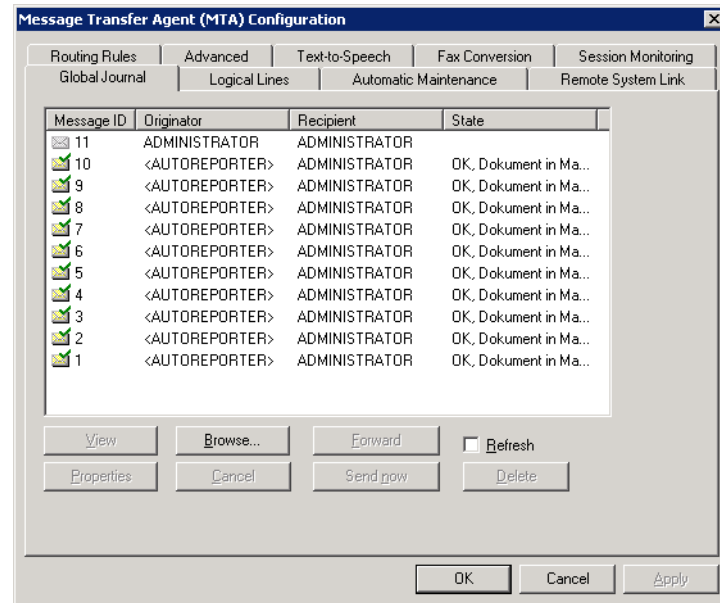
You can activate a different behavior for Ergo via a parameter. When user quotas are active and a user has exceeded his/her quota, Ergo then switches automatically to the Info Mode for the corresponding mailbox. A greeting is then played to the caller, but he/she cannot leave a message.

Remote system links

When the option **Use authentication for Remote System Links** is activated, a password is required as validation for each remote system link. A secure connection is guaranteed through the use of this option.

7.1.5 Global Journal

The global journal displays information about in and outbound messages from the XPR server.



Messages can be sorted either by message ID, originator, recipient, or document state. Message sorting is accomplished by clicking with the mouse pointer on the corresponding field in the header.

Various message operations can be performed through use of the buttons in the lower portion of the dialog. The message ID is selected and subsequently the desired operation.

When the user possesses the appropriate authority, a document viewer can be started through use of the **View** button.

Selecting the **Properties** button displays the contents of the internal journal database fields and the PMF system fields of the selected entry. The displayed information may be used for problem analysis. Therefore, you can export the document and the displayed internal journal database fields in a ZIP file within this display via a click on the **Export** button. In this way it is possible to send a document and the associated information to the support if problems occur.

Send jobs that are still in the MTA queue can be removed with the **Cancel** button. These messages are identifiable by the clock symbol. As soon as a message has been transferred to another APL, this option is no longer available.

Send now immediately sends the selected document from the MTA queue. Documents in the MTA queue are indicated with a clock icon.

The option **Forward** allows messages to be forwarded to other users.

The **Delete** option replaces the contents of the message with the text “document already deleted by administrator”. Through this the journal entry remains and therefore the information about the transaction is retained, but the storage space required by the document is drastically reduced.

The **Browse** option allows the user to search for either a message ID, originator, recipient, or a state. The results of search requests are displayed at the top of the global journal.

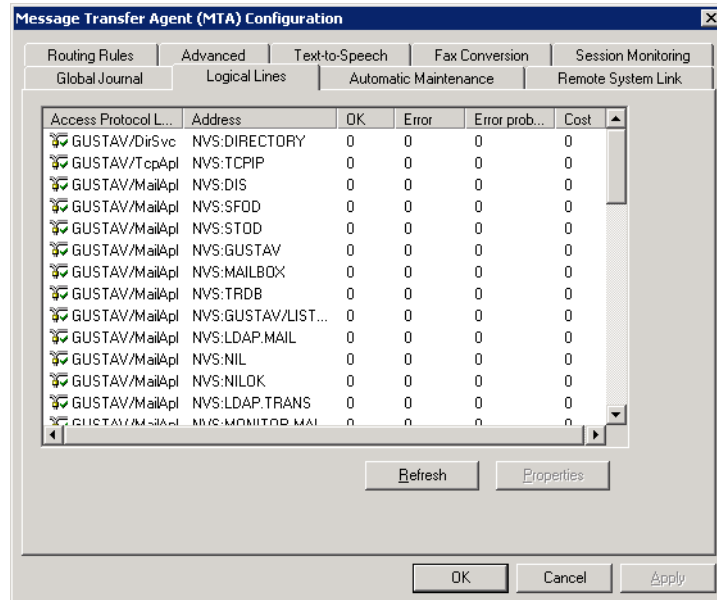
When the **Refresh** option is activated the journal is updated in a real time mode. This option should not be activated for those users that have a relatively slow RAS connection to the XPR server.

A message status is represented by the corresponding icon. Possible icons and their meaning:

Icon	Meaning
	This message has an invalid status! One possible reason could be an APL crash during a transmission process so that the kernel has consequently not received a status report.
	The message has been transferred to an APL or to another XPR server by Remote System Link; up to now no final report has been received.
	The message is queuing up (in a waiting loop) to be transmitted to an APL.
	Successful message transmission according to status report.
	Message delivery could not be executed or an error occurred during the transmission according to status report.
	Successful message transmission according to status report. The mail is now intended for automatic deletion. See Section 7.1.1.1, “Automatic Cleanup”, on page 186 .
	Message delivery could not be executed or an error occurred during the transmission according to status report. Furthermore, the message is now intended for automatic deletion. See Section 7.1.1.1, “Automatic Cleanup”, on page 186 .
	The message has been transferred to an APL or to another XPR server by Remote System Link; up to now no final report has been received. Furthermore, the message is now intended for automatic deletion. See Section 7.1.1.1, “Automatic Cleanup”, on page 186 .
	The target APL has already returned a report about this message. This report is still in the queue though and could not be delivered to the sending APL yet.

7.1.6 Logical Lines

All logical lines registered within the MTA are displayed in the configuration tab Logical Lines. To display this information, select the desired line and click **Properties**.



In the Logical Lines Properties dialog all relevant attributes can be viewed for a logical line and those of lines imported over a remote system link.

Line traffic directions can be defined for the individual logical lines through the option **Line enabled for outbound transactions**. Lines are either defined as bi-directional or explicitly for inbound traffic only.

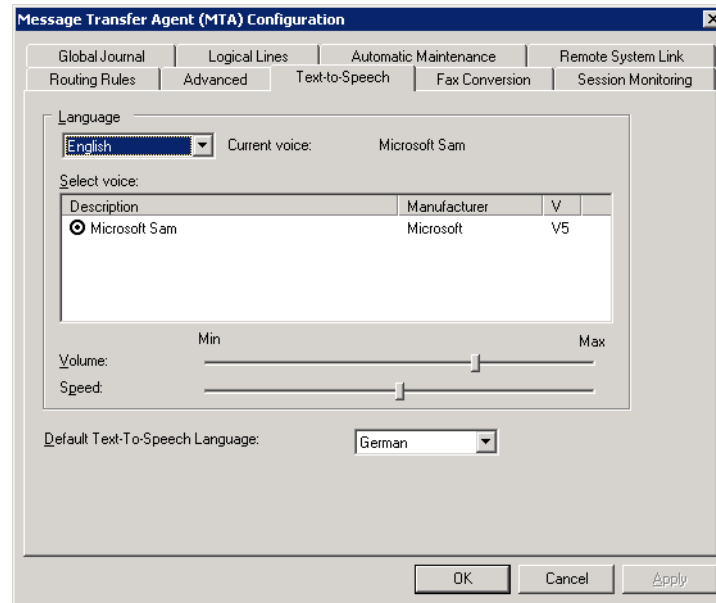
By means of the **preference** for a line it is easy to set a line usage priority. Taking advantage of this possibility, a Least Cost Routing configuration can be easily set up for transmission jobs over various lines to various sites. In a like manner a fall-back strategy can be developed for remote system links. If, for example, a remote system link is normally established over a TCP/IP connection through the Internet, a second line over an ISDN connection could be configured using a lower line priority which would only be used in the event of an Internet interruption or when the amount of data to be transferred is too large. Local lines are always preferred to those imported by a foreign system by default.

The MTA is equipped with a cache in which all line information is stored. Through this cached information the MTA is aware of all lines and their properties at the start of the server. Included in this cached information are the attributes and characteristics of lines imported over a remote system link.

Statistical information and dynamic error probabilities are also displayed within the dialog.

7.1.7 Text-to-Speech

Text messages can be converted into voice messages over the Microsoft SAPI version 5.1 interface for speech synthesis.



This requires the installation of an SAPI-conformable text-to-speech software, which provides a speaker in the respective language. Furthermore, text-to-speech and the corresponding TTS language must be added as additional XPR feature license.

Subsequently, select a **Voice** for each of the supported **Languages** in this tab. XPR tries to recognize the language of the text to be put out and takes the speaker set for the recognized language for conversion. If no language has been recognized, the **Default Text-To-Speech Language** set here is used. The **Volume** and **Speed** of the voice playback can be set through use of the sliders. The settings also apply for connected satellite systems.

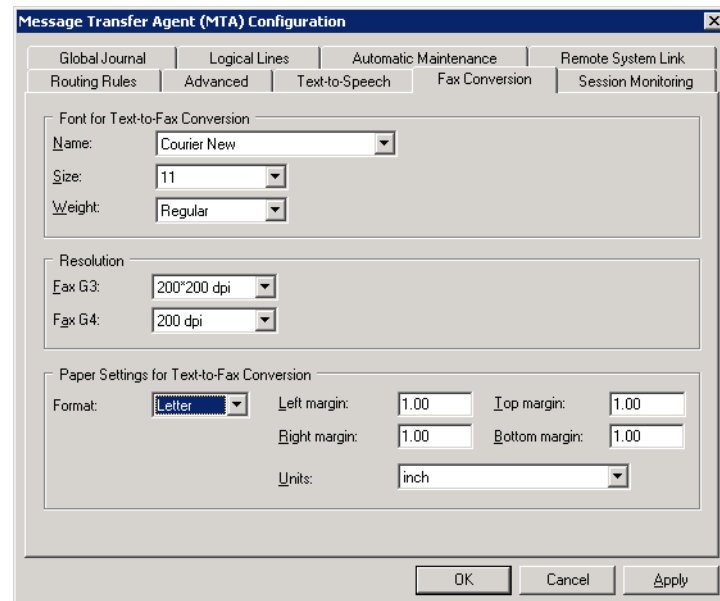
The e-mail output via text-to-speech must also be activated in the respective voicemail system:

- Ergo – See [Section 10.4.2.2, “Parameter Tab Options”](#), on page 620.
- Evo – See [Section 10.4.1.3, “Parameter Tab Options”](#), on page 598.
- PhoneMail – See [Section 10.4.3.9, “Parameter Tab Options”](#), on page 645.
- VMS – See [Section 10.4.4.8, “Parameter Tab System”](#), on page 684.

7.1.8 Fax Conversions

These settings determine the look and format of fax documents that arrive on the XPR server as text document and are converted into fax before transmission. You find an overview of the text formats in [Section A.2, “Text Formats”, on page 1585](#).

These text formats are cleanly inserted in fax stationery created with Communications. For other formats that are converted to Fax by means of application conversion as described in [Section A.8, “Application Conversions”, on page 1592](#) you need to take greater care when using fax stationery. In case of these documents a graphics page is created from the document, which is then covered with the fax stationery. As a result, the company logo on the fax stationery may hide text. A side effect could also be an additional page, so that e.g. the text and the fax stationery comes out as fax on separate pages.



Firstly, the utilized type of **Font for Text-to-Fax Conversion** can be set via **Name**, **Size** and **Weight**. Next, the **Resolution** for **Fax G3** respectively **Fax G4**, appropriate for such a conversion, should be set. Lastly, the paper size and the margins must be entered under **Paper Settings for Text- to- Fax Conversion**. For margin entries you can default set the **Units**.

If the server is set to the use of a Russian or Turkish codepage via **Control Panel > Regional and Language Options > Advanced > Language for non-Unicode programs**, a matching font must be selected here. Matching fonts are suffixed for Russian with CYR and for Turkish with TUR.

Possible settings for Russian are:

- Arial CYR
- Courier New CYR
- Times New Roman CYR

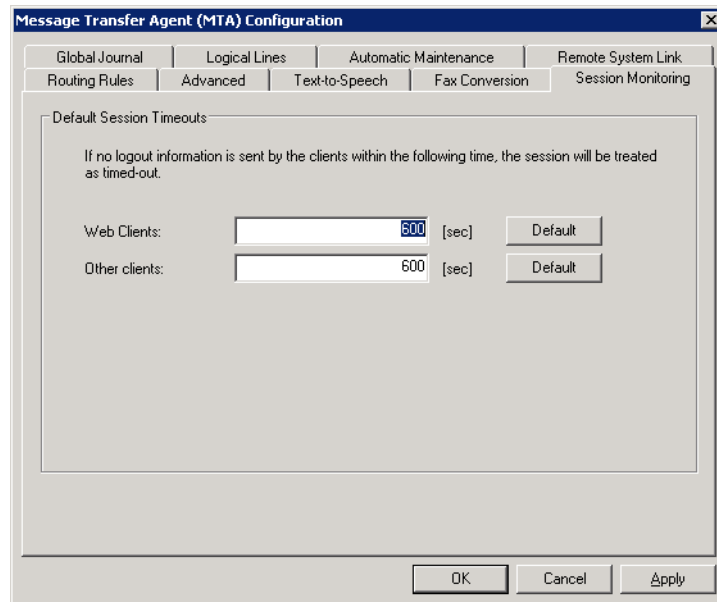
Message Transfer Agent (MTA)

Possible settings for Turkish are:

- Arial TUR
- Courier New TUR
- Times New Roman TUR

7.1.9 Session Monitoring

As administrator, you can view in the Web Assistant the currently logged-in users as well as a history of the logged-in clients. The clients, though, need not log off from the XPR server. Therefore, a client that was shut down without explicit log-off would still be considered active. To evade this problem, a client is implicitly assumed logged off after some time. Since the clients usually query the server as to whether new messages are to be retrieved in regular intervals, you can still determine the desired information via the aforementioned time limit.



Therefore, this time limit can be set here separately for the Web APL (**Web Clients**) and for all other login options. Never pick a value for **Web Clients** that falls below the automatic Web APL logoff. See the configuration parameter [Time-out of connection](#) with the Web APL in this context.

Please note that this mechanism does not consider any clients that connect to the XPR server by POP3 or IMAP4. Therefore, such clients are not displayed in the Web Assistant as clients.

7.2 Maintenance Script

The XPR server automatically executes maintenance and clean-up tasks. Through the use of a script language, it is possible to precisely define the various tasks. The script to be performed is in the [MaintenanceScript \[REG_SZ\]](#) registry value.

IMPORTANT:

Note that with an XPR server update a modified script would be overwritten again by the script default version. To avoid this, save the modified version under a different name in the `<XPR Install>\res\maint` directory. The new name with complete path specification is then to be entered in the [MaintenanceScript \[REG_SZ\]](#) registry value.

The script can contain an arbitrary number of task groups, performed at a fixed time:

```
<TaskGroup>
{
  Periodicity = <TimeSpec>
  InformOnFailure = <User>
  InformOnSuccess = <User>
  Task
  {
    <Task>
    <Task>
    ...
  }
}
```

`<TaskGroup>` is an arbitrary name for a group of `<Tasks>` that is to be collectively started.

`<TimeSpec>` in format `n[s,m,h,D,W,M,Y]@hh:mm` gives the time `hh:mm` and intermittence `n`, with which the `<TaskGroup>` is to be executed. The suffix `@hh:mm` gives the time at which the `<TaskGroup>` is started. The prefix `n[s,m,h,D,W,M,Y]` refers to the periodicity: 10s (every 10 seconds), 30m (every 30 minutes), 6h (every 6 hours), 15D (every 15 days), 4W (every 4 weeks), 2M (every 2 months), 7Y (every 7 years). With `Periodicity = 6h@0:00` the associated `<TaskGroup>` is started every day at 00:00, 06:00, 12:00, and 18:00.

`<TimeSpec>` in the format `DD@hh:mm`. Here `DD` corresponds to the English weekday abbreviations, thus MO, TU, WE, TH, FR, SA, SU. Consequently you can e.g. with `Periodicity = SU@12:00` start an associated `<TaskGroup>` every Sunday at 12:00.

`<TimeSpec>` in the format `!<Date>@hh:mm`. This task is executed just once at the set date `<Date>`. `<Date>` is specified as `YYYY-MM-DD`. Thus for example `Periodicity=!1999-12-31@23:00`. With this example a separate database backup was generated at the turn of the year 2000.

<User> are XPR user names to be informed of the success or failure of a <Task>. However, `InformOnSuccess` is as yet only a wildcard for a planned new feature not implemented so far.

NOTE:

If in a script paths are specified via network, please consider that a Windows service is operated in the system context. Consequently, the service is **not** privileged to access the network. The MTA must be given an account with the corresponding privileges by the Service Control Manager if network access is required.

7.2.1 Actions

All commands <Task> described here can also be executed independently from the Maintenance Script from the command line prompt. For this purpose, the InfoTool utility is available in the directory <XPR Install>\SDKTools. Certain actions can only be done through the use of the InfoTool and not directly from the Maintenance Script. These are explicitly listed under the relevant description. Exception: the parameter `record=` is abbreviated as `rec=` in the command line utility InfoTool.

Call: `InfoTool node=\\<Server> <Task>`

<Server> is the server name of a Windows server in UNC notation, on which a XPR database (InfoStor) runs. If the call is being executed locally, the parameter `node=` may be excluded.

The following actions can be started through <Task>:

```
EXPORT record=<Record> file=<Filename> [-ANSI]
```

The records for the database CORREL, GEB, JOURNAL, DISTRIB and RECH are exported in the file <Filename>. Database fields are always separated with a tab. Via the `record=FULL` specification, all these databases can be simultaneously saved to a file. The parameter `FULL` is only available in the Maintenance Script, and corresponds to the InfoTool command `FULLEXPORT`.

When using the `CORREL` parameter with the InfoTool you can deploy the optional parameter `-ANSI`. As a result the Correlation database is exported in the ANSI format. This is written in the export file by a corresponding codepage marking at the beginning of the file. In case of a later import, this codepage marking must be present. As of XPR 6, the Correlation is written in the ANSI format (Codepage 1252). Correlation Databases created before this version were, in contrast, written in the OEM format as it was used in the former MS-DOS.

Example: `EXPORT record=CORREL file=c:\tmp\correl.txt`

A file has the following format:

DOMAIN	CLASSNAME	CLASS	KEYNAME	KEY
FERENGI	USER	MK	GROUP	USER
FERENGI	USER	MK	MAILBOX	MK
FERENGI	USER	MK	NAME	Martin Koser
FERENGI	USER	MK	PREFERRED	MAILBOX
FERENGI	USER	MK	PASSWORD	*****
FERENGI	USER	SUPERVISOR	NAME	Group definition ...
FERENGI	USER	SUPERVISOR	PRIVILEGES	FFFFFFFFFFFFFFFF...
FERENGI	USER	USER	NAME	Group definition ...
FERENGI	USER	USER	PRIVILEGES	1480fb815f00000...
FERENGI	USER	POSTMASTER	GROUP	USER
FERENGI	USER	POSTMASTER	MAILBOX	POSTMASTER
...				

```
EXPORT rec=USER file=<Filename>
```

The user database is exported in a usable form for extraneous applications as a file <Filename>. In the first line the user database field names appear separated by tab stops. The following lines contain a data record each. This format can, for example, be read in by Microsoft Excel. The numbers should be read in as string since Excel removes leading zeros which often appear with telephone numbers. Please note, that here only the fields are exported that are contained in the \$USER mask.

NOTE:

This function is only available through the InfoTool. The EXECUTE action listed below must be used if this is called up from the maintenance script.

```
EXPORT rec=UC_USER file=<file name> [srv=<UC server>]
```

UC_USER is not a CLASSNAME. Instead, all users are exported with a value in the CONUSER field. Another export restriction is possible via the optional parameter *srv*. This parameter queries the CONSRV field. The user database is exported in a usable form for extraneous applications as a file <Filename>. In the first line the user database field names appear separated by tab stops. The following lines contain a data record each. This format can, for example, be read in by Microsoft Excel. The numbers should be read in as string since Excel removes leading zeros which often appear with telephone numbers. Please note, that here only the fields are exported that are contained in the \$USER mask.

```
EXPORT record=SHORT file=<Filename>
```

The alias database (global contacts) is exported to the <Filename> file in a form that can be used by foreign applications. See also EXPORT record=SHORT.

```
EXPORT record=RUND file=<Filename> class=<LName>
```

The distribution list <LName> is exported in a usable form for extraneous applications as a file <Filename>.

Example: EXPORT record=RUND file=rund.txt class=TESTLISTE

CLASSNAME	CLASS	KEYNAME	KEY
RUND	TESTLISTE	GLIST	
GLIST	TESTLISTE	1	NVS:FAXG3/1234
GLIST	TESTLISTE	2	NVS:FAXG4/2343
GLIST	TESTLISTE	3	NVS:SMTP/hugo@do.main.com
GLIST	TESTLISTE	4	NVS:FERENGI/MK

```
IMPORT rec=<Recordtype> file=<Filename>
```

The records CORREL, JOURNAL, GEB, DISTRIB and RECH can be imported again. Many applications (Microsoft Excel, Microsoft Word, dBase, etc.) have an export format that uses TABs as separators. In this manner it is quite simple to import user information from extraneous systems. Such a user import contains a mask description of the fields from the extraneous system plus the user data. In the CORREL mode, password/PIN can also be imported in the clear text. These are then encoded during the import. The password or PIN must be preceded by a ^ for this purpose. This command is only available over the InfoTool.

```
IMPORT rec=USER|SHORT file=<Filename>
```

A list with the applicable export format is imported. It is inserted into the user database without deleting the existing data. In the `USER` mode, password/PIN can also be imported in the clear text. These are then encoded during the import. The password or PIN must be preceded by a `^` for this purpose. This command is only available over the InfoTool.

```
IMPORT rec=RUND file=<Filename> class=<LName>
```

A distribution list is imported in the relevant export format. No old entries are deleted. Distribution lists are not restricted to the number of entries. This command is only available over the InfoTool.

```
DELDDB record=<Recordtype> age=<Age-in-Days>
[originator=<NVS Address>]
[recipient=<NVS Address>|finalrecipient=<NVS Address>]
[flags=<Flags>] [options=<Options>]
```

`JOURNAL` or `GEB` record types, that are older than `<age-in-days>` days, will be deleted. When journal entries are deleted, the associated message file is also deleted. In the graphic configuration interface, a minimum of three days can be set so that messages are still available for at least a weekend. In the script a minimum of one day can be entered since everyone performing modifications at the script should be aware of the consequences.

`<Age-in-Days>` can be set directly as well as via one of the variables listed further below. Calculating is possible here as well be subtracting or adding a fixed value from or to a variable. If such a subtraction results in a value smaller than 0, the variable value is used.

Examples:

```
$ (LIFETIME) -10
$ (LIFETIME) +5
15
```

Optional parameters are only possible when the `<Recordtype>` is `JOURNAL`.

```
[originator=<NVS Address>]
[recipient=<NVS Address>|finalrecipient=<NVS Address>]
```

Complete or partial NVS address in the form `NVS:NODE/USER`. Final recipient is also the recipient, but here the address after execution of the routing rules. A partially specified address is always compared from the beginning. Wildcards are not permitted.

Examples:

With the specification of `originator=NVS:FAXG3`, `DELDDB` is only used for data records the originator address of which begins with `NVS:FAXG3`.
 With the specification of `recipient=NVS:SERVER/MEIER`, `DELDDB` is only used for data records received by user `MEIER`.
 With the specification of `finalrecipient=NVS:EXCH`, `DELDDB` is applied to all messages sent to an Exchange user.

```
flags=<Flags>
```

Deletes only the data records that contain all set *<flags>*. *<Flags>* is a comma separated list of the flags READ, PRINTED, ARCHIVE, DELORG, DELREC, DELARC and DELPOP. The DEL flags refer to messages that were deleted by the originator (DELORG), recipient (DELREC), archive (DELARC) or POP3 client (DELPPOP). The READ, PRINTED and ARCHIVE flags can be prefixed with an exclamation mark (!) to negate the condition.

Example: `flags=READ` deletes only the data records that have already been read. `flags=!READ` deletes unread data records only.

`options=<Options>`

If the option `FILEONLY` is set, the document will be deleted and replaced with a short text containing deletion information. The database entry in the journal remains intact. Through the use of database queries, it is possible to reconstruct what has happened to the document.

IMPORTANT:

If possible, the `options=FILEONLY` option should always be set. A complete deletion of documents and database entries should only be executed in an emergency. A set MWI signal is not reset when unread documents are deleted completely. If, however, the file is previously deleted by means of this option, the journal entry is kept and the MWI signal is simultaneously reset for this unread message.

Through use of the option `REMOVECONVERSIONS`, original documents are retained and all conversions deleted. When used with voice files, the original may also be converted into a compressed format. The codec settings in the MTA configuration are used for this purpose.

By means of the `DELETESOFT` option, the flags `DELORG` (deleted by the originator) and `DELREC` (deleted by the recipient) are set. By means of suitably querying these flags upon deletion with the `FILEONLY` option, the message (body) can, for example, be deleted on the XPR server side and harddisk space saved. In addition, the internal flag `DELETE_MAINTENANCE` is set. In case of a replication with, for example, Microsoft Exchange or Lotus Notes, the corresponding APLs thus know that the delete flags have been set by the maintenance script. This is considered and the document not deleted with Microsoft Exchange or Lotus Notes. This option is also recommendable some days before the physical deletion process, since the Notification APL will then register the deletion at any rate.

NOTE:

Several options, each separated by comma, can be specified. If you use counter-based CIT, the last of a sequence of `DelDB` commands must be a

DelDB record=Journal age=\$(LifeTime). This implicitly checks the consistency of the new message counter which is used by the counter-based CIT.

EXECUTE cmd=<Command>

A Windows shell command or a batch file is executed. Since no user interaction is possible, this function should only be used together with the automatic backup (see below). No interactive programs must be started (e.g. editors). The essence of the **EXECUTE** command is to start backup-scripts that allow specific backup extensions. Beyond that, InfoTool can be called from the maintenance script, therefore enabling the use of commands normally not directly available in the maintenance script. Example:

```
EXECUTE cmd="..\sdktools\infotool rec=USER  
file=..\backup\user.txt"
```

MASKEXP file=<Filename>

Exports all mask descriptions from the correlation in the *.mdl format. These masks are used, for example, by the Web Assistant. This command is only available over the InfoTool.

MASKIMPORT file=<Filename>

Imports all mask descriptions into the correlation in the *.mdl format. This command is only available over the InfoTool.

CLASSIMPORT class=<Classname> file=<Filename> [delete=1]

Correlation data records of the CLASS <Classname> are imported. If the option delete=1 is set, all correlation data records with CLASS=<Classname> will be deleted. This command is only available over the InfoTool.

Example: A new privilege list is to be installed on the server. The new privileges are contained in a correlation-export file as privlist.txt. The following command deletes all old PRIVILEGES definitions and imports the new ones then. Other correlation data records *are not* modified.

```
CLASSIMPORT class=PRIVILEGES file=privlist.txt delete=1
```

FULLEXPORT file=<Filename> [-ANSI]

The complete database is exported as the file <Filename>. A full-export is the short form of separate exports of the JOURNAL, RECH, DISTRIB, GEB and CORREL databases. The resulting file qualifies as a backup for the database contents. The Correlation database is exported in the ANSI format via the optional -ANSI parameter. This is written in the export file by a corresponding codepage marking at the beginning of the file. In case of a later import, this codepage marking must be present. As of XPR 6, the Correlation is written in

the ANSI format (Codepage 1252). Correlation databases created before this version were, in contrast, written in the OEM format as it was used in the former MS-DOS.

NOTE:

This command is only available over the InfoTool. In the Maintenance Script the normal EXPORT with parameter FULL should be used.

FULLIMPORT file=<Filename>

The complete database is imported from the file <Filename>. A full-export is the short form of separate exports of the JOURNAL, RECH, DISTRIB, GEB and CORREL databases. It preconditions the previous FULLEXPORT. This command is only available over the InfoTool.

REMOVE path=<Wildcard> age=<Days> [option=[x] [,WARN] [,RECURSIVE]]

In the <Wildcard> path all files older than <Days> days are deleted. If the option X is present, all files are deleted. Otherwise only a message is generated. With the WARN option, a message in the XPR log is given by every delete operation. With RECURSIVE, all <Wildcard> subdirectories are also edited.

PURGE <Message ID>

Removes the document file that associates <Message ID>. The file is replaced by the short message "Document has been deleted by system administrator". This keeps the journal entry with all information such as incurred charges, but the actual message taking a lot of space is removed. This command is only available over the InfoTool.

UpdateAllMWI

Sends for all MWI stati another instruction to the PBX so that the PBX sets the mailbox LED on the telephones correctly.

IMPORTANT:

Through this a command is sent to the PBX for each configured telephone. This may overload the PBX especially when it is otherwise loaded during the execution period of these commands.

VERIFY Options=CASE[,FIX]

Checks the address book database for consistency with regard to the attributes LOWER and UPPER and directly modifies incorrect entries if the option FIX is specified.

QUOTA [User=<Username>]

The database field `QUOTAUSED` is asynchronously actualized with the amount of harddisk storage space used by each user. By optionally specifying a particular user, this task is only performed for this user and is mainly intended for interactive InfoTool operation.

OldUserCleanup

This task removes all non-active user entries from the database. Non-active user entries are those entries which do not have a password or PIN number. In this case the following happens:

- All documents received by the user are tagged as being deleted by the user.
- All documents sent by the user are tagged as being deleted by the user.
- All documents received for and sent by this user will be deleted, if these documents are not also attributed to a second user.
- All entries from the user in the Correlation database will be deleted.
- The user will be removed from all distribution lists.
- If an executable program (with complete path) is listed in `HKLM\Software\Wow6432Node\PP-COM\MRS\MTA\UserRemovalExtension`, this program will be called with the user name as the first command line parameter.

IMPORTANT:

If for any reason documents on the server have an `owner_originator` or `owner_recipient` of the `NVS : <Servername>/<LocalUser>` format and this `<LocalUser>` does not have a password or PIN number, all documents and database entries will be deleted for this user. If you are not sure whether this applies to your server installation, you should at least save the `folders`, `database` and `userdata` directories before installing this maintenance job.

UpdateAsrGrammar

Updates the grammar used by the Caller Guide for speech recognition of the user names. See also [Enable addressing via names](#).

7.2.2 Variables

Within the expression `<Username>` and `<Task>` the following variables are allowed:

`$(ADMINISTRATOR)`

Administrator's name. Entered at the time of the XPR installation.

`$(POSTMASTER)`

Name of the user who is to receive all undeliverable mail. With the system installation this is always set to `POSTMASTER`.

If these values require modifications, you can find these definitions in the registry under the key `HKLM\Software\Wow6432Node\PP-COM\MRS\Infostor\Accounts`.

`$(BACKUP)`

Backup directory as defined in the [BackupDirectory \[REG_SZ\]](#) value.

`$(FOLDER)`

Document directory as defined in [FolderDirectory \[REG_SZ\]](#).

`$INTERACTIVE`

This is a list of all interactive services, including those that are not executed by `$NONINTERACTIVE`. It should be observed that no parenthesis are used with this variable. Since this is an enumeration of several services, these are not required.

NOTE:

The following descriptions of the `$(LIFETIME. . .)` variables refer to their use in the standard maintenance script. The meaning of these variables immediately changes when they are used in other applications.

`$(LIFETIME)`

Maximum document life in days. This corresponds to the default in the **Automatic Cleanup** of the MTA configuration.

`$(LIFETIMECOMPRESS)`

This value corresponds to the specification of **Compress representation and voice after... days** in the **Maintenance Cleanup Options** tab.

`$(LIFETIMEDELETED)`

This value corresponds to the specification of **Remove deleted documents after... days** in the **Maintenance Cleanup Options** tab.

\$ (LIFETIMEEMAIL)

This value corresponds to the specification of **Remove e-mail after... days** in the **Maintenance Cleanup Options** tab.

\$ (LIFETIMEINBOUND)

This value corresponds to the specification of **Remove inbound documents after... days** in the **Maintenance Cleanup Options** tab.

\$ (LIFETIMEOUTBOUND)

This value corresponds to the specification of **Remove outbound documents after... days** in the **Maintenance Cleanup Options** tab.

\$ (LIFETIMEPASSTHROUGH)

This value corresponds to the specification of **Remove pass-through documents after... days** in the **Maintenance Cleanup Options** tab.

\$ (LIFETIMEREAD)

This value corresponds to the specification of **Remove read documents after... days** in the **Maintenance Cleanup Options** tab.

\$ (LIFETIMESERVICE)

This value corresponds to the specification of **Remove MWI indication after... days** in the **Maintenance Cleanup Options** tab.

\$ (LIFETIMEUNREAD)

This value corresponds to the specification of **Remove unread documents after... days** in the **Maintenance Cleanup Options** tab.

\$ (LIFETIMEUSERDEFINED)

This value corresponds to the specification to the **User defined parameter** in the **Maintenance Cleanup Options** tab.

\$NONINTERACTIVE

This is a list of all services that do not allow the XPR server to notice whether a recipient deletes these documents. This is the case with all services in which no status information can be returned. An example is Fax. This service is defined in the [NonInteractiveServices \[REG_SZ\]](#) value.

\$ (ROOT)

Directory under which XPR is installed as defined in the [LocalSystemList \[REG_MULTI_SZ\]](#) value.

\$ (SCRIPTDIR)

Path of the *<XPR Install>\RES\MAINT* directory.

Example: Backup of the XPR databases

```
Backup
{
  Periodicity = 24h@0:00
  InformOnFailure = $(Administrator)
  InformOnSuccess=
  Task
  {
    Execute cmd=$(ScriptDir)\backup.bat
    Export record=FULL file=$(Backup)\fullexp.exp
    Export record=correl domain=$(node) file=$(Backup)\correl.txt
    Export record=correl domain=$(node)/$SYSTEM file=$(Backup)\correlsys.txt
  }
}
```

The **<TaskGroup>** Backup performs the following functions every 24 hours at 0:00:

- Execution of the script `backup.bat`
- Full database export to `fullexp.exp`
- Performs address book export to `correl.txt`
- Export of the system data to `correlsys.txt`

Example: Deleting according to age

```
RemoveOld
{
  Periodicity=2D@2:00
  InformOnFailure=$(Administrator)
  InformOnSuccess=
  Task
  {
    DelDB record=Journal age=$(LIFETIME)
    DelDB record=Geb age=$(LIFETIME)
    Remove path=$(Folder) age=$(LIFETIME) option=x,recursiv
  }
}
```

The **<TaskGroup>** RemoveOld performs the following functions every 48 hours at 2:00:

- Deletes all journal database entries including documents older than `$(LIFETIME)` days.
- Deletes all charge cost database entries older than `$(LIFETIME)` days.
- Recursive deletion of all files that are in the path `$(Folder)` and older than `$(LIFETIME)` days.

Example: Permanently removing messages the recipient has deleted

```
RemoveDeleted
{
  Periodicity=24h@3:00
  InformOnFailure=$(Administrator)
  InformOnSuccess=
  Task
  {
    DelDB record=Journal originator=$NONINTERACTIVE flags=DELREC age=10
    DelDB record=Journal originator=$INTERACTIVE recipient=$INTERACTIVE
      flags=DELREC,DELOG age=3
  }
}
```

The *<TaskGroup>* RemoveDeleted performs the following functions every 24 hours at 3:00:

- All inbound messages are automatically deleted when the recipient has already deleted theirs (DELREC) and the message is more than 10 days old. Moreover, the message must be sent by an originator that cannot automatically delete the message, for example a fax device.
- All e-mails – both the originator and recipient are interactive – are deleted that have been deleted by the originator and recipient and are older than 3 days.

7.3 Backup

To avoid losing data in case of a system crash or hardware defect it is mandatory to save XPR server data in regular intervals. This section describes the **Smart Backup & Restore** feature, which is configured via the Web Assistant. This is a special backup script. It is executed by the MTA.

IMPORTANT:

For this feature to work, the installing user must be the one who was also assigned to the services upon the installation.

In case of Smart Backup, the “Temp” folder of this user is deployed during the backup generation. Memory available on the drive of the “Temp” folder should therefore be observed. The “Temp” folder is best located on the drive offering the most free memory.

The backup file should subsequently be moved to another location in the network for security reasons. Memory is then cleared as side effect.

IMPORTANT: The backup zip format cannot store files larger than 4Gb.

In case folders backup file is larger than 4Gb we suggest to:

- Reduce DocumentLifeTime to less than 30 days.
 - Change CompressionType (under MTA, REG_SZ) to "XZ".
The compression ration for this format is better than bz2 (however it is also slower).
This will make folders backup file smaller.
-

The Web Assistant and this mechanism can be used to perform a regular backup and to reinstall the backed up data on an XPR server newly set up. As precondition we assume that a server is set up with identical hard and software in case data recovery becomes necessary. In particular the XPR server is newly installed on this server as well so that server components realized as services correctly register with the system. To meet this requirement, a corresponding imaging software could be used. With this software you can create an image after the initial installation, which can later be brought in if, for example, the harddisk crashes.

Owing to the XPR database size and in particular to the document directory and the resulting time required for a backup, it is impossible to receive an exact image at a fixed time. Such possible deviations only concern data that were processed during the backup creation, though. Likewise, they do not affect the general ability to recover data. The only way to avoid this would be to stop the XPR server except for the kernel components, which is normally unacceptable.

Message Transfer Agent (MTA)

A system backup at a later date does not have to include the entire data amount but can restrict itself to important data so that the entire system is not unnecessarily loaded by the backup process. Only the data amount just sufficient for recovering the system in case of a complete data loss must be saved. This is performed by the backup script described in the following.

The backup configured by the Web Assistant is indicated in the MTA as maintenance job and stored as individual script with the name `backup.scr` parallel to the default maintenance script. See also [Section 7.2, "Maintenance Script", on page 214](#).

7.3.1 Syntax of the Backup Script

```
BACKUP
{
  Periodicity = <TimeSpec>
  Task
  {
    BACKUP options=<options> path=<path>
  }
}
```

The `Periodicity = <TimeSpec>` specification defines at which times a backup shall be performed. `<TimeSpec>` in the format `n[s,m,h,D,W,M,Y]@hh:mm` specifies the time `hh:mm` and periodicity `n` with which the backup is executed. The suffix `@hh:mm` indicates the time at which the backup is started. The prefix `n[s,m,h,D,W,M,Y]` refers to the periodicity: `10s` (every 10 seconds), `30m` (every 30 minutes), `6h` (every 6 hours), `15D` (every 15 days), `4W` (every 4 weeks), `2M` (every 2 months), `7Y` (every 7 years). With `Periodicity = 6h@0:00` the backup would be executed each day at 0:00, 6:00, 12:00 and 18:00 o'clock. You can use the Web Assistant to set daily, weekly and monthly backups.

`<path>` specifies the path in which the backup is stored. The created files are stored there under a name of type `YYMMDD_hhmm.tar`. This file must be integrated in the customer's normal security concept so that the option is given to restore the system from such a file. Default-set is `c:\windows\temp` if the MTA does not operate under a user account. The temp directory of the user account will be used otherwise.

IMPORTANT:

The created files are not automatically deleted. To avoid an overloaded disk, remove them manually or using an appropriate tool in regular intervals.

`<options>` is a comma-separated list of the backup options, which contains the data to be considered in a backup. Possible options are:

Option	Description
NCO	The NCO configuration files <code>NcoMainTree.xml</code> and <code>VariableProposals.xml</code> are backed up. All other data available in the <code><XPR Install>\NCO</code> directory are dynamically created at runtime.
registry	The registry section <code>HKLM\Software\Wow6432Node\PP-COM\MRS</code> of the kernel computer is backed up in the <code>regexp_serverconf.reg</code> file.
InfoStor	Complete export of the user and system data (Correlation database) and the database with the message headers (Journal database) to the file <code>fullexp.exp</code> .

Table 9 Backup Options of the Backup Script

Option	Description
Folders	Complete copy of the directories under the <code>MrsFolders\$</code> share. This includes all messages on the system.
Userdata	Complete copy of the directories under the <code>MrsUserData\$</code> share. This includes, for example, the users' personal greetings.
ISC	Complete copy of the directories underneath of <code><XPR Install>\ISC</code> . Here you find everything about <i>System Networking</i> .
UCC	The PostgreSQL database mrsddb is written in the <code>dump.sql</code> file. The SQL database of Web Collaboration is written in the <code>fastviewer.sql</code> file. This requires the user to have write access to the <code>MRSFolders\$</code> share under which the SQL server operates. The following files from the <code><XPR Install>/UCC/application_host/</code> directory are backed up: <pre> applets/conference/ConferencingApplication.xml binders/terminal/bindings/conference.xml providers/sip-connectivity/sip-connectivity.xml providers/streaming-mps/streaming-mps.xml </pre> From the <code><XPR Install>/UCC/common/conf</code> directory the <code>instance_8dff7acb-6780-4b7d-9089-e2684fc8b326-localhost.xml</code> file is backed up. The following OpenScape Web Client files: <pre> C:\Program Files\webconferenceserver\settings.ini <XPR Install>/cyPHONEWeb/config/*. * <XPR Install>/cyPHONEWeb/.keystore </pre>
SATELLITE	The registry section <code>HKLM\Software\Wow6432Node\PP-COM\MRS</code> of the satellite computers is backed up in the <code><satellite name>.reg</code> files.

Table 9 Backup Options of the Backup Script

7.3.2 Recovery

A backup copy is restored via a corresponding Web Assistant transaction. The restoration occurs in the background as maintenance job. During this time no other maintenance jobs may be executed. Beyond that, the system should not be actively used during restoration. The operating services should be restricted to the following:

- NameLoc
- LICSVL
- CfgSvc
- XmrSvc
- InfoStor
- MTA
- MailApl
- WEBAPL

Other services may hamper the restoration.

IMPORTANT:

OpenScape Web Client must be stopped before the recovery.

7.3.3 Transactions

The MTA knows the following transactions that are sent by the Web Assistant in the **Smart Backup & Restore** context:

```
BACKUP CMD="DISABLE"
```

The Backup.scr file is deleted.

```
BACKUP CMD="EXECUTE"
```

The backup is now being performed.

```
BACKUP CMD="SAVE" OPTIONS=<options> PATH=<path>  
SCHEDULE=<plan> TIME=<time>
```

The Backup.scr file is overwritten with the new settings. The parameters have the following meaning:

See [Section 7.3.1, "Syntax of the Backup Script", on page 229](#) for <options> and <path>.

<plan> can be DAILY, WEEKLY or MONTHLY.

<time> is the time in format HH:MM at which backups are to be performed.

```
BACKUP CMD="RESTORE" FILE=<file>
```

A recovery of <file> starts immediately.

7.3.4 Backing up the PostgreSQL Database

The MTA service, the Connection APL as well as the PostgreSQL service must run under the same user account for the MD5 check to take place successfully. This is not possible under Windows Server 2003 because the PostgreSQL service must not run under a user account with local administrator privileges on this operating system. See <http://archives.postgresql.org/pgsql-bugs/2011-08/msg00035.php> on this. Local administrator privileges, however, are required by the MTA. In addition, this user account needs *Full Control* of the `<XPR Install>\postgresql` directory.

The Smart Backup invokes `pg_dump`, which, in case of different users and MD5, expects the input of a password on the command line that must not automatically be transferred. The following workaround tempers the security settings for PostgreSQL, thus solving this problem in case of Windows Server 2003. For Windows Server 2008 you better use the same user account for the services.

To do this you need to change the `md5` to `trust` in the `<XPR Install>\postgresql\data\pg_hba.conf` file in the following section. The entry for IPv4 is used by Windows Server 2003. Windows Server 2008 uses IPv6.

Before:

#	TYPE	DATABASE	USER	CIDR-ADDRESS	METHOD
# IPv4 local connections:	host	all	all	127.0.0.1/32	md5
# IPv6 local connections:	host	all	all	:::1/128	md5

After:

#	TYPE	DATABASE	USER	CIDR-ADDRESS	METHOD
# IPv4 local connections:	host	all	all	127.0.0.1/32	trust
# IPv6 local connections:	host	all	all	:::1/128	trust

7.4 XPR Server Rules

The configuration of the XPR server is highly flexible through use of “rules”. Every transaction (dialog or store-and-forward) is checked for conformity with the rules within the router MTA.

Recipient addresses are transformed by means of rules. Routing is implemented with rules. Rules transform recipient addresses either by pattern-matching or through an address book lookup.

Rules configure the XPR server for the areas

- **Routing rules**

All routings within XPR are determined by such rules. In XPR there are no hardwired routing allocations.

- **Carbon copy rules (send copies)**

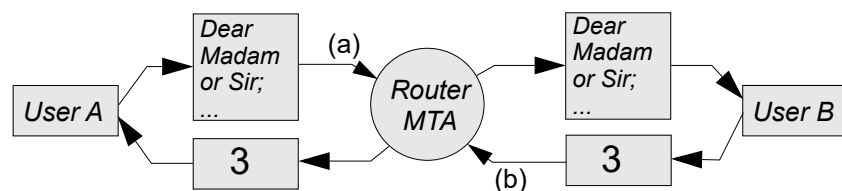
Send copies are used, for example, for department printers, postmaster accounts, archiving etc.

- **Awake rules**

The Mail APL can be instructed to send a copy according to conditions and a time frame given in these rules. In this way faxes that have not been read within three days could be automatically sent to an administrator or a postmaster account.

7.4.1 Rule Application within the Kernel

The following graphic illustrates the path a document and corresponding reports travel through the server:



User A sends a document to user B and receives the appropriate status report. On the way from A to B, the routing rules are applied with (a).

Applying carbon copy rules is controlled by the registry value [CarbonMode \[REG_SZ\]](#). This value may contain the comma separated strings `DOC`, `REPORT`, `REPEAT` and `HIDE`.

If the CarbonMode contains the `DOC` string, the carbon copy rules are applied with (a); but after using the routing rules. With `REPORT` they are used for (b).

Carbon copy rules are by default only used with reports that have a final status e.g. `OK` or `FAILURE`. If the application of rules is also desired for reports without final status (redial etc.), `REPEAT` must be specified in addition.

Hidden transactions are generally created by the system to document administrative processes. With these hidden transmissions the `HIDE` flag is set. If `HIDE` were specified as `CarbonMode`, the rules would also be applied to hidden transactions.

7.4.1.1 Application of the Routing Rules

When switching, the kernel attempts to apply all rules in a sequential order. At the same time, the rerouting rules are internally numbered and applied in canonical sequence. As soon as the condition of a rule is satisfied, the kernel then continues the process through-out the rule list. You can customize this behavior in the registry via the following values under the key

`HKLM\Software\Wow6432Node\PP-COM\MRS\MTA.`

RecursiveReRout [REG_DWORD]

Default:	1
Possible values:	0 – Apply routing rules once. 1 – Apply routing rules recursively.
Remark:	See also ReRoutLevel [REG_DWORD] .

This value determines whether the router is to apply the rules list recursively until with a list run-through no target address alteration occurs anymore. Otherwise the list will be run through only once.

ReRoutLevel [REG_DWORD]

Default:	10
Possible values:	0...n

Through `ReRoutLevel` the maximum number of rules are specified that could lead to a change in the recipient. With 1, for example, rule evaluation is terminated as soon as a rule has been successfully applied. The kernel creates debug information in the event that more than one rule has been used.

7.4.2 First Rules Examples

7.4.2.1 Routing through Pattern Matching

Rerouting of G3 fax documents addressed as +49240490* to the G4 fax address +49240492*:

```
NVS:FAXG3/\+49240490*=NVS:FAXG4/\+49240492*
```

This rule would forward an incoming Fax G3 message, e.g. addressed to +492404906650, as Fax G4 to +492404926650. All document conversions, etc. are performed automatically. Please note that each number is normalized before being processed by the routing rules. Each normalized number is either prefixed by a + sign for an international number or by a p for a private or internal number. The + sign must be indicated by a backslash in the rules.

Rerouting of all inbound Internet mails from one SMTP domain to another domain.

```
NVS:SMTP/*@firm.com=NVS:SMTP/*@firm.de
```

This rule forwards all inbound Internet messages addressed to anyone in the firm.com domain to the same user account in the firm.de domain.

In pattern matching the “*” is used for an arbitrary portion of the address.

7.4.2.2 Routing via Address Books

Rerouting of Fax G3 documents addressed to a number with the format +49123490* to Internet addresses defined in the address book (user database):

`NVS:FAXG3/\+49123490*=NVS:SMTP/<DB>`

This rule edits an incoming Fax G3 message, e.g. addressed to +491234905678. The server first tries to locate the user that has the +491234905678 address in the FAXG3 field. If a corresponding user is found in the user database, his/her e-mail address is determined from the SMTP field. If this address exists, the fax is automatically routed to the corresponding address. All document conversions, etc. are performed automatically. The example requires an address book entry such as the following:

USER	miller
FAXG3	+491234905678
SMTP	miller@acme.com

For the fax address +491234905678 user `MILLER` is determined first. Subsequently, the destination address is converted into the SMTP address `miller@acme.com` assigned to user `MILLER`.

7.4.3 Rule Structure

Rules can contain up to four elements and an optional comment.

```
Address1[condition]=address2[assignment]"comment"
```

Examples

```
NVS:FAXG3.*/*[ORG=NVS:FAXG3/001*]=NVS:LN/<DB>"Comment"
NVS:FAXG3.*/*=NVS:LN/<DB>[PRIO=1]"Comment"
```

`Address1` and `Address2` have the NVS address format. In addition the `NODE`, `CLASS` and `USER` fields can contain the wildcards `*` (no or several arbitrary characters) and `?` (exactly one character). The `[Condition]` is always applied to the recipient address of a transaction. If `Address1` and recipient address match, `[Condition]` is evaluated. If the requirements of `[Condition]` are fulfilled, `Address1` will be substituted with `Address2`. The variables in `[Assignment]` would also be set to their given values.

Besides the direct replacement of the address pattern by wildcards, there exists a much more effective conversion, namely the conversion via database references. Dissimilar address types can be transcribed through the use of correlation entries found within the user database.

7.4.3.1 Rule Element Address1 Structure

The recipient of a transaction is checked against the rule governing the address section `Address1`, to decide if the rule is applicable.

`Address1` has the format: `NVS:NODE.CLASS/USER`

Example

```
NVS:FAXG3.*/*\+32*
```

In the event that `Address1` and the recipient correspond with another, the rule is further evaluated. In this example the transaction to the recipient `NVS:FAXG3/32155` would be further evaluated.

7.4.3.2 Rule Element Structure - Condition

`Condition` is used to define additional prerequisites that must be met in order for a rule to be used. `Condition` can consist of one or more of the following conditions (logical AND operation) separated by semicolons:

```
ABORT =,<,>,! = n
```

Apply rule only if the `ABORT` variable is equal, greater than, less than, or not equal to `n`.

The ABORT default value is 0, but can be set in the [Assignment] portion to avoid e.g. recursions. See [Section 7.4.3.4, "Rule Element Structure - Assignment"](#), on page 245.

AGE >, >= *n*<*s*, *m*, *h*, *d*>

With awake rules only. This condition is met if the job's age is greater or equal *n* seconds (*s*), minutes (*m*), hours (*h*) or days (*d*). For example, with an age greater or equal 10 days the condition AGE>=10d.

FLAG =, !=, <, > Flag1, Flag2...

Rule only applies if the condition is fulfilled. In case of = all specified flags must be set. In case of != at least one of the specified flags must not be set. In case of < none of the specified flags must be set and in case of > it is sufficient if at least one of the specified flags is set. Most flags are automatically assigned by the MTA. Possible flags are:

Flag	Meaning
ADMINDELETE	If a message carries this flag, the message body is deleted as soon as an OK or FAILURE report arrives. The body is replaced with the short information that the message has been deleted. In order to delete e.g. all fax documents after their transmission, you can use the following rules: <pre>NVS:FAXG3.*/* [ORG!=NVS:FAXG3.*/*; FLAG!=ADMINDELETE]= NVS:FAXG3.*/* [FLAG=ADMINDELETE]</pre> <pre>NVS:FAXG4.*/* [ORG!=NVS:FAXG4.*/*; FLAG!=ADMINDELETE]= NVS:FAXG4.*/* [FLAG=ADMINDELETE]</pre> Attention: This option prevents the Unified Messaging or Integrated Messaging access via a telephone user interface since the documents are deleted on the XPR server as soon as e.g. an acknowledgement of receipt is delivered by the Exchange server.
ARCHIVE	Document recorded in archive.
AUTOTIMECPY	Document was generated by an awake rule.
CARBONCOPY	Document was generated by a carbon copy rule.
CIT	CIT signal sent.
CONFIDENTIAL	A message must not be forwarded when it carries this flag.
COST	Document booked in charge acquisition.
DONTFORWARD	Document was not forwarded.
EXLINE, EXLN	The MTA sets this flag automatically when a CLASS is defaulted in the destination address for a send job. This is the case if, for example, an APL or a client does not send to NVS:FAXG3/4711 but addresses to NVS:FAXG3.I0.0101/4711. The MTA also only uses this flag internally: it prevents the CLASS from being dismissed and newly determined with rescheduling a document.
EXTERNCOPY	Document is copied through the router.
FLAG1, FLAG2	Flag 1 and 2. These flags are set in the [Assignment] portion to pointedly avoid recursions.

Flag	Meaning
GATEIN	This document has come in via a Remote System Link.
GATEOUT	This document was forwarded via a Remote System Link.
HIDE	Document is not displayed.
LOCALUSER	This flag is exclusively set by the SMTP APL if it detects on grounds of its configured Local Domains table or by the MX records of its name server that the XPR server is a mail server for the destination address domain.
MAXREPSFAIL	Maximum number of repeats has been attained. Status set to failure.
NODELDOC	Document is not deleted during the physical deletion of the journal entry.
NODELMID	Document message ID was externally created.
NOPREFERRED	This flag is set in the [Assignment] portion so that the <i>Preferred</i> routing rule is not used in subsequent routing rule applications anymore.
NOREPORT	Standard reports are suppressed when report mails are used. For internal use only!
PRINTED	Document has been printed.
READ	Document has been read.
TXUNKAK	Special flag for VU-S charge invoice. Is not used by XPR anymore.

Example: FLAG=PRINTED, READ signifies that a rule is only applicable when a document has been read or printed.

FOLDER=<Folder Name>

Presetting is FOLDER=INBOX;

Example of subfolder: FOLDER=INBOX/TRASH (INBOX is always a path element).

FORMAT=<format-list>, FRM=<format-list>

Rule is applied only when the document format is contained in the format list <format-list>. A <format-list> is an abbreviation list (separated by commas) of all supported formats. See [Appendix A, "Document Formats"](#).

Example:

```
NVS:FAXG3.*/*[FRM=DCX,ASC;ABORT=0]=
NVS:FAXG3.I0.0101/*[ABORT=1]
```

Fax documents with the formats DCX and ASC are only sent via the fax line with class I0.0101. To avoid recursions, the value of the ABORT variable (default: 0) is set to 1 after using the rule.

FORMAT!=<format-list>, FRM!=<format-list>

Rule only applies when document format is not contained within the format list.

```
GROUP(ORG)=<Group Name>
GROUP(REC)=<Group Name>
```

The recipient (REC) and the originator (ORG) must belong to the group <Group Name>. An application example is a Robinson list which blocks certain fax numbers for transmission: NVS:FAXG3.*/*
*[GROUP(REC)=ROBINSON]=NVS:NIL/FAIL

LEN =,>,< != n

Rule only applies when the length of the document is equal , greater than, less than or not equal the n bytes.

ORG=<Address-Wildcard>, ORG!=<Address-Wildcard>

Apply rule only if the originator matches the address format <Address-Wildcard> or not.

Example: NVS:FAXG4/*[ORG=NVS:FAXG4/\+49*]=NVS:FAXG3/*

Fax G4 documents with the recipient NVS:FAXG4/* are routed to FAXG3 by this rule if the recipient address is of type NVS:FAXG4/+49*. Thus this rule would send all Fax G4 documents to a recipient in Germany as Fax G3.

ORGDB(<Field>)=<String>, ORGDB(<Field>)!=<String>

The system attempts to determine the originator's user name with the help of the database. The function operates analog to RECDB().

Example: NVS:FAXG3.*/*[ORGDB(OPTION1)=X]=NVS:FAXG4/*

Here an outgoing Fax G3 is rerouted as Fax G4 to the same number if in the originator database entry in the OPTION1 field the X value has been entered.

PRIO =, >, <, != *n*

Apply rule only when the transmission operation priority is equal, greater than, less than, or not equal *n*. Priorities fall within the area of 0 to 30000. 0 is the highest priority. The following standardized text priorities may also be used for *n*: URGENT (1000), HIGH (4000), NORMAL (5000), LOW (6000), NIGHT (10000).

PRIVMODE =, != <Mode>

The internal flag *PRIVMODE* is verified. *PRIVMODE* can have the following values:

Value	Meaning
EMAIL	E-mail
FFU	Fax-fax converter
FFUACN	Fax-fax converter confirmation
KGCHK	ID assignment check
PR	Department printer information
SMTP	SMTP-mail
TLXTTX	Transition telex-teletex
TTU	TTU transition
TTUACN	TTU acknowledgment
VOICE	Voice

PRIVOGROUP (ORG)=<Private Group of the originator>
 PRIVOGROUP (REC)=<Private Group of the originator>
 PRIVRGROUP (ORG)=<Private Group of the recipient>
 PRIVRGROUP (REC)=<PrivateGroup of the recipient>

Same as GROUP, however, for private groups.

RECDB(<Field>) =, != <String>

The system attempts to determine the recipient's user name with the help of the database. If successful, the contents of the user database field <Field> is compared with that of the <String>.

SUBJ=<Text>

Compares the contents of <Text> with that of the Subject field. Conditions are applicable if they are present in Subject. The subject field can always be up to 80 characters when using an XPR server.

SUCCESS =, >, <, != *n*

Apply rule only when transaction SUCCESS code is equal, greater than, less than, or not equal to *n*. The variable *n* can either be a number or a string.

Code	Meaning
0 UNDEFINED	Success undefined, no report as of yet.
1 UNKNOWN	Success is unknown, transaction continues.
2 OK	Transaction successfully completed.
3 FAILURE	Transaction failed. No further redial.
4 REJECT	Call collision. Redial will be performed.
5 REPEAT	Faulty completion. Redial will be performed.
6 DELAYED	Processing successfully completed, recipient to receive information at next login. This status is applicable when a document is sent to an e-mail subscriber who is currently not logged in. The information has been successfully written to the subscriber's mailbox.

TIME=h1:m1-h2:m2

Rule only applies if the current time is between h1:m1 o'clock and h2:m2. For example, if TIME=17:00-8:00, only use a rule between 5 p.m. and 8 a.m.

TYPE =, >, <, != *n*

Rule only applies when the transaction type is equal, greater than, less than, or not equal *n*.

Code	Meaning
1 DOCUMENT	Document send process.
2 REPORT	Report send process.
3 TRANSACTION	Opening of a new dialog.

WDAY =, != wd1, wd2, ...

Apply rule only if the current week day appears in the list or not. For example: WDAY=MO, DI, MI, DO, FR or WDAY!=SA, SO specifies that the rule is to be applied only Mondays through Fridays. The initial letters of the English weekday descriptions can also be used as abbreviation. The above example would thus read WDAY=MO, TU, WE, TH, FR.

Example: Using condition

NVS:FAXG3.*/*[RECDDB(OPTION1)=XYZ]=NVS:LN/<DB>

Incoming fax to NVS:FAXG3/+491234567890. Only the user with fax number 491234567890 will be determined. In the event that a match is found, the OPTION1 user database field is read and then compared with the string XYZ. With a successful comparison the Lotus Notes address is read out of this user's LN field and the fax sent to this address.

NOTE:

For some applications it is useful when database fields are added to facilitate any routing decisions. [Section 4.4, "The Mask Description Language MDL"](#), on page 112 explains in detail how to expand the user database by new fields.

7.4.3.3 Rule Element Address2 Structure

`Address` defines how the transaction recipient is transformed if a rule is to apply. Three different versions are available.

`Address` can either have an explicit format: `NVS:NODE[.CLASS]/USER`

Or it consists of a database request: `NVS:NODE[.CLASS]/<DB>`

In this example the recipient's database is queried and `<DB>` is then replaced by the entry. In the event that a database entry from the originator is required for the routing decision, `<ODB>` would be used.

The third version simply uses the originator address `<ORIG>` as address.

An example is the usage of a carbon copy rule with report form. See [Section 7.4.8, "Automatic Report Transmission by Mail"](#), on page 262.

Example: Database query (1)

```
NVS:FAXG3.*/*[ORG!=NVS:FAXG3.*/*]=NVS:PR/<ODB>
```

In this example, all outgoing Fax G3 documents defined in the originator's database also are routed to the printer. This rule could be used as carbon copy rule.

Example: Database query (2)

```
NVS:FAXG3/*=NVS:SMTP/<DB>
```

All documents sent to a Fax G3 address are to be examined. The first step is to determine if a user with the Fax G3 number `*` exists. If a user is found, then the user's SMTP mail address is queried from the database. If both operations are successful, the document is sent to the SMTP mail address. If an operation fails, this rule has no effect.

Example: Explicit form

If the recipient corresponds to the transaction type `Address1` and requirements in `[Condition]` are met, `Address1` is replaced with `Address2`.

```
NVS:FAXG3/\+49832*[PRIO=4]=NVS:TXSF/\+498888*
```

If a fax with priority 4 is sent to the address `NVS:FAXG3/+49832155`, the address is changed to `NVS:TXSF/+498888155` and the fax sent to this address.

7.4.3.4 Rule Element Structure - Assignment

In addition to the recipient, other characteristics of the transaction can also be modified. For this purpose, the recipient address must match `Address1` and `[Condition]` be fulfilled. `[Assignment]` can consist of one or several expressions separated by semicolon:

```
ABORT=n
```

The `ABORT` variable is set to value *n*. The `ABORT` value can be queried under `[Condition]` in other rules to prevent recursion. The default `ABORT` value is 0.

```
DEFER=n
DEFER=hh:mm
DEFER=hh:mm@day
DEFER=hh:mm@nd
```

Transmission time is delayed by *n* seconds to the time *hh:mm*, to the time *hh:mm* at the next weekday *day* of `[MO,DI,MI,DO,FR,SA,SO]` or `[MO,TU,WE,TH,FR,SA,SU]` or set to the time *hh:mm* in *n* days.

```
FLAG=ADMINDELETE | FLAG1 | FLAG2 | NOPREFERRED
OFLAG=FLAG1 | FLAG2
CFLAG=FLAG1 | FLAG2 | NOPREFERRED
```

The flags `ADMINDELETE`, `FLAG1`, `FLAG2` respectively `NOPREFERRED` can be set. These flags can later be queried in `[Condition]`. In contrast to the `ABORT` variable, `Flag1, 2` is also maintained outside a routing operation. `ABORT` is only valid during the routing process and cannot be queried further.

In case of a carbon copy rule a message copy is created. This copy only adopts the flags set in the carbon copy rule by `FLAG`. Here, this command does not set the corresponding flag but copies its value from the original message. Therefore, with `FLAG` in a carbon copy rule all flags listed in `[Condition]` are possible. Via `CFLAG` you can replace the flags for the copy itself. Via the `OFLAG` version you can additionally set a flag for the original message.

```
FOLDER=<Folder>
```

Shifts the message to an inbox subfolder if the recipient is a user.

```
FORM=<file name>
```

With a carbon copy rule use a report form for mail transmission. See [Section 7.4.8, “Automatic Report Transmission by Mail”](#), on page 262.

```
NORMALIZE=1
```

The destination address is normalized via this option. An example of use might be the following:

The customer sends his/her fax documents via SMTP with the syntax `<number>@<domain>`. The MTA translates this syntax into `NVS:FAXG3/<number>` via routing rule. In this case, the MTA uses the NCO without user-dependent normalization. The `NORMALIZE=1` option is added to normalize this number. As a result, the rule appears e. g. like this:

```
NVS:SMTP/*@fax.voip.intern=
    NVS:FAXG3/* [FLAG=NOPREFERRED;NORMALIZE=1]
```

```
ORIG=<NVS address>
```

Setting the originator. This is useful for returning a report form to the originator of a message per carbon copy rule. In this case you do not want using the primal message originator as report originator since he/she is actually the report's recipient. Therefore choose e.g. the user `POSTMASTER` as originator of the report. Rule example:

```
NVS:*/*[FLAG!=CARBONCOPY]=
<ORIG>[FORM=rpt.frm;ORIG=NVS:$(NODE)/POSTMASTER]
```

This rule sends the originator a report form for each message. `POSTMASTER` is then the report form's originator. Please take into consideration that such a rule may trigger an infinite recursion. This is the case, for example, if the originator uses an out-of-office wizard or a similar feature for automatic replies.

`PRIO=n`

The priority of the transaction will be set to `n` if the recipient address is of type `Address1`, and the `[Condition]` is satisfied.

`SUBJ=<Text>`
`OSUBJ=<Text>`
`CSUBJ=<Text>`

The Subject is set on `<Text>`. The variants `OSUBJ` and `CSUBJ` are intended for use with carbon copy rules and flag the original or the copy. The subject field can always consist of up to 80 characters when using an XPR server. The following variables may be contained in `<Text>`:

Variable	Meaning
{ORG}	Message originator as complete NVS address. Example: NVS:FAXG3.I0.0101/1234567890
{ORGNODE}	Service used by the message originator. Example: FAXG3
{ORGUSER}	Address of the message originator. Example: 1234567890
{REC}	Message recipient as complete NVS address.
{RECNODE}	Service used for the recipient. Example: EXCH
{RECUSER}	Recipient address
{SUBJ}	Original Subject which can thus be completed. The subject field can always consist of up to 80 characters when using an XPR server.

7.4.4 Extended Rule Syntax

Remember the rule structure:

```
Address1[condition]=address2[assignment]"comment"
```

7.4.4.1 Regular Expressions

You can use regular expressions for addresses and within the conditions. They offer a significantly more precise language for creating rules more flexibly and beyond that you can filter parts from the found address that are separately queried in the conditions and can be used for creating a new address.

The following table contains an overview of the elements that constitute a regular expression:

Element	Description
.	corresponds to each character except a line break.
*	corresponds to no or several copies of the previous expression.
[]	a character class that corresponds to any character within the brackets. If the first character is a '^', then this specification applies to all characters except the ones in brackets. Ranges can be specified by means of '-'. Example: [a-z]
+	corresponds to one or several copies of the previous expression.
?	corresponds to no or one copy of the previous expression.
	corresponds either to the previous or to the following expression.
()	groups a number of regular expressions to a new regular expression.
[: <ctype> :]	is another option to represent a character class. This representation can also be used in the character class described above. <ctype> is one of the following expressions:
	alnum corresponds to [0-9A-Za-z]
	alpha corresponds to [A-Za-z]
	cntrl corresponds to each character with an ASCII smaller than 0x20
	digit corresponds to [0-9]
	graph corresponds to each printable character
	lower corresponds to [a-z]
	print corresponds to graph and ' ' (blank)
	punct corresponds to [!.,;:]
	space corresponds to [\f\n\r\t\v]
	upper corresponds to [A-Z]
	xdigit corresponds to [0-9A-Za-z]

All other characters represent a regular expression that exactly corresponds to this character. By means of the ‘\’ character a special character can be used as normal character again. If a backslash is to be used in an expression as a backslash, it must be given twice (e.g. \\).

Examples

Expression	applies to
. *	any arbitrary character chain
* *	precisely two stars
www\.cycos\.com	www.cycos.com

Subpatterns

So that regular expressions can be used, the Address1 and Address2 portion must be set in inverted commas. The individual parts (subpatterns), found in Address1, can then be used in other parts.

The following syntax serves this purpose: %[<n>] <i>

<i> corresponds to the subpattern number, with 0 corresponding to the entire pattern. [<n>] is an optional length specification and restricts the number of subpattern characters to be considered.

This can also be applied to subpatterns collected in [Condition]. To access these, the following syntax is used analog to the subpatterns collected in addresses: # [<n>] <i>

Example:

```
"NVS:FAXG[34] (\..+)?/<.+>" [ %1 ?= "^0+900.*" ] = NVS:NIL/FAIL
```

This would find all valid Fax G3 and G4 addresses and check in the condition whether the number starts with 0..0900.. . In such a case the send job would be dismissed.

Regular expressions within a subcondition can be compared using the new ?= operator. The operator = would perform a simple comparison of the given character chain, regardless upper and lower case (case insensitive).

Further operators with regular expressions are <= and >=, which are only valid with numeric variables or flags.

Abbreviations for regular expressions

' ' => [\t] *

One blank in one expression applies to several blanks. If you want to filter exactly one blank, '\ ' or [] must be used.

'%c' => <[:print:]>

'%d' => <-?[:digit:]+>

'%s' => <[:graph:]+>

These have the same significance as with the `printf()` function of the C-standard-library.

'%f' => <[.0-9A-Z_a-z]*>

A valid file name.

'%t'

Corresponds to '%s' plus German special characters.

'%L' => <.*>

Arbitrary string with blanks.

Logic composition of the subconditions

You can link the single subconditions via the operators `&` (logic AND) or `|` (logic OR). The older syntax performs always only a logic AND of the single conditions with the operator `;` used up to now corresponding to `&`. To invert a logic value you can use the operator `!` (logic NOT).

By means of the brackets `()` you can skip the normal right association.

Example:

```
...[ !(SUBJ ?= "I LOVE YOU") | ABORT > 1 ] = ...
```

Functions

Three functions can be used: `len()`, `node()` and `addr().node()` and `addr()` have as argument either `O` (Originator) or `R` (Recipient) and deliver of the NVS address (NVS:NODE.CLASS/ADDRESS) the NODE and ADDRESS portion each.

`len()` can have an arbitrary string value as argument and redelivers the string length. The variables `SUBJ` or `ORG` can, for example, be an argument.

Example:

```
...[len(SUBJ) > 75] = ... [SUBJ = "{SUBJ[60]}...(truncated)"]
```

If the subject field of a message is longer than 75 characters, it will be shortened to 60 characters and the string "... (truncated)" added. The subject field can with the XPR server consist of a maximum of 80 characters.

New operators for the assignment portion of the address

Besides the familiar `=` you can now also use `+=` and `-=`: they enable incrementing a variable e.g. `ABORT` and adding or removing flags.

Example:

```
[FLAG -= READ]
```

This removes `READ` flag.

Comment lines in routing rules

Each line that begins with `;` is considered a comment line.

7.4.5 Meta Rules

The following special rule serves to simplify procedures.

`NVS:*.*/*=<PREFERRED>`

This rule defines the inbound routing for all services and proceeds as follows:

1. Attempts to ascertain the recipient `NVS:*.*/*` from the user database.
2. If a corresponding user exists, then the database field `PREFERRED` in the user database will be queried.
3. If an entry is found, the service defined in `PREFERRED` is read from the users database.
4. If this service exists as entry in the user database, then the document would be routed there.

Example: Application of the preferred rule

Incoming fax to 9099. An entry exists in the user database for user `AAA` with the following database field contents:

USER	AAA
PREFERRED	EXCH
FAXG3	9099
EXCH	AAA@EX.ORG

The Meta Rule determines the user `AAA` from the information in `FAXG3` and `9099`. The `PREFERRED` field from user `AAA` contains the entry `EXCH` (Microsoft Exchange) and the `EXCH` field contains the entry `AAA@EX.ORG`. The fax addressed to `9099` (`NVS:FAXG3/9099`) would therefore be routed to the Exchange gateway `NVS:EXCH/AAA@EX.ORG`.

Additionally, the database field `PREFERRED` is used for entering services preferences from the alias list. If a message is addressed to a user through the contact function of Communications, the service entered in this field is suggested and the corresponding address copied.

7.4.6 RouteLets

Under RouteLets, individual function expansions are implemented as DLL, and therefore allow extremely complicated transformations of routing information. The call is executed as follows:

```
NVS:*.*/*=<CUSTOM,dllname.dll>
```

This routing rule calls the function

```
extern int WINAPI CustomRoute (T_DESC *desc)
```

in the DLL `dllname.dll`, which then executes a transformation.

An example of the application is the implementation of least cost routing through the use of internal tables to find the cheapest telecommunications provider.

7.4.7 Examples and Uses

7.4.7.1 Routing Rules

Fax rerouting according to document format to dissimilar lines

```
NVS:FAXG3.*/*[FORMAT=TXT;ABORT=0]=NVS:FAXG3.I0.0101/*[ABORT=1]
NVS:FAXG3.*/*[FORMAT=FG3;ABORT=0]=NVS:FAXG3.I0.0201/*[ABORT=1]
```

Every document in text format (TXT) addressed to a Fax G3 address (NVS:FAXG3/*) is put out via line .I0.0101. Every document in the internal Fax G3 format (FG3) is put out via line .I0.0201. As soon as either rule is applied, the ABORT variable is set to 1. Since [Condition] assumes ABORT=0 in both rules, recursion is prevented.

Incoming fax switching

```
NVS:FAXG3.*/*=NVS:$ (NODE) /<DB>
NVS:FAXG3.*/*[ORG=NVS:FAXG3.*/*]=NVS:$ (NODE) /$ (POSTMASTER)
```

Fax G3 documents routed to any number are transmitted to the appropriate users on the XPR system \$ (NODE) , provided the appropriate database definitions are found. If no database definition is found for the Fax G3 address, the document is routed to user \$ (POSTMASTER) defined with the system installation. In addition it must be a document with originator FAXG3, since only incoming documents are sent to the postmaster.

NOTE:

Routing rules may contain the variables: XPR system name \$ (NODE) , default recipient \$ (POSTMASTER) , system administrator \$ (ADMINISTRATOR) , or default printer \$ (DEFPRINTER) . The default printer is configured in the Print APL.

Fax from the scanner via SMTP to the XPR server

```
"NVS:SMTP/scantofax@fax.mrs"[SUBJ?="[:digit:]+"]=NVS:FAXG3/#0
"NVS:SMTP/scantofax@fax.mrs"[SUBJ?="[:alpha:]+"]=NVS:NIL/FAIL
```

Scanned documents are sent to an SMTP address of the XPR server. In this process the fax address is transferred in the subject field. If the subject field contains digits, they are copied as fax address and the document is sent as fax. If no digits are contained, the second rule applies as an error report is sent to the originator.

Preventing official-channel optimizations

The preferred rule of the routing rules would effect the delivery of an SMS message to a user of the individual XPR server in a way that this message arrived as e-mail. So that this official-channel optimization does not take place, the

NVS:SMS.*/*[FLAG!=NOPREFERRED]=NVS:SMS/*[FLAG=NOPREFERRED]
rule can be implemented before the preferred rule so that it is no longer applied to SMS messages.

ISDN APL at two PBXs

Scenario: ISDN APL connected to two PBXs with an S_{2M} line in each case.

For outbound calls there must consequently be a criterium for assigning single users to a specific PBX. For this purpose, we introduce a new database field PBX. A user can now be assigned by entering PBX1 or PBX2 as content. This information can be queried in the routing rules, so that an outgoing call from the XPR server to the user dials the correct logical line and thus the correct PBX:

```
NVS:PLAYWAVE.*/*[ORGDB(PBX)=PBX1;FLAG!=FLAG1]=
NVS:PLAYWAVE.I0.0101/*[FLAG=FLAG1;FLAG=NOPREFERRED]

NVS:PLAYWAVE.*/*[ORGDB(PBX)=PBX2;FLAG!=FLAG1]=
NVS:PLAYWAVE.I2.0101/*[FLAG=FLAG1;FLAG=NOPREFERRED]

NVS:TELELIB.*/*[ORGDB(PBX)=PBX1;FLAG!=FLAG1]=
NVS:TELELIB.I0/*[FLAG=FLAG1;FLAG=NOPREFERRED]

NVS:TELELIB.*/*[ORGDB(PBX)=PBX2;FLAG!=FLAG1]=
NVS:TELELIB.I2/*[FLAG=FLAG1;FLAG=NOPREFERRED]

NVS:PHONEMAIL.*/*[ORGDB(PBX)=PBX1;FLAG!=FLAG1]=
NVS:PHONEMAIL.I0.0101/*[FLAG=FLAG1;FLAG=NOPREFERRED]

NVS:PHONEMAIL.*/*[ORGDB(PBX)=PBX2;FLAG!=FLAG1]=
NVS:PHONEMAIL.I2.0101/*[FLAG=FLAG1;FLAG=NOPREFERRED]
```

If four S₀ lines go to a PBX via a 4BRI card instead of one S_{2m} line, another problem appears: several physical lines cannot be combined to one logical line. The above rule would thus only fully load the first S₀ line. In this case you can extend the content of the PBX field and evenly distribute the users of the PBX connected via the 4BRI card among the four physical lines. In the following you see the adjusted rule for the PlayWave protocol only:

```
NVS:PLAYWAVE.*/*[ORGDB(PBX)=PBX1-1;FLAG!=FLAG1]=
NVS:PLAYWAVE.I0.0101/*[FLAG=FLAG1;FLAG=NOPREFERRED]

NVS:PLAYWAVE.*/*[ORGDB(PBX)=PBX1-2;FLAG!=FLAG1]=
NVS:PLAYWAVE.I0.0201/*[FLAG=FLAG1;FLAG=NOPREFERRED]

NVS:PLAYWAVE.*/*[ORGDB(PBX)=PBX1-3;FLAG!=FLAG1]=
NVS:PLAYWAVE.I0.0301/*[FLAG=FLAG1;FLAG=NOPREFERRED]

NVS:PLAYWAVE.*/*[ORGDB(PBX)=PBX1-4;FLAG!=FLAG1]=
NVS:PLAYWAVE.I0.0401/*[FLAG=FLAG1;FLAG=NOPREFERRED]
```

You can apply this principle analog for the IP APL, whereat the problem of several physical lines to one PBX does not occur.

Voice-only system

In the default configuration the recipient of a TUM transaction is determined by database query. In case of a voice-only system all TUM transactions are processed by the Mail APL. In a voice-only system you can thus substitute the relatively slow database query by directly assigning the TUM transactions to the Mail APL.

Set the following rule as the first one on top of the other routing rules:

```
NVS:$ (NODE) /* [TYPE=TRANS]=NVS:MAILBOX/* [ABORT=1]
```

Then look for the following entries:

```
NVS:*.*/*=<PREFERRED>  
NVS:*.*/*=<PRIVRULES,$REC.rules>
```

Modify them to:

```
NVS:*.*/* [TYPE=DOC]=<PREFERRED>  
NVS:*.*/* [TYPE=DOC]=<PRIVRULES,$REC.rules>
```

Flagging a voicemail as “Private”

Scenario: Incoming voicemails are forwarded to the customer's mail system via SMTP or Exchange Connector. The customer now demands the messages bound for the external mail system be flagged as *Private*, because the assistants may access the e-mails of their bosses but they may not access voicemails.

This can be achieved by the following rule:

```
NVS:VOICE.*/*=NVS:VOICE.*/* [FLAG=CONFIDENTIAL]
```

Default settings

You can easily toggle different settings through the configuration menus on the XPR monitor. The following default routing rules are preset with the `$ (NODE)` and `$ (POSTMASTER)` being replaced by the corresponding values:

```
; Standard Routing Rules
NVS:STAND-IN/*=NVS:$ (NODE) /*
```

Transform messages to the stand-in to his/her e-mail address.

```
NVS:VOICE.*/*[FLAG!=EXTERNCOPY & FLAG!=NOPREFERRED]=<NW>
```

Special voicemail network rule.

```
NVS:*.*/*=<PREFERRED>
```

Apply preferred rule.

```
; Extended rules:
; an address representing a regular expression must be quoted
; subconditions may combined by '&' or '|',
; ';' is equivalent to '&'
; '?' denotes a regular expression match
; evaluation order of subexpressions can be grouped by '(' ')'
"NVS:FAXG[34] (\..+)?/*" [node (ORG) ?="FAXG[34]"]=
  NVS:$ (NODE) /POSTMASTER
```

Example of applying regular expressions. Incoming Fax G3 and Fax G4 messages that could not be assigned to a recipient by the preferred rule, still have their original destination address. Subsequently, the XPR server would want to resend these messages itself. To prevent this, these messages are sent to the postmaster account.

```
NVS:VOICE.*/*[node (ORG)=VOICE;FLAG!=NOPREFERRED]=NVS:NIL/FAIL
```

Analog to fax messages, voicemails are not sent to the postmaster account but the originator receives an error report.

```
NVS:SMTP.*/*[node (ORG)=SMTP;FLAG=LOCALUSER;
  addr (ORG) !=MAIL-REPORT]=NVS:$ (NODE) /$ (POSTMASTER)
NVS:LN.*/*[node (ORG)=LN]=NVS:$ (NODE) /$ (POSTMASTER)
```

Analog to fax messages, transmission occurs to the postmaster account for SMTP and Lotus Notes if no recipient has been found via the preferred rule. Otherwise the XPR server would send these messages to itself (SMTP) or resend them via the gateway to the sending system (LN).

```
NVS:*.*/*=<PRIVRULES,$REC.rules>
```

Perform the user's private rules. These can be configured by the Communications user.

7.4.7.2 Carbon Copy Rules (Send Copies)

Via another batch of rules the recipients of job copies can be defined. An example are printers as recipients of an automatic archiving printout.

As already mentioned, the carbon copy rules application decision is taken by the actual carbon copy rules and the contents of the CarbonMode registry value. Therefore the following table provides an overview of possible contents of this value:

CarbonMode	Meaning
DOC	Apply to every document transmission
REPORT	Apply to final reports e.g. reports with status OK or FAILURE.
REPEAT	Apply to all reports. I.e. also to reports caused by, for example, redialing. This value is only useful in connection with REPORT.
HIDE	Apply rules to so-called "hidden" transactions as well. Hidden transactions are generally created by the system to document administrative processes. By hidden transmissions the flag HIDE is set.

Example: CarbonMode: REPORT (1)

```
NVS:TCPIP.*/*[ORG=NVS:FAXG3.*/*;SUCCESS=DELAYED; REC!=NVS:TCPIP/
$(POSTMASTER)] =NVS:TCPIP/$(POSTMASTER)
```

Reroute all incoming Fax G3 documents addressed to a user currently not logged in, to the TCP/IP address of the \$(POSTMASTER) account. In order to prevent recursion, the rule is only used if the addressee is not \$(POSTMASTER).

Example: CarbonMode: REPORT (2)

```
NVS:.*/*[REC!=NVS:PRINTER/*] =NVS:PRINTER/LASER"Printer"
```

Reroutes a copy from all transactions to the address NVS:PRINTER/HPLASER. To prevent recursion, the recipient is not equal to NVS:PRINTER.

NOTE:

Distribution lists cannot be used in carbon copy rules.

Service modification

In some instances it is desirable to modify not only the user address, but also the service that is provided.

Example: NVS:*.*/*=NVS:COPY/<DB>

In the user database the account of MEIER should have the LANA entry in the COPY field. Alternatively user SCHULZ should have the NVS:PPC/SOND entry in the COPY field.

A copy of mail sent to user MAYER, would be created and sent to NVS:COPY/LANA. By user SCHULZ, a copy would be made and sent to NVS:PPC/SOND. If the corresponding database address field contains a complete NVS address, the service (NODE) will be substituted as well.

IMPORTANT:

This option should only be used when no other possibility exists. If a complete NVS address is entered in a database mask, this field can *no longer* be used for inbound routing.

Default settings

Default settings are easily accessed through the configuration menus on the XPR monitor. The following *carbon copy rules* are activated for the relevant setting.

Incoming fax documents are copied to the default printer puts out all incoming fax documents to the first installed Print APL printer.

```
NVS:*.*/*[ORG=NVS:FAXG3.*/*;FLAG!=CARBONCOPY;FLAG!=NOPREFERRED]=
$(DEFPPRINTER) [FLAG=NOPREFERRED]
NVS:*.*/*[ORG=NVS:FAXG4.*/*;FLAG!=CARBONCOPY;FLAG!=NOPREFERRED]=
$(DEFPPRINTER) [FLAG=NOPREFERRED]
```

Incoming fax messages are copied to a user-defined printer expects a printer in the PRINTER user database field. If a user specifies this printer, each incoming fax can be put out at this device.

```
NVS:*.*/*[ORG=NVS:FAXG3.*/*;FLAG!=CARBONCOPY;FLAG!=NOPREFERRED]=
NVS:PRINTER/<DB> [FLAG=NOPREFERRED]
NVS:*.*/*[ORG=NVS:FAXG4.*/*;FLAG!=CARBONCOPY;FLAG!=NOPREFERRED]=
NVS:PRINTER/<DB> [FLAG=NOPREFERRED]
```

7.4.7.3 Awake Rules

Awake rules define under which circumstances and after what time period documents should be “awakened”. The Mail APL administers the awake rules. Time periods used for the awake rules can range from seconds to months. Besides the awake rules to be edited in the MTA configuration, the following registry values in key HKLM\Software\Wow6432Node\PP-COM\MRS\MailApl influence the awake rules' behavior:

AllowRecursiveAwake [REG_DWORD]

Default:	0
Possible values:	0 – Apply routing rules once. 1 – Apply rules several times recursively.

Analog to the corresponding routing rules behavior, awake rules can be run through several times until no rule is applied anymore. Differing from the routing rules, this default setting is to apply the rules once.

DatabasePollRate [REG_DWORD]

Default:	60
Possible values:	Seconds

Polling rate in which the journal database is processed by the awake rules. The poll rate must always be less than the minimum value entered as the age condition. If an age condition is specified for an age of 10 seconds, the poll rate must be set to 1 second. If the age condition is in days, then a polling rate of 3600 seconds (1 hour) is sufficient.

MaxAwake [REG_DWORD]

Default:	64
Possible values:	0..256

Maximum number of awake rules. Memory is reserved for the number of awake rules entered here.

Example:

DatabasePollRate: 3600

```
NVS:TCPIP.*/*[SUCESS=DELAYED;AGE>=7d]=
    NVS:$(NODE)/$(POSTMASTER)[SUBJ=7 Tage ohne Login]
NVS:TCPIP.*/*[SUCESS=OK;AGE>=10d;FLAG!=READ;FLAG!=PRINTED]=
    NVS:$(NODE)/$(POSTMASTER)[SUBJ=10 Tage nicht gelesen oder gedruckt]
NVS:.*/*[ORG=NVS:FAXG3.*/*;SUCESS=DELAYED;AGE>=4d]=
    NVS:$(NODE)/$(POSTMASTER)[SUBJ=4 Tage altes Fax]
NVS:.*/*[ORG=NVS:FAXG4.*/*;SUCESS=DELAYED;AGE>=4d]=
    NVS:$(NODE)/$(POSTMASTER)[SUBJ=4 Tage altes G4]
```

Every hour (3600 seconds) documents are investigated to see if one of the four AWAKE conditions apply.

Awake Rule 1:

Mail sent to a TCP/IP user who has not logged-in for a period of more than 7 days. (SUCCESS=DELAYED). A copy of this mail with the subject "7 days without login" will be sent to the postmaster account \$(POSTMASTER).

Awake Rule 2:

Mail sent to TCP/IP user that was received (SUCCESS=OK), but has not been read or printed within a 10-day period would be sent to the postmaster account \$(POSTMASTER).

Awake Rules 3 and 4:

Incoming Fax G3 and G4 messages that are not processed within a 4-day period are sent as a copy to the postmaster account \$(POSTMASTER).

Specials with variable usage

The variables {REC}, {RECNODE} and {RECUSER} do not deliver the original recipient but the new one already. Therefore, using these variables in the awake rules is pointless. This problem can be easily evaded by using regular expressions:

```
"NVS:*.*/<.*>"[ORG=NVS:*/*;AGE>60s;FLAG!=READ]=
NVS:TU512/POSTMASTER
[SUBJ=Fax, da vom Empf. %1 seit 60s ungelesen;FLAG=NOPREFERRED,HIDE]
```

The first sequence <.*> is inserted in the subject by the %1.

Default settings

The awake rules are deactivated in the MTA configuration. In addition to the individually defined ones, you can activate the following default:

Incoming documents are rerouted to a postmaster if not read

```
NVS:*.*/*[ORG=NVS:FAXG3.*/*;AGE>=10d;FLAG<READ,PRINTED]=
NVS:$(NODE)/$(POSTMASTER)
NVS:*.*/*[ORG=NVS:FAXG4.*/*;AGE>=10d;FLAG<READ,PRINTED]=
NVS:$(NODE)/$(POSTMASTER)
NVS:*.*/*[ORG=NVS:VOICE.*/*;AGE>=10d;FLAG<READ,PRINTED]=
NVS:$(NODE)/$(POSTMASTER)
```

7.4.8 Automatic Report Transmission by Mail

Some e-mail systems do not support the complete report information from the XPR server. E-mail reports can be created for these systems, whereby the missing information is excluded from the report.

Example: A fax is sent from an external mail system e.g. SAP R/3 or Microsoft Exchange over the XPR gateway. Occasionally, this external mail system transmits insufficient report information to the user or to a third person in the event of an error. The report forms described in the following allow the distribution of additional report information to the originator or a third person.

7.4.8.1 Report Forms Installation

Report forms are simple text files, which are stored in the directory `res\forms`. In order to activate these forms, the report mode must be switched on in the carbon copy rules. The value `Report` must also be inserted in the `CarbonMode` Key in the registry.

The mail report must now be activated through the appropriate carbon copy rule. Example:

```
NVS:*.*/*[TYPE=REPORT;ORG=NVS:LN/*]=NVS:LN/<ODB>[FORM=report.ok]
```

Report forms can be applied to the various status reports through use of the `SUCCESS` condition.

Example: Lotus Notes

```
NVS:*.*/*[TYPE=REPORT;SUCCESS=OK;ORG=NVS:LN/*]=
    NVS:LN/<ODB>[FORM=report.ok;FLAG=-NOPREFERRED]
NVS:*.*/*[TYPE=REPORT;SUCCESS=FAILURE;ORG=NVS:LN/*]=
    NVS:LN/<ODB>[FORM=report.bad;FLAG=-NOPREFERRED]
```

Example: Microsoft Exchange using ExchApl / ExUmApl

```
NVS:*.*/*[TYPE=REPORT;SUCCESS=OK;ORG=NVS:EXCH/*]=
    NVS:EXCH/<ODB>[FORM=report.ok;FLAG=-NOPREFERRED]
NVS:*.*/*[TYPE=REPORT;SUCCESS=FAILURE;ORG=NVS:EXCH/*]=
    NVS:EXCH/<ODB>[FORM=report.bad;FLAG=-NOPREFERRED]
```

The `NOPREFERRED` flag is removed here from the report form. If a message carries this flag, it is automatically transferred to the report form. In this way the report form is not associated with the original originator and thus never reaches him/her. This flag is, for example, set with SMS messages by default, so that no report forms on sent SMS messages would reach the originator without this adaption.

Example: Microsoft Exchange On premises 2016 or higher or Exchange Online using EwsApi

```
NVS:./*[TYPE=REPORT;SUCCESS=OK;ORG=NVS:SMTP/*]=NVS:SMTP/
<ODB>[FORM=report.ok;FLAG=-NOPREFERRED]
```

```
NVS:./*[TYPE=REPORT;SUCCESS=FAILURE;ORG=NVS:SMTP/*]=NVS:SMTP/
<ODB>[FORM=report.bad;FLAG=-NOPREFERRED]
```

7.4.8.2 Report Forms Structure

The report form is a simple text file that may contain the following variables:

Variable	Meaning
{COST}	Charge information.
{COSTUNITS}	Number of cost units (Charge pulses).
{DATE}	Date in the format of the default language set on the server.
{DIGEST[, <Max>]}	A portion of the sent message is embedded in the report. This can be either text or a string indicating the type of message. In case of a fax, for example, only the type can be stated. The maximum length can be defined through the optional entry <Max>. The algorithm used for building the Digest attempts to retrieve the text without a loss of information. Example: Empty lines, greetings, ...
{DOCUMENT}	The sent document is enclosed in the report as attachment. If this document is a fax with cover page, the actually sent fax cover page is then displayed in the report. In the individual send journal e.g. only the original document would otherwise appear with the XPR server probably attaching the fax cover page to it per Application Converter. If the conversion to fax should produce an error, the original document inclusive all attachments is sent in the report.
{FILENAME}	Readable list of file names for the original message including attachments.
{FORMAT}	Original message format (e.g. Voice, Fax or e-mail).
{MID}	XPR message ID.
{ORGID}	Originator ID for telematics services.
{ORGNAME}	Readable form of the originator address. If information about the fax originator is contained in the Alias database, this could appear as a name instead of a fax number.
{ORGNODE}	Incoming service. The NODE portion of an NVS:NODE/USER address.
{ORGORGNAME}	Readable form of the original originator for documents that are forwarded to other users.
{ORGORGNODE}	The original {ORGNODE} for a forwarded document.
{ORGORGUSER}	The original {ORGUSER} for a forwarded document.
{ORGRECNAME}	Readable form of the original recipient for documents that are forwarded to other users.

Variable	Meaning
{ORGRECNODE}	The original {RECNODE} for a forwarded document.
{ORGRECUSER}	The original {RECNODE} for a forwarded document. This value is also interesting in a document sent to an Exchange or Notes address. For a fax, the respective gateway address would be entered by the routing rules in {RECNODE}, whereas here the originally dialed fax number would be sustained.
{ORGUSER}	Originator address. The USER portion of an NVS:NODE/USER-address.
{RECID}	Recipient ID for telematics services.
{RECNAME}	Readable form of the recipient address. In case of a fax, this can be e.g. the recipient ID.
{RECNODE}	Target service. The NODE portion of an NVS:NODE/USER address.
{RECUSER}	Recipient address. The USER portion of an NVS:NODE/USER-address.
{REPEATS}	Number attempts required for the successful transmission of a document.
{REPORTTIME}	Time of the last XPR report for original message.
{SENDTIME}	Local time of the originator at which the document was sent (timezone of the originator).
{SENDTIMEREC}	Local time of the recipient at which the document was sent (timezone of the recipient).
{STATE}	Readable delivery status.
{SUBJECT[, <Max>]}	Subject line of the original message. The maximum length can be defined through the optional entry <Max>. If the subject is longer, it will be truncated and "..." is appended. The subject field can always consist of up to 80 characters when using an XPR server.
{TIME}	Creation time of the report. The format corresponds to the default language set on the server.

Example: Report forms

```

=====
XPR Report: OK
=====

From:      {ORGNAME}
To:        {RECNAME}
Original-To: {ORGRECNAME}
MID:       {MID}
State:     {STATE}
Cost:      {COST}
Subject:   {SUBJECT}
Digest:    {DIGEST,256}
=====

```

7.4.8.3 Subject Customizing

The subject of a report is in case of a fax usually a reference to the document, thus for example “Fax Message (MID)”. Since from this you cannot clearly gather that it is a fax message delivery report with the message ID `MID`, you can customize the subject field in the carbon copy rule. The following rules are examples of reports on fax messages to Microsoft Exchange:

```
NVS:FAXG3.*/*[TYPE=REPORT;SUCCESS=OK;ORG=NVS:EXCH/*;FLAG!=HIDE]=
    NVS:EXCH/<ODB>[FORM=fax-report.ok;FLAG=HIDE;CSUBJ=Delivered: {SUBJ}]
NVS:FAXG3.*/*[TYPE=REPORT;SUCCESS=FAILURE;ORG=NVS:EXCH/*;FLAG!=HIDE]=
    NVS:EXCH/<ODB>[FLAG=HIDE;FORM=fax-report.fail;CSUBJ=Undeliverable:
    {SUBJ}]
```

As result a report on a successfully delivered fax under Exchange would receive the subject “Delivered: Fax Message (MID)”. Via the `CSUBJ` parameter you can thus arbitrarily modify the report subject.

7.4.8.4 Normal Report Suppression

If the normal default report for the recipient APL is to be suppressed, the `NOREPORT` flag must be set for the carbon copy rule sending the report. This flag influences the original message and suppresses the transmission of the default report so that only the report mail created by the carbon copy rule is sent as a document. Example:

```
NVS:*//*[TYPE=REPORT]=NVS:MAILBOX/<ODB>[FORM=report.ok;FLAG=NOREPORT]
```

7.4.9 Error Handling

The absence of rules would lead to catastrophic routing errors. If there were, for example, no rules for the incoming routing of Fax G3 documents, all incoming fax documents would be directly sent to the same number to which they were addressed. In an ideal situation this would lead to a resonance catastrophe for the server.

XPR generates a warning in the event such a routing situation is discovered.

Example: No routing rules

The routing rules do not include any entries. Now a fax arrives at the system which is addressed to the number 8324567. Since the address cannot be translated through any application of a rule, the target address remains `NVS:FAXG3/8324567`. This fax will then directly be sent to the external number 8324567...

7.4.10 Recursions

When applying rules, be sure to avoid recursions. Recursions will be detected by the system, but never the less, it's an unnecessary system load.

7.4.11 Tips for setting Rules

Since rule set processing is always performed a number of times (max. 10 times) if a hit is detected during a cycle, the defined rules should be examined closely. The following two entries have eventually the same effect. A rule set is processed with the first rule several times and with the second rule only once, though.

```
NVS:SMTP.*/*=NVS:SMTP.*/*[PRIO=1000]
NVS:SMTP.*/*[PRIO!=1000]=NVS:SMTP.*/*[PRIO=1000]
```

If multiple rules are needed, it may be necessary to change the number of permitted rules in the registry. The default setting for [MaxReRoutRules](#) [REG_DWORD] is 64 entries. You must restart the XPR server for changes to take effect.

7.4.12 Testing new Rules

The XPR monitor should be used in all instances of rule modification to test the effects of the modification. To do this, configure a viewer which displays the MTA topics *RuleEvaluation*, *RoutingEngine* and *Messages*.

7.5 Watchdog Process

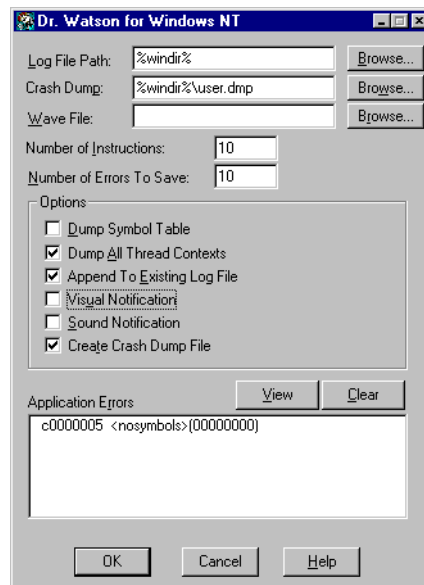
Locked-up or failed XPR services can be restarted through use of the Watchdog processes. The Watchdog is integrated in the XPR .EXE program and continuously monitors all XPR services within a distributed system. In the event of e.g. memory protection fault by a service, the Watchdog will automatically attempt to correct the error.

To activate the XPR Watchdog service, select the MTA configuration dialog in the XPR monitor. There select the **Automatic Maintenance > Watchdog > Monitor NT services, automatically restart on failure**. Automatic monitoring of the system should begin within the next 30 seconds.

The standard Windows configuration does not immediately terminate a process due to an exception error. Instead, a dialog box is displayed informing the user of the error. In the meantime, the faulty process remains in the memory and the Watchdog prevents this process from restarting until a user clicks OK.

So that the Watchdog can function properly, the user consideration must be switched off. Therefore delete the `debugger` value in the registry in the `HKLM/Software/Microsoft/Windows NT/Current Version/AEDebug` key. Now invoke `"drwtsn32 -i"` to install Dr. Watson.

Subsequently, invoke the Dr. Watson configuration using `drwtsn32`.



Deactivate **Visual Notification** here.

7.5.1 How the Watchdog functions

The Watchdog monitors the Services Control Manager on all computers within XPR systems. Distributed XPR systems are also monitored by the Watchdog.

For this purpose, all XPR processes are integrated ¹ in the monitoring. Also those processes that could not be started upon booting the XPR server can be monitored at a later time after they have been started manually. This could be the case with a distributed XPR server with the APL s on the non-kernel computers.

If an error occurrence is reported by an APL, the Watchdog will attempt to restart the APL up to ten times within an hour. In the event of an error occurring more than ten times in an hour, the Watchdog will no longer attempt to restart the APL and removes it from its list of services to be monitored.

If a kernel module should crash the complete XPR server will be restarted. Three attempts will be made by Watchdog within a one hour period to restart the server. If more than three crashes occur within an hour the Watchdog will no longer try to restart the server.

To allow a cluster system sufficient time to correct a problem itself, waiting periods can be configured before an APL or the XPR server attempts a restart. The following registry values in the key `HKLM\SOFTWARE\Wow6432Node\PP-COM\MRS\Services` serve for this:

WatchdogRestartSystemDelay [REG_DWORD]

Default:	10 – Default 240 – For a cluster system
Possible values:	Seconds

Wait-time prior to system restart by the Watchdog process. In case of a cluster system such as MSCS or VINCA the default is automatically increased so that these systems gain time for their own measures.

WatchdogRetryDelay [REG_DWORD]

Default:	5 – Default 120 – For a cluster system
Possible values:	Seconds

Wait-time prior to system restart by the Watchdog process. In case of a cluster system such as MSCS or VINCA the default is automatically increased so that these systems gain time for their own measures.

If the error is already corrected within the waiting time and externally – for example, by the Cluster Administrator – the XPR Watchdog will not be activated in the first place.

Furthermore, you can set the maximum number of start attempts via [MaxRetries \[REG_DWORD\]](#):

1. The license service (LICSVCL) is not monitored by the Watchdog.

MaxRetries [REG_DWORD]

Default:	20
Possible values:	Number of start attempts

Maximum number of attempts of the watchdog process to restart a process.

If a service is duly shut down, it also logs off from the Watchdog, so that no automatic reboot is performed.

7.5.2 Watchdog Configuration

If an error is recognized, the Watchdog takes from the value in the registry key `Recover-<Service>` a list of commands to be executed prior to the service start. If the service is not found on the kernel machine, the value `Recover-<Computername>-<Service>` is used.

If a kernel module should crash, command lines are executed from `Recover-<Service>` and subsequently from the `Recover Kernel`.

If the MTA should crash, the command `Recover-MTA` must be executed first followed by the command `Recover-Kernel` before the complete XPR server can be restarted.

The following registry values in the key `HKLM\SOFTWARE\Wow6432Node\PP-COM\MRS\Services` can thus be used for corresponding configurations:

Recover-Kernel [REG_MULTI_SZ]

Default:	<Empty>
Possible values:	One command may be entered per line.

These commands are executed by the Watchdog prior to the restart of the XPR server due to the crash of a kernel module. One command may be entered per line.

Recover-<Computer name>-<Service> [REG_MULTI_SZ]

Default:	<Empty>
Possible values:	One command may be entered per line.

These commands are executed by the Watchdog prior to the restart of a `<Service>` on the computer `<Computername>` in a distributed XPR server.

Recover-<Service> [REG_MULTI_SZ]

Default:	<Empty>
Possible values:	One command may be entered per line.

These commands are executed by the Watchdog prior to the restart of a `<Service>`.

7.6 Heartbeat Monitor

The MTA can check the availability of APLs by sending a heartbeat message to the APLs in regular intervals. If an APL does not answer this message the MTA will try to reboot this APL. If this reboot fails, then an external tool can be invoked for terminating the APL hard as last option. In this case the process watchdog would reboot the APL automatically. See [Section 7.5, “Watchdog Process”](#).

The following registry values in the key `HKLM\SOFTWARE\Wow6432Node\PP-COM\MRS\MTA` control the monitor's behavior. No APL is actively monitored by default.

HeartbeatApls [REG_MULTI_SZ]

Default:	<Empty>
Possible values:	<APL name>[,<process name>]
Example	exumapl exumapl5,exumapl

This entry lists the APLs monitored with the heartbeat monitor. If the APL name deviates from the process name, then it must be specified in addition.

HeartbeatInterval [REG_DWORD]

Default:	30
Possible values:	5-300 <seconds>

Interval in which the APLs listed in [HeartbeatApls \[REG_MULTI_SZ\]](#) are queried. This corresponds to the heartbeat.

HeartbeatWaitTime [REG_DWORD]

Default:	5
Possible values:	5-30 <seconds>

Period in seconds in which an answer by the respective APL is waited for.

HeartbeatWarnFails [REG_DWORD]

Default:	3
Possible values:	3-12

Number of successive heartbeat query errors that lead to a warning by the MTA.

HeartbeatErrFails [REG_DWORD]

Default:	6
Possible values:	6-12

Number of successive heartbeat query errors that lead to an error message by the MTA. This value should be greater than [HeartbeatWarnFails \[REG_DWORD\]](#).

HeartbeatRestartFails [REG_DWORD]

Default:	9
Possible values:	9-12

Number of successive heartbeat query errors that make the MTA try a reboot of the affected APL.

Capabilities [REG_MULTI_SZ]

Default:	<Empty>
Possible values:	Complete path to a batch file
Example	C:\OpenScape\xpr\restart-apl.bat

This batch file is invoked rebooting an APL by the MTA fails. Three parameters are handed over to the batch file:

- The host name of the computer on which the APL operates.
- The APL name.
- The process name.

The batch file may have the following content:

```
pskill /accepteula \\%1 %3
```

In this case the external program pskill would be invoked by SysInternals.com for terminating the process on the computer on which this process is running.

7.7 Distributed XPR Server

The XPR server was designed with the concept that all components could be distributed over various nodes. The following steps should be followed:

For a secure installation all services must be started with an account since the default system account has no access to the network. This account must have the privilege `LogOnAsService` and network access authorization. A service is assigned to an account through the Service Control Manager.

Under the key `HKLM\Software\Wow6432Node\PP-COM\MRS\Services` in the values `Kernel [REG_MULTI_SZ]` and `Access Protocol Layers [REG_MULTI_SZ]` you need to specify the name of the computer on which the corresponding XPR service is to be started after the comma in each case. At least one kernel entity of the NameLoc must be started on each of the involved Windows servers. Therefore, numerous lines with NameLoc, whereby the corresponding Windows server name appears behind the comma.

Example of `Kernel [REG_MULTI_SZ]`

```
NameLoc, NTSERVER1  
NameLoc, NTSERVER2  
CfgSvc, NTSERVER1  
CfgSvc, NTSERVER2  
XmrSvc, NTSERVER1  
InfoStor, NTSERVER1  
MTA, NTSERVER1
```

The key `HKLM\Software\Wow6432Node\PP-COM\MRS\MRS Globals` must be replicated on all participating computers. This key contains all the information that must be known for all XPR operations.

The directory tree `<XPR Install>\Res` must be manually reproduced on all participating servers in order to achieve an acceptable performance for the playback of voice prompts. Currently the `Res` contains only static files.

The corresponding APL configuration may only exist locally on the respective computer.

All required steps are described in the *Server Installation* manual.

7.7.1 Firewalls between Nodes of a distributed XPR Server

If you want to install a distributed XPR server in a way that individual components can communicate across a firewall (packet filter), observe the following points:

- Use TCP/IP as communication protocol. For this, remove all other network protocols from all XPR computers.
- Make sure that all computers can “view” each other in the network. To check you need to execute the command `net view \\<Server>` of all XPR computers to all distributed XPR computers and check if the connection is working. You also may have to adapt the `LMHOSTS` file.
- The firewall must accept packets from any XPR computer and forward them as follows:

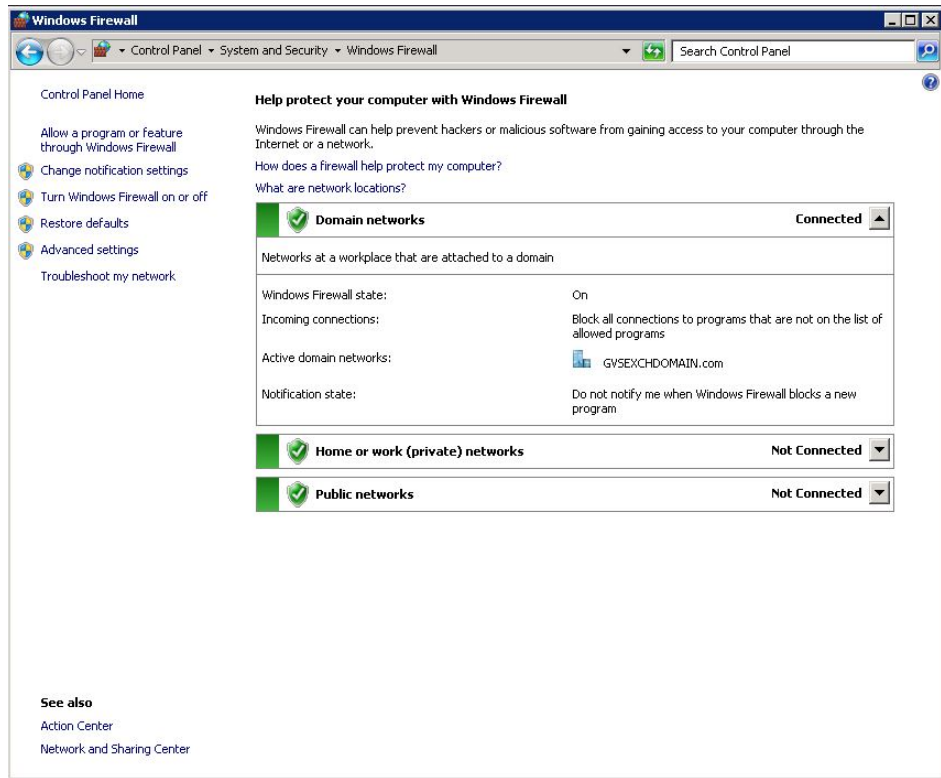
Service		Source	Destination
netbios-ns	TCP/UDP	137	137
netbios-dgm	TCP/UDP	138	138
netbios-ssn	TCP/UDP	1024-65535	139
Microsoft-SMB	TCP/UDP	1024-65535	445
Con APL	TCP/UDP	1-65535	10000-10006
License Service	TCP/UDP	1-65535	13010
License Server	TCP/UDP	1-65535	61740

Table 10 Ports for a distributed System

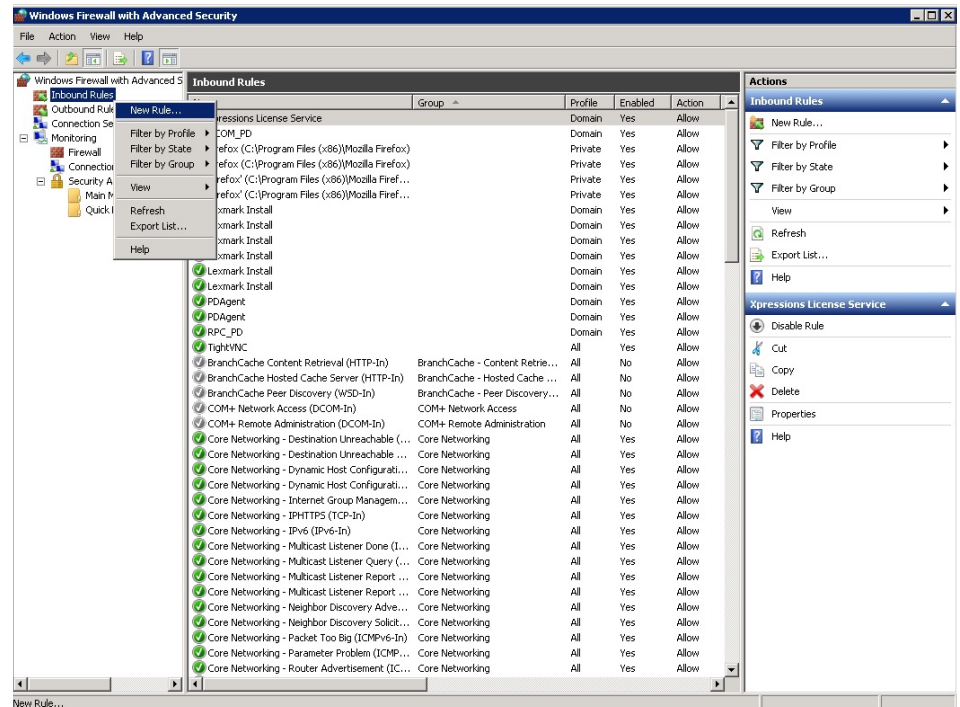
- All other ports are neither needed by Windows nor by the XPR system for internal communication. For using the SMTP APL, TCP/IP APL or Web APL across a firewall, the respective ports **must not be blocked**.
- You will find an overview of the used TCP/IP ports of the XPR server in the table in the following section.

In order to configure the Microsoft Windows firewall to work with Xpressions please follow the steps below.

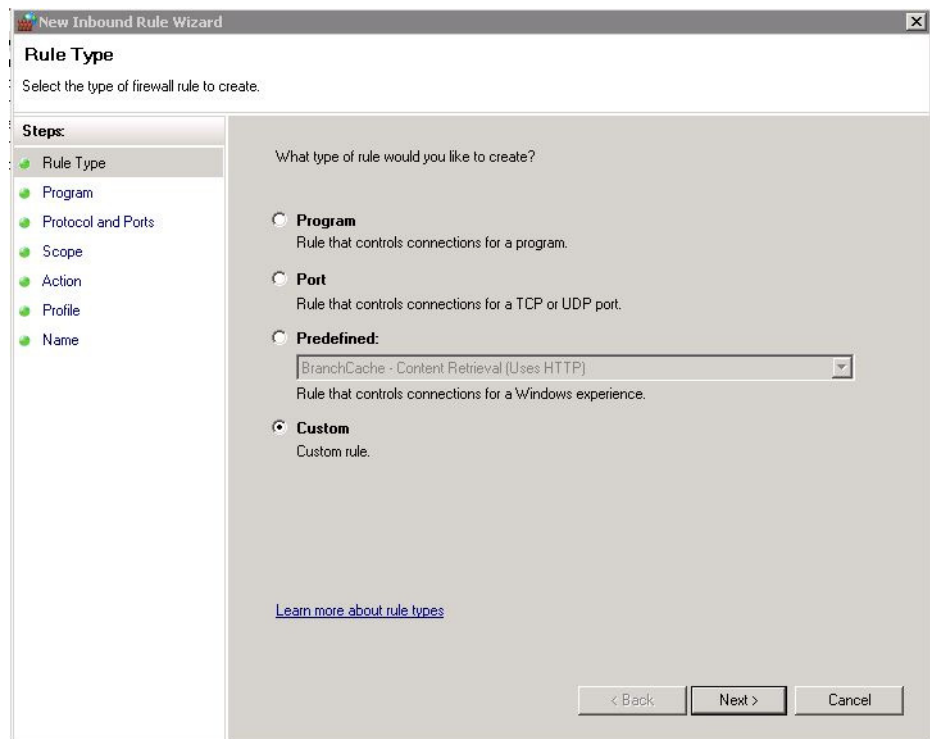
1. Turn Windows Firewall on Control Panel > **System and Security** > **Windows Firewall** > **Turn Windows Firewall on or off**. Click on **OK**.
2. Create a special rule for Xpressions and select Advanced Settings:



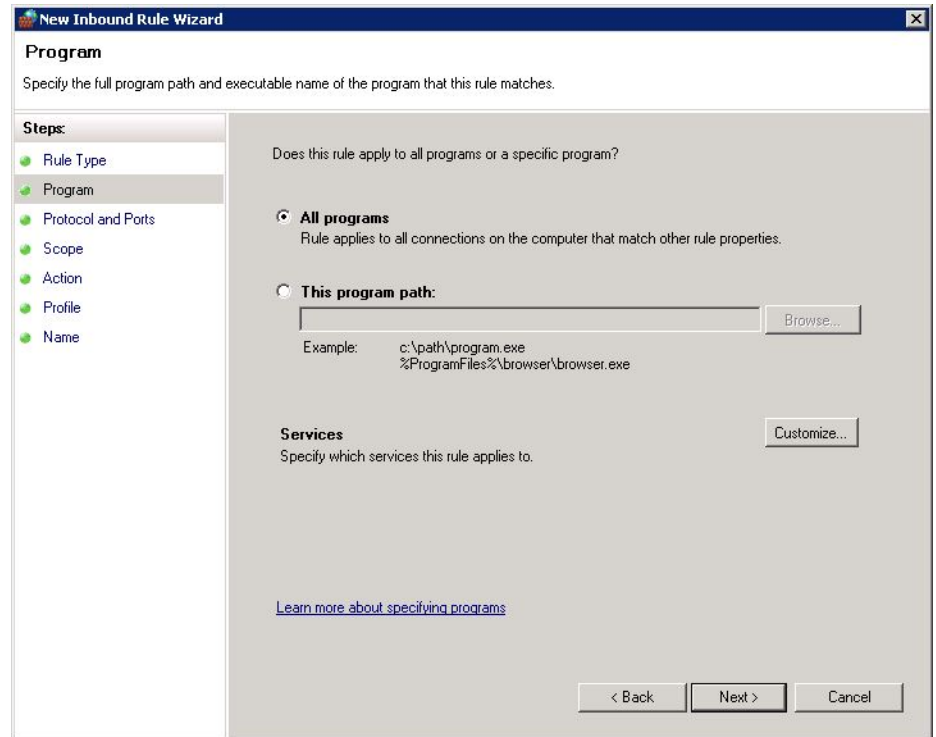
3. Create a New Rule: (Click on Inbound Rules with a right mouse click and select New Rule.)



4. Set the Rule Type to **Custom** and click on **Next**.



5. Set the Rule to be applied to **All programs**.
Click on **Next**.



6. Now set the Protocol type as TCP / UDP according to your system and network configuration.

And Local port to Specific Ports.

Now you can enable the local ports according to the features you have installed on Xpression server, for example:

Port 13010 is mandatory as it is the Xpression License Server port.

Port 8944 and 8945 are for Client communication (MSP unsecure and secure).

Port 5060 and 5061 are for SIP Connectivity (IpApl unsecure and secure).

Port 25 is used by SmtplApl.

Port 110 is used by SmtplApl - Pop3

Message Transfer Agent (MTA)

Port 143 is used by Smtpl - IMAP
Port 443 is used by WebApl.
Port 10000 and 10001 are used by ConApl.

NOTE: For a list of all Xpression ports refer to [Section 7.8, “TCP/IP Ports used by the XPR Server”](#).

NOTE: If you have Apls installed on a satellite this same Firewall settings must be done in the Satellite computer.

7. The Remote port must be set to **All Ports**.
Click on **Next**.

The screenshot shows the 'New Inbound Rule Wizard' window, specifically the 'Protocol and Ports' step. The window title is 'New Inbound Rule Wizard'. The main heading is 'Protocol and Ports' with the instruction 'Specify the protocols and ports to which this rule applies.' On the left, a 'Steps' pane lists: Rule Type, Program, Protocol and Ports (selected), Scope, Action, Profile, and Name. The main area is titled 'To which ports and protocols does this rule apply?'. It contains the following fields: 'Protocol type:' set to 'TCP'; 'Protocol number:' with a spinner box showing '6'; 'Local port:' set to 'Specific Ports' with a list of ports '13010, 8944, 8945, 5060, 5061' and an example '80, 443, 5000-5010'; 'Remote port:' set to 'All Ports' with the same example; and 'Internet Control Message Protocol (ICMP) settings:' with a 'Customize...' button. A link 'Learn more about protocol and ports' is at the bottom left. Navigation buttons '< Back', 'Next >', and 'Cancel' are at the bottom right.

8. Set the Scope for any local IP addresses.
Restrict the Scope for Remote IP addresses on the Kernel to the Satellites and Clients.

Select remote IP addresses - **These IP addresses**
Click on **Add**.

New Inbound Rule Wizard

Scope
Specify the local and remote IP addresses to which this rule applies.

Steps:

- Rule Type
- Program
- Protocol and Ports
- Scope**
- Action
- Profile
- Name

Which local IP addresses does this rule apply to?

☒ Any IP address

☐ These IP addresses:

[Empty list box]

Add... Edit... Remove

Customize the interface types to which this rule applies: Customize...

Which remote IP addresses does this rule apply to?

☐ Any IP address

☒ These IP addresses:

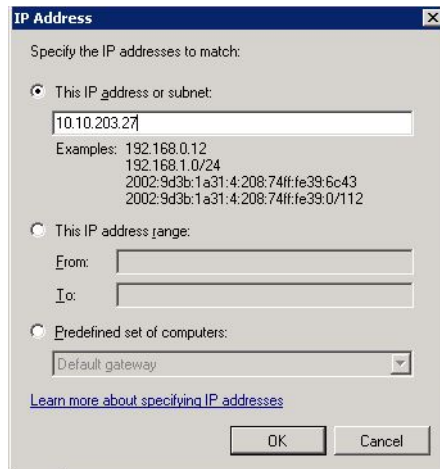
[Empty list box]

Add... Edit... Remove

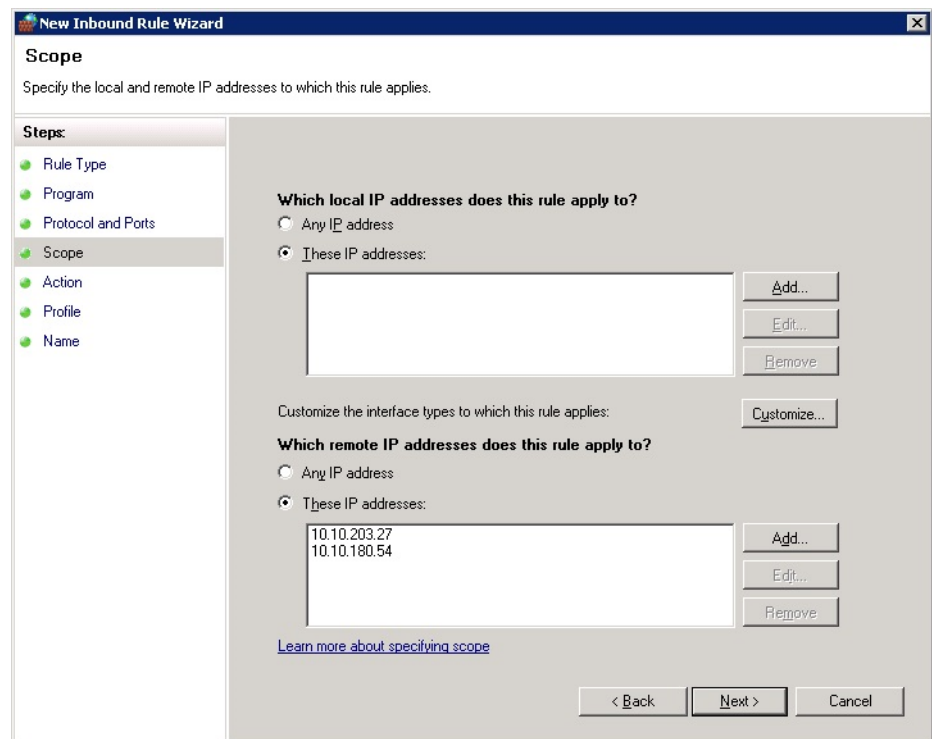
[Learn more about specifying scope](#)

< Back Next > Cancel

- Set the IP Address, subnet or range.
Click on **OK**.

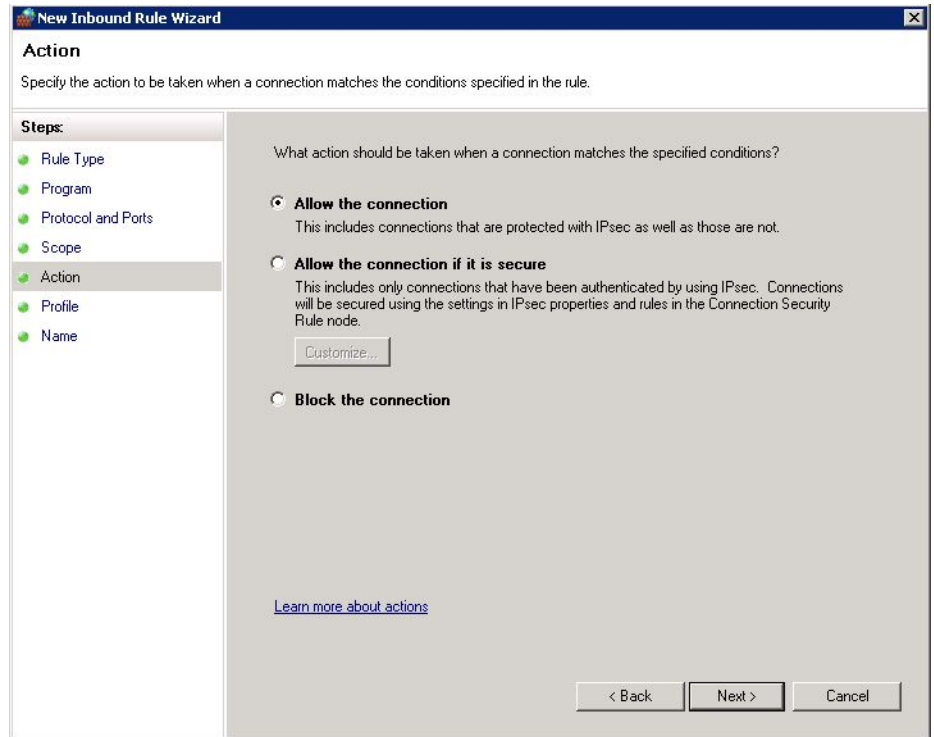


The **IP Address** dialog box is used to specify IP addresses to match. It contains three radio buttons: **This IP address or subnet:** (selected), **This IP address range:**, and **Predefined set of computers:**. The first option has a text field containing **10.10.203.27** and a list of examples: **192.168.0.12**, **192.168.1.0/24**, **2002:9d3b:1a31:4:208:74ff:fe39:6c43**, and **2002:9d3b:1a31:4:208:74ff:fe39:0/112**. The second option has **From:** and **To:** text fields. The third option has a dropdown menu showing **Default gateway**. At the bottom are **OK** and **Cancel** buttons, and a link [Learn more about specifying IP addresses](#).

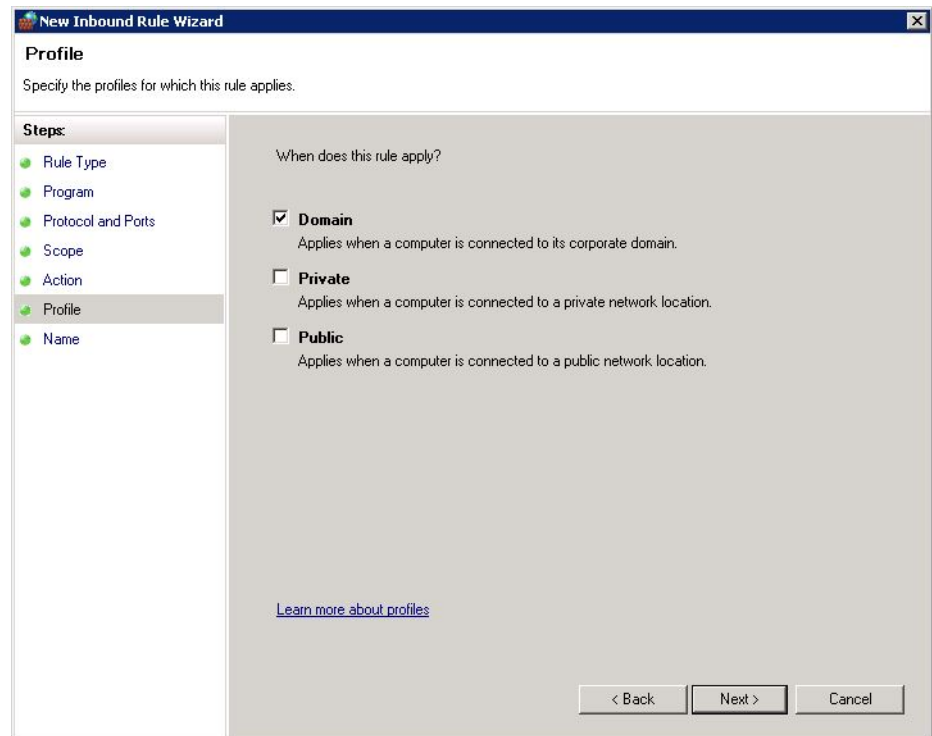


The **New Inbound Rule Wizard** - **Scope** step is used to specify the local and remote IP addresses to which this rule applies. It features a **Steps** list on the left with **Scope** selected. The main area has two sections: **Which local IP addresses does this rule apply to?** and **Which remote IP addresses does this rule apply to?**. Both sections have radio buttons for **Any IP address** and **These IP addresses:** (selected). The **These IP addresses:** sections have text fields and **Add...**, **Edit...**, and **Remove** buttons. The local section is empty, while the remote section contains **10.10.203.27** and **10.10.180.54**. There is also a **Customize...** button for interface types. At the bottom are **< Back**, **Next >**, and **Cancel** buttons, and a link [Learn more about specifying scope](#).

10. Set the Rule to **Allow the connection** for the criterias you have set.
Click on **Next**.



11. Specify the Profile where you want this rule to be applied.
Click on **Next**.



12. Name the Rule and describe it.

New Inbound Rule Wizard

Name

Specify the name and description of this rule.

Steps:

- Rule Type
- Program
- Protocol and Ports
- Scope
- Action
- Profile
- Name**

Name:
Xpressions

Description (optional):

< Back Finish Cancel

13. Click on **Finish** button.

7.8 TCP/IP Ports used by the XPR Server

The XPR server uses the following TCP/IP ports:

Component	Port	Comment
SMTPAPL	25	SMTP server
WEBAPL	80	HTTP server
CONAPL (web conference)	80	Web conference server
CTIAPL	102	Hicom 300 (ACL-H3)
SMTPAPL	110	POP3 server
All	135	Distributed XPR Server* * Used only during cluster and satellites installations
All	137	Distributed XPR Server
All	138	Distributed XPR Server
All	139	Distributed XPR Server
SMTPAPL	143	IMAP4 server
LDAPAPL	389	LDAP APL anonymous bind or simple bind
WEBAPL	443	Secure HTTP server
CONAPL (web conference)	443	Web conference server
All	445	Distributed XPR server (SMB via TCP/IP)
LDAPAPL	636	LDAP APL strong authenticated bind (secure sockets)
SMTPAPL	993	IMAP4 server with secure sockets
SMTPAPL	995	POP3 server with secure sockets
CTIAPL	1040	Hicom 300 (CallBridge), HiPath 4000 (CAP) and OpenScape Voice (CSTA).
TCPAPL	1107	With updates of old versions this port can still be used for client access.
REPAPL	1433	ODBC port for accessing SQL servers.
IPAPL	1720 (TCP)	H.225-, H.245 signaling (CorNet-IP)
ABCAPL	2533	ABC-A protocol of the Alcatel 4400 PBX.
CTIAPL	2555	Alcatel 4200, Alcatel 4400 and Alcatel OmniPCX Office (CSTA).
Media Server	3000 to 3240	RTP/RTCP
CTIAPL	3211	EADS TELECOM 65xx (CSTA)

Table 11 XPR Server Ports used

Component	Port	Comment
CONAPL (web conference)	5000	Web conference server
CONAPL	5004 (TCP)	XML-RPC of the web conference server.
IPAPL	5004 (UDP) to 5006 (UDP)	RTP-, RTCP-, T.38 initialization (CorNet-IP)
PRESENCEAPL	5060	Microsoft Live Communications Server query. Cannot be used combined with the IP APL SIP connection.
IPAPL Media Server	5060	SIP via TCP or UDP Cannot be used in combination with the Microsoft Live Communications server connection via the Presence APL.
IPAPL Media Server	5061	SIP via TLS.
CONAPL	5432	Access to PostgreSQL database.
CTIAPL	7001	HiPath 3000 (CSTA)
TCPAPL	8944	Client access and remote system link
TCPAPL	8945	Client access by SSL.
MSP	8945	XPR Service Provider (client applications) by SSL
MSP	8968	XPR Service Provider (client applications)
CONAPL	10000	RPC connection. It is used, for example, to display parts of the Web Assistant in the Web Client (voicemail integration).
IPAPL	12500 to 12500 + 200	T.38 port range First T.38 port (12500) configurable.
LICSVCL	13010	License service
CSTAAPL	13040	Port for the client access of <i>OpenScape Web Client</i> .
IPAPL	29100 (UDP) to 29100 + 400 (UDP)	RTP port range First RTP port (29100) configurable.
CLA	61740	License server

Table 11 XPR Server Ports used

These ports should not be blocked in case of usage of the respective feature via firewall.

Component	Port	Comment
ConApl	7789	Port for the client access of OpenScape WebClient.
ConApl	8443	Port for the client access of OpenScape WebClient.

Table 12 These ports must be blocked via firewall in case the respective feature is installed on OS Xpressions Server.

NOTE: Apache Tomcat server may have unfixed vulnerabilities that are impacting OpenScape Xpressions. Apache Tomcat server is no longer maintained by OpenScape Xpressions since it was part of UCC Components that is out of support and OpenScape UC integration must be used on its place.

For this reason, we strongly recommend to uninstall any UCC components installed on OpenScape Xpressions server and if it is not possible, at least block the access to the above ports.

7.9 Message Waiting Indication (MWI)

IMPORTANT:

The kernel mechanism described in the following section has found a successor - the Notification APL - which is significantly more effective. If you want to use this mechanism just the same, the Notification APL needs to be uninstalled. Web Assistant settings that affect notifications always refer to the Notification APL.

Notifying a user when a new message comes in is also called CIT in the XPR server. CIT means Computer Integrated Telephony. Its definition contained at the beginning especially the feature Message Waiting Indication (MWI).

Through the use of CIT, incoming user messages are signaled over the telephone. This is accomplished either by sending a Message Waiting Signal through the PBX or through routing as an SMS message.

For the actual configuration, refer to [Section 7.1.4, “Advanced”, on page 202](#).

To set the signal the MTA reverts to specific database fields. The required database fields are `CIT` and `CIT_<Service>`. In addition, the user for whom the Message Waiting Indication shall be set must have the corresponding privileges.

When the signal is to be set, the MTA queries the database for the existence of the field `CIT_<Service>`, over which the incoming message is delivered. For the service Fax G3 this would be the database field `CIT_FAXG3`. If this database field is missing or not filled in for the user, the database field `CIT` would be checked. If this field contains the required delivery information the signal would then be set.

As a prerequisite the user must have been granted privileges for `CIT_<Services>`. For e-mail services the privilege `CIT_EMAIL` is required. Consequently, privileges are used to determine that no Message Waiting Indication should be set for specific services. Simply revoke the users privilege for the corresponding service.

Resetting the signal is also accomplished through the use of database fields. The fields `XCIT` and `CIT` are used for this purpose. As with signal setting the field `XCIT` is first checked and when empty the `CIT` field subsequently queried.

Examples of setting the signal

- A `FAXG3/234323` for user Mayer is received. The kernel will try to determine from the database field `CIT_FAXG3` from user Mayer, the address to which the CIT signal is to be routed.

If this address exists, then a message in the form of “Fax G3 from 234323 received” will be sent. If this field does not exist, then a field with the entry `CIT` will be searched for, and the message sent to the corresponding address.

If the contents of `CIT_FAXG3` or `CIT` contains only one service – this is in effect a reference to another database field – the database field of this service is additionally read to compose a complete address. If the database entry has the form `NODE/USER` such as `VOICE/33432`, then this will be used to construct the send address.

In addition to the existence of an address, the user must have the `CIT_<service>` privilege set for the corresponding original service in the user database. In the event the privilege is not set, then no message waiting indication will be sent. In our example user Mayer requires the privilege `CIT_FAXG3`.

- User Mayer has all CIT privileges. Mayer receives a fax from `FAXG3/234323`, which is rerouted from the MTA to `NVS:NODE/MAYER`.

Entries from the user database Mayer:

USER	MAYER
CIT	SMS/0172234323

Consequently, Mayer receives an SMS message for every incoming message.

Similar is the reference in the SMS field for a mobile telephone number:

USER	MAYER
CIT	SMS
SMS	0172234323

Here Mayer also receives an SMS message for each incoming message.

- A fax from `FAXG3/234323` is received for `NVS:NODE/MAYER`. User Mayer has in the database the following entries:

USER	MAYER
CIT_VOICE	SMS/0172234323
CIT	CIT_BASIC/432

Mayer receives an SMS message for every incoming voice message. All other incoming messages initiate a Hicom CIT signal.

The SMS protocol can be installed via the SMS APL and the Hicom addressing via the V.24 APL or the CTI APL. The protocol name can differ from the example of the V.24 APL shown here depending on the APL.

Examples of signal resetting

IMPORTANT:

Single services are by default configured in a way that no `CIT_OFF` is sent. It is, for example, *not* useful to send `CIT_OFF` to SMS or VOICE. If the **Send voice as**

CIT message option is used it may however very well be useful to send a `CIT_OFF` to Voice. Here `VOICE` must then be removed from the list of displayed protocols in the configuration.

- Mayer has read all fax documents received and the CIT signal should now be reset. The kernel attempts to ascertain from the database the address `XCIT`. If this address exists, the message `CIT_OFF` is sent to the database field `XCIT`. In the event the database field does not exist, a search is made for the `CIT` field where the message is finally sent.

The addresses formed from one of the two possible database fields are treated as with setting the signal. Just like there the corresponding CIT privilege must have been assigned here.

- Mayer has all CIT privileges and reads the mail. Database entries are:

```
USER          MAYER
CIT           SMS/0172234323
```

Mayer does not receive a `CIT_OFF` message, since SMS is included in the list of the protocols for which resetting the signal is required in the configuration.

7.9.1 Counter-based CIT

The counter-based CIT differs largely in one aspect from the CIT described up to here: XPR registers in the `NEWMSG` database field the number of new, unread messages. The CIT signal will not be reset until this counter reaches 0.

To activate the counter based CIT, the option **CIT reset when all messages are read or deleted** must be selected in the configuration.

7.10 Simple Network Management Protocol (SNMP)

Using standard Windows tools you can create SNMP traps for all event reports. The XPR server uses this to support SNMP. There are three options of writing reports:

1. By means of [SnmppMode \[REG_DWORD\]](#) the most important error reports are written in the event display.
2. Each APL already writes status information in the event display of the **System** section. This information can be converted into SNMP traps by means of **evntwin**. See [Section 7.10.1, "Translating Events into Traps"](#).
3. Via the MTA's active-alert mechanism, all log messages of the classes *Fatal Error*, *Error*, *Warning* and *Information* can be written in the event display. See [Section 7.1.1.3, "Active Alerts", on page 193](#). Message 19 of the MTA must be converted into an SNMP trap by means of **evntwin**. See [Section 7.10.1, "Translating Events into Traps"](#).

NOTE:

Owing to the system complexity no fixed filter can be specified for event reports. Therefore, we recommend a three-month monitoring period, in which all reports that occur are logged. In accordance with the project engineer an individual filter list can then be generated.

7.10.1 Translating Events into Traps

NOTE:

Another method of creating SNMP traps is via the [System Info SNMP Agent](#).

If SNMP was installed on the computer, you can have event reports predefined in an application converted into traps by means of the **evntwin** program. Enter in the **start menu** under **Run** `evntwin` to start the program.

NOTE:

Please note that **evntwin** is used to convert events into traps and not for configuring traps.

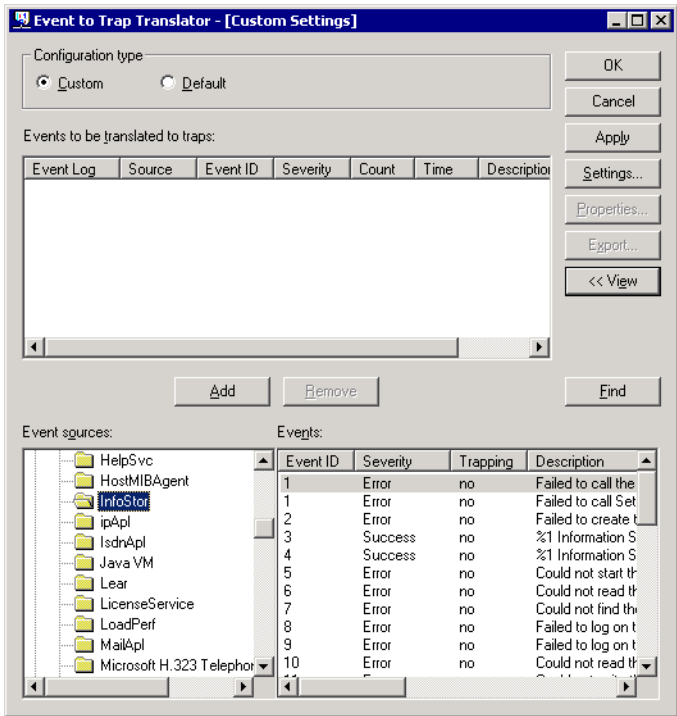
After starting the program enable **Custom** in the **Configuration type** section and expand the window with a click on the **Edit**.

In the window named **Event sources** you can see all of your XPR server services with predefined event reports. The report with **ID 19** of the **MTA** directory is particularly important since it generates the active alert reports by two flexible variables.

The **XMRSVC** messages are important for system networking. There you find the following messages, for example:

- Update IDs not matching: is <> but it should be <>
- Current update id <> of local site <> does not match confirmed updated id <> on remote site <>.
- Site <> is up
- Site <> is down
- ISC document restore failed. <>

More important reports are found in the **InfoStor** directory. Open the **InfoStor** folder to display **Events** with Event ID, Severity and Description.



The following table lists the most important events of the InfoStor service:

Event	Description
5	Could not start the %1 Information Store thread.
6	Could not read the configuration parameter of the %1 Information Store.
7	Could not find the node name of the %1 Information Store.
8	Failed to log on to the %1 Name Locator.

Event	Description
9	Failed to log on to the %1 Status Dispatcher: Code %1.
10	Could not read the configuration parameter of the %1 Information Store.
11	Could not write the configuration parameters of the %1 Information Store.
13	The directory (%2) for the database could not be created.
14	cTree database error: %2
19	The %1 system configuration is not valid.
20	The %1 Information Store must run on the kernel node. This error can be caused by a missing or invalid CLUSTER license.
4097	Could not open %2 database. Error Code %3
4098	Database %2 is corrupt, trying to rebuild...
4099	Database %2 rebuild failed with error %3
4101	Could not create %2 database: %3
4103	Could not initialize the ISAM engine.
4104	Could not close the database.
4105	The %1 Name Locator reports that a %2 has already been registered on system %3.
4106	The %1 cluster configuration is invalid on this system: %2
4107	The %1 cluster configuration is invalid on this system: No SLAVE node is defined in LocalSystemList.
4108	The %1 cluster configuration is invalid on this system: No KERNEL node is defined in LocalSystemList.
4109	The %1 cluster configuration is invalid on this system: A SLAVE node is defined in LocalSystemList but the cluster is not active.
4110	The %1 cluster configuration is invalid on this system: KERNEL and SLAVE are identical in LocalSystemList.
4111	The %1 cluster configuration is invalid on this system: No CLUSTER license is available.

The specifications %1, %2 and %3 are variables that are adapted to specific context conditions of the event. %1 can describe the product name while %2 may describe the database name or %3 a service state.

Besides the InfoStor event reports the report in the **MTA** directory with **ID 19** and the description **%1%2** already mentioned is particularly important. This report generates the variable active alert reports of the XPR systems. We recommend to translate this report into a trap.

NOTE:

License violations are displayed in the event bar as error with the source MTA (**ID 20**).

Select the events that you want to translate from the list by marking the respective **Event** and clicking **Add**. You can select as many events as you want. Keeping the shift key pressed and using the cursor keys you can also select several or all events simultaneously.

Now a window opens that displays the event **Properties**. If you have selected several events, only the properties of the first event appear. You can view the properties of the other events by selecting the corresponding event and clicking **Properties**.

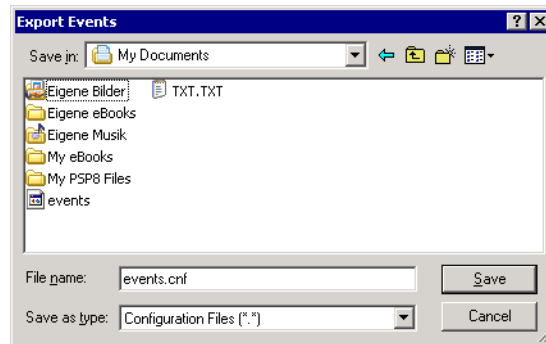
From the properties you can gather the **Trap specific ID**, which serves for identifying the event in the further proceedings. The **Enterprise OID** is linked to the source. In addition, the **Source** and the **Log** are listed. Under **Generate trap** you can set when a trap is generated. You can define this via the **event frequency** by means of **if event count reaches** and also additionally via a **time interval**. The time interval is activated with a tick before the **within time interval** field and by entering a time in seconds. Click **OK** to confirm your entries and the selected events appear in the **Events to be translated to traps** field.

The screenshot shows a 'Properties' dialog box with the following fields and values:

- Source: MTA
- Enterprise OID: 1.3.6.1.4.1.311.1.13.1.3.77.84.65
- Log: Application
- Event: 19
- Trap specific ID: 1073872915
- Generate trap:
 - if event count reaches: 1
 - ☐ within time interval: 0 seconds
- Description: %1 %2

Buttons for 'OK' and 'Cancel' are located in the top right corner.

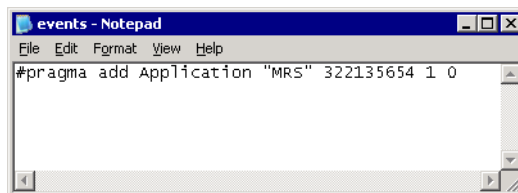
Next select the events to be translated with a mouseclick. Keeping the shift key pressed and using the cursor keys you can also select several or all events. After making your selection push the **Export** button.



Enter a suitable name for the file and select a corresponding file folder as storage location. Make sure the file has the **cnf** extension and click on **Save**.

Open the file with a **text editor**, for example Notepad.

The entry found there starts with `#pragma`. The `add` parameter indicates that you want to add an event-to-trap configuration. Furthermore, the `Application` protocol, the `MRS` source, the `322135654` trap ID, the event frequency `1` and the time interval `0` are listed.

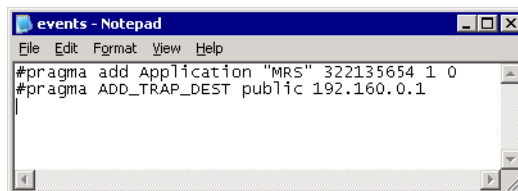


Add the SNMP management system address as follows:

```
#pragma ADD_TRAP_DEST CommunityName HostID
```

The *CommunityName* is the corresponding name carried by the area in which the management system is located. *HostID* describes the IP address of the management system. For example:

```
#pragma ADD_TRAP_DEST public 192.160.0.1
```



Save the modifications and perform the following command in the command line:

```
evntcmd /s server_name /v 10 /n file name
```

The translation of events into traps and the trap destinations are configured by means of `Evntcmd`. `/s servername` indicates the computer on which the translation of events into traps, trap destinations or both are to be configured. If you do not specify a computer, the configuration occurs on the local computer. `/n` indicates that the SNMP service is not to be rebooted, if the computer receives

trap configuration modifications. *filename* specifies the configuration file that you have created by means of evntwin. /v indicates the status report types to be displayed during the trap and trap destination configuration. This parameter must be a whole number between 0 and 10. If you enter value 10, all report types, inclusive process tracking reports and warnings as to the successful trap configuration are displayed. With value 0 no report is displayed.

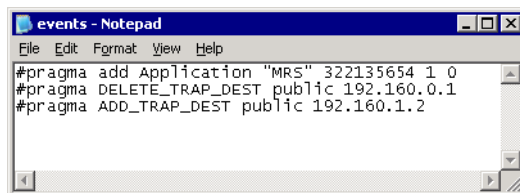
The command emits the following lines:

```
[Wrn08] Verbose level set to 10.
[Wrn05] Command line parsed succesfully.
[Wrn08] Succesfully parsed Trap(ADD, MRS, 3221225472, 1, 0).
[Wrn10] lexic [2:4]: hit EOF.
[Wrn08] Successfully parsed Trap(ADD_TRAP_DEST, public, 192.160.0.1).
[Wrn10] lexic [2:4]: hit again EOF.
[Wrn05] Configuration file 'filename.cnf' parsed successfully.
[Wrn08] Connecting to 'server_name' registry...
[Wrn05] Registry connected to 'server_name'.
[Wrn08] Succesfully set existing event '3221225473'.
[Wrn08] Succesfully set address '192.160.0.1'.
[Wrn05] Commands processed successfully.
[Wrn03] You need to restart the SNMP service...
```

After finishing this process you need to reboot the SNMP service.

7.10.1.1 Modifying the SNMP Management System

To modify the SNMP management system you need to enter the following commands in your CNF file:



Delete the connection to the old manager by DELETE_TRAP_DEST and add a new manager by ADD_TRAP_DEST.

As in the previous section you now need to perform the following command in the command line:

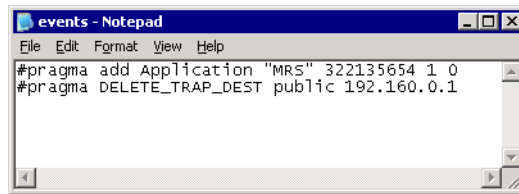
```
> evntcmd /s server name /v 10 /n file name
```

After the output of the corresponding information you need to reboot the SNMP service for the modifications to take effect.

7.10.1.2 Deleting the SNMP Management System

To delete an SNMP management system you need to enter the following lines in your CNF file:

Message Transfer Agent (MTA)



As in the previous section you now need to perform the following command in the command line:

```
> evntcmd /s server name /v 10 /n file name
```

After the output of the corresponding information you need to reboot the SNMP service for the modifications to take effect.

Message Transfer Agent (MTA)

Message Transfer Agent (MTA)

8 System Networking

System Networking (SN) is a mechanism for exchanging messages between different messaging servers (XPR or XPR and PhoneMail servers). The protocol implements functions for the actual message exchange as well as a net-wide configuration management and a comprehensive system and message reporting.

The information contained in this chapter is divided into the following sections:

- [General Structure of an SN Network](#)
- [Administrative Network Access](#)
- [The XPR Location Profile](#)
- [The XPR Network Profile](#)
- [Configuration Management of the SN Network](#)
- [Configuration Management in PhoneMail Networks](#)
- [General Configuration of an SN Network](#)
- [User Addressing in an SN Network](#)
- [User-Message Exchange between SN Network Nodes](#)
- [Exchanging User Messages in PhoneMail Networks](#)
- [SMTP Routing via Relay Host](#)
- [Security Mechanisms](#)
- [Adjusting the Maintenance Script](#)

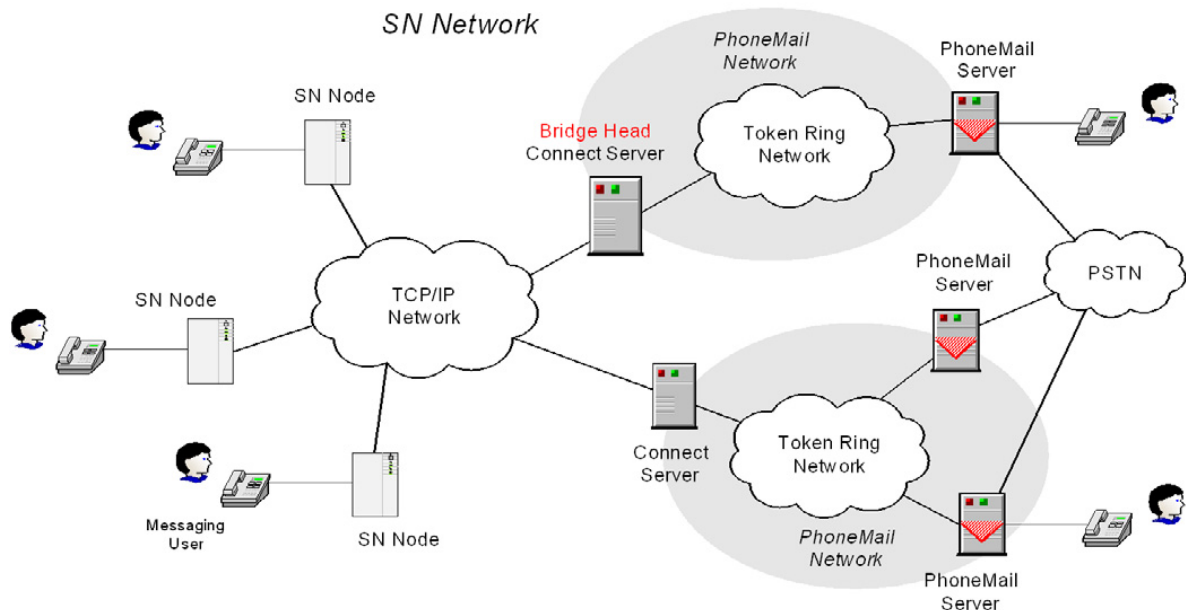
8.1 General Structure of an SN Network

The objective of an SN network configuration is the combination of several independent messaging systems to a virtual total system. In such a scenario the users of the systems involved can exchange messages. In doing so the relevant users get the impression as if they would be working at a common messaging system.

To achieve this, different information must be interchanged between the single messaging systems. This includes individual information of the respective system locations and address information of the associating messaging users¹. The information is exchanged via so-called location or network profiles.

The following figure illustrates the basic structure of a SN network.

1. Address information of distribution lists can be exchanged via System Networking as well.



SN networks differ XPR server to a SN node network. The message and data transport is effected between these nodes on the basis of SMTP and thus via the SMTP APL and the transport protocols TCP/IP. If required, PhoneMail networks can also be integrated into an SN network.

The so-called Bridge Head Connect Server serves for the configuration information exchange between an XPR-based SN network and PhoneMail networks. In the XPR based SN network it is represented as virtual XPR node. It is however not always necessarily involved in the actual message exchange, since this communication always occurs directly between the participating XPR node and Connect servers.

Only the Bridge Head Connect Server is known as SN node to the XPR-based SN network from the PhoneMail network. All other servers of the PhoneMail network are 'hidden' behind this node.

The voice mail user configuration and administration is performed at the respective XPR and PhoneMail systems.

About the following

In the following paragraphs of this chapter predominantly those SN networks are considered that are exclusively realized on the basis of the XPR server. Respectively, the following terms are used in the following form:

SN node:

Describes an SN node on the basis of a XPR server.

SN network:

Describes an SN network that merely consists of SN nodes on the basis of the XPR server.

Descriptions concerning the integration of PhoneMail systems will be given in individual sections. For detailed descriptions of the PhoneMail server please refer to the respective manuals.

8.2 Administrative Network Access

An SN network is configured via the *Web Assistant* application of the XPR server. The *network administrator* account is used for this purpose. This XPR account exists independently from all other accounts of the XPR server. It is stored on each network node platform in encrypted format and not as part of the XPR Correlation Database. A private/public pair of keys is used for the encoding.

As network administrator and administrator account are strictly differentiated, the configuration of the actual SN network and all other XPR server settings is a clearly administratively separated procedure.

Since SN allows a network-wide configuration management, the network administrator account is identical on all SN nodes of a network.

IMPORTANT:

An XPR server does not accept messages in an SN network until you have logged in on this system as network administrator.

8.3 The XPR Location Profile

The location profile contains all information of an SN network node. It is exchanged between the single SN nodes in the scope of the configuration management. In this way each network node receives a precise image of any other node of the SN network.

The following terms are significant in connection with the location profiles:

Local site profile

A location profile bound to the SN node on which it is stored is called local location profile.

Imported site profile

A location profile is considered imported when it describes the properties of another, remote SN node. If an SN node exports a location profile, an imported location profile is created from it in other SN network nodes.

The only exception is the recovery of an SN node (cf. [Section 8.7.3, "Restoring an SN Node", on page 322](#)).

Exporting node

Describes an SN node that sends its local location profile to other SN network nodes.

Importing node

Describes an SN node that receives the local location profile of another SN network node.

In the next sections you find the following information about the location profile:

- [Site Profile Information](#)
- [Protocol Export](#)
- [Site Profiles and PhoneMail Systems](#)

8.3.1 Site Profile Information

The fields of a location profile specify the information defined by the associated SN node and exported to other SN network nodes.

These are the fields:

- [XPR server name](#)
- [Location number](#)
- [Display name](#)
- [Location prefixes](#)
- [Site name \(Site ID\)](#)
- [Address](#)
- [Location name recording](#)
- [Extension number ranges](#)
- [Default protocols](#)
- [Default database fields](#)
- [Public key](#)

Detailed overview of the field contents:

XPR server name

Defines the XPR server name unique for the entire network. This name serves for the identification of the respective node in an SN network that only consists of XPR based nodes.

Location number

In PhoneMail networks a SN node cannot be identified under its unique XPR server name. In this case the node is identified by the location number.

If an SN network exclusively comprises XPR servers, no location number must be specified for the SN node.

Display name

Defines name under which the SN node is displayed. The location name is used by default.

Location prefixes

Defines the location prefixes of the respective SN node. Within the SN network these prefixes serve for addressing different nodes with user message exchange.

Example: 4711

Site name (Site ID)

The location name is the unique description of an SN node location in the network.

Example: Berlin

Address

Defines the IP address or the qualified domain name of a SN node. This address is required for addressing nodes on the TCP/IP transport layer.

Example: 10.10.10.10 or mycomputer.mydomain.mycompany.com

Location name recording

Contains a voice file the content of which is put out on other nodes for the TUI greeting of the respective node. The file can be adapted to individual requirements by importing nodes.

Extension number ranges

Describes the extension ranges that can be addressed via the respective SN node. For the range definition, two wildcard characters are available:

- Defines coherent extensions as extension range.
Example: 214–256
- x Serves as wildcard character for an arbitrary digit position.
Example:
2xx defines an extension range of the extensions 200 to 299

The XPR server can manage up to 500 extension ranges.

IMPORTANT:

Installations with more than 500 extension ranges require an individual project release.

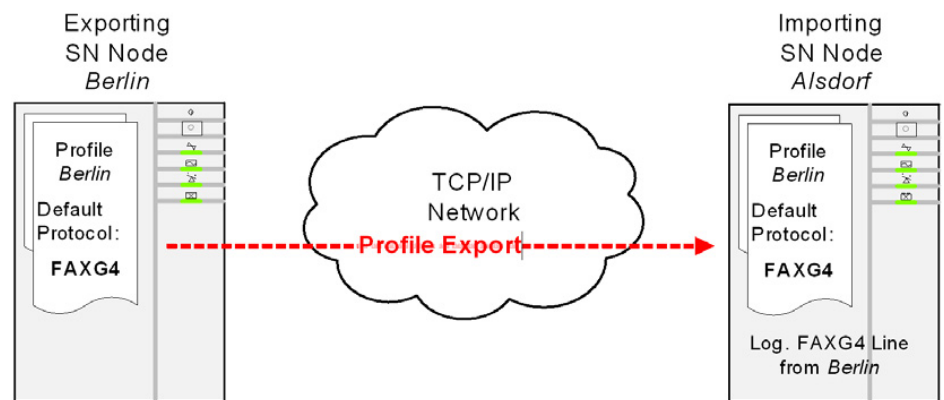
Default protocols

Defines the XPR protocols exported by the associating SN node to other SN network nodes. Each protocol listed here generates the map of a corresponding logical line under the SMTP APL of the importing XPR server².

Via this mechanism it is possible to centrally administer services on an XPR server in the SN network, and to provide them for other SN network nodes.

You find further information about exporting protocols in [Section 8.3.2, “Protocol Export”, on page 306](#).

Example: FAXG4



In this example, the SN node *Berlin* provides node *Alsdorf* with the FAX G4 service. Consequently, site *Alsdorf* does not require an independent Fax G4 access to the PSTN. It sends all Fax G4 messages via node *Berlin* instead.

Default database fields

Defines the user-related database fields of the XPR correlation database exported by the associating SN node to other SN network nodes. The relevant user information is thus available to the SN network nodes that import this location profile.

Example: NAME, VOICE, PHONE, RECORDED NAME

Public key

The message exchange between SN nodes is performed in encrypted form (see [Section 8.12, “Security Mechanisms”, on page 329](#)). The public key is respectively required for the future message decoding of the respective node.

² The logical lines thus generated on a XPR server are listed under the server's SMTP APL correspondingly to their exporting SN nodes.

8.3.2 Protocol Export

As already described, the protocol export serves for centralizing services within an SN network. There are protocols, though, that should not be exported against this background. Such protocols are specified in a so-called black list and can therefore not be selected for the protocol export in case of default settings.

The black list excludes the following protocols or logical lines from export to other SN nodes:

Logical lines	Protocols	Furthermore
• of the E2k APL • of the EXCH APL • of the LN APL • of the MAIL APL • of the NOT APL • of the PRINT APL • of the SMTP APL • of the TCP APL • of the WEB APL • of the MTA • of Lear	• PHONEMAIL • VMS • ERGO • VOICE	• unavailable lines • transaction lines • imported lines

Table 13 Black List of the log. Lines and Protocols for System Networking

If you want to exclude entries listed above from exclusion, you can specify such exceptions in the so-called white list³.

3. The white list is defined in the registry value `ExportProtocols` under the key `HKLM\Software\Wow6432Node\PP-COM\MRS\MTA\ISC`.

8.3.3 Site Profiles and PhoneMail Systems

If PhoneMail networks are integrated into an SN network, the site profile sent to the Bridge Head Connect Server only include the following profile fields:

- Display name
- Location prefixes
- Location number
- Address
- Location name recording
- Extension number ranges
- Public key

8.3.4 Message Transmission String

Within XPR there is a permanent limit of 63 characters for the message transmission string. This string is a combination of the voicemail number plus the qualified domain name (FQDN) of XPR plus the permanent prefix "IMCEAVOICE-" plus the SMTP protocol name "NVS:SMTP/" or "NVS:SMTP.0/".

To make this limit more manageable, use the IP address instead of the FQDN for all sites. In most cases this modification must be performed after the network has already been configured. The reason is that the transmitted string is mostly significantly shorter when the network is configured.

NVS:SMTP/_ISC_@remoteserver.userdomain.subnet.com

Keep the following in mind as formula:

$[(NVS:SMTP/) 9 \text{ for the protocol prefix of the SMTP APL} + (IMCEAVOICE-) 11 \text{ for network prefix} + \text{the maximum number of digits in the site prefix (MSPL)} + (\_) 1 \text{ for the underscore} + \text{the maximum number of digits in the user extensions (MEL)}^4 + (@) 1 + \text{FQDN}]$

$9 + 11 + \text{MSPL} + 1 + \text{MEL} + 1 + \text{FQDN} = \text{Total Character String (TCS)}$

TCS must not exceed 63 characters. If this should happen just the same, use the IP address for the SMTP address in the site profile.

8.3.4.1 Correcting the Message Transmission String

1. Log on to the *Web Assistant* as network administrator.
2. Verify that the *System Networking* does not feature any crossed-out connection icons for any site.
Fix these problems before you continue.
If the red icon is caused by the FQDN length, the site profile must first be repaired by the support.
3. Open the local site profile.
4. Overwrite the FQDN for the **SMTP Address** with the IP address of the XPR server computer on which the SMTP APL is installed.
5. Click on **Save**.
6. Click on **Next**.
7. Click on **Back**.
8. Click on **Apply changes**.
9. Click on **Reload**.

4. If extension ranges of different lengths are used, use the longest one for the calculation.

10. Verify that no crossed-out connection icons are displayed for any site. Solve these problems.
11. Repeat these proceedings at every site by logging on to the *Web Assistant* in each case.
12. Subsequently, the network profiles must be repaired on all XPR servers involved. To this, you can use InfoTool, DBTool or the *Web Assistant* to change the SMTP address suffix to the respective IP address. If this causes problems, please consult the next higher support level.

8.4 The XPR Network Profile

Network profiles serve for exchanging information of single messaging users and distributors between SN locations.

8.4.1 Network Profile Usage

If for example the information of a user is to be exchanged between his/her local and a remote SN network node, the local network node generates a network profile. This profile contains all user-significant address fields of the local Correlation Database that were defined with the relevant remote network node in the local location profile for data exchange.

After the transfer of this network profile to the remote SN node, the database information contained in the profile are stored in the remote correlation database. These entries are additionally supplemented by the SOURCE database field, which is assigned the name of the original XPR server as value.⁵

Furthermore, the following two database entries are created in the Correlation Database of the remote node for the database information of the original SN node.

The '*Node_<SN Network Node>*' user group

This user group contains the name '*Node_<Name of the original server>*' and receives the privileges that correspond to a newly configured XPR user. The users received by a server are added to the associated user group, thus being granted the corresponding privileges for sending and receiving messages.

The '*Broadcast*' contact

This contact named *Broadcast* is assigned to the user group of the original SN network node. It is used for addressing all messaging users of the associating SN network node.

8.4.2 Network Profiles and PhoneMail Systems

The user-specific address fields of the local Correlation Database that are forwarded to the Bridge Head Connect Server in case of a PhoneMail integration is defined in the location profile of the Bridge Head Connect Server.

5. Users who have been imported this way from another SN location, are also called phantom users there.

8.5 Configuration Management of the SN Network

The configuration management of the SN network comprises the areas:

- [Exchange of SN Node Configuration Modifications](#)
Exchange of information about the SN node configuration between all SN network nodes (exchange of location profiles)
- [Information Exchange](#)
Exchange of information about messaging users and distribution lists between defined SN network nodes (network profile exchange)
- [Remote Access](#)
Remote access to each SN network node for configuring the local location profiles

The three areas in detail:

8.5.1 Exchange of SN Node Configuration Modifications

One major SN task is the automatic distribution of node configuration and XPR server data. The result is that an SN node is provided with the following information of all other SN network nodes.

- The individual SN node configurations
- Defined protocol access of the respective XPR server

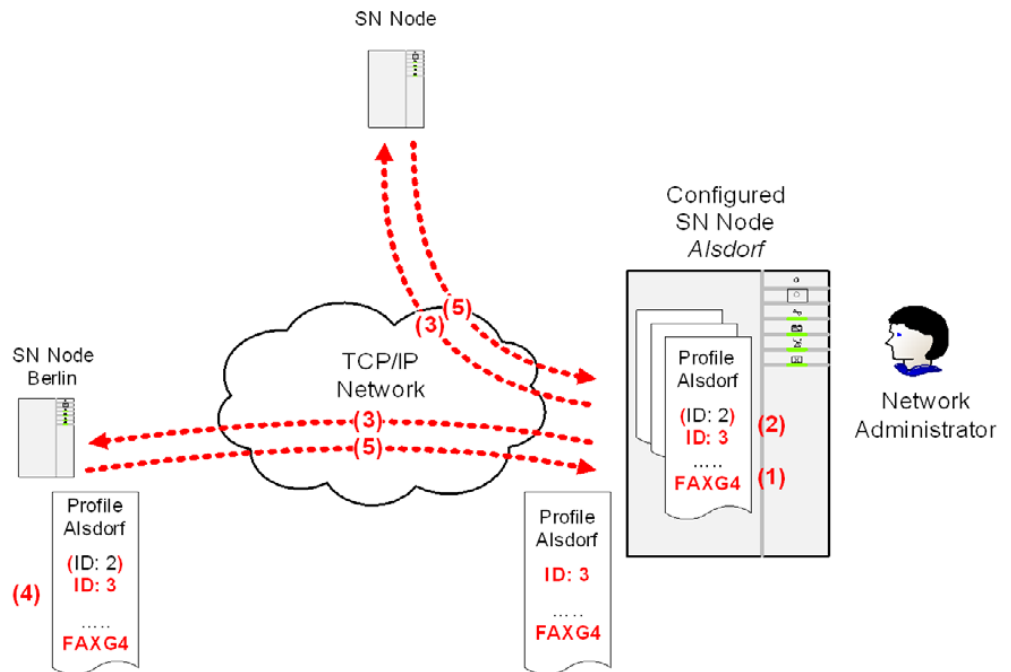
To achieve this, a new or reconfigured node sends its configuration data to the other SN network nodes. The relevant location profiles are exchanged between the SN nodes for this purpose.

Information received by a node is not forwarded to third SN nodes.

Each message on configuration updates is furnished with an update ID by the sending SN node. On the basis of this ID, received systems can recognize, whether a configuration update is actually current. If this is the case, the update ID is copied to the associated, previously imported location profile along with the modified configuration information. If the update ID is obsolete, the information contained in the message inclusive the update ID is dismissed.

All configuration updates are transferred between the SN nodes in encrypted format (cf. [Section 8.12, "Security Mechanisms", on page 329](#)).

Let's now take a look at modifying a location profile in detail. We take the *Alsdorf* SN node as example. This node has already sent its current site profile with update ID 2 to all SN network nodes in the course of normal data exchange. Among these nodes is node *Berlin*, in which the profile is thus stored. The FAXG4 protocol is now added to the *Alsdorf* node with the modification occurring locally.



1. After logging in to the *Alsdorf* SN node, the network administrator adds the FAXG4 protocol to the local site profile.
2. After the configuration has been finished the SN node in *Alsdorf* notifies the other SN network nodes about the modification. In doing so it enhances the local profile update-ID from 2 to 3 and
3. sends it with the modifications performed to all SN nodes it knows.
4. This profile is also received by the node *Berlin*. It checks the transmitted Update ID. It is more recent than the one of the location profile stored with the node. Therefore the node copies all transmitted modifications. The other SN network nodes proceed in the same way.
5. All nodes receiving the updated profile acknowledge its receipt. If a node does not acknowledge receipt of the modification, the *Alsdorf* SN node resends the modifications to the relevant node.

8.5.2 Information Exchange

If several messaging systems are to be networked to a virtual total system, each single system must know all address information of the messaging users and distribution lists spread in the network. New or modified address information of the users and distribution lists must be exchanged between the single SN network nodes. This is done via sending user-individual network profiles, which contain the Correlation Database fields defined in the location profile (cf. [Section 8.4, “The XPR Network Profile”, on page 310](#)).

The address information of all messaging users and distribution lists is transferred to other SN network nodes by default. To exclude defined users or distribution lists from this mechanism, the NOREPLICATION field exists in the correlation database. If this field is set, the relevant address information is not transferred to other SN network nodes.

All address information is transferred between the SN nodes in encrypted format (cf. [Section 8.12, “Security Mechanisms”, on page 329](#)). Such items of information are – like site profiles – not be passed on to third SN nodes either.

Three modes are supported for network profile exchange. These are:

- [Profile Exchange via the 'Push' Mechanism](#)
- [Profile Exchange via the 'Piggy-Back' Mechanism](#)
- [Automatic Profile Exchange](#)

8.5.2.1 Profile Exchange via the 'Push' Mechanism

The 'push' mechanism realizes a unique address information exchange with selected SN network nodes. The exchange of the associated network profiles is triggered and the involved SN nodes are defined in the *Web Assistant* application via the 'push' action.

If several network profiles are to be exchanged between two SN nodes, they are always transmitted in one single SMTP message. If, however, the network profiles of a great number of users are exchanged via the 'push' mechanism, the maximum message size of an SMTP configuration can be exceeded. To avoid this, a maximum of 100 objects⁶ is transmitted in one SMTP message by default. If a higher amount of data must be exchanged, it is divided into several SMTP messages.

6. The number of objects that are sent in an SMTP message can be defined in the registry key `SmtptMessageSize` under the key `HKLM\SOFTWARE\Wow6432Node\PP-COM\MRS\MTA\ISC`. The default is 100 objects.

8.5.2.2 Profile Exchange via the 'Piggy-Back' Mechanism

In case of the 'piggy-back' mechanism a user's address information is exclusively exchanged when he/she sends a message. With the actual message the relevant data are transmitted 'piggy-back' style to the SN destination node of the relevant message only.

To make sure that in this mode all addresses of the messaging users and particularly of the distribution lists are exchanged once, the SN network is normally initialized with a 'push' action.

8.5.2.3 Automatic Profile Exchange

In this mode all intermediately modified address information is transmitted to the relevant SN network nodes in fixed intervals⁷. With the transmission of a network profile the current update ID of the correlation database is inserted. This information is stored in the received SN node with the associating user information. Based on this ID a subsequently received network profile can be checked for up-to-dateness.

If several network profiles are to be exchanged between two SN nodes, it is easiest to transmit them in one single SMTP message. If an XPR server with a great number of users is added to an SN network, the maximum message size of an SMTP configuration may well be exceeded in case of *one* SMTP message. To avoid this, a maximum of 100 objects⁸ is transmitted in one SMTP message by default. If a higher amount of data must be exchanged, it is divided into several SMTP messages.

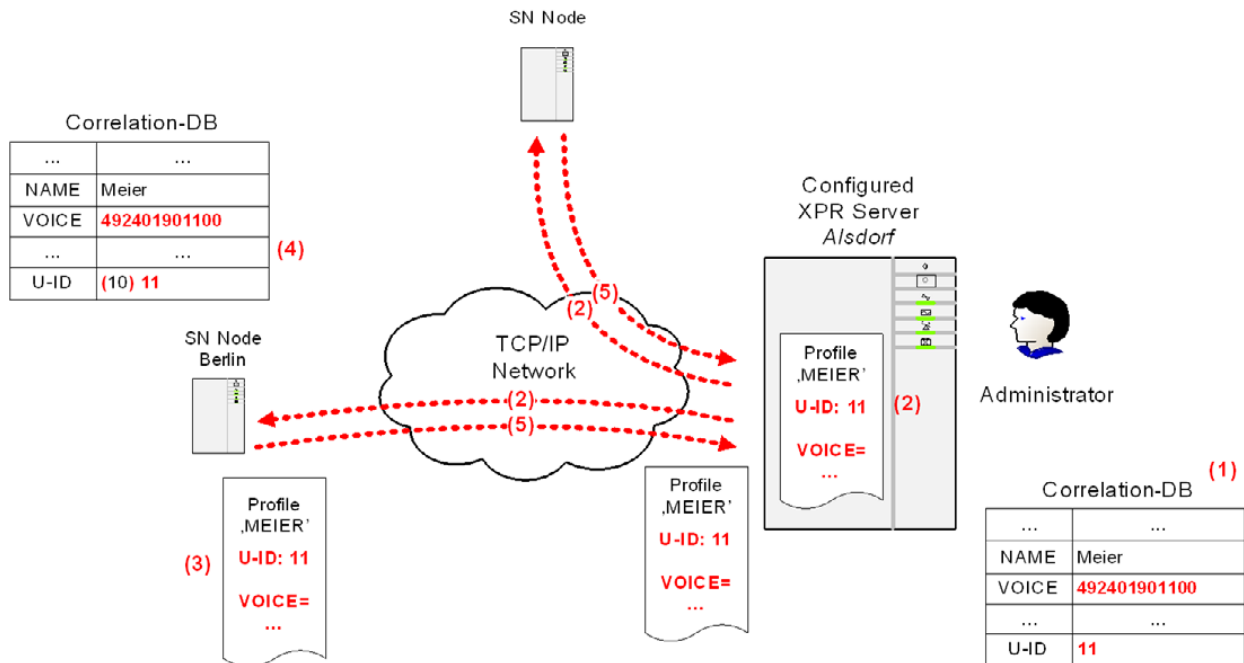
Let's have a look at the sending of a network profile by the automatic exchange in detail.

We take the *Alsdorf* SN node as example. This has already sent the address information of its messaging users and distribution lists to all nodes of the SN network in the course of the normal data exchange. The Update ID 10 of its Correlation Database has also been transferred. The node *Berlin* is e.g. in the SN network, so that the relevant address information exist in its Correlation Database.

The administrator of the XPR server in *Alsdorf* now adds the voice box number of a new localized user named *Meier*.

7. The time between two transmissions is defined in the registry key `ReplPollTime` under the key `HKLM\SOFTWARE\Wow6432Node\PP-COM\MRS\MTA\ISC`. The default is 5 minutes.

8. The number of objects that are sent in an SMTP message can be defined in the registry key `SmtptMessageSize` under the key `HKLM\SOFTWARE\Wow6432Node\PP-COM\MRS\MTA\ISC`. The default is 100 objects.



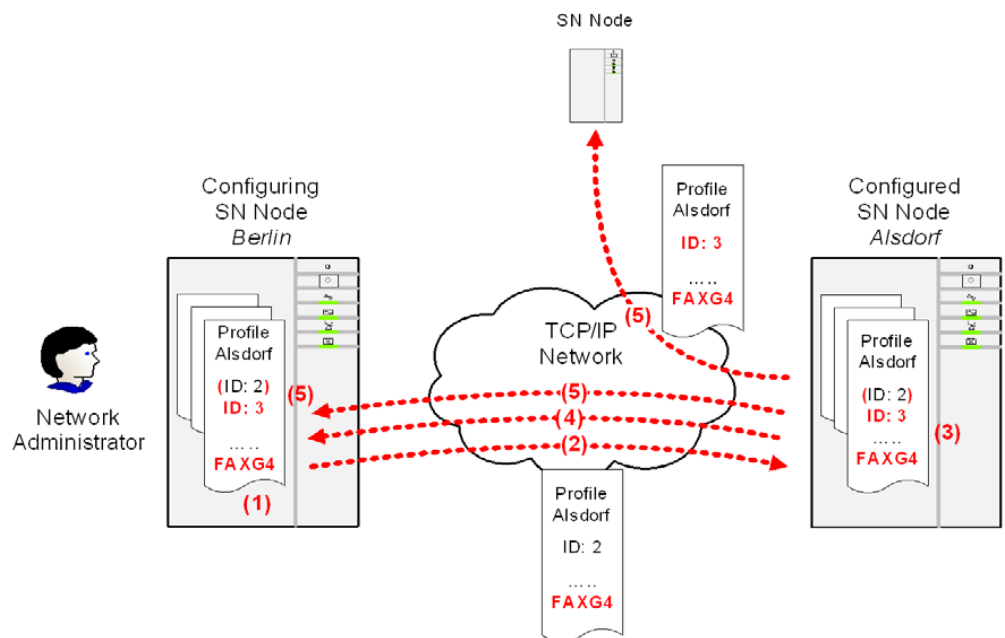
1. After the XPR administrator has logged in at the XPR server *Alsdorf*, he/she adds the voice box number to user *Meier*'s profile.
2. After the configuration has been finished the SN node in *Alsdorf* notifies the other SN network nodes about the modification. It sends a network profile with the relevant correlation database field and the associating update ID to all SN nodes it knows.
3. This profile is also received by the node *Berlin*. It checks the transmitted Update ID. It is more recent than the one the node has in its store.
4. Therefore the node copies the transmitted modification as well as the new update ID to its correlation database. The other SN network nodes proceed in the same way.
5. All nodes receiving the network profile acknowledge its receipt. If a node does not acknowledge receipt of the modification, the *Alsdorf* SN node resends the modifications to the relevant node.

8.5.3 Remote Access

Via the SN remote access the network administrator can access all SN network nodes for configuration from any node. He/she only needs to log in on the node used as access under the network administrator account valid in the entire network.

After the selection of the SN node to be configured, its local SN configuration can be modified. Therefore modifications are performed in the copy of the respective location profile.

The following figure illustrates a successful modification by remote access. The SN node *Alsdorf* has already sent its current location profile with update ID 2 to node *Berlin* in the course of normal data exchange. The profile has been stored there. Now the protocol FAXG4 is added to this location profile. However, this does not take place locally at the respective node *Alsdorf*, but remote from node *Berlin*.



1. After logging in to the SN node *Berlin*, the network administrator adds the FAXG4 protocol to the non-local location profile of location *Alsdorf* stored there.
2. When the configuration is accomplished, node *Berlin* transfers the modification in the format of the changed site profile to the relevant node *Alsdorf*. The last profile update ID is maintained.
3. Node *Alsdorf* first checks the transmitted update ID after receiving the profile. This ID corresponds with 2 to the ID of the node's current site profile. The performed modification has thus been performed on the basis of the current node configuration. Node *Alsdorf* correspondingly copies the protocol modification to its local site profile and increases the update ID of its profile.
4. Subsequently the SN reporting informs node *Berlin* and thus the network administrator that the transmitted modifications have been copied.

5. The modifications performed now need to be communicated to the other SN network nodes. This process corresponds to the description in [Section 8.5.1, “Exchange of SN Node Configuration Modifications”, on page 312.](#)

Note that in this configuration mechanism modifications are only communicated to the remaining SN network by the node concerned.

8.6 Configuration Management in PhoneMail Networks

If required, PhoneMail networks can also be integrated into an SN network that only consists of XPR network nodes. In this case every administrative information exchange between an XPR node and a PhoneMail network occurs via the Bridge Head Connect Server.

The Bridge Head Connect Server is part of the PhoneMail network and behaves in direction to the XPR-based SN network like an XPR network node.

Only the Bridge Head Connect Server is known as SN node to the XPR-based SN network from the PhoneMail network. All other servers of the PhoneMail network are 'hidden' behind this node.

8.6.1 Exchange of Configuration Modifications

The exchange of configuration modifications between an XPR network node and a PhoneMail network is performed by sending location profiles. This behavior corresponds to the mechanism within an SN network that only consists of XPR servers.

Since this profile exchange is always edited by the Bridge Head Connect Server in case of a connection of XPR node and PhoneMail networks, this selected server is always originator or recipient of such a site profile from the XPR node's point of view.

Bridge Head Connect Server as site profile recipient

In this case the Bridge Head Connect Server receives the location profile of an XPR network node. In this function the server behaves like an XPR network node that receives a location profile from another XPR network node (cf. [Section 8.5.1, “Exchange of SN Node Configuration Modifications”, on page 312](#)). If the received information has a more up-to-date configuration level, the server also passes new information on towards the connected PhoneMail networks.

Bridge Head Connect Server as site profile originator

If the node configuration within the PhoneMail network changes, the Bridge Head Connect server transfers the modifications to the XPR network nodes. The mechanism corresponds to the description in [Section 8.5.1, “Exchange of SN](#)

[Node Configuration Modifications](#)", on page 312.

8.6.2 Exchange of User and Distribution Lists

The exchange of information about users and distribution lists between an XPR network node and a PhoneMail network is performed by sending network profiles. This behavior corresponds to the mechanism within an SN network that only consists of XPR servers.

Since this profile exchange is always edited by the Bridge Head Connect Server with a connection of XPR node and PhoneMail networks, this selected server is always sender or recipient of such a network profile from the XPR node's point of view.

Bridge Head Connect server as network profile recipient

In this case the Bridge Head Connect server receives the network profile of a XPR network node. In this function the server behaves like a XPR node that receives a network profile from another XPR network node (cf. [Section 8.5.2, "Information Exchange"](#), on page 314). If the received information has a more up-to-date configuration level, the server also passes new information on towards the connected PhoneMail networks.

Bridge Head Connect server as network profile originator

If address information of users or distribution lists of a node change within the PhoneMail network, the Bridge Head Connect server transfers the modifications to the XPR network nodes. The mechanism corresponds to the description in [Section 8.5.2, "Information Exchange"](#), on page 314.

8.6.3 Remote Access

A remote access between XPR nodes a PhoneMail network node is not possible.

8.7 General Configuration of an SN Network

IMPORTANT:

To ensure trouble-free operation of an SN network, a WEB APL must be installed on each XPR server of the SN network. In case of a distributed-server installation, the WEB APL **must** be installed on the kernel system.

Now that we are familiar with an SN network's configuration management, we take a look at the establishment of a new SN network.

Three installation sections are differentiated:

- [Configuring the first Node of an SN Network](#)
- [Adding a Node to an SN Network](#)
- [Restoring an SN Node](#)
- [Integration of PhoneMail Networks](#)

Each of the following sections is a description of the general procedure and of the SN mechanisms interesting in the respective case. You find an exact step-by-step configuration guide in the *Web Assistant* manual.

8.7.1 Configuring the first Node of an SN Network

Each SN network begins with the configuration of the first SN node. This node is configured with the following steps in the *Web Assistant* application on the relevant XPR server.

1. Assigning a password for the network administrator account
2. Configuration of the local location profile for the node

After these steps the XPR server defines all internal structures for an SN node. In this process an asymmetrical pair of keys (private/public key) is generated for communicating with other nodes that follow later. In addition, the local location profile is assigned the XPR server name. Heed this when adding a node to an SN network again (cf. [Section 8.7.3, "Restoring an SN Node", on page 322](#)).

After configuring the first SN node the network can be extended with further nodes.

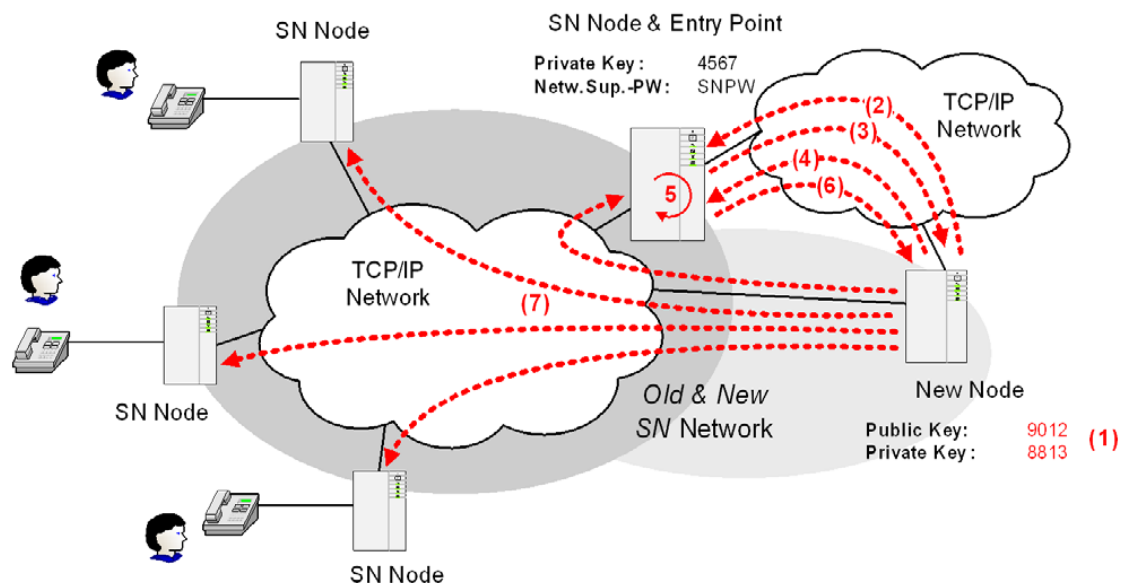
8.7.2 Adding a Node to an SN Network

In the last section we have configured the first SN network node and we will now see how a new node is added to an existing SN network.

Requirements for adding a new SN node are:

- An XPR server as new SN node, installed ready-for-use with the SN
- TCP/IP connection to the entry point⁹
- The entry point IP address
- For safety reasons it must be ensured that the integration of a new node in an existing SN network cannot occur without a security instance. Therefore, adding a new SN node also requires the network supervisor password of the existing SN network¹⁰.

How the mechanism for adding a new SN node works on the basis of this information:



1. The new node generates at first an asymmetrical pair of keys. This pair consists of a private and a public key.
2. Subsequently the new node sends an uncoded *Get Public Key Request* to the selected entry point.

9. Each SN network node that does not operate as connect server may serve as entry point. Pre-condition is that the IP address of the network node is known before the new node is added.
10. Furthermore it is considered useful to know the public key of the desired entry point with configuring a new node (cf. the following configuration procedure).

3. Thereupon the entry point transmits its uncoded public key to the new node. This key is then displayed to the administrator in the *Web Assistant* at the new node and can be checked there for correctness.
4. If the administrator confirms the correctness of the received public key, the new node sends an *Add Site Request* to the entry point. This request is encrypted with the public key of the entry point and contains the previously generated public key of the new node and the network administrator password.
5. The entry point decodes the received request with its private key and checks the transferred password.
6. If the transmitted password corresponds to the password of the existing SN network, the entry point accepts the new log-in. It consequently transfers all location profiles to the new node that the entry point knows in the SN network. These items of information are encrypted with the public key of the new node.
If the transmitted network administrator password was invalid, no further communication occurs from the entry point side.
7. The new node copies the received location profiles and sends its individual location profile to all SN nodes it knows. The single transmissions are encrypted with the respective public key of the relevant SN node in this process.

Adding the new node to the existing SN network is thus accomplished.

8.7.3 Restoring an SN Node

Now that we know the general procedure of generating the first and adding a new SN node, one question still needs to be answered: how do we reintegrate a node that used to belong to an SN network after its deactivation?

SN provides for this case a specific mechanism. This mechanism optimizes the configuration of a node to be restored by restoring its former location profile from the information that still exists in the SN network. Requirement for this recovery is that the XPR node name used with the initial integration is maintained after the node platform recovery.

Using this node restoration, no new location profile is created on the node before its connection to the SN network. Instead, the connection to the SN network immediately starts in the *Web Assistant*. During this connection the entry point automatically sends all SN network location profiles to the new node. One of these profiles corresponds to the SN configuration of the node to be added before the node's deactivation. This profile carries – as assumed – the same name as the associating XPR node. Based on this sameness the node recognizes its

former profile and adopts it as individual current configuration.

IMPORTANT:

During the login of the node that is to be restored at the SN network, the node sends a corresponding SMTP message to the selected entry point. By default, an SMTP address based on the XPR node name is used.

If the entry point addresses the response to this message with the name-based SMTP address, problems might occur if no resolution of this name is possible in the transport network.

To handle this problem, the value **OrgAddress** exists under the registry key `HKLM\Software\Wow6432Node\PP-COM\MRS\MTA\ISC`. You must enter an originator address of the node to be restored into this value in case of the described failure, that can be resolved in the transport network – e.g. its IP address.

8.7.4 Integration of PhoneMail Networks

As already described, the integration of PhoneMail networks in an XPR-based SN network occurs with a Bridge Head Connect Server. The Bridge Head Connect Server is part of the PhoneMail network and behaves in the XPR-based SN network direction like an XPR network node.

You find more information on this topic in the Bridge Head Connect Server product documentation.

8.8 User Addressing in an SN Network

In an SN network you find the following options to address users.

- Prefix dialing
- Co-location dialing
- Convenient dialing

Which of these options can or have to be used depends on the network configuration.

You find further information about the configuration of the different addressing modes in the *Web Assistant* manual.

8.8.1 Prefix Dialing

Addressing via the site prefix represents the default option to address a user at another SN site. In this case, the SN site prefix is set forward to the actual extension of the user. The general format of a user's address thus reads: *<Site prefix><Extension>*.

This type of addressing makes the following demands on the SN node configuration:

- Assignment of site prefixes for the SN nodes involved.
- Arbitrary distribution of the extensions among the sites involved.

8.8.2 Co-Location Dialing

In case of co-location dialing, a user's extension need not be prefixed. The general format of a user's address thus reads: < [Site prefix]><Extension¹¹>.

If a user is addressed via co-location dialing, the XPR server suppresses the site greeting playback of the remote node. Users that communicate between co-locations thus gain the impression as if working at a common messaging system.

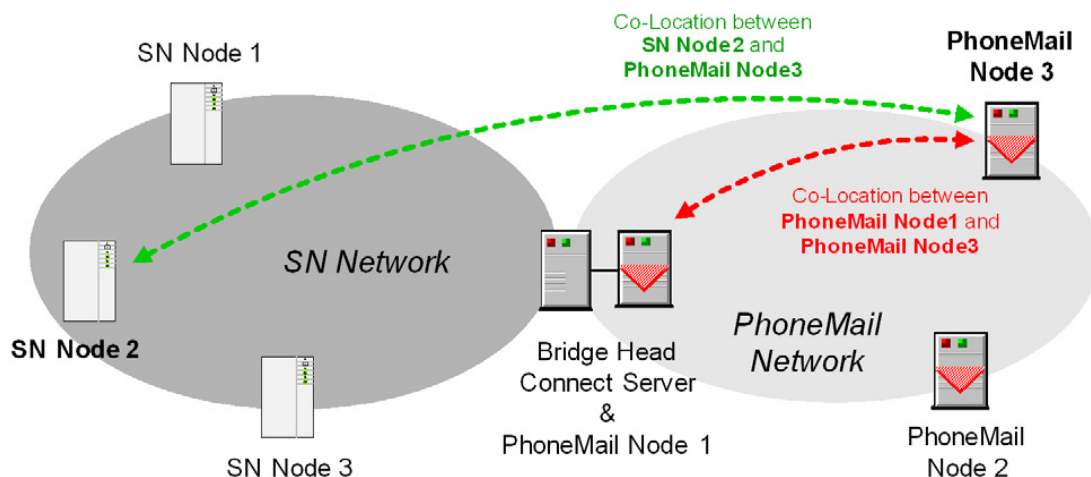
This type of addressing makes the following demands on the SN node configuration:

- Assignment of site prefixes for the SN nodes involved.¹²
- Activating the **Co-location** options for the sites involved.
- No overlapping of the extensions among the sites involved.

Co-location selection between XPR and PhoneMail nodes

If XPR server and PhoneMail nodes are to be configured as mixed co-locations, a configuration specialty applies.

Let us contemplate the example of the following figure.



A XPR server (SN node 2) and the PhoneMail node 3 are to be configured as mutual co-location.

11. Specifying the prefix is optional.

12. Though in this case no prefix needs to be specified for addressing, a prefix must be defined during the configuration.

In this case it is not sufficient to configure the co-location relation in PhoneMail node 3 and SN node 2. Beyond that, a co-location relation must be established between PhoneMail node 3 and the PhoneMail node connected to the Bridge Head Connect Server of the PhoneMail network: in our example thus PhoneMail node 1.

If you do not consider this specialty, no messages can be exchanged between SN node 2 and PhoneMail node 3.

IMPORTANT:

If a co-location relation is established between a PhoneMail node and a XPR server, the following applies in general:

A co-location relation between the relevant PhoneMail node and the PhoneMail node connected to the Bridge Head Connect Server of the PhoneMail network must be established as well.

8.8.3 Convenient Dialing

In case of convenient dialing, a user's extension must not be preceded with a site prefix.

This type of addressing makes the following demands on the SN node configuration:

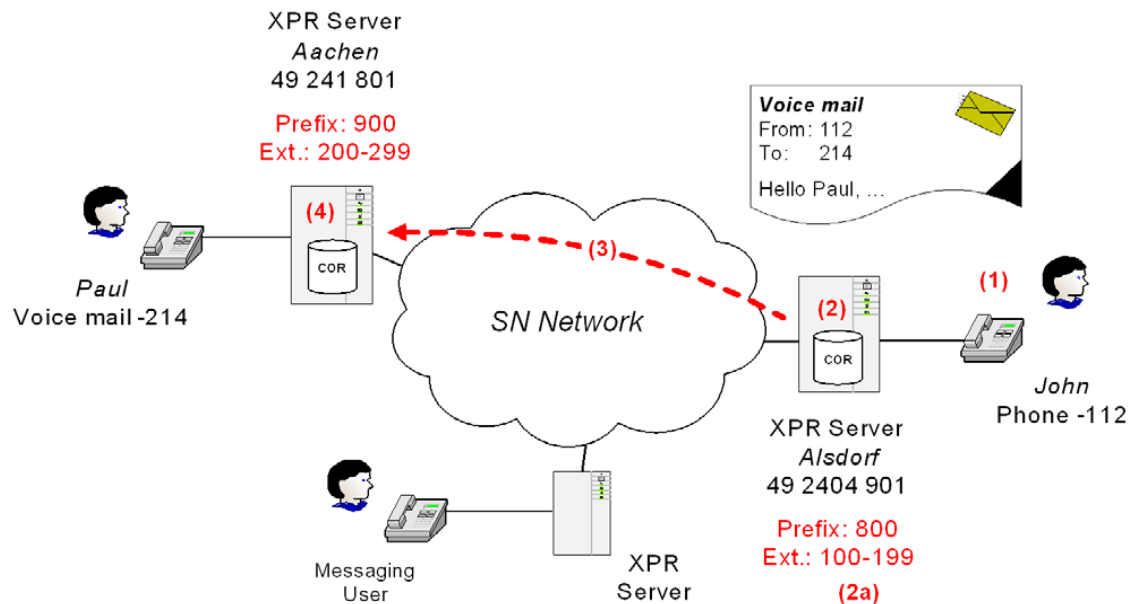
- No assignment of site prefixes for the SN nodes involved.
- No overlapping of the extensions among the sites involved.

8.9 User-Message Exchange between SN Network Nodes

After the configuration of an SN network, the messaging users of the locations involved can exchange messages. In doing so they get the impression that all users operate a common messaging system.

The transmission of messages between different SN network nodes occurs on the basis of node-individually assigned prefixes. These must be placed before the desired address with addressing a recipient.

The following figure shows sending a voice message within an SN network using co-location addressing.



1. In our example, user John creates a voice message for his colleague Paul. Paul is user of the XPR server in *Aachen*, which is also part of the SN network to which the XPR server in *Alsdorf* belongs. John enters Paul's voice mailbox number as destination address of the message – 214.
2. After sending the message, the sending XPR server searches its Correlation Database for entries with the voice box number 214. As a rule, this information was previously shared by the exchange of network profiles between the SN network nodes. Accordingly, user Paul is known to the XPR server in *Alsdorf* at the XPR server in *Aachen*.

If Paul's user information has not yet been exchanged between the nodes, there is another way for the *Alsdorf* SN node to identify the corresponding destination server. It compares the destination address with the extensions that have been configured for the diverse SN nodes. Since the extension 214 is part of the extension range in *Aachen*, the SN node in *Aachen* would also be recognized as destination system.

3. Consequently, the XPR server in *Alsdorf* sends the voicemail to the XPR server in *Aachen* via the SN network.
4. The XPR server in *Aachen* receives the message and stores it in the mailbox that has been configured for the user. This can either be directly on the XPR server or on an external system – e.g. a Lotus Notes server. In the second case, the accordingly configured database field PREFERRED is analyzed for the respective user.

8.10 Exchanging User Messages in PhoneMail Networks

The addressing of messages sent between XPR and PhoneMail nodes corresponds within the XPR-based SN network to the addressing described in [Section 8.9, “User-Message Exchange between SN Network Nodes”, on page 326](#).

Please refer to the PhoneMail server documentation for a description of the addressing within a PhoneMail network.

8.11 SMTP Routing via Relay Host

Messages are directly routed between the SN network nodes by the relevant SMTP APLs – thus point to point. This means: when an SN node sends a message to another node of the SN network, it addresses the message via its SMTP APL directly to the fully qualified name of the target node.

If the **Send e-mail via relay host** option is activated in the SMTP APL of a node, the messages of this node are not directly routed for the SN network any more, but indirectly via a relay host. This routing fails though, as long as the relay host used has no routing information about the other SN nodes.

If no routing information is to be maintained in the relay host for the SN nodes, the SMTP APL can also directly rout messages for the SN nodes when the **Send e-mail via relay host** option is configured. To this, the relevant SMTP APL merely needs to be informed about the fully qualified names of the SN nodes.

Proceed as follows:

IMPORTANT:

The following modifications must only be performed in the SN nodes if the **Send e-mail via relay host** option is active, or no routing information is to be maintained in the configured relay host.

1. Log on to the Web Assistant as network administrator.
2. Switch to the page **System networking > Site profiles**.
3. Open each of the available site profiles and note down the portion that follows the @ character of the SMTP address of each SN node.

Example:

For the SMTP address `_ISC_@host.alsdorf.cycos.com` note down:
`host.alsdorf.cycos.com`.

4. Start the registry editor by entering the command `regedt32` in the Windows command line.

5. Open the registry value

`HKLM\SOFTWARE\Wow6432Node\PP-COM\MRS\SmtpApl\DontRelay`¹³,

and enter in it all address portions that you have noted down in step 3. Use a new line for each address portion.

6. Open the registry value

`HKLM\SOFTWARE\Wow6432Node\PP-COM\MRS\SmtpApl\Receive_AllowRelay`¹⁴,

and enter in it all address portions that you have noted down in step 3. Use a new line for each address portion.

7. Reboot the SMTP APL to activate the modifications made.

The SMTP APL thus routes all messages destined for the specified addresses directly.

8.12 Security Mechanisms

SN is a mechanism for exchanging messages and network information. These often sensitive data must obviously be secured during their transmission.

SN uses a combination of a symmetrical and an asymmetrical encoding procedure for any communication with other network nodes. Furthermore, all profile and password data in the single network nodes are administered asymmetrically encrypted.

Each SN network node generates an individual, asymmetrical private/public pair of keys during its initial installation. This pair of keys is used for the entire following communication with other network nodes. Since asymmetrical encoding is very computation-bound, not all message data to be transmitted are encrypted applying this method. Instead, each message is encrypted with a symmetric key specifically developed for it. Only this key is subsequently asymmetrically encrypted and attached to the symmetrically encrypted message. The recipient of the respective message then decodes the symmetrical key first. With this key he/she can then recover the actual message.

¹³.If this value is not contained in the registry, generate it manually as REG_MULTI_SZ

¹⁴.If this value is not contained in the registry, generate it manually as REG_MULTI_SZ

8.13 Adjusting the Maintenance Script

An SN network exchanges a relatively large number of messages, which are usually deleted after the normal lifespan of documents has expired. We recommend to delete such messages much earlier for keeping the system performant. For this purpose, you can insert some commands in the Maintenance Script between the following lines:

```
Delldb record=Journal age=$(LifeTimeDeleted) flags=DELREC
Delldb record=Journal age=$(LifeTimeUnread) flags=!READ options=DELETESOFT
```

These commands are inserted for deleting messages sent by SMTP and AMIS. In addition, we delete the messages to the postmaster, which are normally Non-Delivery Reports (NDR).

```
Execute cmd="logserv flg=wrn script=Mod_Maint msg=Begin_SMTP_Cleanup"
Delldb record=journal age=10 finalrecipient=NVS:SMTP
Execute cmd="logserv flg=wrn script=Mod_Maint msg=End_SMTP_Cleanup"
Execute cmd="logserv flg=wrn script=Mod_Maint msg=Begin_AMIS_Cleanup"
Delldb record=journal age=7 recipient=NVS:AMIS
Execute cmd="logserv flg=wrn script=Mod_Maint msg=End_AMIS_Cleanup"
Execute cmd="logserv flg=wrn script=Mod_Maint msg=Begin_NIL_Cleanup"
Delldb record=journal age=7 recipient=NVS:NIL
Execute cmd="logserv flg=wrn script=Mod_Maint msg=End_NIL_Cleanup"
Execute cmd="logserv flg=wrn script=Mod_Maint msg=Begin_POSTMASTER/NDR_Cleanup"
Delldb record=journal age=20 originator=NVS:*/POSTMASTER
Execute cmd="logserv flg=wrn script=Mod_Maint msg=End_POSTMASTER/NDR_Cleanup"
```

9 Number Conversion Object (NCO)

NOTE:

The OpenScape Voice PBX used to be called HiPath 8000 before product version 3.1 R2. General OpenScape Voice information applies in this chapter also for the previous version HiPath 8000.

The information contained in this chapter is divided into the following sections:

- [What is NCO?](#)
- [Calling Number Handling in the XPR Server](#)
- [Technological Concepts](#)
- [NCOAdmin Start – Access to NCO Configurations](#)
- [Configuring the NCO Elements](#)
- [Configuration Example of Number Conversion Objects \(NCO\)](#)
- [NCO in a Corporate Network Environment](#)
- [The Number Conversion Prepare Tool](#)
- [Reference to the Number Conversion Administrator \(NCOAdmin\).](#)

9.1 What is NCO?

NCO describes a concept for phone number conversion within the XPR server and is the successor to the previous DNO rules. It owes its name to the definition of so-called Number Conversion Objects, which form the central component for the NCO implementation.

NCO describes a quite complex part of the XPR server. Therefore, do not worry if you get the feeling of not having understood NCO in full detail after reading this chapter. The information on the following pages will, however, enable you to take your first independent steps within the large area of NCO phone number conversion. Introductory examples will get you on the right way.

NCO supports you as beginner as it already delivers an executable basic configuration after its installation. This configuration already covers the bigger part of possible XPR server installations.

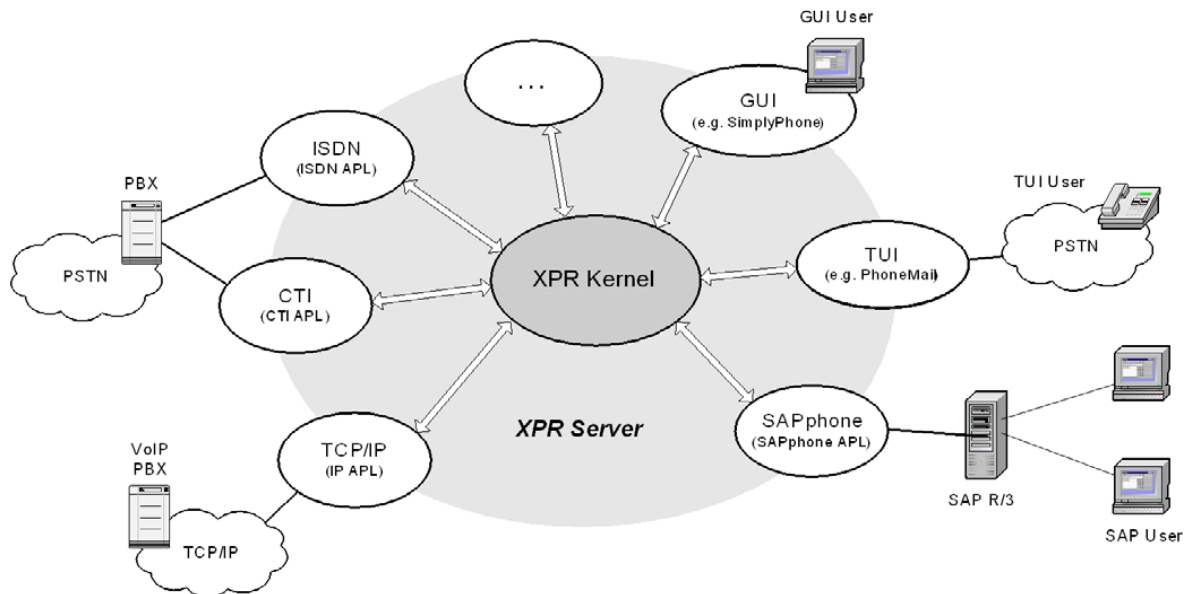
To deepen your knowledge we recommend independent experimenting at the system. Generate a copy of a location, call type checker, normalization and localization rule set each for this purpose. Then define a new NCO and assign it the generated copies. Based on this configuration and the NCO tester you can subsequently research the NCO behavior.

First we will take a look at NCO basics. This is to prepare the technical understanding for the descriptions that follow later.

9.2 Calling Number Handling in the XPR Server

The XPR server as Unified Messaging platform brings together a large number of messages from different communication systems. Since the items of information received in this way are differently structured, an individual type of message processing is required.

The following figure represents an example of a Unified Messaging solution based on the XPR server. In this solution, different external communication systems are connected to the XPR server via individual interfaces. Thus e.g. a PBX via the ISDN APL, or TUI users via the voicemail script PhoneMail.



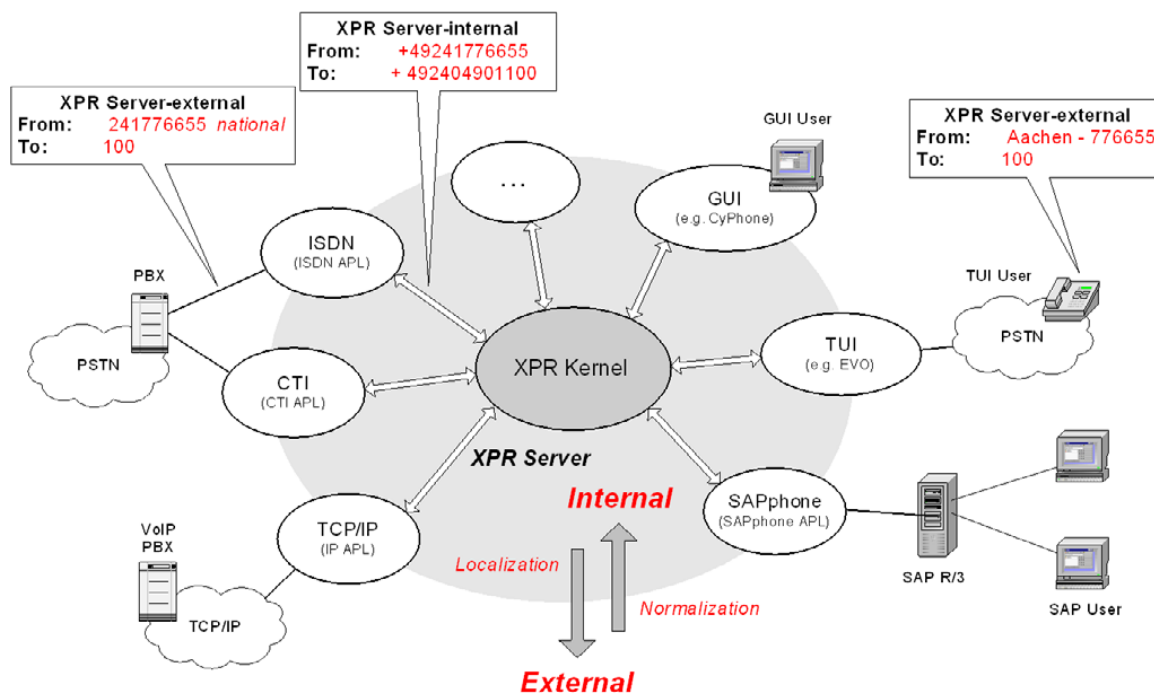
The central XPR server task is in this environment to evaluate and process the messages received by the connected systems. In this process, address and phone number information transmitted along with messages is particularly important.

The phone number information format often varies with the messages structured according to the system. Therefore, a system-depending phone number conversion is required. Since the individual communication properties of the connected systems are in particular available in the external XPR interfaces, it is considered useful to perform this conversion exactly there.

The phone numbers received by the XPR server and so converted are administered in a defined format – the normalized phone number format – during the following message processing within the server.

Number Conversion Object (NCO)

The following figure shows this phone number conversion as an example of our XPR server environment already seen.



The XPR server receives a call from the connected PBX via the ISDN APL. The phone number information contained therein is available in an external (local) phone number format. In order to prepare this information for further processing within the XPR server, the ISDN APL as receiving communication interface performs the described phone number conversion. This process is also called normalization. The result is a phone number in the internal (normalized) phone number format.

Example:

Local (external) Calling Number:	100
	↓
Normalized (internal) Calling Number:	+ 492404901100

After being processed within the XPR server, the message leaves the server via another interface. This interface must make sure that the phone numbers contained in the message are converted in a format that the receiving system – a TUI user here – can evaluate. This process is called localization and results in an external (local) phone number.

Example:

Normalized (internal) Calling Number: + 492404901100



Local (external) Calling Number: 100

The described phone number conversion has two vital advantages:

- The external interface, performing the respective conversion, has all information about the external system. This enables an optimal evaluation of the transferred phone number information.
- As long as a phone number is processed within the XPR server, it is available in a uniform format. All XPR components with a fixedly defined phone number structure can work with this format.

9.3 Technological Concepts

The information contained in this chapter is divided into the following sections:

- [The general NCO Concept](#)
- [The NCO Elements](#)
- [The normalized NCO Phone Number Format](#)
- [NCO Clients and Connect Points](#)
- [Location, Phone Numbers and Prefixes](#)
- [NCO Conditions](#)
- [Localization and Normalization Rules](#)
- [Batch and regular Expressions](#)
- [Call Type Checker and Conditions](#)
- [Administering NCO Variables – Name Areas](#)
- [Export and Import of NCO Elements](#)
- [Range Lists](#)
- [Saving the NCO Configuration](#)
- [Structure of the NCO Installation for a XPR Reinstallation.](#)

9.3.1 The general NCO Concept

As already described, NCO is based on so-called Number Conversion Objects. Each of these NCOs combines all items of information required for a desired phone number normalization or localization. Among these are e.g. location or rule set information. Each configured NCO is addressed via a so-called connect point.

All NCO clients can access an NCO. The clients are mostly XPR server modules that communicate with external systems or components. They are in charge of converting phone numbers transferred to them on their interfaces.

If the ISDN APL receives e.g. a phone number on one of its ISDN trunk groups, it transfers this number to the NCO framework specifying an individual connect point. There the associated NCO is determined from the specified connect point. The phone number can then be normalized with the rules contained in the NCO. The result of the conversion is subsequently passed on to the ISDN APL.

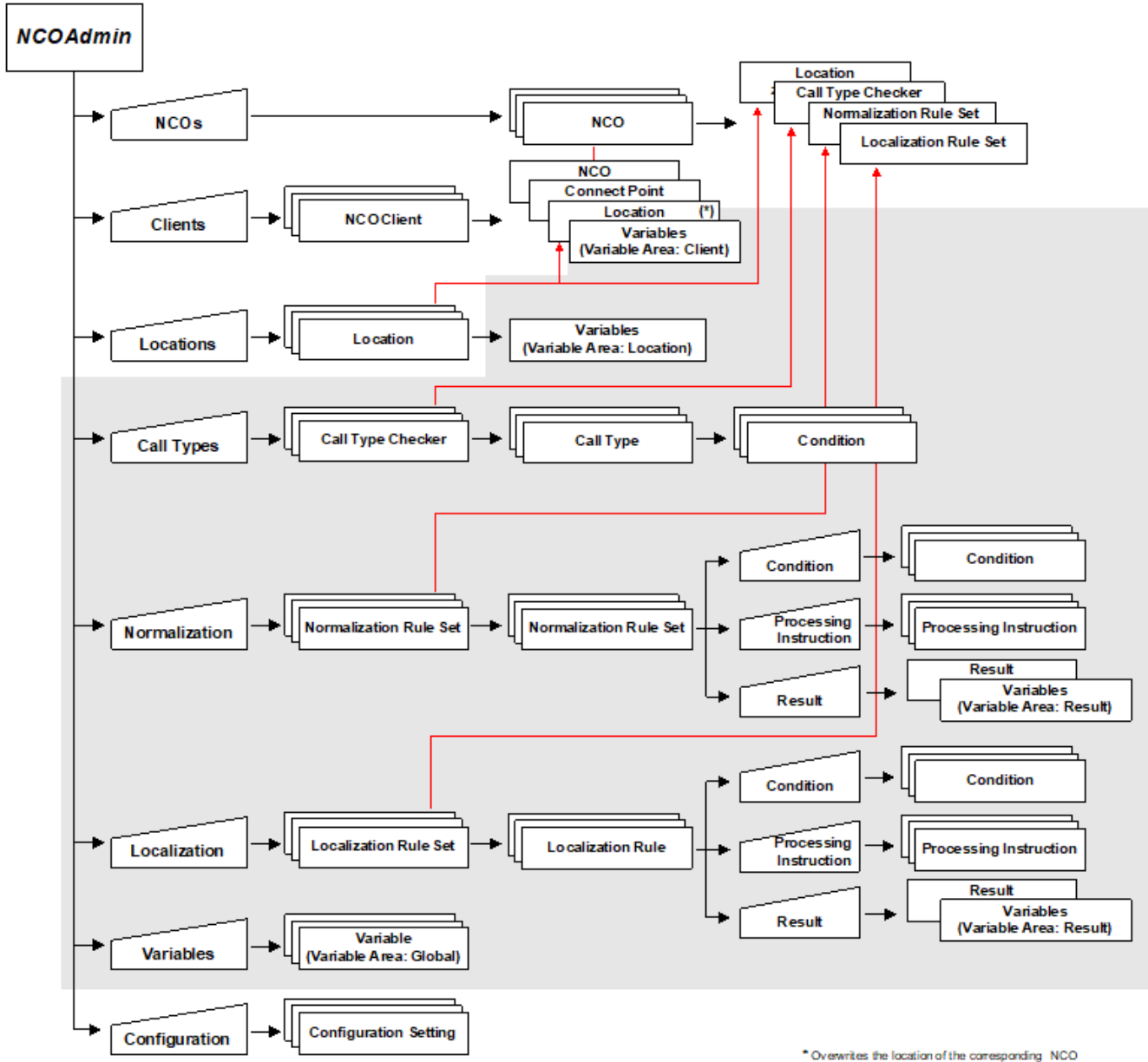
After this first overview of the NCO operating principle, we will take a closer look at the single NCO components.

9.3.2 The NCO Elements

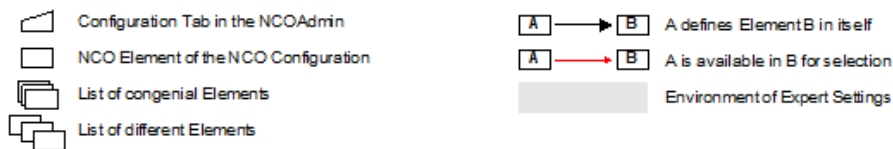
The NCO operating principle is based on different components and modules, which will be introduced in this section in detail.

Let us start with a first overview that clarifies all important NCO elements and their configuration relation in the NCOAdmin.

Number Conversion Object (NCO)



* Overwrites the location of the corresponding NCO



9.3.2.1 *NCOAdmin* – The NCO Administration

NOTE:

If the *NCOAdmin* is started directly via its program file and not via the settings in a telematics APL, all NCO tabs, except for the **Locations** tab, are only accessible via specifying a password.

System administrators and service personnel can obtain their password to unlock the relevant tabs from the service partner in charge.

The XPR application *NCOAdmin* serves for configuring all NCO elements. It is installed in the `<XPR Install>\bin` directory and started with the `NumberConversionAdmin.exe` file there. In this case it operates on the computer system on which the XPR server is configured.

Beyond that it can also be operated on a system other than the XPR server. Under such circumstances the XPR server from which the NCO configuration data are to be loaded must be specified when the application is called.

The *NCOAdmin* can be operated in three modes:

- Locally on the XPR server the NCO configuration of which is to be processed.
- On a computer system available in the same network as the XPR server the NCO configuration of which is to be processed.
- On a computer system that can access via the Internet the XPR server the NCO configuration of which is to be processed.

Depending on the mode the *NCOAdmin* is started in, special information may need to be provided at its start.

You find continuative information on the *NCOAdmin* in [Section 9.4, “NCOAdmin Start – Access to NCO Configurations”](#), on page 387.

9.3.2.2 Number Conversion Object (NCO)

The Number Conversion Objects (NCO) are the central NCO modules. Each NCO combines the following four elements:

- A location
- A rule set for phone number normalization
- A rule set for phone number localization
- A call type checker

By defining different NCOs, phone numbers can be normalized or localized in different ways.

With the installation of XPR server components, default NCOs are already automatically defined, which ensure a phone number conversion basic function. Which NCOs are defined depends on the NCO clients installed along with an XPR server.

9.3.2.3 Location

The term location describes all necessary phone number information required to determine its exact 'position' in the international hierarchical communication network. This information is the basis for a correct phone number localization or normalization. One item of the location information is e.g. the area code, which applies for the configured XPR server. You find more on location information in [Section 9.3.5, "Location, Phone Numbers and Prefixes", on page 350](#).

With the XPR server installation, the location configured for the server is integrated in the NCO configuration.

IMPORTANT:

The phone number information for XPR users is stored in the Correlation Database of the XPR server in normalized format. The respective normalization always takes place on the basis of the corresponding location information. If location settings are modified in an existing XPR environment, the phone number information of existing users is **not** automatically updated in the Correlation Database.

As a consequence, corresponding modifications of the user information must be performed manually. For this purpose, you can use the XPR tool *Number Conversion Prepare* with the following command prompt:

```
numberconversionprepare update nocn
```

Number Conversion Prepare **does not** adjust the **CIT** database field in the process.

9.3.2.4 Normalization Rule Set

The normalization rule set defines the rules according to which the XPR server converts the phone numbers it receives. With the XPR server installation, various normalization rule sets are already configured. These are usually sufficient for a common XPR installation.

You find continuative information on NCO rules in [Section 9.3.7, “Localization and Normalization Rules”](#), on page 357.

9.3.2.5 Localization Rule Set

The localization rule set defines the rules according to which the XPR server converts the phone numbers it sends to external systems or assigns to a user. With the XPR server installation, various localization rule sets are already configured. These are usually sufficient for a common XPR installation.

You find continuative information on NCO rules in [Section 9.3.7, “Localization and Normalization Rules”](#), on page 357.

9.3.2.6 Call Type Checker

On the basis of location information¹ the call type checker determines the call type of a phone number transferred to it. This information can be used, for example, to check privileges that can be configured in the XPR server for users².

A call type checker can redeliver one of the following call types:

- **Internal**
The phone number to be converted describes a subscriber using the subscriber code of the associated location.
- **Local**
The phone number to be converted describes a subscriber in the local network of the associated location.
- **National**
The phone number to be converted describes a subscriber in the country network of the associated location.

1. The request for determining the call type of a phone number always occurs with the definition of an NCO. The location information referenced in this NCO is used as basis for determining the call type.

2. Through use of a call type checker, each connection setup can be individually allocated to one of the four evaluation groups *International*, *National*, *Area* or *Internal*. If the corresponding privilege (*International*, *National*, *Local* or *Internal Call Privilege*) has not been assigned to the user initiating the connection or his/her user group, the XPR server rejects the connection request.

- **International**
The phone number to be converted describes a subscriber outside the country network of the associated location.
- **Unknown**
The phone number to be converted cannot be assigned to any of the above call types.

Example:

If the location includes e.g. the country code *49* and the phone number to be converted begins with the country code *1*, the call type checker determines the call type *International*.

Call type checkers are called by NCO clients independently from the normalization or localization of a phone number.

A call type checker is already preinstalled along with the XPR server installation.

Central component of each call type checker are its associated conditions. You can find more on this in [Section 9.3.6, “NCO Conditions”, on page 353](#).

9.3.2.7 NCO Clients

All XPR server modules that communicate with external systems are counted among NCO clients. In this function they normalize or localize received phone numbers by invoking the corresponding NCO program routines of the `NumberConversion.lib`.

We differentiate two types of NCO clients:

- Service-specific clients
- User-specific clients

Depending on the client type there are different manners of handling a phone number conversion request. Let us take a closer look at these two types in the following section. Details on the actual phone number conversion process will be described in [Section 9.3.4, “NCO Clients and Connect Points”, on page 347](#).

Service-specific NCO clients

All XPR server APLs are counted among the service-specific NCO clients. When they convert phone numbers, no actual XPR users are affected but solely systems connected from outside (e.g. a connected PBX).

For each service-specific NCO client configured in the XPR server, a corresponding entry is made on the **Clients** tab of the NCOAdmin with the server installation. The client name used is defaulted by the respective name of the associated XPR service.

User-specific NCO clients

User-specific NCO clients comprise all XPR modules that realize an interface to XPR users. All TUI and GUI interfaces – thus e.g. PhoneMail or optiClient – are counted among these clients.

With the XPR server installation, the NCO clients *TUI* and *GUI* are configured on the **Clients** tab of the NCOAdmin by default.

9.3.2.8 Connect Points

Each NCO client provides connect points. The assignment of the individual client resources to these connect points depends on the client implementation. For instance, the ISDN APL provides one connect point per trunk group, whereas the CTI APL provides one connect point per CTI link.

The connect points are automatically created during the setup of a client resource.

It is possible to assign an individual NCO to a single client resource because of the assignment of connect point and NCO. This NCO will then determine the format of the corresponding phone number conversion.

For further information on the connect points, please refer to [Section 9.3.4, “NCO Clients and Connect Points”, on page 347](#).

9.3.2.9 Variables

Many settings in NCO are administered in the variable format. Among these are the configuration parameters of the configured locations, the transfer of special parameters during the conversion rule run-through, or the conversion results.

All NCO variables are of type *String*. For the logical variable contents the string values *true* and *false* are used.

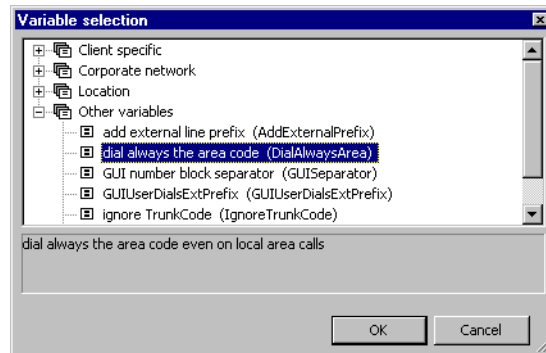
To simplify the configuration of a variable, a variable suggestion list is available. This list contains all variables that can be used in the NCO by default. The `VariableProposals.xml` file determines which variables are contained in the suggestion list.

Please note: the use of a variable is not determined by the suggestion list folder in which the variable is contained.

Example:

The variable *AreaCode* is stored in the *Location* folder. That does **not** mean that it may exclusively be used on the **Locations** tab of the NCO settings. Instead, it can be used in any place of the NCO framework.

Number Conversion Object (NCO)



If individual variables are to appear in the suggestion list during an XPR server installation, they can be integrated in the `VariableProposals.xml` file by the administrator. The `VariableProposals.xml` file is part of the XPR server and stored under the path `<XPR Install>\res\mrs\NCO\ General`. The description of the single variables is available in [Section 9.9.13, “NCO Variables Reference”, on page 495](#).

IMPORTANT:

If the `VariableProposals.xml` file has been customized, it must be manually saved before XPR server updates. This procedure prevents an unintended overwriting of information while the XPR server is updated.

Variables can be statically added via the NCOAdmin application or allocated with values. Depending on the execution of specific rules or conditions it is also possible to generate variables dynamically, or allocate them with values.

All variables can additionally be referenced in rules or conditions. In this way the variable values can e.g. influence the course of a phone number conversion. If a variable value is to be accessed in a rule or condition, it is referenced with the notation `<variable name>`.

9.3.3 The normalized NCO Phone Number Format

Each normalized phone number can be represented under NCO in the following phone number structure:

<format identifier><phone number portion>;<appendix>

Let us take a closer look at these phone number elements.

9.3.3.1 Format identifier

Normalized phone numbers are available in two formats – the *international* or the *private* one. The format used for a phone number can be recognized by the leading format identifier:

- + The following phone number is available in the international format.
Example: +492404901100
- P The following phone number is available in the private format.
Example: p100
- + The following phone number is available in the international format.
Example: +492404901100

Each normalized phone number has a format identifier.

9.3.3.2 Phone number portion

This part of a normalized phone number defines the actual phone number information.

Not every normalized phone number has a phone number portion. In a communication setup it occurs relatively often that no originator number is transferred. In such a case the normalized phone number may only exist of the format identifier *p*.

9.3.3.3 Phone Number Appendix

Processing phone numbers within the XPR server may require the administration of supplementing communication information. For this purpose it is possible to attach further information to a phone number in the variable format.

Such an appendix is separated from the actual phone number by a semicolon (;) and has the format:

<variable name>=<variable value>

Information is always attached when the phone number to be normalized contains additional information that cannot be part of the normalized format. So that this information is not lost with the normalization, it is attached in normalized phone number format to the actual phone number.

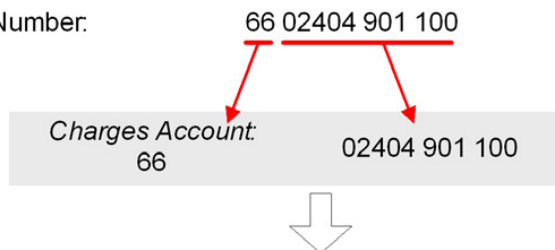
Specifying an appendix in a normalized phone number is optional.

Example: Call charges evaluation via prefix dialing

A company realizes call charges assignment via the individual code of a call account. This procedure is now to be introduced with the communication of CTI clients within an XPR environment as well.

Let us illustrate these coherences.

Dialed (local) Calling Number:



Normalized Calling Number +492404901100;Account=66

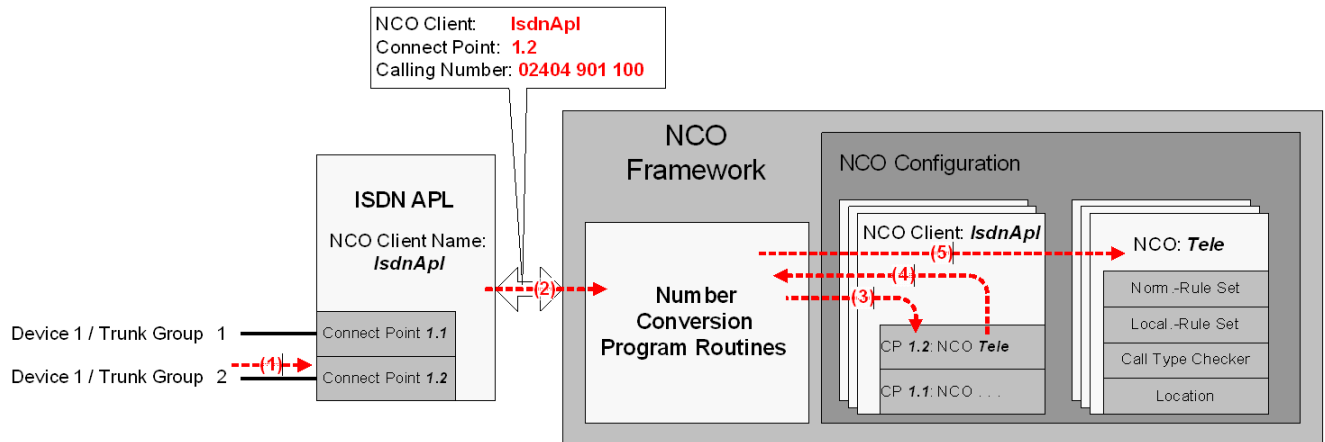
The phone number dialed in the CTI application contains, besides the actual dial information of the phone number, the call account prefix. This prefix, however, cannot be integrated in the phone number portion of the normalized phone number format in a suitable format. Therefore it is inserted in the normalized phone number as appendix of the format `Account=66`.

9.3.4 NCO Clients and Connect Points

Let us now take a look at the phone number conversion process for the service-specific and user-specific NCO clients already described.

Service-specific NCO clients

We select the ISDN APL as service-specific example.



The ISDN APL as service-specific NCO client defines connect points during its configuration. It does so for each of its trunk groups³. On this basis it can later convert phone numbers group-dependently if required.

Like all other service-specific NCO clients it proceeds as follows:

1. The APL receives a phone number from an external system as part of a message.
2. It transfers this phone number information to the NCO framework for conversion. With the phone number information it also sends its NCO client name (**IsdnApl**) and the trunk group connect point on which it has previously received the message (**1.2**).
3. The NCO framework consequently accesses the client configuration named **IsdnApl**. The relevant connect point **1.2** is referenced there. If in the conversion call under (2) no connect point has been specified, the **Standard Connect Point** is used in the following.
4. The assignment of connect point **1.2** and e.g. the NCO **Tele** takes place in the NCO configuration.
5. Subsequently, the settings (location, call type checker and conversion rules) of the thus specified NCO **Tele** are accessed.

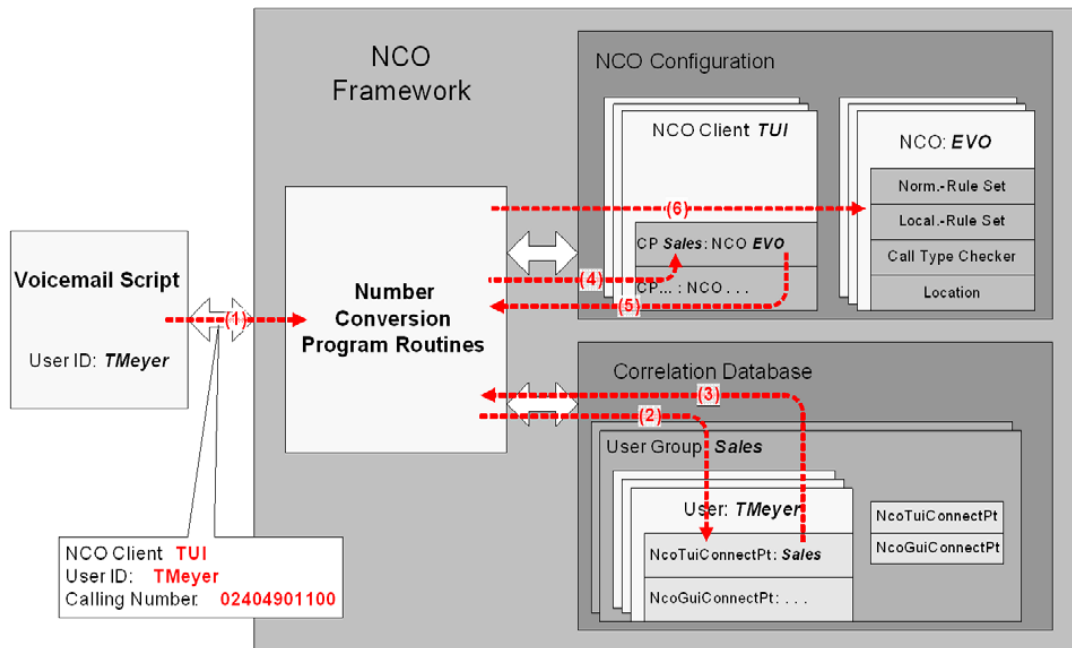
3. The format in which an NCO client defines connect points depends on its module implementation. The ISDN APL defines e.g. for each configured trunk group a connect point of the format: **<device number>.<trunk group number>**.

Number Conversion Object (NCO)

On the basis of this information the desired conversion can consequently be performed. The resulting normalized phone number is subsequently sent to the APL⁴.

User-specific NCO clients

We select the TUI script EVO as user-specific example.



User-specific NCO clients do not address their associated NCO directly by transferring a connect point.

Let us see how such an NCO client performs a conversion.

1. A user transfers a phone number to the TUI script for further processing. The script transfers this phone number information to the NCO framework for conversion. Along with the phone number information it also sends its NCO client name **GUI**⁵ and the user ID of the logged-in user (**TMeyer**).
2. The NCO framework subsequently accesses the XPR user database with the user ID information.
3. There the content of the `NcoTuiConnectPt`⁶ database field (**Sales**) is read out for the relevant user. This information determines the connect point used for further processing the TUI script information. If no entry is available there, the content of the XPR user group database field of the same name is accessed. If this database field is empty as well, the

4. The call type checker is invoked by a service-specific NCO client in the same way. The result returned to the client is, however, no converted phone number but the determined call type.

5. GUI scripts transfer the NCO client name **GUI**, TUI scripts the name **TUI**.

6. GUI scripts access the `NcoGuiConnectPt` database field, TUI scripts access `NcoTuiConnectPt`.

Standard Connect Point is used in the following.

4. The thus determined **Sales** connect point is subsequently referenced in the previously defined **TUI** NCO client.
5. There the assignment of connect point **Sales** and the NCO **EVO** takes place. If the addressed connect point is unknown, the **Standard** NCO is used in the following.
6. With this information the NCO framework accesses the settings (location, call type checker and conversion rules) defined in the NCO **EVO**.

On the basis of this information the desired conversion can be performed, the result of which is subsequently sent to the voicemail script⁷. This mechanism enables the definition of an individual conversion of GUI or TUI phone numbers for each XPR user.

7. The call type checker is invoked by a service-specific NCO client in the same way. The result returned to the client is, however, no converted phone number but the determined call type.

9.3.5 Location, Phone Numbers and Prefixes

IMPORTANT:

The phone number information for XPR users is stored in the Correlation Database of the XPR server in normalized format. The respective normalization always takes place on the basis of the corresponding location information. If location settings are modified in an existing XPR environment, the phone number information of existing users is **not** automatically updated in the Correlation Database.

As a consequence, corresponding modifications of the user information must be performed manually. For this purpose, you can use the XPR tool *Number Conversion Prepare* with the following command prompt:

```
numberconversionprepare update nocn
```

Number Conversion Prepare **does not** adjust the **CIT** database field in the process.

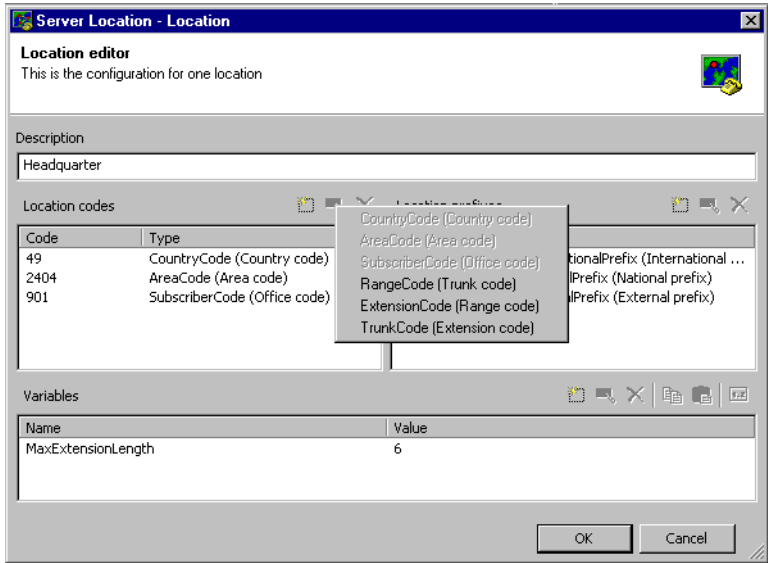
The location information is a NCO basic information, thus significantly influencing the phone number conversion. It is composed of the following information:

- Location codes
- Location prefixes

Let us take a closer look at them.

Location codes

The location codes in the XPR server environment describe all necessary phone number information required to determine its exact position in the international hierarchical communication network. This information is the decisive base for a correct phone number normalization within the XPR server.



The following location codes are available:

- Country code
Defines the country code of the relevant location.
- Area code
Defines the area code of the relevant location.
- Subscriber code
Defines the subscriber code of the relevant location.
- Range code
Defines the range lists under which the telephone terminal devices of XPR users in this location are externally accessible. Numbers that are not contained in a range code upon its definition will be normalized to private phone numbers. If no range code is defined, all phone numbers are externally accessible.
You find more detailed information on range lists in [Section 9.3.12, “Range Lists”, on page 376](#).

IMPORTANT:

If an extension range has been configured, simultaneous definition of an extension code is not possible any more.

- Extension code
Defines a simple extension code under which the telephone terminal devices of XPR users in this location are accessible. This option is in most cases only used if the XPR server is operated at a single MSN without using a PBX.

IMPORTANT:

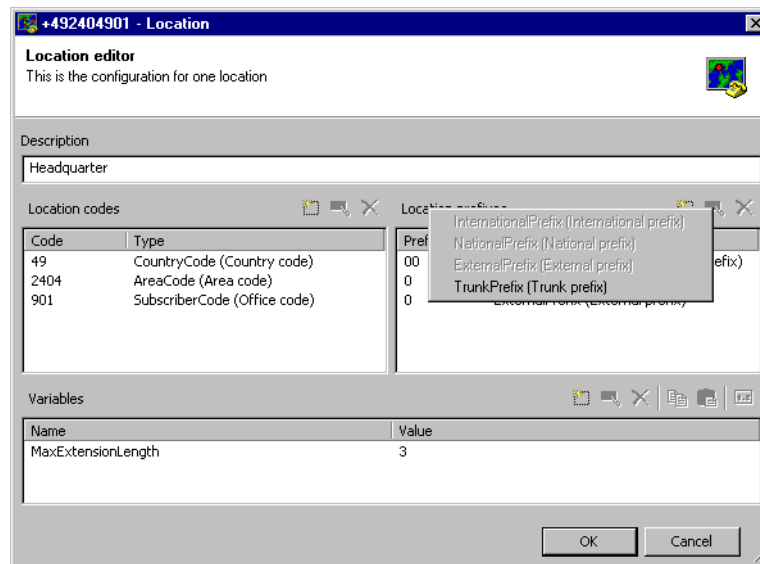
If an extension range has been configured, simultaneous definition of a range code is not possible any more.

- Trunk code
Defines *exclusively* the trunk code under which the XPR server is connected to a PBX. This code is passed from the PBX to the XPR server with phone number transfers if required.

Location prefixes

Location prefixes describe the behavior of the PBX or the telecommunication network during the establishment of communication relations.

Number Conversion Object (NCO)



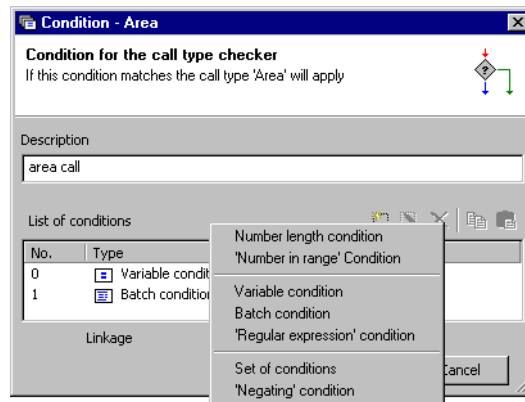
The following location prefixes are available:

- **International prefix**
The international prefix informs the communication network that the upcoming phone number begins with a country code and requests an international remote connection.
- **National prefix**
The national prefix informs the communication network that the upcoming phone number begins with an area code and requests a national remote connection.
- **External prefix**
The external prefix defines a digit dialed by a subscriber to establish an outside line connection at a PBX. This prefix is also often called outside line dialing number.
- **Trunk code**
Particularly networking PBXs via cross connections may require the XPR server to add a trunk code to the phone number to be dialed. This number can be defined under the trunk prefix.
A trunk prefix needs to be configured only rarely.

9.3.6 NCO Conditions

Conditions are used within NCO at two points.

- Within the call type checker to determine the applying call type.
- Within conversion rules to define a condition under which the associating conversion rule is executed.



The following condition types are currently available:

- Batch condition
- Negating condition
- Number in range condition
- Number length condition
- Regular expression condition
- Set of conditions
- Variable condition

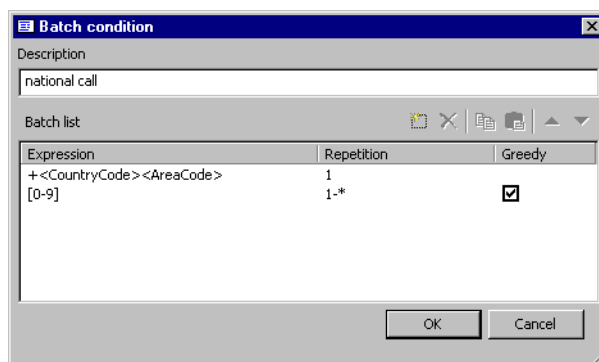
All conditions configured for a call type checker or an individual conversion rule can be linked via the logical operators AND or OR. An individual selection of these operators for specific conditions is not possible at this point. The condition type *Set of conditions* however enables such a configuration (cf. [Section 9.3.6.6, “Set of Conditions”, on page 356](#)). Negating a more complex, logical condition tie is possible as well. Cf. also [Section 9.3.6.2, “Negating Condition”, on page 354](#).

Let us take a closer look at the operating principles of the various condition types.

9.3.6.1 Batch Condition

The batch condition defines in most cases several, single, regular-expression-based portions, which replace the definition of a complex regular expression. This method of generating regular expressions⁸ is a significant facilitation for the administrator configuring a condition.

Example:



In this case we have a batch condition with two expression portions. These are to check whether a phone number is available in a national phone number structure. The defined expression portions are applied as a whole to the phone number to be converted. If a phone number matches the structure defined by the expression portions, the condition is fulfilled.

From our two example expression portions follows e.g. that a phone number begins with a '+' character followed by the content of the *CountryCode* variable. This expression is to be followed by at least another digit (**Repetition=1-***).

You find continuative details on operation mode and generation of a batch expression in [Section 9.3.8, "Batch and regular Expressions", on page 367](#).

9.3.6.2 Negating Condition

A negating condition negates one of the conditions it contains.

9.3.6.3 Number Range Condition

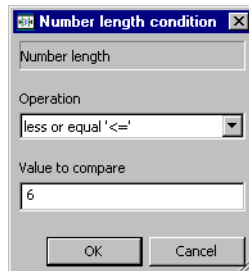
The number in range condition determines whether a transferred phone number falls into a defined number range. Various adaptations are selectable for this check.

You find continuative information in [Section 9.3.12.7, "The Condition of Type Number Range", on page 382](#).

8. The regular expression syntax used by NCO corresponds to the JavaScript (ECMAScript) syntax.

9.3.6.4 Number Length Condition

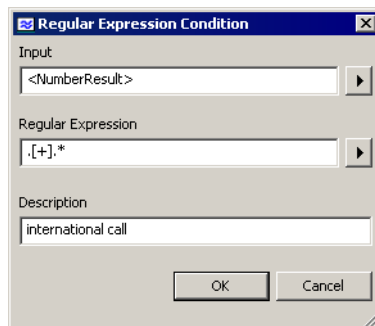
This condition checks the length of a transferred phone number. Various comparison operators are selectable. You find detailed information in the reference portion under [Section 9.9.11, “NCO Conditions”, on page 468](#).



If in our example the phone number to be converted is shorter than 7 digits, the condition delivers value *true*.

9.3.6.5 Regular Expression Condition

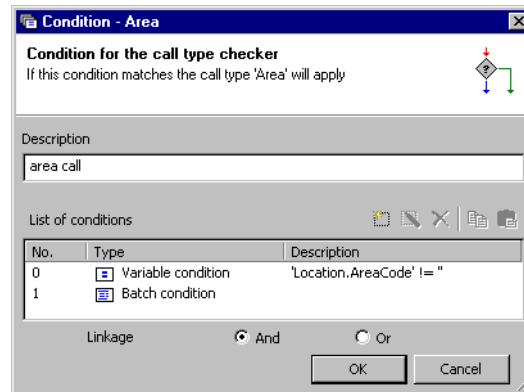
A rule of the regular expression type checks the format of a transferred input according to a defined regular expression.



In our example the content of the *NumberResult* variable is examined. If it can be mapped by the regular expression *.[+]**, our condition is considered fulfilled.

9.3.6.6 Set of Conditions

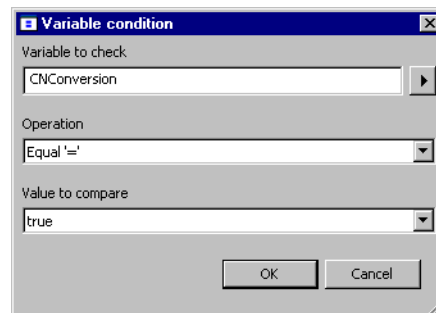
The condition type *Set of conditions* enables grouping of several conditions of an arbitrary type. These can then be arbitrarily linked with an AND or OR operator, which is independent from the linking operator of the superordinate condition level.



In our example the two conditions defined in the condition set are linked with AND. In the superordinate condition level the OR operator can be used. This enables a combination of the logical operators AND and OR.

9.3.6.7 Variable Condition

A variable condition compares the content of a variable to be defined with a value to be specified. Various operators are available for comparison. You find detailed information in the reference portion under [Section 9.9.11, "NCO Conditions"](#), on [page 468](#).



In our example the condition is *true*, if the *CNConversion* variable has the *true* content.

9.3.7 Localization and Normalization Rules

These rules control the conversion behavior within NCO.

We differentiate three rule areas:

- **Preprocessing rules**

Preprocessing rules are used for a preparative phone number adaption. With phone number normalization such adaptations are e.g. removing an individual trunk line number transferred by the PBX.

Preprocessing enables establishing the conversion rules to follow on a generally valid phone number format. This simplifies re-using conversion rules at different places within NCO.

All rules defined in this area are run through in succession.

- **Conversion rules**

Conversion rules are used for the actual phone number conversion.

All rules of this area are run through to the first match. The conversion then continues with the first rule in the postprocessing area.

NOTE:

So that a rule is considered fulfilled, its processing instruction must apply as well as its associated, previously checked condition (cf. [Section 9.3.7, "Condition", on page 3599](#)).

- **Postprocessing rules**

These rules are used for a post-adaption of phone numbers already converted. With phone number localization such an adaption can be e.g. adding the location-individual digit for outside line dialing in the PBX.

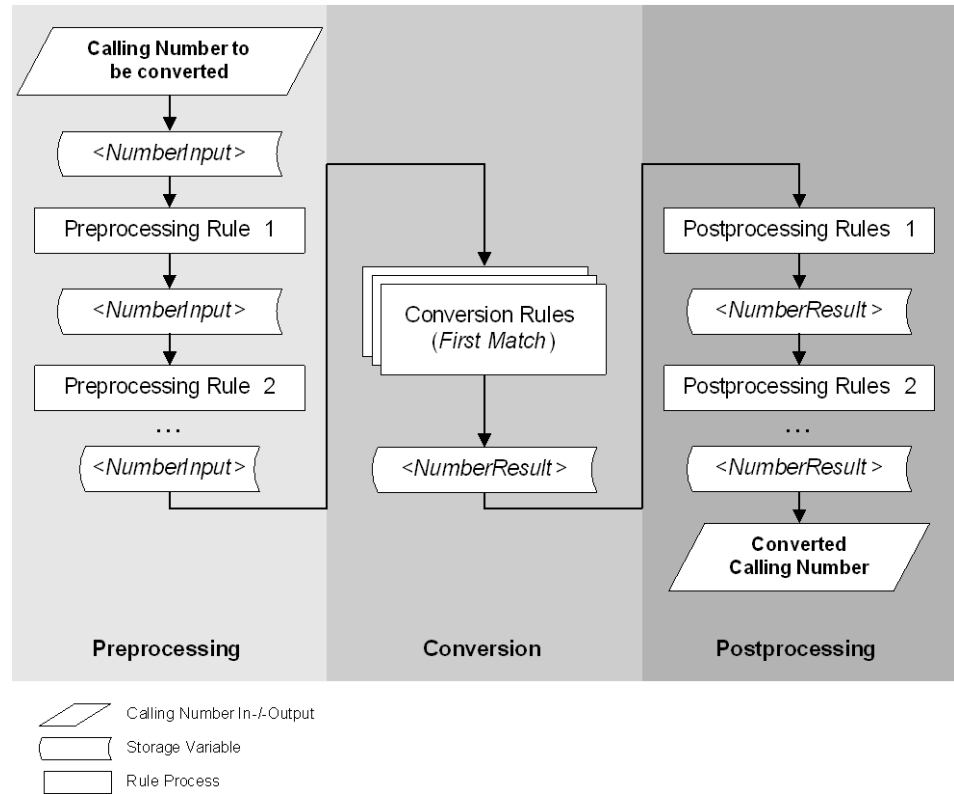
Postprocessing enables establishing the previous conversion rules on a generally valid phone number format. This simplifies re-using conversion rules at different places within NCO as well.

All rules of this area are run through in succession again.

From the names of these three rule areas you can already gather the sequence in which they are run through. It must however be ensured that results of a rule already executed are passed on to the following one. This is in most cases done via the variables *NumberInput* and *NumberResult*.

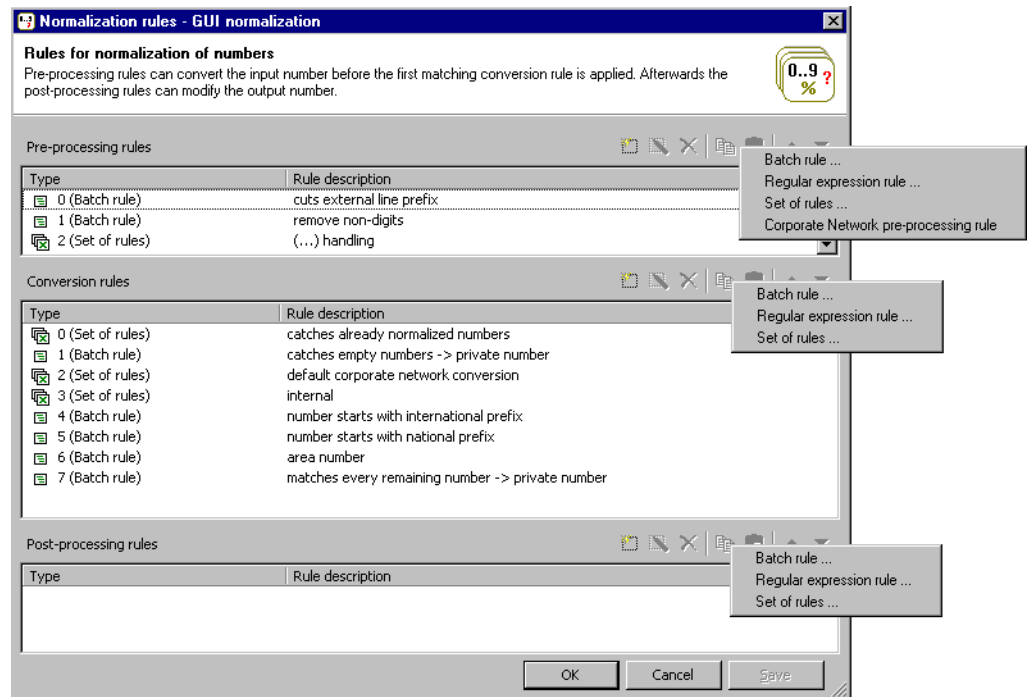
Number Conversion Object (NCO)

The following figure represents once again a phone number to be converted, running through the rule areas and their rules. Furthermore, you can see in which of the variables *NumberInput* and *NumberResult* the intermediate results of the conversion rules are buffered.



The following rule types are available in the various rule areas:

- Batch rule
- Regular expression rule
- Set of rules



Each rule is composed of three parts:

- **Condition**

Defines the condition under which the associating processing instructions are applied to the transferred phone number. You find a detailed description of the available condition in [Section 9.3.6, "NCO Conditions", on page 353](#).

- **Processing instruction**

Describes the actual processing instruction according to which the transferred phone number is converted if the associating condition has been fulfilled.

- **Result**

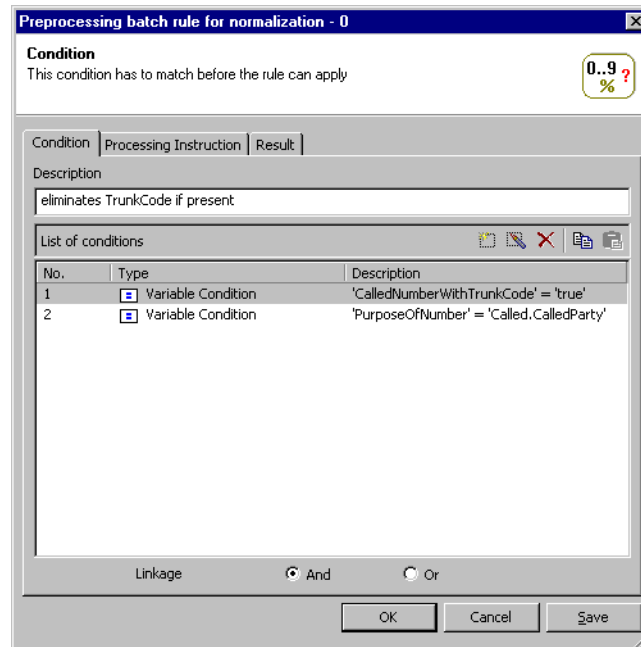
The result describes the composition of the converted phone number after running through the associating processing specification.

Let us take a closer look at the operating principles of the various rule types.

9.3.7.1 Batch Rule

The batch rule defines in most cases several, single, regular-expression-based portions which replace the definition of a complex regular expression. This method of generating regular expressions⁹ is a significant facilitation for the administrator.

Let us look at a simple batch rule example. We start on the **Condition** tab:



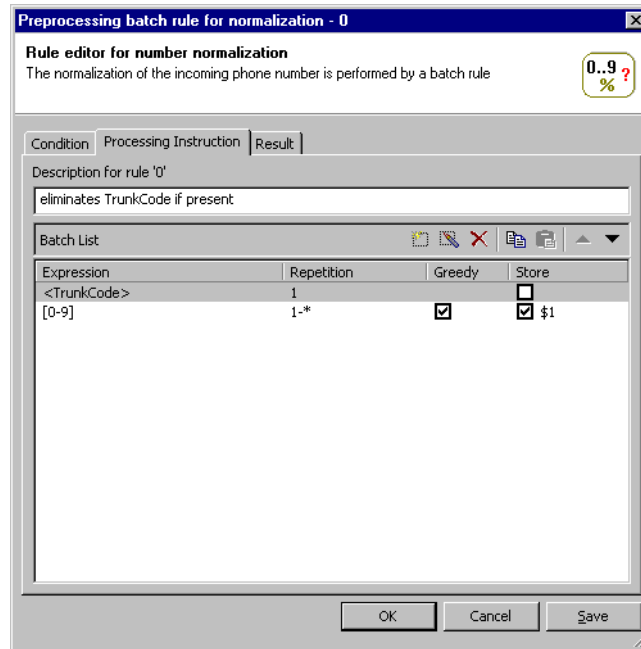
In the condition definition we can see that the processing instruction of the selected batch normalization rule is only executed if

- the connected PBX transfers the trunk code (*PBXSendTrunkCode=true*)
- and (*linkage operator AND*)
- the phone number is a destination number (*PurposeOfNumber=Called.CalledParty*).

You find continuative information on NCO conditions in [Section 9.3.6, "NCO Conditions"](#), on page 353.

9. The regular expression syntax used by NCO corresponds to the JavaScript (ECMAScript) syntax.

Next we take a look at the actual processing instruction of the batch rule, which will only be executed after the fulfillment of all previously discussed conditions. We switch to the **Processing Instruction** tab:



In our example two expression portions are defined. They are to filter out a trunk code transferred with the phone number by the connected PBX to the XPR server.

How does this happen?

The defined expression portions are applied as a whole to the phone number to be converted. If the phone number matches the structure defined by the expression portions, the phone number elements described by the respective expression portions are individually processed.

From the two expression portions in our example results e.g. a phone number to begin with the content of the *TrunkCode* variable. An arbitrary number of digits is to follow. Only if the phone number to be converted matches this defaulted structure, the batch rule modifies the original phone number.

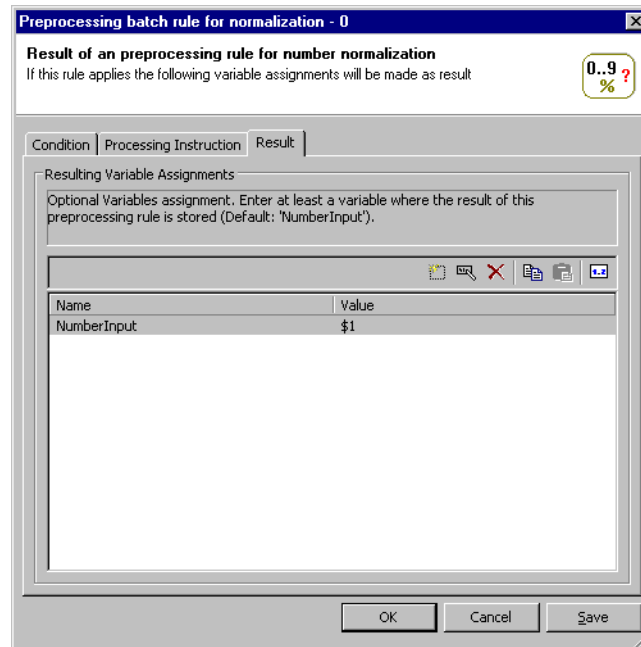
If the expression portions in our example are true, the value that corresponds to the content of the *TrunkCode* variable is not further processed (**Store** is inactive). The following digits are buffered in the \$1 runtime variable (**Store** is active). Several intermediate results to be saved are administered in different runtime variables. The respective variable names are automatically defaulted by the system after activation of the storage option. They have the \$n format.

You find continuative details on operation mode and generation of a batch expression in [Section 9.3.8, "Batch and regular Expressions", on page 367](#).

The processing instruction in our example is thus fulfilled. We continue on the **Result** tab. The layout of the following figure corresponds to the representation for all preprocessing and postprocessing rules.

NOTE:

The representation of the **Result** tab varies depending on the associated rule area (preprocessing and postprocessing or conversion rules).



As we already know, the final result of a preprocessing rule is stored in the *NumberInput* variable and in this way passed on to the following rule. In our example the final result merely derives from the *\$1* runtime variable that emerged in the processing instruction. If several intermediate results have previously been stored in different runtime variables, they can be arbitrarily combined to a final result at this point.

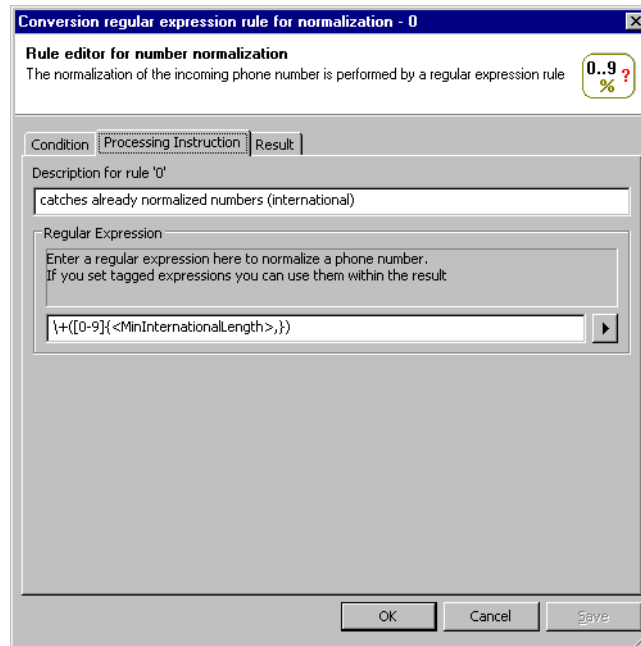
A batch rule is considered a match if its associated condition *and* its processing instruction have been fulfilled.

9.3.7.2 Regular Expression Rule

A rule of type regular expression changes a transferred phone number according to a regular expression defined in the rule. On this we return to the short normalization rule example.

The **Condition** tab can – as with the batch rule – define conditions under which the processing specification described in the following is executed. You find continuative information on NCO conditions in [Section 9.3.6, “NCO Conditions”, on page 353](#).

We therefore immediately access the **Processing Instruction** tab.



As we can see, this rule type contains solely one regular expression applied to the phone number to be processed, if the previous condition has been fulfilled. The result of the expression applied is buffered in the system variable `$1` by default.

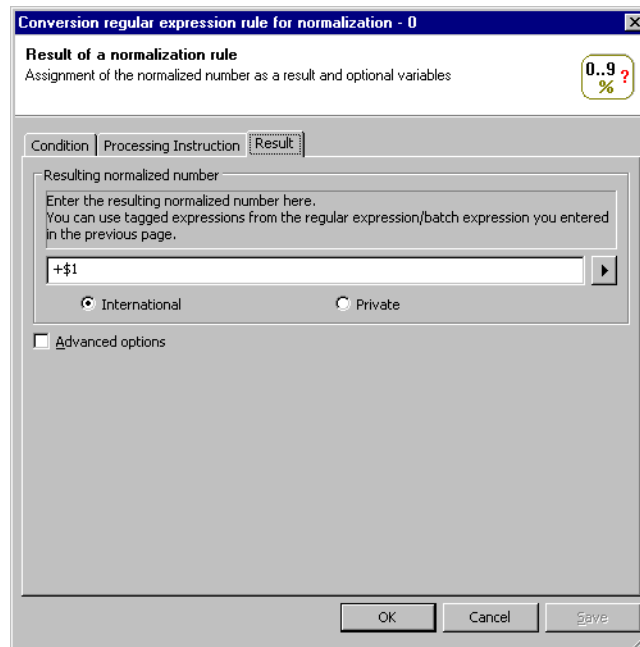
NOTE:

Next to the entry field for the regular expression a selector icon is available to access a menu with different operators for regular expressions. More information on the regular expression syntax is provided by the appropriate literature. The regular expression syntax used by NCO corresponds to the JavaScript (ECMAScript) syntax.

Next we switch to the **Result** tab, which corresponds to the conversion rule representation in the layout of the following figure.

NOTE:

The representation of the **Result** tab varies depending on the associated rule area (preprocessing and postprocessing or conversion rules).



The rule result obviously only consists of the intermediate result previously stored in the variable `$1`. Via the International option the result has only been prefixed with the '+' character, which describes the normalization into an internationalized format.

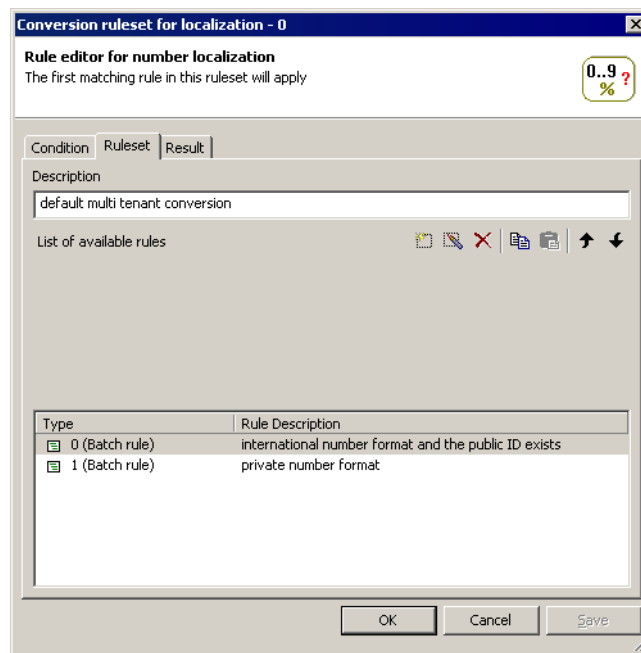
A regular expression rule is considered a match if its associated condition and processing specification have been fulfilled.

9.3.7.3 Set of rules

This type serves for grouping rules in comprehensive rulebooks. A set of rules may contain various rules of the types described here, which are executed after fulfilling a condition. Each of the included rules has an individual condition that must be fulfilled for the execution of the respective associating processing specification.

The **Condition** tab can define conditions under which the rules described in the following are executed. You find continuative information on NCO conditions in [Section 9.3.6, “NCO Conditions”, on page 353](#).

We therefore immediately access the **Ruleset** tab.



The set of rules in our example encloses two batch rules. These have an individual condition that follows the method of operation already described.

The **Result** tab corresponds to the tabs of the above rule types.

A set of rules is considered a match if its individual condition, the condition of a rule contained and its associating processing instructions have been fulfilled.

9.3.7.4 Corporate Network Pre-Processing Rule

In addition to the previously described rules the Corporate Network Pre-Processing rule is available. It represents a special case within the conversion rules and is merely used for the configuration of a Corporate Network environment.

You find more detailed information about configuring Corporate Network in [Section 9.7, “NCO in a Corporate Network Environment”, on page 418](#).

9.3.8 Batch and regular Expressions

The processing instruction of a batch rule is based analog to a regular expression rule on a regular expression. Expressions of this type are known to be difficult to write and even more difficult to understand in their standard format. On the other hand, regular expressions are very effective and phone number conversion cannot be done without them. Therefore NCO integrates a simplified format of regular expression mapping – the staple or batch rule.

With such a batch rule a regular expression is divided into several smaller expression portions. For these, different properties can be configured by means of a GUI. The actual expression portion is formed by the expected character pattern, which may consist e.g. of the string *1234*, the regular expression *[0-9]* or the *<CountryCode>*¹⁰ variable. By means of further options the following properties can subsequently be configured for each expression portion:

- how often it is expected (e.g. *0-**, *5*, *2-3*, ***)
- whether the matched pattern is to be stored in a runtime variable (*\$1*, *\$2*, ...) for further processing
- whether this regular expression is to behave *Greedyly*

NOTE:

Defining batch expressions in batch conditions is possible in the same way. In this case it is not possible to store patterns in runtime variables.

Special characters

Specific characters usually serve special functions within regular expressions. Since this does not apply for batch expressions, they can be used here without *Escape* characters. Among these characters are:

`* ? + ( ) { } $ \`

¹⁰. If variables are referenced in batch expressions, they are specified in the *<variable name>* notation.

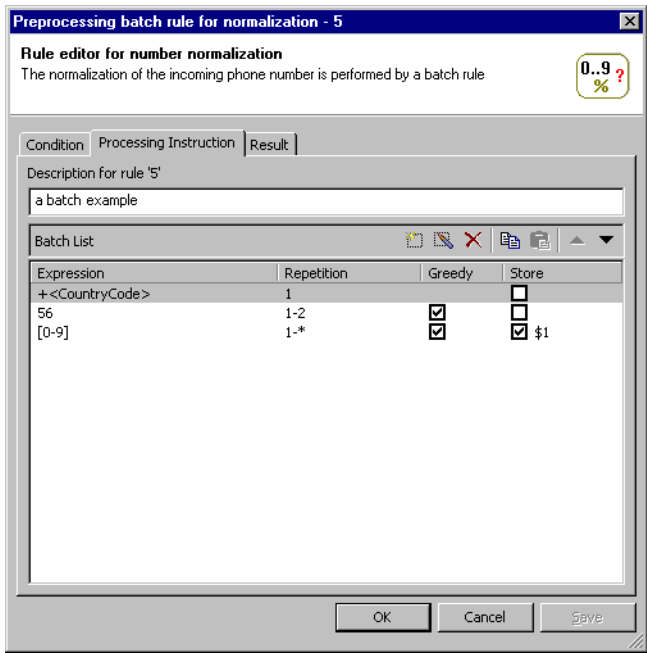
Repetition options

The batch rule realizes the configuration of repetition options for expression portions. Examples are:

- 5 The expression portion occurs exactly 5 times.
- 2–4 The expression portion occurs 2 to 4 times.
- ? The expression portion does not occur at all or only once. 0–1 can be specified as alternative.

A first short example

A short example will clarify the batch rule principle. To this we compare the processing instruction of a batch rule with its corresponding regular expression:



The common regular expression that corresponds to this batch rule reads:

```
\+<CountryCode> (? : 56) { 1, 2 } ( [ 0 - 9 ] * )
```

The *Greedy* option

Defines the behavior of an expression portion when phone number digits match this as well as the following expression portion.

If this option is set for the first expression portion, this portion takes as many digits as enabled by its regular expression (longest match). If this option is deactivated for the first expression portion, this portion takes only as many characters as required for fulfilling its regular expression. The following digits are left to the next expression portion (shortest match)¹¹.

Another short example

Let us illustrate the *Greedy* option function by means of a simple example.

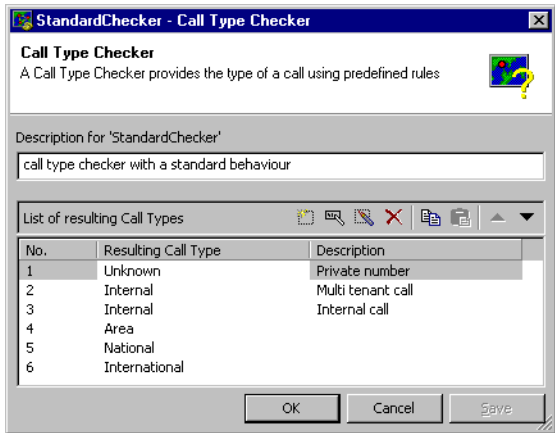
We want to apply the following batch expressions to the phone number *02409901191*.

Batch	Regular Expression	Greedy Option	Phone Number Matches
Expression portion 1	[0-9]	deactivated	0240
Expression portion 2	9	deactivated	9

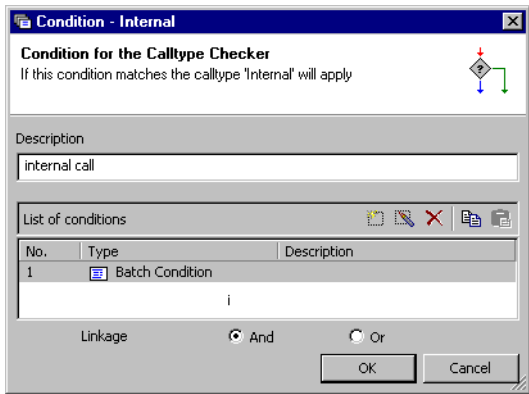
11. You find more information on this option in the appropriate literature about regular expressions.

9.3.9 Call Type Checker and Conditions

On the basis of location information¹² the call type checker determines the call type of a phone number transferred to it. Cf. [Section 9.3.2.6, “Call Type Checker”, on page 341](#).



Each call type checker contains a call type list. At least one NCO condition is assigned to each of these call types. If several conditions are defined, they can be linked to each other via the logical operators AND or OR. An individual selection of these operators for specific conditions is not possible at this point.



If all conditions of a call type are fulfilled, a match follows and the checked phone number is assigned the associating call type.

The call type list is run through to the first match.

The above example shows the *Internal* call type. Exactly one batch condition is configured for this call type. If a phone number to be checked fulfills this condition, the *Internal* call type is assigned to this phone number.

For the conditions of a call type checker, various condition types are available. These are:

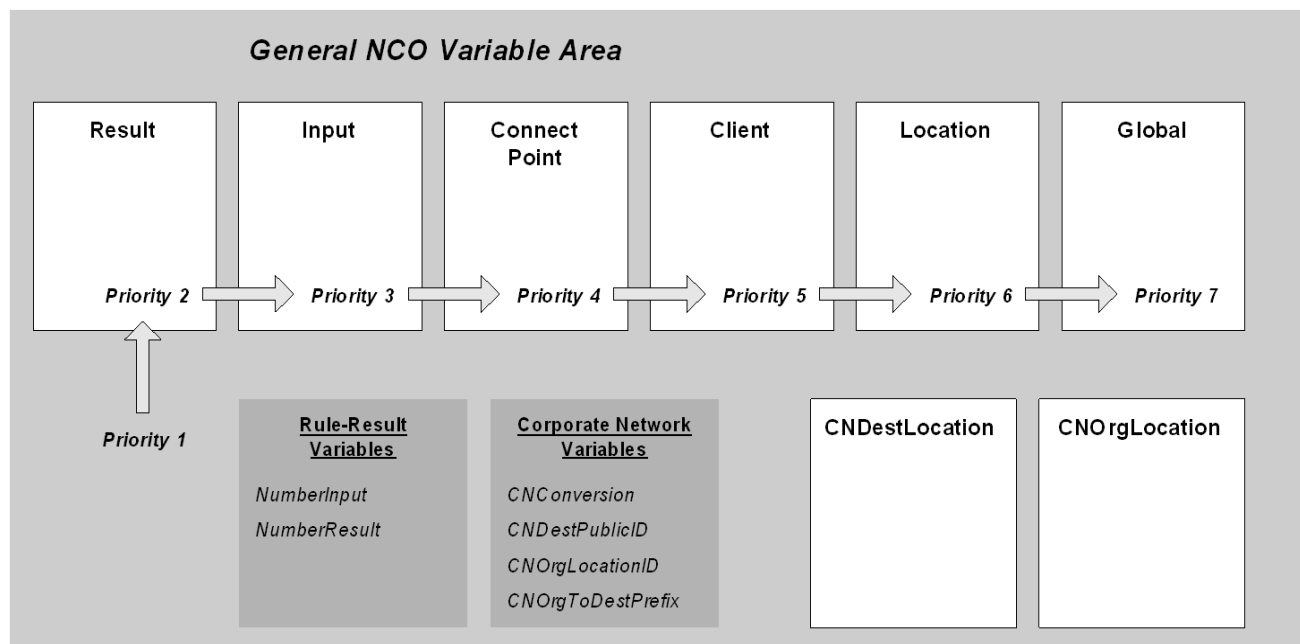
¹².The request for determining the call type of a phone number always occurs with the definition of a NCO. The location information referenced in this NCO is used as basis for determining the call type.

- Number length conditions
- Number range conditions
- Variable check conditions
- Batch conditions
- Regular expression conditions
- Set of conditions
- Negating conditions

You find a detailed description of the available condition in [Section 9.3.6, “NCO Conditions”](#), on page 353.

9.3.10 Administering NCO Variables – Name Areas

To improve the administration of the available NCO variables, they are in most cases assigned to different name areas. The following figure illustrates this structure and its internal cohesions.



Depending on the use of a variable, it is administered in one of the following five name areas.

- **Result**
Variables of this name area are in most cases used within the execution of rule records. Associated variables are configured in the NCOAdmin on the **Result** tab of the single conversion rules.
- **Input**
contains variables transferred to NCO by the NCO clients within the scope of phone number conversion. Since variables of this name area are defined by the program code of the respective NCO clients, they are not to be added via the NCOAdmin.
- **Client**
Variables of this name area can be defined for selected NCO clients and control the client-individual phone number conversion. Variables of the client name area are configured in the NCOAdmin on the **Clients** tab.
- **Location**
contains variables that determine the location properties. Variables of this name area are configured in the NCOAdmin on the **Locations** tab.

- **Global**
contains variables that are to be directly usable for all NCO elements. Variables of this name area are configured in the NCOAdmin on the **Variables** tab.
- **CNOrgLocation**
contains variables that define the information of an originator location in a Corporate Network environment.
- **CNDestLocation**
contains variables that define the information of a destination location in a Corporate Network environment.

Besides the variables of the described name areas also those are available that exist parallel to the described name areas, thus directly in the general NCO variable area.

These variables are:

- NumberInput
- NumberResult
- CNConversion
- CNDesPublicID
- CNOrgLocationID
- CNOrgToDestPrefix

Variables of the same name in different name areas

The administration of variables in name areas has various advantages. One is that variables of the same name can be configured in different name areas.

Looking for a variable

If a variable name is referenced during a phone number conversion, NCO must, as the case may be, first determine the name area in which the relevant variable was defined. In doing so, NCO searches the various name areas depending on a defined priority.

1. General NCO variable area
2. Result
3. Input
4. Client
5. Location
6. Global

The first variable found with the variable name specified is used by NCO for further processing.

The name areas *CNDestLocation* and *CNOrgLocation* are not automatically searched. Variables of these two structures must therefore always be addressed with the name area notation (see below).

Transfer of variables by an NCO client

Within the scope of a phone number conversion, NCO clients can default individual variable contents for the conversion. If an NCO client defaults such a variable content, and if the relevant variable is defined in the NCO with another value already, the client-individual variable content overrides the NCO content of the variable.

Example:

For the ISDN APL of an XPR server the **PBX sends Called Numbers with Trunk Code** option is activated in the APL settings. This makes the relevant ISDN APL transfer the variable *CalledNumberWithTrunkCode=true* to the NCO with each of its conversion invocations.

If the *CalledNumberWithTrunkCode* variable is already defined in the NCO with the *false* value, this content is temporarily overridden with the *true* value by the relevant ISDN APL for each phone number conversion.

Name area notation

If variables of the same name are defined in different variable areas, problems may occur with the above variable search.

Example:

The variable *Version* is defined for the name areas *Input* and *Client*. In a phone number conversion rule this variable is now to be accessed in the *Client* name area. As we can see above, NCO would, with referencing a variable, use the variable of the *Input* name area (*Input* is searched before *Client*) only via the name *Version*.

How can we access the desired variable in the *Client* name area in such a scenario?

By means of the name area notation. The actual variable name is prefixed with the description of the desired name area and followed by a dot. For the above example the result is: *Client.Version*.

Variables administered parallel to the name areas can only be addressed via their names.

9.3.11 Export and Import of NCO Elements

To realize a user-friendly configuration the XPR server supports the option to export and import NCO configuration data. In this process all relevant information is converted into XML-based files.

By means of the export/import function of the NCOAdmin application, configuration modifications can be optimized in a test environment. After their efficiency approval they can be copied to a productive system.

The following NCO configuration units can be exported or imported:

- Single NCOs inclusive assigned elements
(sets of rules, location, call type checker)
- Single locations
- Single call type checkers
- Single normalization or localization rule sets

9.3.12 Range Lists

The range list is another NCO conversion variant. It serves for extension-dependent phone number conversion. By means of a phone number to be converted it is checked for being contained in the number range of a defined range list. If this is the case, the associating phone number conversion can be performed.

But in which cases is an extension-dependent conversion of phone numbers considered useful? An example:

A company has many employees that can be reached at their workstation via a PBX. There are also internal telephones via which an external connection can be set up, but their phone numbers are not to appear in the public telecommunication network. Among these telephones are e.g. devices in the warehouse or in various recess rooms.

An extension-depending conversion of these internal telephones makes sure that for external calls made from these devices the number of the head office is inserted as originator number.

Before we continue with configuring an extension range, we need to familiarize ourselves with details significant for range lists.

9.3.12.1 What is a Range List?

A range list defines various phone numbers to be handled in a specific way in case of a phone number conversion.

9.3.12.2 Range List Structure

A range list consists in the most simple case of the specification of dedicated phone number ranges. The phone number ranges contained are separated by a semicolon (;) and can

- correspond to a single phone number or
- to a consecutive number range.

Consecutive number ranges are defined with a hyphen (–). The phone numbers that limit the range must consist of the same number of digits.

Examples: 200;300;400–410;20–25

Adding a common code

Further common codes can be assigned to the above described notation. These codes are then prefixed to each single phone number of the phone number ranges mentioned.

In a range list a common code is separated by a colon from the respective expression that follows.

Example 1: 999:200;300;400-410
corresponds to: 999200;999300;999400;999401;...999410

Example 2: 2404:999:200;300;400-410
corresponds to:
2404999200;2404999300;2404999400;2404999401;...2404999410

9.3.12.3 Check Directions for a Number Range List

Checking whether a phone number to be converted is available in a range list occurs according to the number range conditions of the conversion rules called. Three different directions can be configured in NCO for this check.

- Check from right to left
- Check from left to right
- Check from left to right with skipping entire number portions

Check from right to left

With this extension check the digits of a phone number to be converted are compared with the phone number ranges of the range list from the end to the beginning. How many digits of a phone number are compared is determined by the length of the extensions defined in the *phone number ranges*.

Examples:

Range List	Phone number	Result
200;300;400-410	+492404999100	Phone number is not part of the range
200;300;400-410	+492404999405	Phone number is part of the range
10-99	110	Phone number is part of the range

Check from left to right

The check from left to right compares phone numbers with the defined phone number ranges from the beginning to the end. The number of digits used for a comparison results from the *phone number range* definition as well.

Examples:

Range List	Phone number	Result
999200;999300-999400	999100	Phone number is not part of the range
999200;999300-999400	999305	Phone number is part of the range

Check from left to right with skipping entire number portions

This variant is based on the above check from left to right. Here, however, sinistral phone number portions can be defined. If these portions are contained in a phone number to be converted, they are skipped in the check and no longer considered.

Examples:

Range List	Phone number	to be skipped	Result
999200;999300-999400	305	–	Phone number is not part of the range
999200;999300-999400	305	999	Phone number is part of the range

9.3.12.4 Match Behavior using Common Codes

In [Section 9.3.12.2, “Range List Structure”](#) we have already seen that common codes can be added to a range list. This leads to a special match behavior with checking a phone number for its availability in a range list.

Generally applies:

*If portions of a phone number to be checked are compared with a common code (CC) of a range list, the common code must be a **complete** match.*

Some examples in which we perform comparisons from right to left will clarify this principle.

Range List	Phone number	Result
2404:999:200;300;400-410	405	Phone number is part of the range
2404:999:200;300;400-410	999405	Phone number is part of the range
2404:999:200;300;400-410	2404999405	Phone number is part of the range
2404:999:200;300;400-410	99405	Phone number is not part of the range, since 99 does not completely match CC 999.
2404:999:200;300;400-410	4999405	Phone number is not part of the range, since 4 does not completely match CC 2404.
2404:999:200;300;400-410	2504999405	Phone number is not part of the range, since 2504 does not completely match CC 2404.

9.3.12.5 Assigning Variables during a Check-up

If common codes are added to a range list, variable names can be assigned to them if required.

Example: Area=2404:Con=999:200;300;400-410

If common codes structured in this way match a phone number to be checked, all specified variables are allocated with the associating common codes.

Example:

Range List	Phone number	Allocated Variables
Area=2404:Con=999:400-410	999 405	Con=999
Area=2404:Con=999:400-410	2404 999 405	Area=2404 and Con=999
Area=2404:Con=999:400-410	99 405	no assignment, since the phone number is not contained in the range list.

9.3.12.6 Definition of a Range List

IMPORTANT:

If range lists are defined for a location, the associating conversion rules must evaluate these. Only the rules for the USA currently perform this evaluation by default. For the conversion rules of other countries, manual adaptations must be executed, so that configured range lists can be used.

Range lists can be defined in two ways:

- In the format of a location code and thus as part of a location
- In the format of a variable

Let us take a closer look at both options.

Number range list as location code

A number range list can be defined under the location codes. A new phone number range is added to the desired location for this purpose.

For each number range list the elements already described can hereupon be defined. The contents of the **Country Code**, **Area Code** and **Subscriber Code** fields determine the common number portion.

NOTE:

Entries in the **Country Code**, **Area Code** respectively **Subscriber Code** fields are only accepted if no corresponding entries are specified in the relevant location.

Range list as variable

Each variable can be edited as range list via the **Edit as Number Range** option of the context menu opened with the right mouse button.

In the **Common Code** field a common number portion of the number range list can now be defined. Under **Number Ranges** the single phone number ranges are configured.

9.3.12.7 The Condition of Type *Number Range*

A condition of type *Number Range* is added to a conversion rule or to a call type checker like all other conditions. Cf. [Section 9.3.6, “NCO Conditions”, on page 353](#). It offers special setting options, though.

Range list to be checked

Defines, which range list is to be used for checking the condition. Besides lists previously defined, a phone number range to be used for the check can be manually entered here as well. The same notation applies as described in [Section 9.3.12.2, “Range List Structure”, on page 376](#).

Check mode

The check direction to be used is selected here. If the **From left to right** option is active, an expression to be skipped can be specified.

9.3.13 Saving the NCO Configuration

The NCO configuration contains the information of all NCO elements. It is stored in the `<XPR Install>\NCO` directory under the share *MrsNCOConfig* and based on XML files. After the XPR server installation at least the two files `NCOMainTree.xml` and `VariableProposals.xml` are available.

The `NCOMainTree.xml` file contains the configuration of all defined NCOs with their location information and rule sets.

The `VariableProposals.xml` file includes a structured list of various variables provided to the administrator with the NCO configuration. You find the precise list in [Section 9.9.13, “NCO Variables Reference”, on page 495](#).

The additional files `NCOUpdateInfo.xml`, `NCOMainTreeLock.xml` and `NCOConfigLock.xml` are dynamically generated by the XPR server. They administer the access to the configuration data.

After modifications to the configuration the XPR server generates beyond that the two directories `MainTreebackup` and `DiffTree`. They serve for automatic updating the configuration or for logging the modifications performed.

9.3.14 Structure of the NCO Installation for a XPR Reinstallation

We have understood quite a bit about NCO, its elements and operating methods by now. Using this knowledge we turn to the actual installation structure of NCO with a XPR server reinstallation.

NCO is automatically installed with configuring a new XPR server. Three installation steps can be differentiated:

- Installation of NCO basic settings of the XPR server
- Installation of NCO basic settings of the NCO clients
- Further settings

9.3.14.1 XPR Server Basic Settings

With the XPR server basic settings installation, all those configurations are prepared that define the location- and country-specific NCO behavior.

Location-specific behavior

With the XPR server installation, various items of location information are already defined. These include some phone number information defining the server accessibility, for example, the country code, area code or subscriber code.

From these data a basis location is created during the NCO installation. This location is defined as master location and used for all following, automatically generated settings.

Country-specific behavior

The phone number behavior may considerably differ in the various countries. In the US e.g., phone numbers with constant length are used. In Germany, phone number length varies. Another example is Switzerland where an area code must also be dialed for local calls. These circumstances significantly influence the structure of conversion rules.

So that a newly installed XPR server can nonetheless provide a NCO basic functionality, NCO is country-specifically preconfigured as far as possible. The XPR server is supplied with different sets of conversion rules for this purpose. Depending on the installation location the desired phone number behavior can then be set during the installation.

While the XPR server is installed, the desired sets of rules can be selected after a corresponding country query. Since the phone number behavior is similar in many countries, too, an individual set of rules is not available for each country. For the server installation in a country not mentioned in the rule selection it is sufficient to select the country from the list that corresponds to the phone number behavior of the new server location.

The country behavior selection thus defined is stored in the parameter variable *ResourceCountryCode* with the associated country code. From this setting the following NCO components are automatically generated during the XPR server installation.

- The standard NCO
- The default NCO client
- The standard connect point
- The standard call type checker
- The standard normalization rules
- The standard localization rules

The update elements

These elements are called for the conversion of phone numbers that are still available in the XPR server in the XPR phone number format valid up to now. The result of this conversion are phone numbers that suffice the new NCO phone number format (cf. [Section 9.3.3, "The normalized NCO Phone Number Format", on page 345](#)).

IMPORTANT:

So that phone numbers can be correctly converted into the new NCO-conformable format, they must absolutely be available in the phone number format correct up to now. This means that each phone number must receive the associating area code from the XPR server local network.

The update elements are:

- The update-NCO
- The update-connect point
- The update-normalization rules
- The update localization rules

9.3.14.2 NCO Clients basic Settings

In various other sections we have already mentioned that with the installation of a XPR component some settings are preconfigured by the component.

XPR components can during their installation define the following NCO elements:

- An associating NCO client. Its description results from the name of the associated XPR service (e.g. IsdnApl with the ISDN APL installation).
In this NCO client a standard connect point is generated that the client-individual (see below) NCO is assigned.
- Individual sets of rules for localizing and normalizing
- A NCO that is assigned the following elements:
 - The basis location
 - A standard call type checker
 - The standard or individual sets of rules for localizing or normalizing

9.3.14.3 Further Settings

Among the further settings performed with an XPR server reinstallation is numbered, for example, the configuration of the *TUI* and *GUI* NCO clients.

9.4 NCOAdmin Start – Access to NCO Configurations

NOTE:

The *NCOAdmin* accesses the NCO configuration files of the XPR server. Please make sure that the *NCOAdmin* used and the NCO configuration files are available in the same version.

If this is not the case, an alarm message at the beginning of the Telematic configuration indicates this incompatibility.

The XPR application NCOAdmin is part of the XPR server and serves for configuring NCO elements. In the course of a server installation it is installed in the `<XPR Install>\bin` directory. Subsequently, it can be started there with the `NumberConversionAdmin.exe` file.

NOTE:

It is also possible to start a version of the NCOAdmin that is limited in its function in the configuration dialog of the single Telematic APLs. Switch to the **Device** tab of the advanced settings of the Telematic APL used. The NCOAdmin is started via the **Number Conversion Administration** button.

If the NCOAdmin is started in this way, only the tabs **Locations**, **Clients**, **Variables** and **Configuration** are available.

The NCOAdmin can be operated in three modes:

- **Locally**
The NCOAdmin processes the configuration files of the local XPR server.
 - **Via network**
The NCOAdmin processes configuration files accessible via a local network.
 - **Via Internet**
The NCOAdmin processes configuration files accessible via an Internet connection.
-

IMPORTANT:

To access a configuration file via Internet, the XPR server to be accessed must be equipped with a started WEB APL.

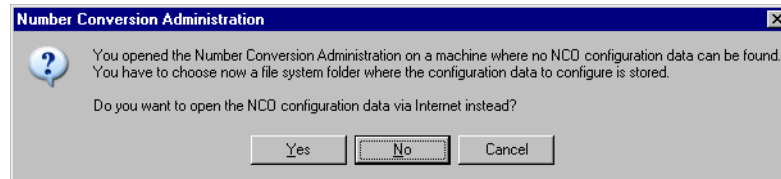
The way the NCOAdmin starts after being called depends on its operation mode.

9.4.1 Access to a local NCO Configuration

With the NCOAdmin start the existence of a share called *MrsNCOConfig\$* on the local computer system is checked. If it is available, the NCOAdmin is started in the Local mode and accesses the configuration files of the local XPR server.

9.4.2 Access to a non-local NCO Configuration

If no share named *MrsNCOConfig\$* is available on the local computer system, the initially started NCOAdmin demands further information on the storage location of the NCO configuration to be used. The NCOAdmin first queries whether the relevant data can be accessed via a network or via Internet.



For the non-local program start, three alternatives are available:

- **Yes**
The NCOAdmin is started in the Internet mode.
- **No**
The NCOAdmin is started in the Network mode.
- **Cancel**
The NCOAdmin start is canceled.

Depending on the selected operation mode the correspondingly required access information is queried. This information is stored in the local system registry and evaluated with the next program start.

NOTE:

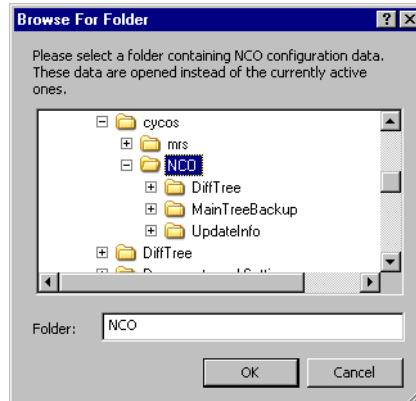
The NCOAdmin operation mode can be modified via the NCOAdmin **File** menu.

Let us now take a look at the NCOAdmin start in the Internet and Network mode.

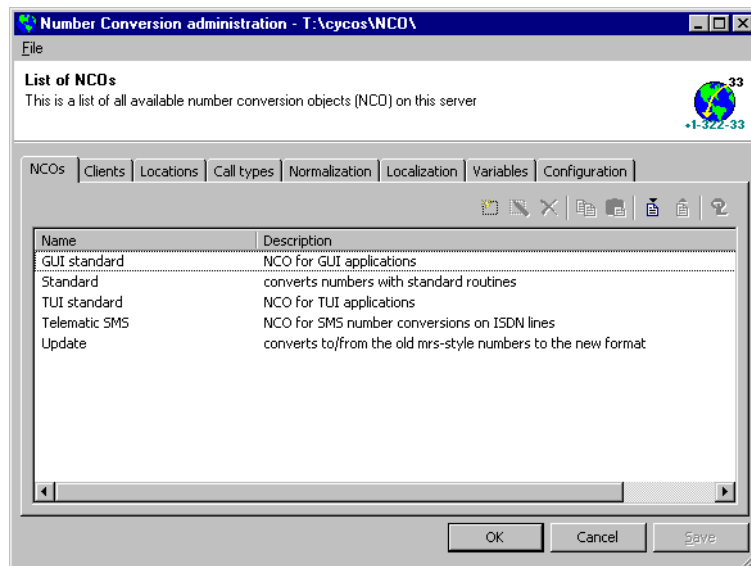
9.4.2.1 Network Access to an NCO Configuration

After selecting **No** in the previous dialog prompt in [Section 9.4.2, “Access to a non-local NCO Configuration”](#), on [page 388](#) proceed as follows.

1. Select the storage location for the NCO configuration files that you want to configure.



2. Click the **OK** button. NCOAdmin opens the desired configuration and starts with these settings.



IMPORTANT:

As soon as you save an NCO configuration, it will become active on the relevant XPR server within the next 60 seconds. Faulty settings may **trouble** the XPR server operation.

3. After performing the desired configuration modifications select the **Save** button.
4. Confirm the storage query by clicking the **OK** button.

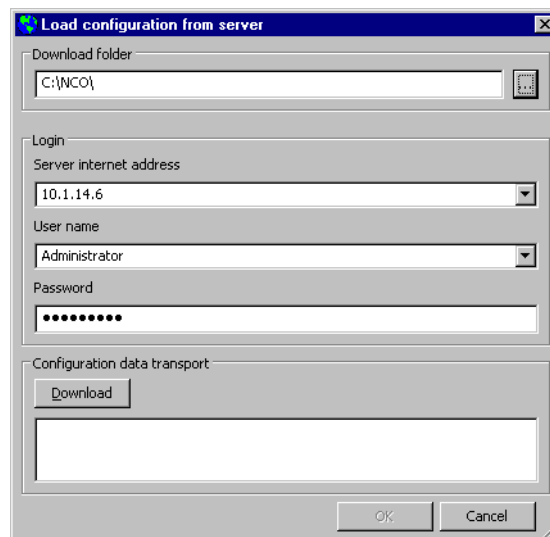
9.4.2.2 NCOAdmin with Internet Access to an NCO Configuration

IMPORTANT:

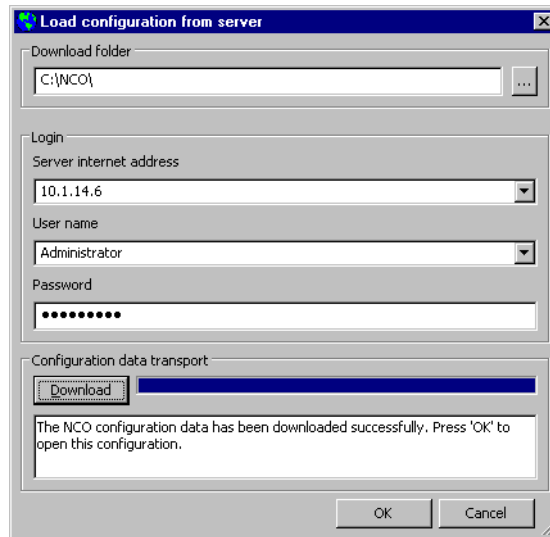
To access a configuration file via Internet, the XPR server to be accessed must be equipped with a started WEB APL.

After selecting **No** in the previous dialog prompt in [Section 9.4.2, “Access to a non-local NCO Configuration”](#), on page 388 proceed as follows.

1. Specify a local folder in the **Download folder** field to store the configuration files of the remote XPR server.

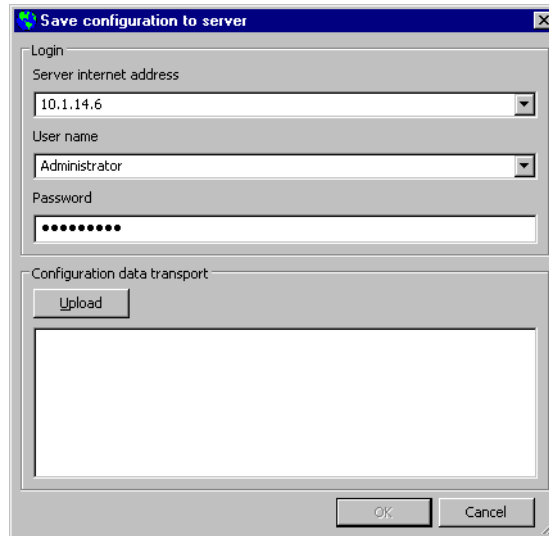


2. In the **Server internet address** field enter the IP address of the XPR server from which the configuration files are to be loaded.
3. In the **User name** field specify an XPR user name. Under this account the NCOAdmin logs in at the XPR server.
4. In the **Password** field enter the password for the specified XPR user.
5. Push the **Download** button. NCOAdmin loads the configuration files from the specified XPR server. If communication problems should occur, error reports in the log window point to the problem.



6. Click the **OK** button. NCOAdmin opens the locally saved configuration and starts with these settings.
7. After performing the desired configuration modifications select the **Save** button. Modifications are thus saved in the locally stored configuration files.
8. In the **File** menu select the **Save and activate > Save to network (via Web) and activate** option. The modified configuration files are transmitted to the remote XPR server.

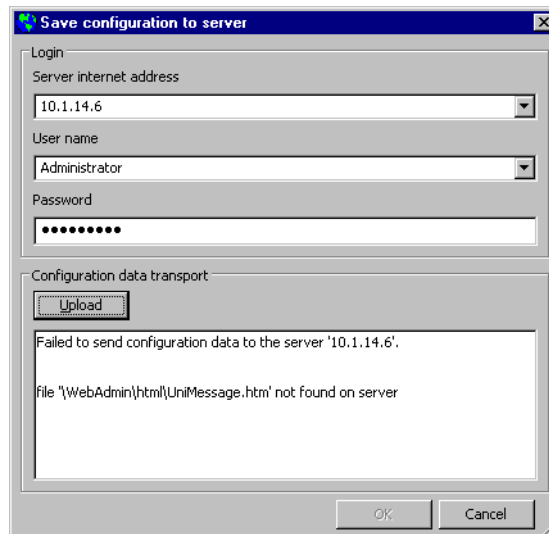
9. In the **Password** field enter the password for the specified XPR user again.



IMPORTANT:

Uploading a modified NCO configuration immediately activates it on the relevant XPR server. Incorrect settings may then immediately lead to **troubles** during XPR server operation.

10. Push the **Upload** button to transfer the modified configuration. If communication problems should occur, error reports in the log window point to the problem.



11. Close the storage dialog with the **OK** button.

9.5 Configuring the NCO Elements

NOTE:

The NCOAdmin accesses the NCO configuration files of the XPR server. Please make sure that the NCOAdmin used and the NCO configuration files are of the same version.

If this is not the case, an alarm message at the beginning of the Telematic configuration indicates this incompatibility.

NOTE:

If the NCOAdmin is started directly via its program file and not via the settings in a Telematic APL, all NCO tabs, except for the **Locations** tab, are locked by password query.

System administrators and service personnel can obtain their password to unlock the relevant tabs from the service partner in charge.

This section deals with the detailed configuration of the most important NCO elements. Among these elements are NCOs, locations, variables, number range lists, conditions and conversion rules.

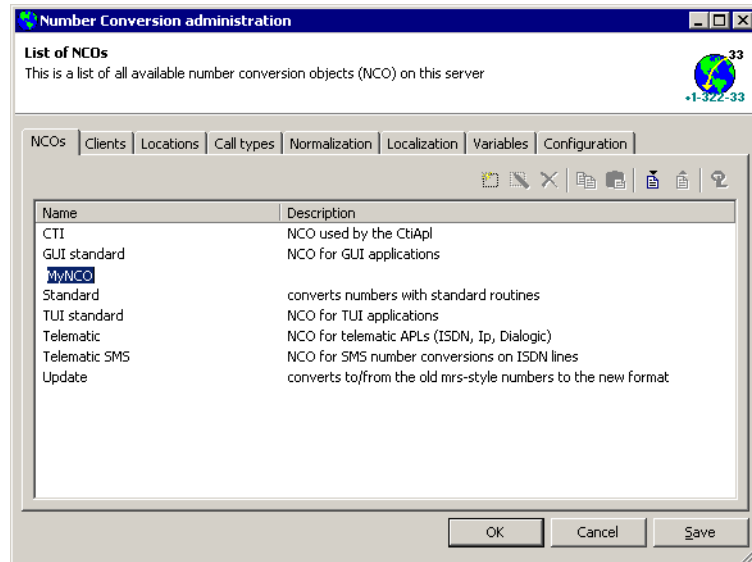
The information contained in this chapter is divided into the following sections:

- [Defining a new NCO](#)
- [Defining a new Location](#)
- [Defining a new Variable](#)
- [Defining a new Number Range List](#)
- [Defining a new Condition](#)
- [Defining a new Conversion Rule Set.](#)

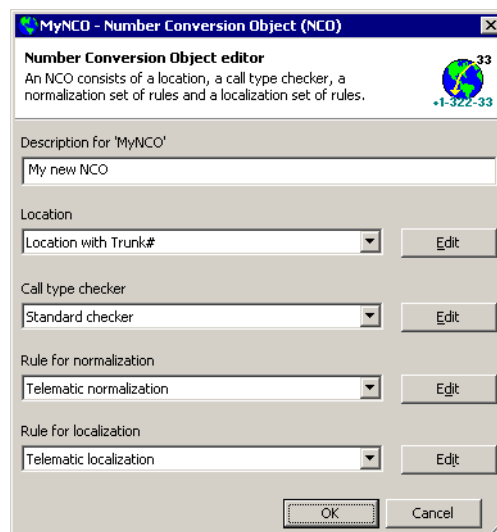
9.5.1 Defining a new NCO

How to define a new NCO.

1. Switch to the **NCOs** tab in the NCO Admin.
2. Click the **Add** icon in the toolbar.
3. Assign a descriptive name to the newly generated list entry in the **Name** column.



4. Select the new NCO with a **double click**.
5. Enter a short descriptive text for the new NCO in the **Description** field of the opened NCO editor.



6. Select the location to be used for the NCO in the **Location** field.

7. Select the call type checker to be used for the NCO in the **Call type checker** field.
8. Select the normalization rules to be used for the NCO in the **Rule for normalization** field.
9. Select the localization rules to be used for the NCO in the **Rule for localization** field.
10. Confirm your entries with the **OK** button.

9.5.2 Defining a new Location

IMPORTANT:

The phone number information for XPR users is stored in the Correlation Database of the XPR server in normalized format. The respective normalization always takes place on the basis of the corresponding location information. If location settings are modified in an existing XPR environment, the phone number information of existing users is **not** automatically updated in the Correlation Database.

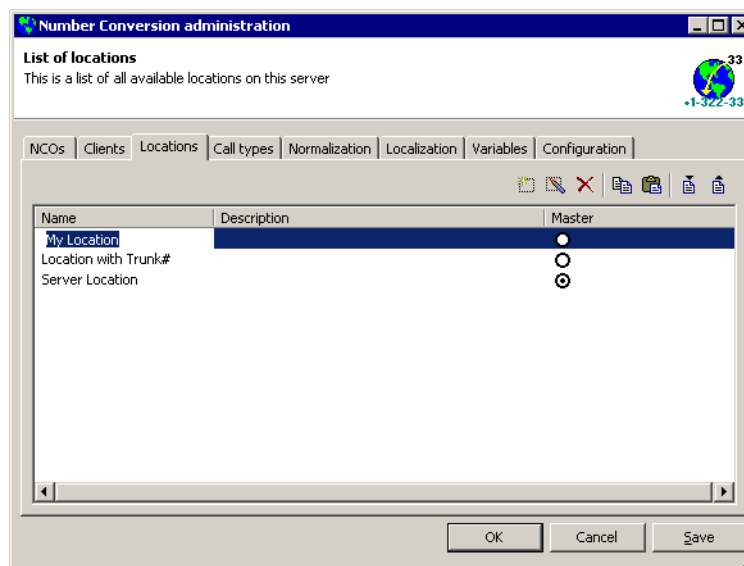
As a consequence, corresponding modifications of the user information must be performed manually. For this purpose, you can use the XPR tool *Number Conversion Prepare* with the following command prompt:

```
numberconversionprepare update nocn
```

Number Conversion Prepare **does not** adjust the **CIT** database field in the process.

How to define a new location.

1. Switch to the **Locations** tab in the NCO Admin.
2. Select the *Server Location* entry in the location list. This entry contains the most important local location information, which only needs to be adapted in most cases.
3. In the toolbar select **Copy** and **Paste**.
4. Assign a descriptive name to the newly generated list entry in the **Name** column.



5. Select the new location with a **double click**.
6. Enter a short descriptive text for the new location in the **Description** field of the opened location editor.

My Location - Location

Location editor
This is the configuration for one location

Description
My new Location

Code	Type
49	CountryCode (Country code)
2404	AreaCode (Area code)
901	SubscriberCode (Office code)

Prefix	Type
00	InternationalPrefix (International prefix)
0	NationalPrefix (National prefix)
0	ExternalPrefix (External prefix)

Variables

Name	Value
MaxExtensionLength	6

OK Cancel

7. Customize the location codes, prefixes and variables according to your requirements. Use the **Add**, **Remove** and **Change Value** icons for this purpose.
8. Confirm your entries with the **OK** button.

9.5.3 Defining a new Variable

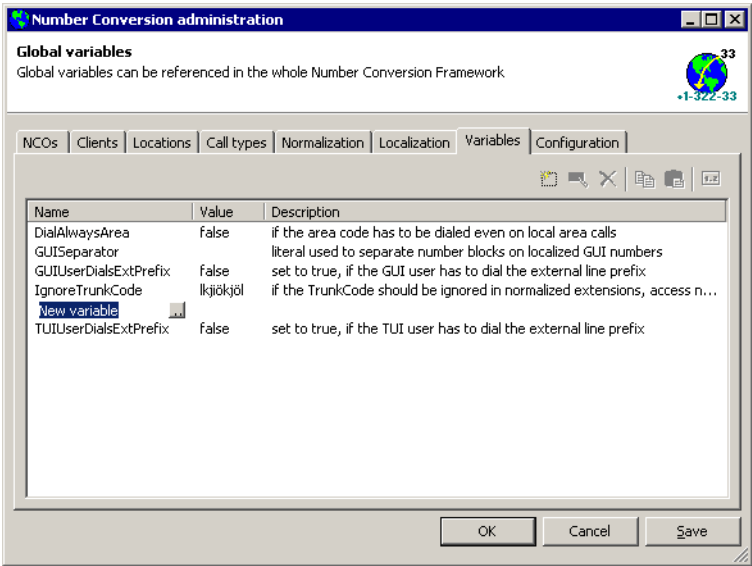
IMPORTANT:

NCO clients can default individual contents for NCO variables for phone number conversions. Such individual client defaults may temporarily override the content that is defined for the corresponding variable in the NCO configuration.

Variables can be modified at different locations of the NCOAdmin. For example, within a location, within a conversion rule or in the **Variables** tab.

How to define a new variable in one of these sectors.

- 1. Select the **Add** icon in the respective toolbar for variables.



- 2. Click the **Search** icon within the newly generated list entry at the end of the **Name** column.

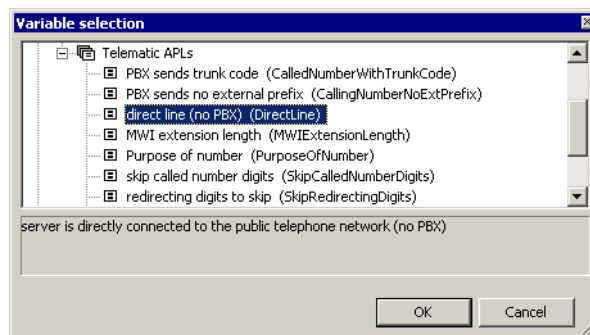
3. Select the desired variable in the open variable list with a **doubleclick**.

NOTE:

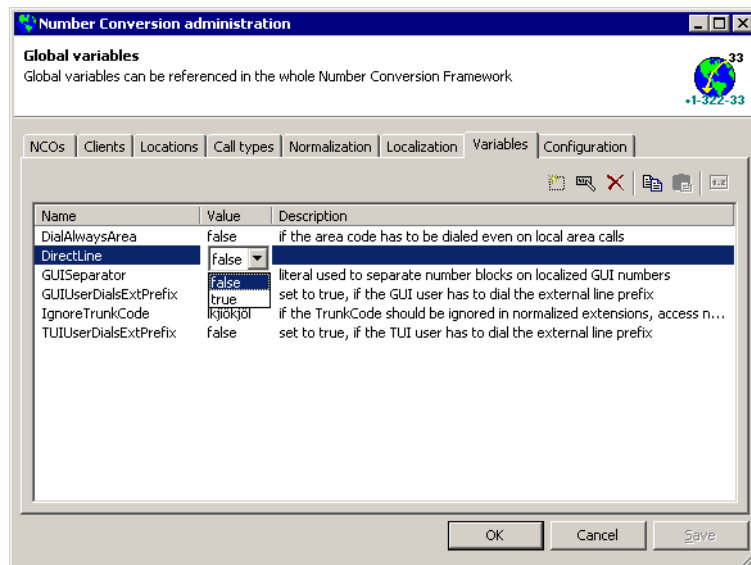
The use of a variable in the NCO configuration is not determined by the suggestion list folder in which the variable is contained.

Example:

The variable *AreaCode* is stored in the *Location* folder. That does **not** mean that it may exclusively be used on the **Locations** tab of the NCO settings. Instead, it can be used in any place of the NCO framework.



4. Subsequently, select the value of the new variable with a **doubleclick** for editing.



5. Confirm your entries with the **OK** button.

9.5.4 Defining a new Number Range List

Number range lists can be defined within a location or within a variable. See also [Section 9.3.12.6, “Definition of a Range List”, on page 380](#).

9.5.4.1 Defining a Number Range List within a Location

NOTE:

Entries in the **Country Code**, **Area Code** respectively **Subscriber Code** fields are only accepted if no corresponding entries are specified in the relevant location.

How to define a new number range list within a location.

1. Switch to the **Locations** tab in the NCO Admin.
2. Select the location you want to assign a number range with a **doubleclick**.
3. Click the **Add** icon in the toolbar of the location codes.
4. Select **RangeCode** in the dialog now open.
5. Enter the country code of the desired number range in the **CountryCode** field of the list editor.

6. Enter the area code of the desired number range in the **AreaCode** field of the list editor.
7. Specify the code of the desired extension in the **SubscriberCode** field.
8. Click the **Add** icon in the toolbar to define the number ranges of the number range list.

9. Define the desired number ranges of the number range list. This may require several list entries.

NOTE:

Each entry must contain either a single extension or a coherent number range of the format
<Extension 1> – <Extension2>.

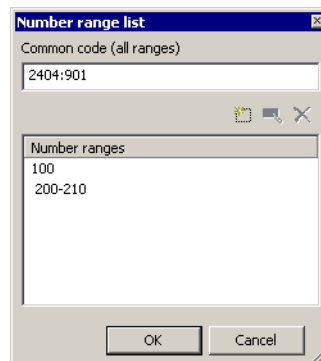
10. Confirm your entries with the **OK** button.
11. Close the location editor with the **OK** button.

9.5.4.2 Defining a Number Range List as Variable

To define a number range list as variable, the variable concerned must first be defined in general format. This can take place at different locations in the NCOAdmin. For example, within a location, within a conversion rule or in the **Variables** tab. After defining the variable, it can be edited as number range list.

How to convert a variable already defined into a number range list.

1. Select the desired variable with the **right mouse button**.
2. Select **Edit as number range** in the dialog now open.
3. If desired, specify the country code, area code and subscriber code of the desired number range in the **Common code** field of the list editor. In doing so, use the notation *<country code>:<area code>:<subscriber code>*.



4. Click the **Add** icon in the toolbar to define the number ranges of the number range list.
5. Define the desired number ranges of the number range list. This may require several list entries.

NOTE:

Each entry must contain either a single extension or a coherent number range of the format

<Extension 1> – <Extension2>.

6. Confirm your entries with the **OK** button.
7. Close the location editor with the **OK** button.

9.5.5 Defining a new Condition

Conditions can be defined in a call type checker as well as in single conversion rules.

How to define a new condition in one of these sectors.

1. Click the **Add** icon in the conditions toolbar.
2. In the now open menu select the condition type that you want to define.
3. Configure the individual settings of the selected condition. See [Section 9.9.11, “NCO Conditions”, on page 468](#).
4. Confirm your entries with the **OK** button.

9.5.6 Defining a new Conversion Rule Set

Rule sets for phone number conversion can be defined in the **Normalization** and **Localization** tabs of the NCOAdmin.

How to define a new rule set in the tab concerned.

1. In the list displayed select a rule set that features a behavior similar to the rule set to be newly defined.
2. In the toolbar select **Copy** and **Paste**. In the ideal case you then only need to perform individual modifications to the rule set previously selected.
3. Assign a descriptive name to the newly generated list entry in the **Name** column.
4. Select the new rule set with a **doubleclick**.
5. Perform the desired modifications to the existing rules. See [Section 9.9.12, "NCO Rules", on page 478](#).
6. Confirm your entries with the **OK** button.

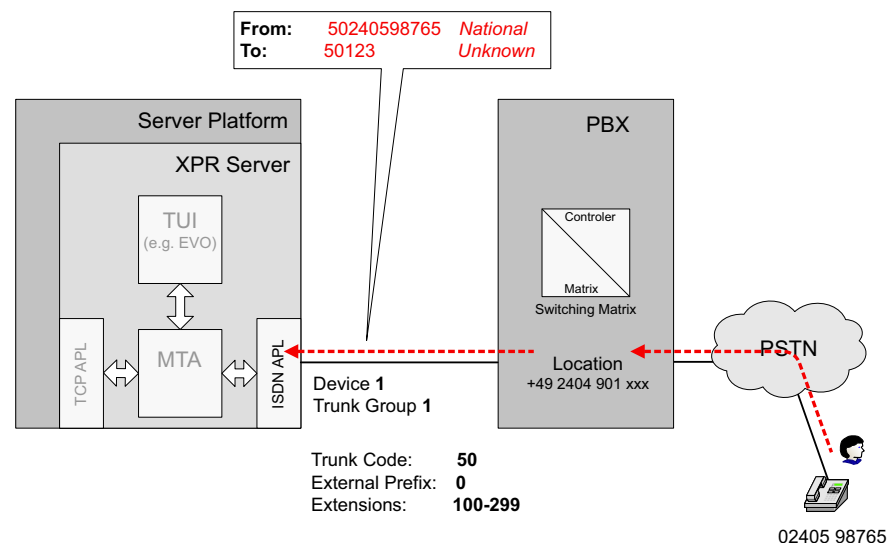
9.6 Configuration Example of Number Conversion Objects (NCO)

After having become familiar with the general NCO coherences we can now deal with the configuration of NCO elements. For this purpose we will have a look at a configuration example.

This example describes the NCO configuration of a common XPR installation. Since the XPR server is already fitted with comprehensive NCO presets, the administrator need not perform a number of configurations here any more. Instead he/she can use preconfigured NCO elements to shorten and facilitate the configuration.

9.6.1 Example Scenario

We take a look at the following figure of a PBX connected to the XPR server ISDN APL.



For the connection some information is defaulted by the PBX used.

- The PBX can be reached under the phone number 0049 2404 901 xxx.
- The PBX awaits a '0' dialed for an outside line.
- The XPR server is connected to the PBX via a trunk code with number 50.
- The PBX does not transfer a trunk code number with phone numbers.
- The XPR users have the extensions 100 to 299 at the PBX.

Beyond that we assume that the XPR server is connected to the PBX via the trunk group 1 of an ISDN APL. The ISDN APL has in the XPR server the device number 1.

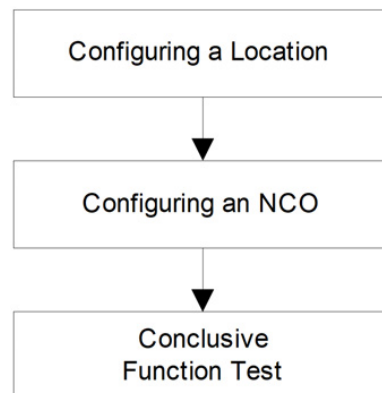
9.6.2 Example Configuration

NOTE:

If the NCOAdmin is started directly via its program file and not via the settings in a Telematic APL, all NCO tabs, except for the **Locations** tab, are locked by password query.

System administrators and service personnel can obtain their password to unlock the relevant tabs from the service partner in charge.

With this scenario information we can already start with the NCO configuration. For this procedure we turn to the next figure. It describes the sequence in which the single configuration steps will be dealt with.



Let us begin with configuring the location we need for our example scenario. Start the NCOAdmin and proceed as follows:

IMPORTANT:

NCO differentiates between upper and lower case with all definitions.

Location configuration

IMPORTANT:

The phone number information for XPR users is stored in the Correlation Database of the XPR server in normalized format. The respective normalization always takes place on the basis of the corresponding location information. If location settings are modified in an existing XPR environment, the phone number information of existing users is **not** automatically updated in the Correlation Database.

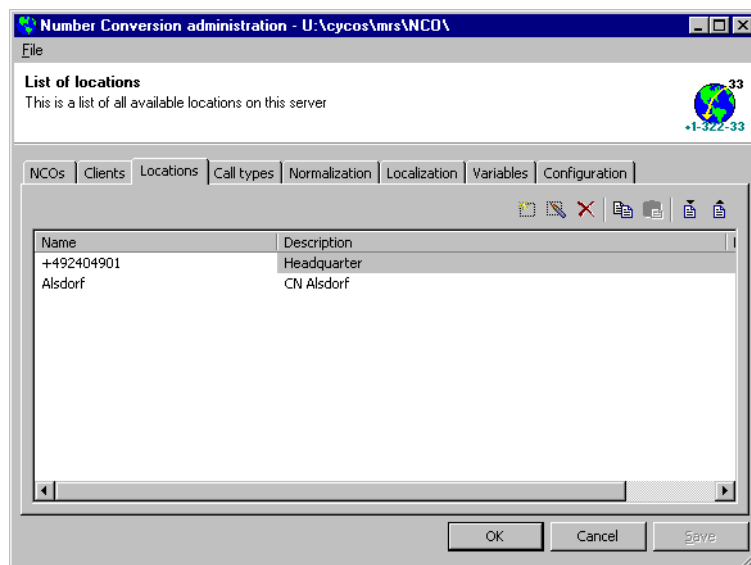
As a consequence, corresponding modifications of the user information must be performed manually. For this purpose, you can use the XPR tool *Number Conversion Prepare* with the following command prompt:

```
numberconversionprepare update nocn
```

Number Conversion Prepare **does not** adjust the **CIT** database field in the process.

An NCO location is generated from the location settings of the XPR server during the installation of the XPR server. We will shortly check this location's settings as the configuration should be complete and correct.

1. Switch to the **Locations** tab in the NCOAdmin.
2. Select the location already automatically generated with a **doubleclick**. This location carries as name the normalized phone number of the XPR servers – in our example **+492404901**.



3. Enter a short descriptive text in the **Description** field.

+492404901 - Location

Location editor
This is the configuration for one location

Description
Headquarter

Location codes

Code	Type
49	CountryCode (Country code)
2404	AreaCode (Area code)
901	SubscriberCode (Office code)
50	TrunkCode (TrunkCode)

Location prefixes

Prefix	Type
00	InternationalPrefix (International prefix)
0	NationalPrefix (National prefix)
0	ExternalPrefix (External prefix)

Variables

Name	Value
MaxExtensionLength	3

OK Cancel

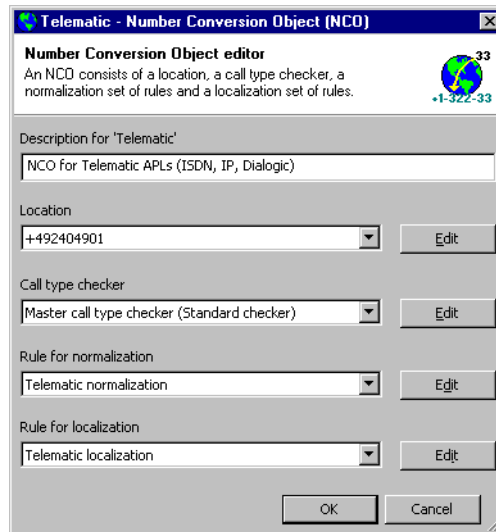
4. Check the location codes and prefixes.
In particular take care of the following settings and adapt them if required:
 - TrunkCode = 50
 - ExternalPrefix = 0
5. Select the *MaxExtensionLength* variable and assign it value **3** if required. The extensions in our example consist of three digits each.
6. Copy all location settings with **OK**.

After accomplishing the location configuration, we continue with configuring the NCO.

NCO configuration

We check the settings of the *Telematic* NCO which have already been preconfigured with the ISDN APL installation.

1. Switch to the **NCOs** tab of the NCOAdmin.
2. Select the **Telematic** entry from the list of all NCOs already configured with a **doubleclick**.

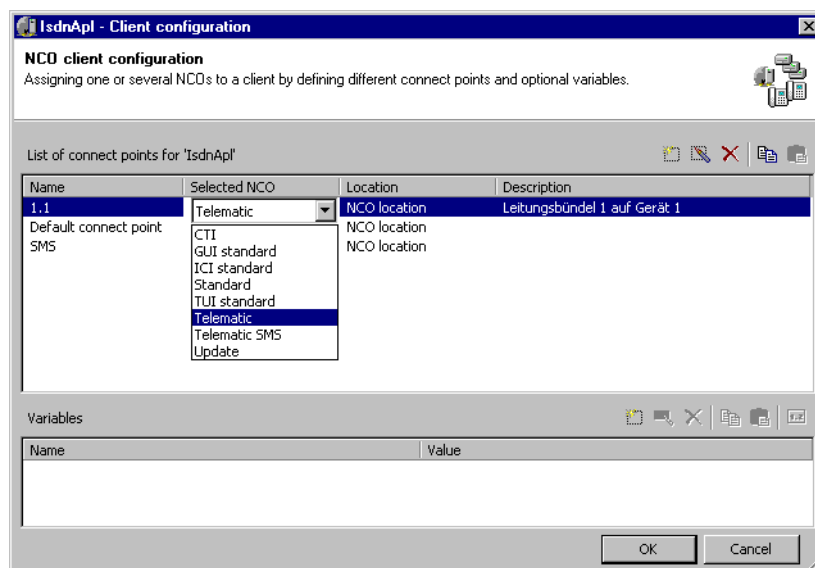


3. Make sure that
 - under *Location* the location just configured is selected.
 - under *Call type checker* the **Standard checker** is selected.
 - under *Rule for normalization* the **Telematic normalization** is selected.
 - under *Rule for localization* the **Telematic localization** is selected.
4. Copy the NCO settings with **OK**.

The required NCO is thus correctly configured. Next comes the NCO client configuration.

NCO client configuration

1. Switch to the **Clients** tab of the NCOAdmin for the NCO client configuration.
2. Select the **IsdnApl** entry from the list with a **doubleclick**.
3. From the *List of Connect Points* select the entry **1.1**. This entry is in the ISDN APL assigned to the trunk group that realizes the communication with the PBX.



4. Make sure that **Telematic** is assigned to this connect point as *Selected NCO*. Furthermore, the **NCO location** entry must be selected under Location.
5. Then copy the NCO client settings with **OK**.

IMPORTANT:

As soon as you save an NCO configuration, it will become active on the relevant XPR server within the next 60 seconds. Faulty settings may **trouble** the XPR server operation.

6. To activate all performed configurations on the XPR server, push the **Save** button.
7. Confirm the storage query by clicking the **OK** button.

The configuration of our example scenario is thus accomplished. Finally we check our configuration with some short system tests.

Function test of an internal phone number of type *Called Party*

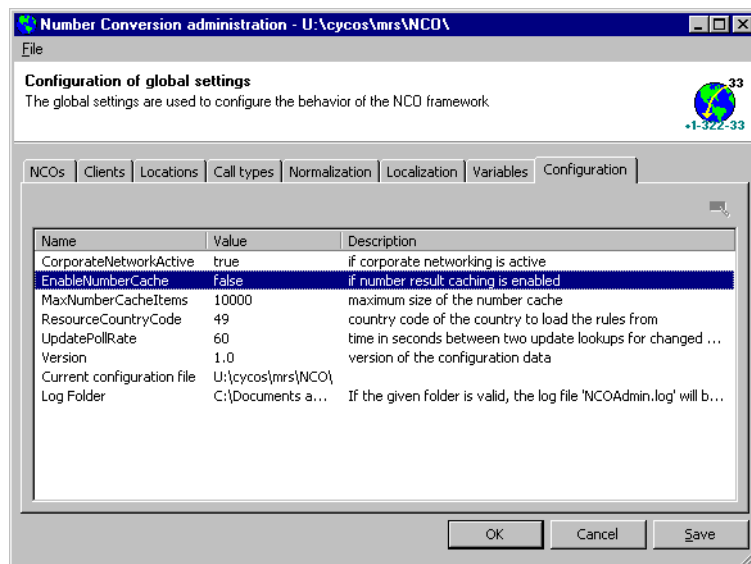
The PBX transfers a call for the extension *100* to the XPR server. This could be e.g. the access number for a voice mail script.

We simulate this scenario in the NCO tester.

1. Switch to the **Configuration** tab of the NCOAdmin.
2. Set the *false* value for the **EnableNumberCache** parameter.

IMPORTANT:

If you execute the NCO tester with activated phone number cache, phone numbers once tested are stored with their respective conversion result. If the you then change the configuration and test a previously tested phone number again, the changed configuration will not take effect. The previously stored conversion result is put out instead.



3. Switch to the **NCOs** tab in the NCOAdmin.
4. Mark in the list the *Telematic* NCO and select the **Test** icon from the toolbar.

Number Conversion Object (NCO)

5. In the *Optional variables* portion click the **Add** icon in the toolbar.

The screenshot shows the 'Telematic - Tester' application window. The title bar is blue with the text 'Telematic - Tester'. Below the title bar, there is a section titled 'Test a Number Conversion object' with a lightbulb icon. The text below this title reads: 'Enter a number in the 'Localized Number' field and press 'Normalize' to execute the normalization process or enter a number in the 'Normalized Number' field and press 'Localize' to see the results of the localization.'

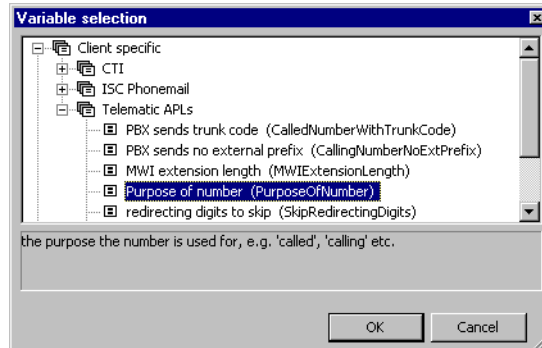
The main area of the window is divided into several sections:

- Conversion:** This section contains three input fields: 'Localized number', 'Normalized number', and 'Resulting call type'. Below these fields are two buttons: 'Normalize' and 'Localize'.
- Location:** This section contains a dropdown menu labeled 'NCO location'.
- Optional variables:** This section contains a table with two columns: 'Name' and 'Value'. The 'Name' column has a value 'New variable' and a small selector icon at the end of the field.
- Output variables:** This section contains a table with two columns: 'Name' and 'Value'.
- Logging:** This section contains a large empty text area.

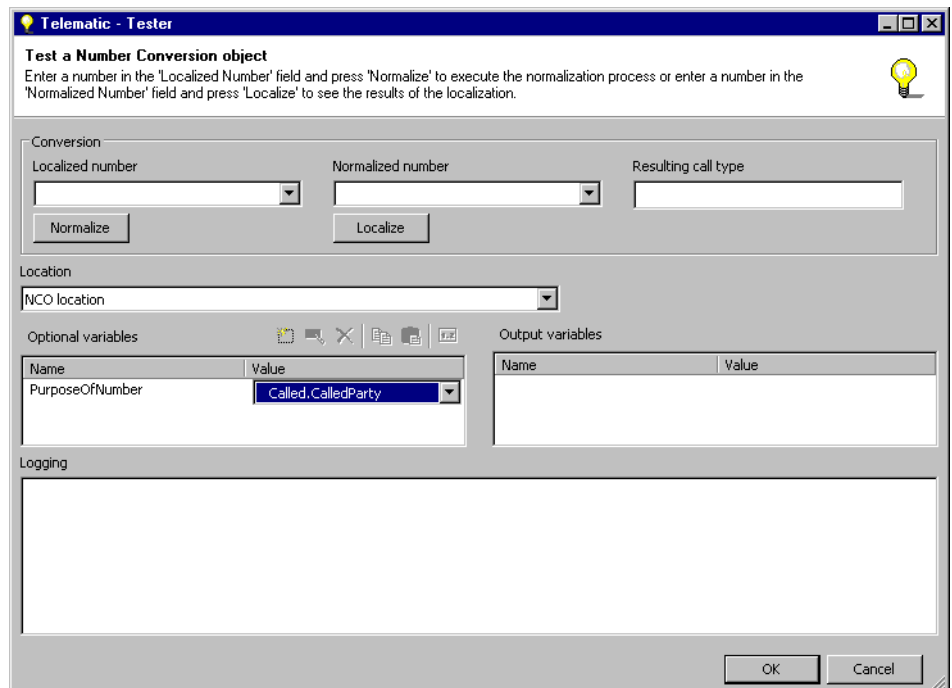
At the bottom right of the window are 'OK' and 'Cancel' buttons.

6. Enable the selector icon at the end of the **Name** field.

7. In the variable selection switch to **Client specific > Telematic APLs** and select the *PurposeOfNumber* variable with a **doubleclick**.



8. Confirm your selection with the **Enter** key.
9. Select the **Value** of our newly added variable.
10. Click the **Change Value** icon in the toolbar of the *Optional variables* portion.



11. Via the selection menu assign the *PurposeOfNumber* variable the **Called.CalledParty** value. This simulates a PBX as *Purpose of Number* transferring the *Called.CalledParty* value.

12. In the **Localized number** field enter the phone number *100* and push the **Normalize** button.

Telematic - Tester

Test a Number Conversion object
 Enter a number in the 'Localized Number' field and press 'Normalize' to execute the normalization process or enter a number in the 'Normalized Number' field and press 'Localize' to see the results of the localization.

Conversion

Localized number: Normalized number: Resulting call type:

Location
 NCO location:

Optional variables

Name	Value
PurposeOfNumber	Called.CalledParty

Output variables

Name	Value

Logging

```

Start testing NCO: 'Telematic'
Number to convert: '100'
Client: ''
Direction: 'InString'
Input variables: 'PurposeOfNumber=Called.CalledParty'
Normalizing number: 100
Input variables: PurposeOfNumber=Called.CalledParty
Rule Telematic normalization: 'a normalize rule for telematic APL use'
  
```


13. The tester states the phone number **+49240490150100** as result in the **Normalized number** field. The **Resulting call type** is *Internal*.

Correct, since we have configured value 3 as maximum internal phone number length.

The trunk code is inserted in the normalized phone number.

14. Then click the **Localize** button. The phone number *100* is displayed in the **Localized number** field as result.

Correct as well.

The XPR server would transfer this phone number to the PBX to address a telephone terminal device with extension *100* connected there.

15. In the logging portion of the tester dialog you can finally track the conditions and rules applied during the conversion process.

Test of an internal phone number of type *Calling Party*

The PBX transfers a call with the internal originator number *100* to the XPR server.

We simulate this scenario in the NCO tester.

16. Change the *PurposeOfNumber* variable to value **Calling.CallingParty**.

17. In the **Localized number** field enter the phone number *100* again and push the **Normalize** button.

Telematic - Tester

Test a Number Conversion object
Enter a number in the 'Localized Number' field and press 'Normalize' to execute the normalization process or enter a number in the 'Normalized Number' field and press 'Localize' to see the results of the localization.

Conversion

Localized number 100	Normalized number +492404901100	Resulting call type Internal

Buttons: **Normalize** **Localize**

Location
NCO location

Optional variables

Name	Value
PurposeOfNumber	Calling.CallingParty

Output variables

Name	Value

Logging

```

Start testing NCO: 'Telematic'
Number to convert: '100'
Client: ''
Direction: 'InString'
Input variables: 'PurposeOfNumber=Calling.CallingParty'
Normalizing number: 100
Input variables: PurposeOfNumber=Calling.CallingParty
Rule Telematic normalization: 'a normalize rule for telematic APL use'
  
```

Buttons: **OK** **Cancel**

18. The tester states the phone number **+492404901100** as result in the **Normalized number** field. The **Resulting call type** is **Internal**.

Correct again.

In this case the trunk code is not inserted in the normalized format since the subscriber with number *100* can be directly reached at the PBX and not behind the trunk code with number *50*.

19. Click the **Localize** button. The result is phone number *100* again.

Correct.

The XPR server would transfer this phone number to the PBX to address the XPR-internal extension *100*.

20. In the logging portion of the tester dialog you can once again track the conditions and rules applied during the conversion process.

Test of a local phone number of type Calling Party

The PBX transfers a call with the local originator number 232425 to the XPR server.

We simulate this scenario in the NCO tester as well.

21. Keep the value **Calling.CallingParty** of the *PurposeOfNumber* variable.
22. In the **Localized number** field enter the phone number 0232425 and push the **Normalize** button.

NOTE:

The figure shows the variable *CallingNumberNoExtPrefix* with value *false*. This setting is default under NCO. We have added it in our test as variable for illustration purposes only.

Since the XPR server expects the inserted external prefix of the PBX for an external calling number, we need to state it in the case of the localized phone number as well.

The screenshot shows the 'Telematic - Tester' application window. The title bar is blue with a yellow lightbulb icon. The main window has a white background. At the top, there's a section titled 'Test a Number Conversion object' with a lightbulb icon. Below this, there's a text box with instructions: 'Enter a number in the 'Localized Number' field and press 'Normalize' to execute the normalization process or enter a number in the 'Normalized Number' field and press 'Localize' to see the results of the localization.' Below the instructions, there's a 'Conversion' section with three fields: 'Localized number' (containing '0232425'), 'Normalized number' (containing '+492404232425'), and 'Resulting call type' (containing 'Area'). There are 'Normalize' and 'Localize' buttons below these fields. Below the 'Conversion' section, there's a 'Location' section with a dropdown menu showing 'NCO location'. Below the 'Location' section, there's a section for 'Optional variables' and 'Output variables'. The 'Optional variables' section has a table with two columns: 'Name' and 'Value'. It contains one row: 'PurposeOfNumber' with value 'Calling.CallingParty'. The 'Output variables' section has an empty table with the same columns. Below the 'Optional variables' and 'Output variables' sections, there's a 'Logging' section with a text area showing the following log entries: 'Start testing NCO: 'Telematic'', 'Number to convert: '0232425'', 'Client: ', 'Direction: 'InString'', 'Input variables: 'PurposeOfNumber=Calling.CallingParty'', 'Normalizing number: 0232425', 'Input variables: PurposeOfNumber=Calling.CallingParty', and 'Rule Telematic normalization: 'a normalize rule for telematic APL use''. At the bottom right of the window, there are 'OK' and 'Cancel' buttons.

Name	Value
PurposeOfNumber	Calling.CallingParty

Name	Value

```
Start testing NCO: 'Telematic'
Number to convert: '0232425'
Client: 
Direction: 'InString'
Input variables: 'PurposeOfNumber=Calling.CallingParty'
Normalizing number: 0232425
Input variables: PurposeOfNumber=Calling.CallingParty
Rule Telematic normalization: 'a normalize rule for telematic APL use'
```

23. The tester displays the phone number **+49240450232425** as result in the **Normalized number** field. The **Resulting call type** is *Area*.

Correct again!

24. Click the **Localize** button. The phone number *050232425* remains displayed in the **Localized number** field as result.

Correct!

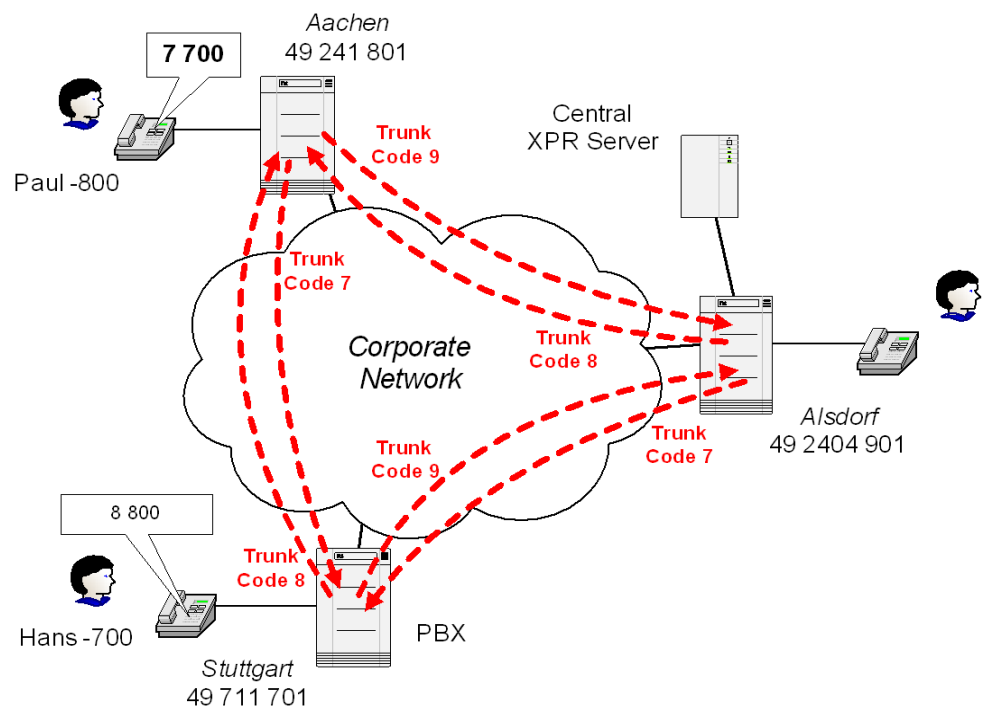
Now you can normalize or localize further phone numbers to familiarize yourself with the tester and the conversion rules.

9.7 NCO in a Corporate Network Environment

This section describes the NCO *Corporate Network* functionality and under which circumstances it is used. Furthermore, a *Corporate Network* configuration example is provided.

9.7.1 Corporate Network

The term *Corporate Network* describes an environment in which various locations share a central XPR server. The following example scenario will illustrate this.



We see a corporate network with three PBXs linked via cross connections. The trunk codes are to be used for abbreviated dialing among the single subscribers.

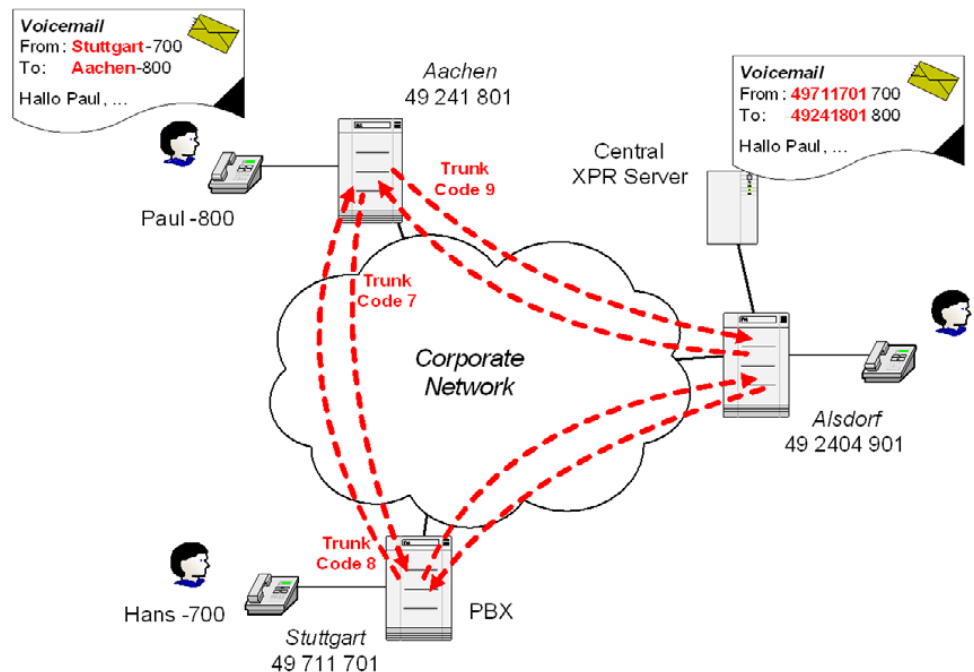
Example:

If Hans wants to call Paul, he dials in Stuttgart the trunk code for Aachen followed by Paul's extension – thus 8800. Paul sees in this case the caller's number 7700 on his telephone display. This is the number under which Hans can be reached from Aachen.

All three locations use the central XPR server in Alsdorf. This server is to map the format of the above 'cross-connection code' with the output – thus localization – of phone numbers. The advantage of this behavior is that e.g. automatic return calls are automatically handled via the corporate network. Beyond that, this phone number format corresponds to what the user is familiar with when dialing.

This behavior of phone number normalization, though, cannot be achieved with the NCO mechanisms described so far.

In the following example Hans sends a voice mail to Paul directly via the XPR server.



The XPR server stores this message internally with the normalized phone numbers for originator and recipient. As soon as Paul retrieves his message from the XPR server, the associating phone numbers are localized. Since the localization algorithm does not have any information about the structure of the cross connections, such information is not available for the localization either.

At this stage we get to the Corporate Network configuration. With the definition of the various Corporate Network locations the XPR server receives their location information and the associating trunk codes. NCO can then use this information in the course of phone number localization.

9.7.2 Corporate Network Rules

For a *Corporate Network* environment function, different corporate network rules are predefined in NCO. They are part of each set of normalization or localization rules and comprise a preprocessing and a conversion rule each.

9.7.2.1 Corporate Network Preprocessing Rule

The Corporate Network preprocessing rule is listed in the preprocessing rule area. It cannot be displayed or edited in detail, but only moved to another position within the rule list. Once it has been inadvertently deleted, it can be added to the respective rule area as **Corporate Network preprocessing rule** again.

The Corporate Network preprocessing rule is merely in charge of defining the content of three NCO variables, which are later used in the conversion rule to be performed.

These variables are:

- CNConversion
- CNDestPublicID
- CNOrgToDestPrefix

The following three sections inform about the contents of these variables.

The **CNConversion** variable

This variable is set to *true*, if the Corporate Network preprocessing rule recognizes a communication request between two Corporate Network locations. *CNConversion* is used to define conditions for the conversion rule to follow later.

The **CNDestPublicID** variable

The public ID of a Corporate Network location defines the portion of a normalized phone number that uniquely defines the relevant PBX location in the international phone number hierarchy. The representation of a normalized phone number is thus:

<public ID><extension possibly incl. trunk code>

Example:

The normalized phone number `+492404901100` is divided into

- the public ID `+492404901` and
- the extension `100`.

The variable `CNDestPublicID` contains the public ID of the relevant Corporate Network destination location. On the basis of this information the conversion rule can later separate the extension from the normalized phone number in simple form.

The `CNOrgToDestPrefix` variable

The preprocessing rule allocates this variable with the trunk code that connects the originator to the destination location in the desired communication direction. The conversion rule uses this information for generating the localized phone number later on.

9.7.2.2 Corporate Network Conversion Rule

The conversion rule performs the actual conversion of the transferred phone number. It uses the variable predefined in the preprocessing rule.

In its predefined format it meets the requirements of most Corporate Network default configurations. Once it has been inadvertently deleted, it can be added to the respective rule area as **Corporate Network rule** again.

9.7.3 Example of a Corporate Network Configuration

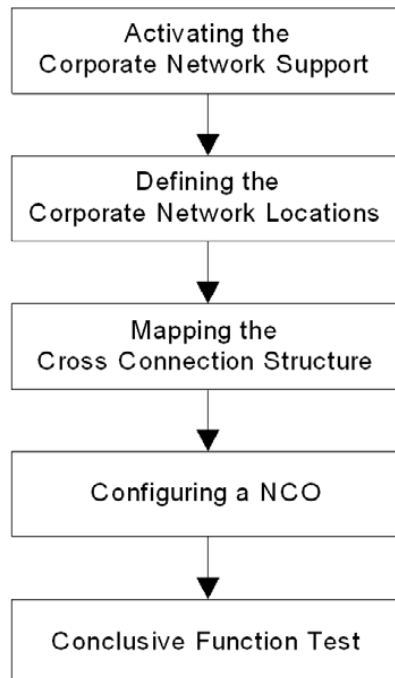
NOTE:

If the NCOAdmin is started directly via its program file and not via the settings in a Telematic APL, all NCO tabs, except for the **Locations** tab, are locked by password query.

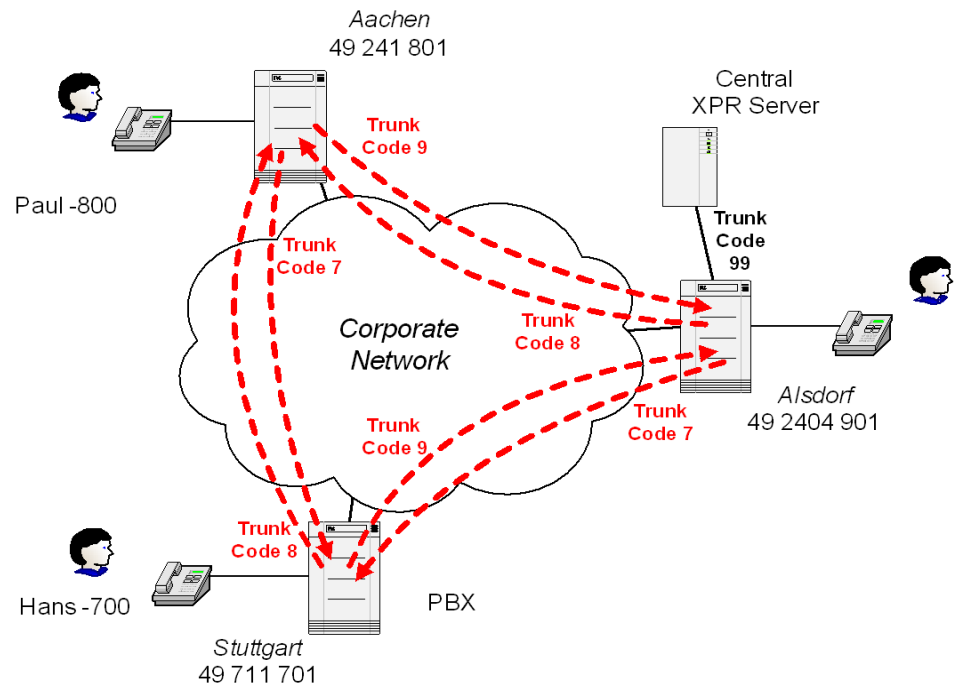
System administrators and service personnel can obtain their password to unlock the relevant tabs from the service partner in charge.

After becoming familiar with the *Corporate Network* function we will now perform an example configuration. We use the previously shown corporate network with the three locations Aachen, Alsdorf and Stuttgart.

Before we start with the configuration, we need to know the required configuration sections:



And here we go ...

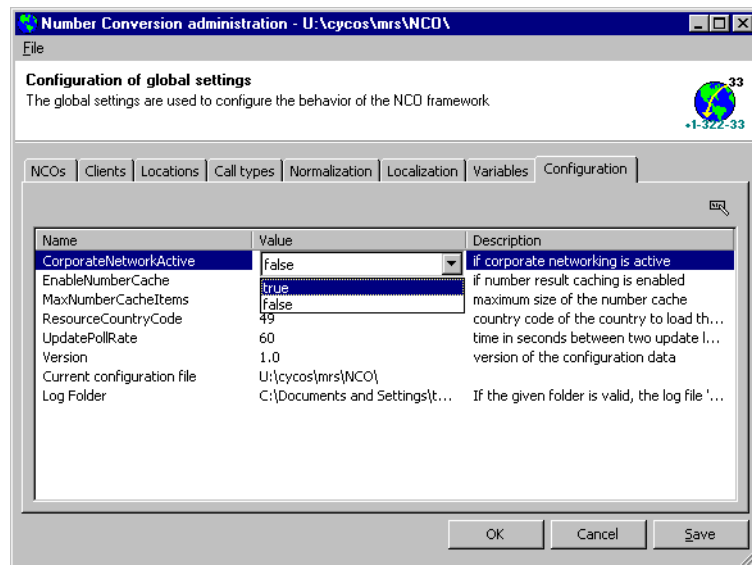


This scenario will now be configured in NCO. Let's start with activating Corporate Network. Start the NCOAdmin and proceed as follows.

Activating the Corporate Network support

Before we can start configuring Corporate Network, it must be activated in the NCOAdmin. What to do:

1. Switch to the **Configuration** tab in the NCO Admin.



2. If necessary, set the value of the variable *CorporateNetworkActive* from *false* to *true*.

NOTE:

This option is automatically activated as soon as the XPR server recognizes the license for the *Long Distance Networking* feature.

3. Confirm this modification with the **Save** button.

Corporate Network is thus active and the dialog elements required for the configuration are displayed in the various dialogs. We can now continue the configuration with defining the Corporate Network locations.

Defining the Corporate Network locations

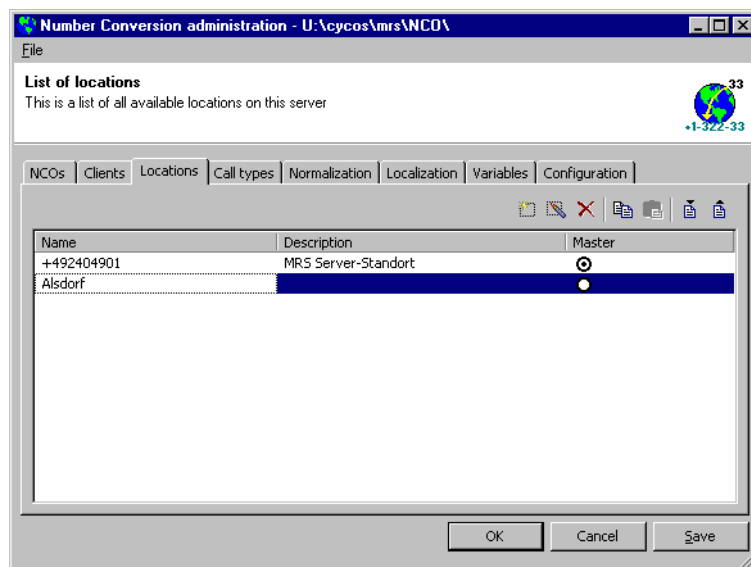
In the second step of the Corporate Network configuration the single Corporate Network locations are defined in NCO. Proceed as follows:

4. Switch to the **Locations** tab in the NCO Admin.

NOTE:

If you want to use an already defined location as Corporate Network location, continue with step 7.

5. Select the **Add** icon in the toolbar to add a new Corporate Network location to the NCO configuration.



6. Enter a unique location name in the **Name** field. In our example we choose the name *Alsdorf*.
7. Select the new Corporate Network location with a **doubleclick**.

8. In the **Description** field of the opening *Location editor* enter a short text for this location.

Alsdorf - Location

Location editor
This is the configuration for one location

Description
CN Alsdorf

Code	Type
49	CountryCode (Country code)
2404	AreaCode (Area code)
901	SubscriberCode (Office code)
99	TrunkCode (Extension code)

Prefix	Type
00	InternationalPrefix (International prefix)
0	NationalPrefix (National prefix)
0	ExternalPrefix (External prefix)

Variables

Name	Value
MaxExtensionLength	4

Corporate network
☒ Corporate Network location

Properties

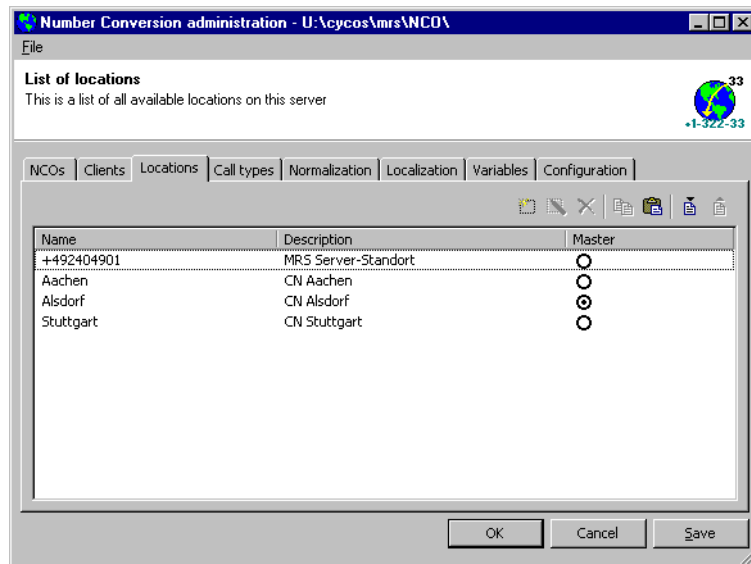
OK Cancel

9. Via the **Add** icon define the following values for the corresponding codes and prefixes.

Code / Prefix	Stuttgart	Aachen	Alsdorf	
Country Code	49	49	49	
Area Code	711	241	2404	
Subscriber Code	701	801	901	
Trunk Code	–	–	99	Central XPR server in Alsdorf
International Prefix	00	00	00	

10. Activate the **Corporate Network location** option in the *Corporate network* section.
11. Confirm the prompt for this location entry at all other Corporate Network locations with **Yes**.
12. Confirm your modifications with the **OK** button.

13. Define the two other Corporate Network locations *Aachen* and *Stuttgart* as described in steps 5 to 12.

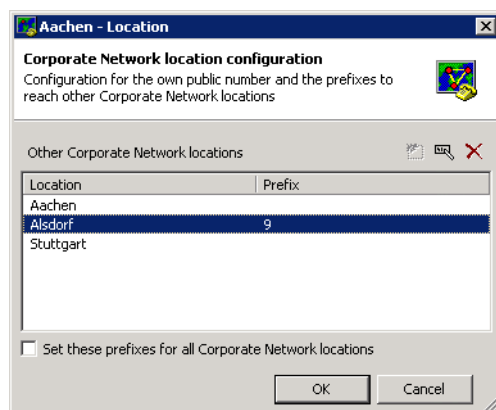


The Corporate Network location configuration in our example is thus successfully accomplished. Next comes the definition of the cross connection that links the PBXs of our three locations.

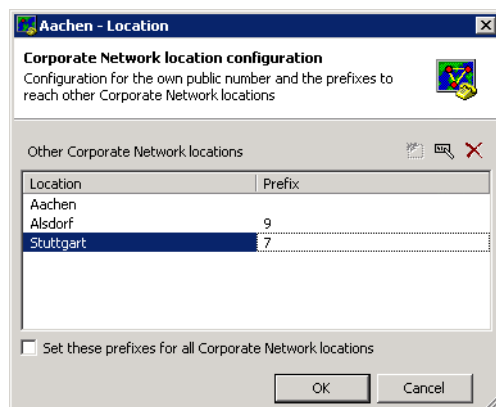
Mapping the cross connection structure

We will now map the cross connection structure in NCO. This is done in the following way.

14. Select one of the new Corporate Network locations with a **doubleclick**. We select location *Aachen*.
15. Push the **Properties** button in the then opening **Location Editor**.
16. From the list now displayed select the first Corporate Network location with a **doubleclick**. This is in our case location *Alsdorf*.



17. Enter under **Prefix** the trunk code 9. This is the number of the cross connection that leads from *Aachen* to *Alsdorf*.
18. From the Corporate Network location list select the next location with a **doubleclick**. This is in our case location *Stuttgart*.

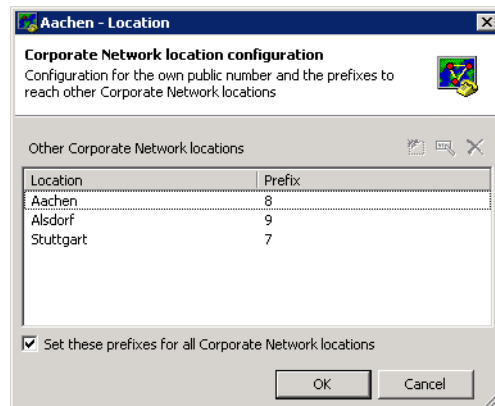


19. Enter under **Prefix** the corresponding trunk code 8 for this location.

NOTE:

You can configure the trunks **centrally** in one location, e. g. *Aachen*, if the trunks of the locations are identical. Enter the prefixes of all trunks and

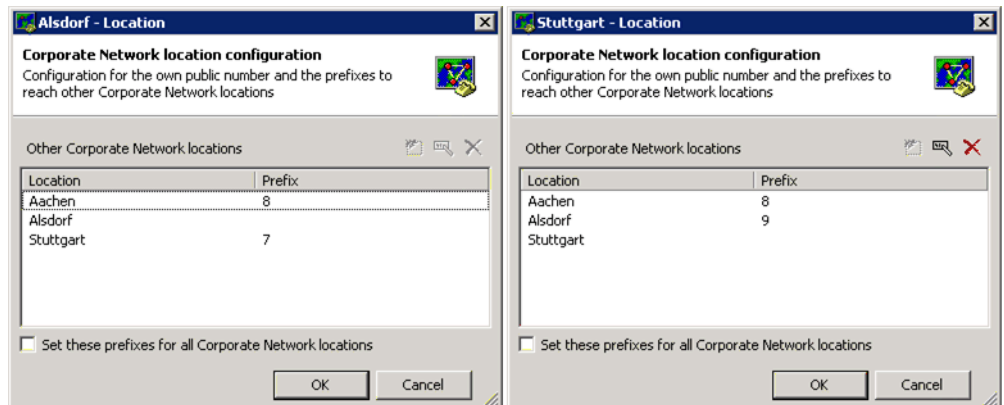
activate the *Set these Prefixes for all Corporate Network locations* checkbox.



In this case, skip step 21.

20. Confirm your settings with the **OK** button and close the location properties dialog in the same way.

21. Repeat steps 15 to 21 for the two other locations *Alsdorf* and *Stuttgart*.



IMPORTANT:

As soon as you save an NCO configuration, it will become active on the relevant XPR server within the next 60 seconds. Faulty settings may **trouble** the XPR server operation.

22. To activate all performed configurations on the XPR server, push the **Save** button.

23. Confirm the storage query by clicking the **OK** button.

All cross connections for our corporate network are thus configured. Up comes a short system test of our Corporate Network configuration.

Function test

Our example configuration will now be tested.

24. Switch to the **NCOs** tab of the NCOAdmin.

25. Mark in the list the *Telematic* NCO and select the **Test** icon from the toolbar.

26. In the **Location** field select the previously defined location *Alsdorf*.

Telematic - Tester

Test a Number Conversion object

Enter a number in the 'Localized Number' field and press 'Normalize' to execute the normalization process or enter a number in the 'Normalized Number' field and press 'Localize' to see the results of the localization.

Conversion

Localized number: 7100 Normalized number: +49711701100 Resulting call type: Internal

Normalize Localize

Location

Alsdorf

Optional variables

Name	Value

Output variables

Name	Value
AddExternalPrefix	false

Logging

```
Start testing NCO: 'Telematic'
Number to convert: '+49711701100'
Client: 
Direction: 'OutString'
Input variables: 'Location=Alsdorf'
Localizing number: +49711701100
Using given location 'Alsdorf' instead of NCO location
Input variables: Location=Alsdorf
Rule Telematic localization: 'Rule for Telematic-Apl use'
```

OK Cancel

27. In the **Normalized number** test dialog field enter **+49711701100** for a message originator in *Stuttgart*. Then click the **Localize** button.

28. The **Localized number** field displays the result **7100**. This is correct, because NCO localizes the entered originator number using the information of location *Alsdorf*. And the cross connection from *Alsdorf* to *Stuttgart* is 7.

29. In the **Location** field select location *Aachen*.

Telematic - Tester

Test a Number Conversion object
 Enter a number in the 'Localized Number' field and press 'Normalize' to execute the normalization process or enter a number in the 'Normalized Number' field and press 'Localize' to see the results of the localization.

Conversion

Localized number: Normalized number: Resulting call type:

Location

Optional variables

Name	Value

Output variables

Name	Value
AddExternalPrefix	false

Logging

```

Start testing NCO: 'Telematic'
Number to convert: '+49711701100'
Client: ''
Direction: 'OutString'
Input variables: 'Location=Aachen'
Localizing number: '+49711701100'
Using given location 'Aachen' instead of NCO location
Input variables: Location=Aachen
Rule Telematic localization: 'Rule for Telematic-Apl use'
  
```


30. Under the same phone number +49700701100 push the **Localize** button again.

31. The **Localized number** field displays the result **7100**. This is correct, too, since the localization now takes place with the information of the location *Alsdorf* and since the tie trunk number from *Aachen* to *Stuttgart* is 7 also.

Our configuration works correctly. You can now check other localizations to familiarize yourself with the Corporate Network configuration.

9.8 The *Number Conversion Prepare* Tool

The XPR tool Number Conversion Prepare is required in productive operation to convert the phone numbers in the Correl database and in journal entries according to the current NCO settings.

This is necessary if

- an XPR server of a version before NCO is migrated to a version with NCO
- NCO settings are modified that change the phone number normalization – for example the originator address of an NCO location.

Beyond that, the XPR tool Number Conversion Prepare fulfills further functions that, however, only concern the development of the XPR server and are only required by the corresponding system developers. Therefore, the following description is restricted to the above applications in productive operation.

After the XPR server installation you find the Number Conversion Prepare tool in the directory: `<XPR Install>\bin`.

9.8.1 How the Tool works

After its invocation the Number Conversion Prepare tool runs through the Correl database of the XPR server and normalizes all entries that you have specified for normalization. You specify such entries in the initialization file `NumberConversionPrepare.ini`.

9.8.2 The Initialization File

The initialization file `NumberConversionPrepare.ini` specifies which entries of the Correl database are normalized after the Number Conversion Prepare invocation. To this it contains mask entries. If an entry in the Correl database fulfills one of these mask entries, it is normalized.

A mask entry of the initialization file is structured as follows:

```
<DOMAIN>;<CLASSNAME>;<CLASS>;<KEYNAME>;<Parameter1>=<Value1>,<Parameter2>=<Value2>, ...;
```

The database fields DOMAIN, CLASSNAME, CLASS and KEYNAME are mandatory specifications; parameters are optional.

Example:

```
*;USER;*;PRIVTEL;Options=IfNumber;
```

NOTE:

The wildcard * is allowed at the beginning and at the end of a database-field name.

The following parameters are supported in a mask entry:

Parameter	Function	Example
SOURCE	Database field type to be converted. <i>Default:</i> KEY	Source=KEY
TargetKn	KEYNAME of the database field to which the conversion result is copied if it is not to be written in Source . Possible for Source=KEY only.	TargetKn=FAXG3
Content	Data type to be converted. <i>Example:</i> Number, NvsAddress, CtiJournal	Content=NvsAddress
Options	Condition or parameter for the conversion. Several options can be linked via '+'. Possible condition or parameters are: • IfNumber: Conversion is only executed if the source information is a number • DeleteOld: Deletes the old database entry, if a conversion has already been performed • ContinueSame: Database entry is not updated.	Options=IfNumber+DeleteOld
Client	The NCO client used for the conversion. <i>Default:</i> Default	Client=Default
CPoint	The connect point used for the conversion. <i>Default:</i> Update	CPoint=Update

Table 14 Parameters for *NumberConversionPrepare.ini*

9.8.3 Invoking the Tool

You invoke the Number Conversion Prepare via the Windows command prompt:

```
NumberConversionPrepare update nocn
```

9.8.4 Using the Tool

How to normalize the phone numbers in the Correl database and in journal entries:

1. Open the initialization file `NumberConversionPrepare.ini` in a text editor if you need to adjust the entries to your requirements.

You find the initialization file in the directory:

```
<XPR Install>\bin
```

If required, adjust the entries of the initialization file.

2. Open a Windows command prompt via **Start > Run**.
3. With the `cd` command switch to the following directory:

```
<XPR Install>\bin
```

4. Execute the following command in the command prompt:

```
NumberConversionPrepare update nocn
```

The entries in the Correl database will now be converted on the basis of the specifications in the initialization file `NumberConversionPrepare`.

9.9 Reference to the Number Conversion Administrator (NCOAdmin)

NOTE:

The NCOAdmin accesses the NCO configuration files of the XPR server. Please make sure that the NCOAdmin used and the NCO configuration files are of the same version.

If this is not the case, an alarm message at the beginning of the Telematic configuration indicates this incompatibility.

NOTE:

If the NCOAdmin is started directly via its program file and not via the settings in a Telematic APL, all NCO tabs, except for the **Locations** tab, are locked by password query.

System administrators and service personnel can obtain their password to unlock the relevant tabs from the service partner in charge.

The information contained in this chapter is divided into the following sections:

- [What is the NCOAdmin?](#)
- [The File Menu](#)
- [NCOs](#)
- [NCO Clients](#)
- [NCO Locations](#)
- [NCO Call Types](#)
- [Normalization Rule Sets](#)
- [Localization Rule Sets](#)
- [Variables](#)
- [Configuration](#)
- [NCO Conditions](#)
- [NCO Rules](#)
- [NCO Variables Reference.](#)

9.9.1 What is the NCOAdmin?

The NCOAdmin serves for configuring all NCO components.

These are:

- Number Conversion Objects (NCO)
- NCO clients
- NCO locations
- NCO call type checker
- Normalization rule sets
- Localization rule sets
- Variables
- NCO configuration

The NCOAdmin is installed in the `<XPR Install>\bin` directory and started with the executable `NumberConversionAdmin.exe` file there.

9.9.2 The *File* Menu

Open active configuration

Opens the NCO configuration of the local XPR server.

Open from file ...

Opens the NCO configuration of a remote XPR server that is located in the same network as the local computer system.

Open from server (via Web)...

Opens the NCO configuration of a remote XPR server accessible via Internet.

Save

Saves NCO configuration modifications in the associating configuration files.

If the NCOAdmin is operated in the local or network mode, the modifications become immediately active.

If the NCOAdmin is operated in the Internet mode, modifications are merely saved in the local copies of the configuration files. These can then be transferred to the relevant XPR server where they activate themselves.

IMPORTANT:

As soon as you save an NCO configuration, it will become active on the relevant XPR server within the next 60 seconds. Faulty settings may **trouble** the XPR server operation.

save as

Saves the current NCO configuration under another name.

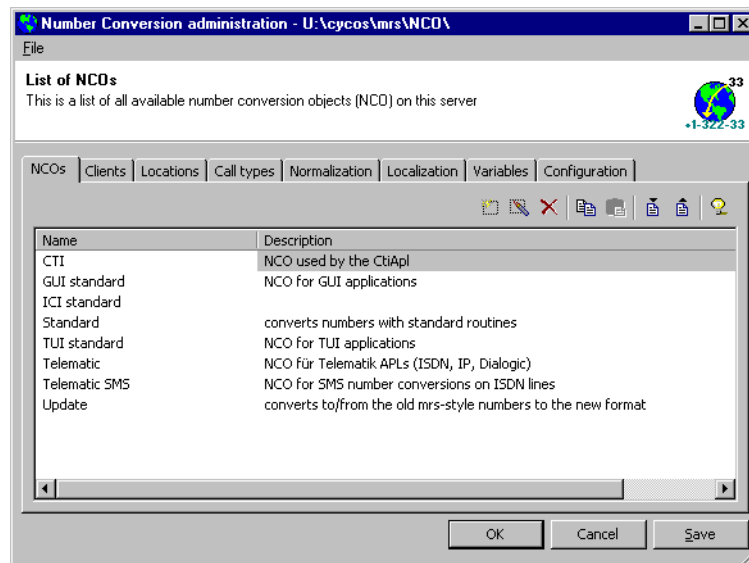
Save and &activate

Saves current NCO configuration modifications performed in the Internet mode in the configuration files of the original XPR server.

IMPORTANT:

As soon as you save an NCO configuration, it will become active on the relevant XPR server within the next 60 seconds. Faulty settings may **trouble** the XPR server operation.

9.9.3 NCOs



On the **NCOs** tab all NCOs are administered. The following options are available:

Add

Adds a new NCO to the list of the already configured ones.

Edit

Opens a configuration dialog with the properties of the NCO selected in the list (cf. [Section 9.9.3.1, "Editing NCO", on page 440](#)).

Delete

Deletes the selected NCO from the list.

Copy

Copies the selected NCO and its assigned configuration to the clipboard.

Paste

Inserts the NCO previously **copied** to the clipboard in the list of NCOs already defined. The indication *Copy of...* is then used for the new entry.

Import

Imports a previously exported NCO configuration in the XPR server. New NCO elements are added during the import to the existing configuration. Imported NCO elements that already exist in the configuration overwrite these.

Export

Exports the selected NCO element configuration to a XML-based configuration file. This file can later be imported in a XPR server.

Default name for the export file is `<Element Name>.xml`.

Test

Opens an editor to test the behavior of the selected NCO (cf. [Section 9.9.3.2, “NCO Tester”, on page 441](#)).

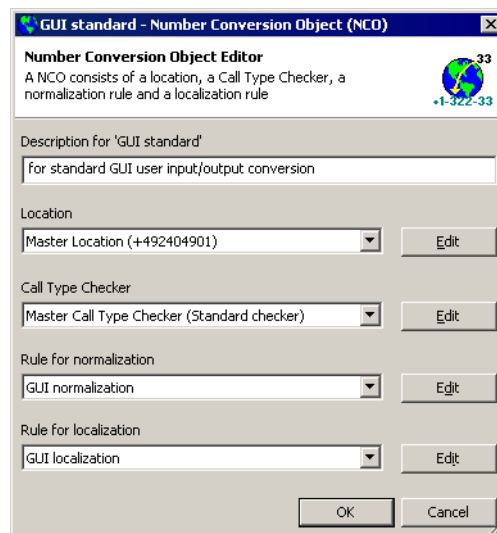
Save

Copies the modifications performed.

IMPORTANT:

As soon as you save an NCO configuration, it will become active on the relevant XPR server within the next 60 seconds. Faulty settings may **trouble** the XPR server operation.

9.9.3.1 Editing NCO



The settings of a selected NCO can be edited in the NCO configuration dialog. Counted among these settings is the assignment of a location, of a call type checker, of a normalizing, and of a localizing rule set.

The following options are available:

Description

Defines a short descriptive text for the selected NCO.

Location

Defines the location assigned to the selected NCO.

Call type checker

Defines the call type checker assigned to the selected NCO.

Rule for normalization

Defines the normalization rule set assigned to the selected NCO.

Rule for localization

Defines the localization rule set assigned to the selected NCO.

Edit

Opens a configuration dialog with the respective properties of the selected location (cf. [Section 9.9.5.1, “Editing Locations”, on page 449](#)), of the selected call type checker (cf. [Section 9.9.6.1, “Editing the Call Type Checker”, on page 455](#)), normalization or localization rule set (cf. [Section 9.9.7.1, “Rule Set Editing”, on page 461](#)).

9.9.3.2 NCO Tester

IMPORTANT:

If you execute the NCO tester with activated phone number cache, phone numbers once tested are stored with their respective conversion result. If the you then change the configuration and test a previously tested phone number again, the changed configuration will not take effect. The previously stored conversion result is put out instead.

See also [Section 9.9.10, "Configuration"](#), on page 466.

The NCO tester is an application for testing the conversion rules of a selected NCO. The following dialog elements are available:

Localized Number

Serves for entering a localized (local) phone number to be normalized with the normalization rules of the previously selected NCO.

Normalized number

Serves for entering a normalized phone number to be localized with the localization rules of the previously selected NCO.

Resulting call type

Displays the call type that results from calling the call type checker of the previously selected NCO.

Normalize

Starts the normalization of the phone number entered in the **Localized number** field.

Localize

Starts the localization of the phone number entered in the **Normalized number** field.

Location

Defines the location the settings of which are used for the respective conversion of the specified phone number.

Optional variables

Serves for defining optional variables to slip in the phone number conversion. In this way a transfer of variables by the NCO client during the conversion invocation can be simulated.

IMPORTANT:

A variable transferred in this way may already exist with a value assigned in the NCO. In this case the value already assigned is overridden with the value defined under **Optional variables** for the duration of the phone number conversion.

Output Variables

Serves to display variables that redeliver conversion rules conclusively. The variables displayed here would be returned to the calling NCO client following a phone number conversion.

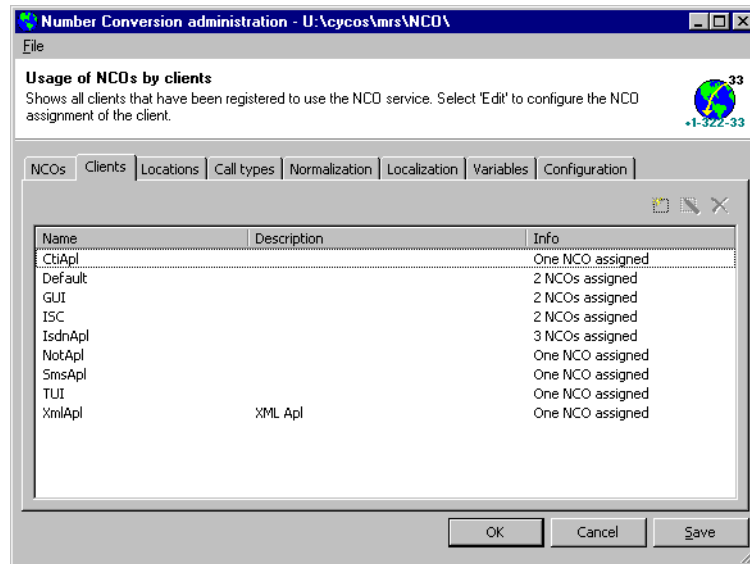
Logging

Serves to put out a conversion log. By means of this log the last conversion process can be tracked (the conditions fulfilled; the matching conversion, pre- and postprocessing rules).

NOTE:

The logging output is particularly useful with checking the function of new rules or for searching errors.

9.9.4 NCO Clients



On the **Clients** tab all NCO clients are administered. The following dialog elements are available:

Add

Adds a new NCO client to the list of NCO clients already configured.

Edit

Opens a configuration dialog with the properties of the NCO client selected in the list (cf. [Section 9.9.4.1, "Editing NCO Clients", on page 444](#)).

Delete

Deletes the selected NCO client.

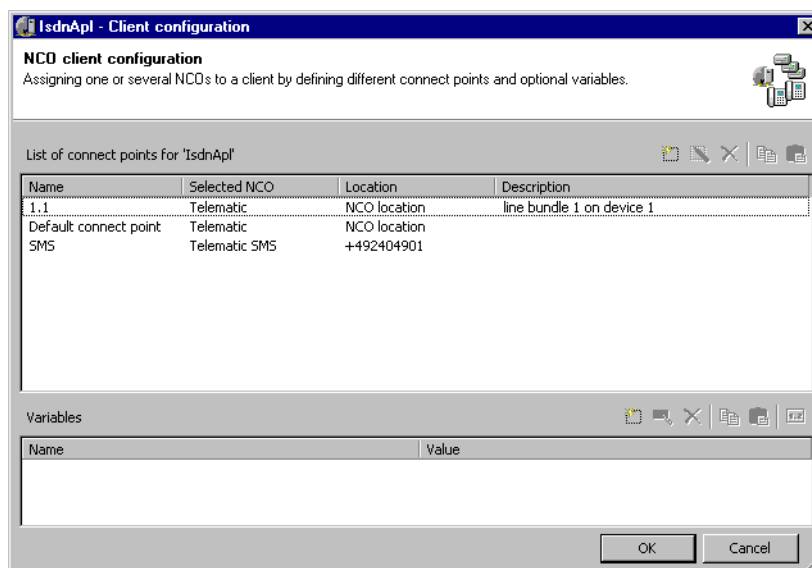
Save

Copies the modifications performed.

IMPORTANT:

As soon as you save an NCO configuration, it will become active on the relevant XPR server within the next 60 seconds. Faulty settings may **trouble** the XPR server operation.

9.9.4.1 Editing NCO Clients



The settings of a selected NCO client can be edited in the client configuration dialog. Among these settings you find the connect point, NCO and location assignments as well as the definition of client-individual variables.

The location defined in the associated NCO is selected under **Location** by default. At variance with this it is also possible to assign any other defined location to any NCO client and NCO combination. This configuration is then preferred to the location defined in the associating NCO.

The following dialog elements are available:

Add

Adds a new element (connect point or variable) to the corresponding list of elements already configured.

Edit

Opens a configuration dialog with the properties of the connect point selected in the list (cf. [Section 9.9.4.2, "Editing Connect Points", on page 446](#)).

Change Value

Sets the value of the selected variable in an editable state.

Delete

Deletes the selected list entry (connect point or variable).

Copy

Copies the selected element (connect point or variable) and its associating configuration to the clipboard.

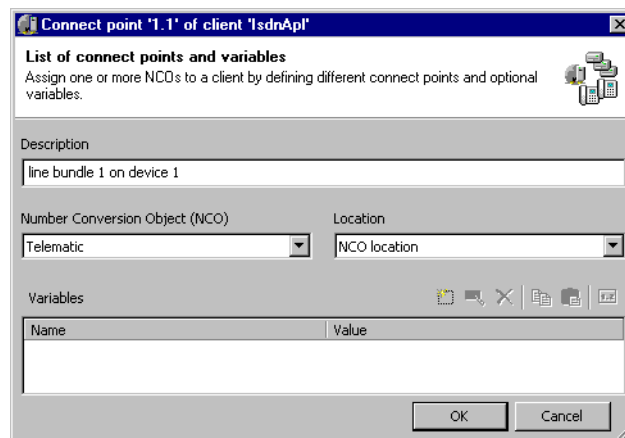
Paste

Inserts the element (connect point or variable) previously **copied** to the clipboard in the corresponding list of elements already configured.

Edit as Number Range

Opens a configuration dialog for entering range lists. A number range can thus be defined for the previously selected variable (cf. [Section 9.9.9.1, “Range List Editor of a Variable”](#), on page 465).

9.9.4.2 Editing Connect Points



The settings of a selected connect point can be edited in the connect point configuration dialog. These settings include the assignment of a NCO and a location to a connect point. Besides that, variables can be added to the selected connect point.

The following dialog elements are available:

Add

Adds a new variable to the list of variables already configured.

Change Value

Sets the value of the selected variable in an editable state.

Delete

Removes the selected variable.

Copy

Copies the selected variable and its assigned value to the clipboard.

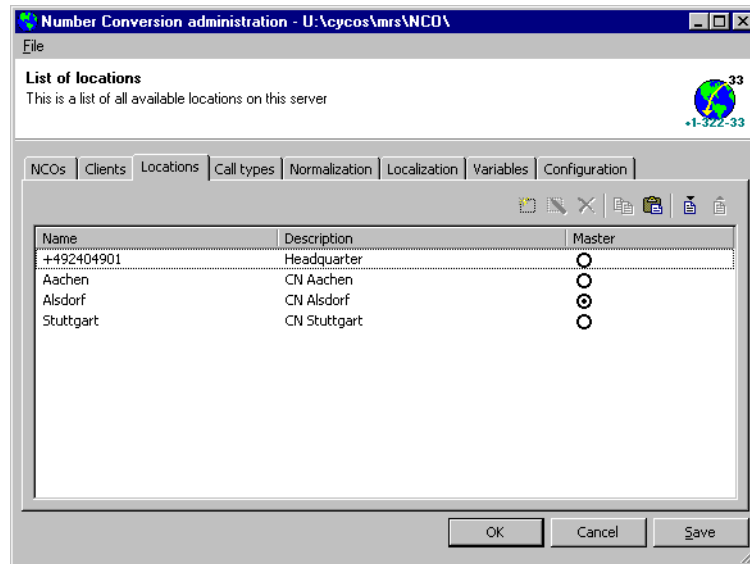
Paste

Inserts the variable previously **copied** to the clipboard in the list of variables already defined.

Edit as Number Range

Opens a configuration dialog for entering range lists. A number range can thus be defined for the previously selected variable (cf. [Section 9.9.9.1, “Range List Editor of a Variable”, on page 465](#)).

9.9.5 NCO Locations



On the **Locations** tab all NCO locations are administered. The following dialog elements are available:

Add

Adds a new location to the list of locations already configured.

Edit

Opens a configuration dialog with the properties of the location selected in the list (cf. [Section 9.9.5.1, “Editing Locations”, on page 449](#)).

IMPORTANT:

The phone number information for XPR users is stored in the Correlation Database of the XPR server in normalized format. The respective normalization always takes place on the basis of the corresponding location information. If location settings are modified in an existing XPR environment, the phone number information of existing users is **not** automatically updated in the Correlation Database.

As a consequence, corresponding modifications of the user information must be performed manually. For this purpose, you can use the XPR tool *Number Conversion Prepare* with the following command prompt:

```
numberconversionprepare update nocn
```

Number Conversion Prepare **does not** adjust the **CIT** database field in the process.

Delete

Deletes the selected location.

Copy

Copies the selected location and its assigned configuration to the clipboard.

Paste

Inserts the location previously **copied** to the clipboard in the list of already existing locations. The indication *Copy of...* is then used for the new entry.

Import

Imports a previously exported location configuration in the XPR server. New NCO elements are added during the import to the existing configuration. Imported NCO elements the name of which already existed in the configuration overwrite these.

Export

Exports the selected location configuration to a XML-based configuration file. This file can later be imported in a XPR server.

Default name for the export file is `<location name>.xml`.

Master

Defines which of the listed locations is configured as *Master Location*.

The *Master Location* option defines an additional location entry within the various location selection menus. If this entry is assigned to an NCO, this reference always represents the location just defined as *Master Location*. If after such an assignment the *Master Location* option is reset to another location, the absolute location assignment of such a reference always changes as well.

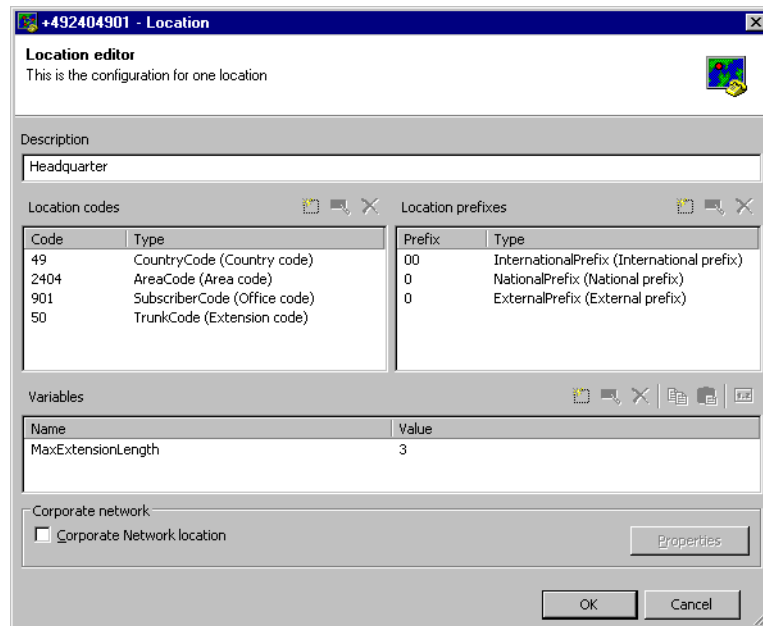
Save

Copies the modifications performed.

IMPORTANT:

As soon as you save an NCO configuration, it will become active on the relevant XPR server within the next 60 seconds. Faulty settings may **trouble** the XPR server operation.

9.9.5.1 Editing Locations



The settings of a selected NCO client can be edited in the location configuration dialog. Among these settings are location codes and location prefixes as well as the definition of location-individual variables.

The following dialog elements are available:

Description

Defines a short descriptive text for the selected location.

Add

Adds a new element (connect point or variable) to the corresponding list of elements already configured.

Change Value

Sets the value of a selected element (location code, location prefix or variable) in an editable state.

Delete

Deletes the selected element (location code, location prefix or variable).

Copy

Copies the selected element (location code, location prefix or variable) and its associating configuration to the clipboard.

Paste

Inserts the element (location code, location prefix or variable) previously **copied** to the clipboard in the corresponding list of elements already configured. The indication *Copy of...* is then used for the new entry.

Edit as Number Range

Opens a configuration dialog for entering range lists. A number range can thus be defined for the previously selected variable (cf. [Section 9.9.9.1, “Range List Editor of a Variable”, on page 465](#)).

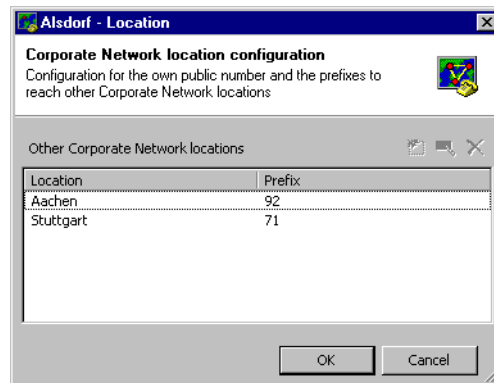
Corporate Network location

Defines whether the selected location is part of a Corporate Network. This option is only displayed if the **CorporateNetworkActive** option on the **Configuration** tab is activated (cf. [Section 9.9.10, “Configuration”, on page 466](#)).

Properties

Leads to the Corporate Network properties of the selected location.

9.9.5.2 Location Settings Corporate Network



The prefix settings of a selected NCO location can be edited for the Corporate Network in the configuration dialog.

The following elements are available:

Add

Adds a new Corporate Network location to the corresponding list of already configured elements. The Corporate Network location option must be active for the desired location (cf. [Section 9.9.5.1, “Editing Locations”, on page 449](#)).

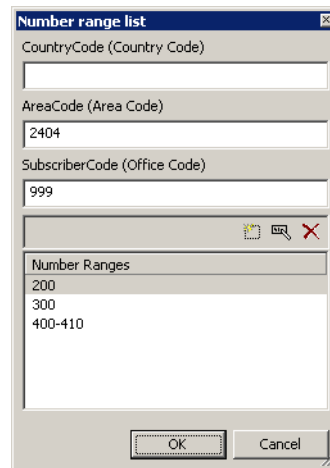
Change Value

Sets the value of the selected prefix in an editable state.

Delete

Deletes the selected location entry.

9.9.5.3 Range List Editor of a Location



Using the range list editor, range lists can be defined within a location in a simple way (cf. [Section 9.3.12, “Range Lists”, on page 376](#)).

NOTE:

Entries in the **CountryCode**, **AreaCode** respectively **SubscriberCode** fields are only accepted if no corresponding entries are specified in the relevant location.

CountryCode (Country Code)

Defines the *CountryCode* variable as optional, common code of a range list.

AreaCode

Defines the *AreaCode* variable as optional, common code of a range list.

SubscriberCode

Defines the *SubscriberCode* variable as optional, common code of a range list.

Number Ranges

Defines the number ranges contained in the number range list. Each entry must contain either a single extension or a coherent number range of the format *<Extension 1> – <Extension 2>*.

Add

Adds a new number range to the list of number ranges already configured.

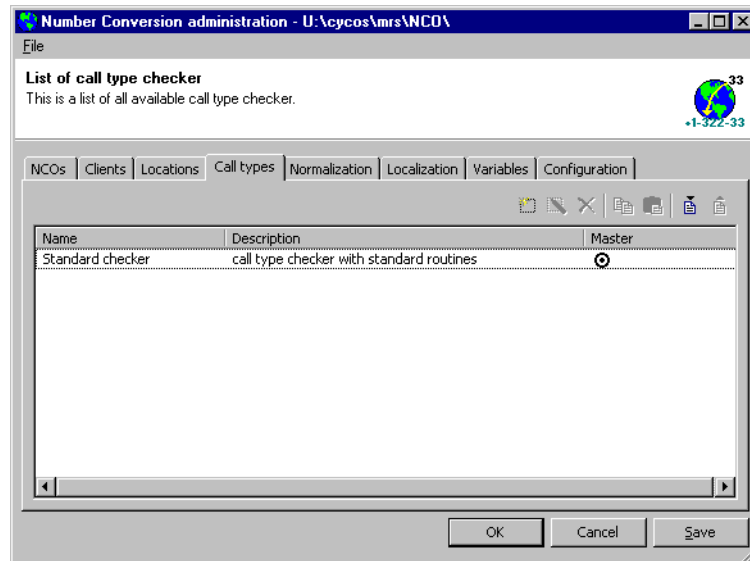
Change Value

Sets the value of the selected number range in an editable state.

Delete

Deletes the selected number range.

9.9.6 NCO Call Types



All NCO call type checkers are administered on the **Call types** tab. The following dialog elements are available:

Add

Adds a new call type checker to the list of call type checkers already configured.

Edit

Opens a configuration dialog with the properties of the call type checker selected in the list (cf. [Section 9.9.6.1, “Editing the Call Type Checker”, on page 455](#)).

Delete

Deletes the selected call type checker.

Copy

Copies the selected call type checker and its assigned configuration to the clipboard.

Paste

Inserts the call type checker previously **copied** to the clipboard in the corresponding list of call type checkers already configured. The indication *Copy of...* is then used for the new entry.

Import

Imports a previously exported call type checker configuration in the XPR server. New NCO elements are added during the import to the existing configuration. Imported NCO elements that already exist in the configuration overwrite these.

Export

Exports the selected call type checker configuration to a XML-based configuration file. This file can later be imported in a XPR server.

Default name for the export file is:

`<name of call type checker>.xml.`

Master

Defines which of the listed call type checkers is configured as *Master Call Type Checker*.

The *Master Call Type Checker* option defines an additional call type checker entry within the various call type checker selection menus. If this entry is assigned to an NCO, this reference always represents the call type checker just defined as *Master Call Type Checker*. If after such an assignment the *Master Call Type Checker* option is reset to another call type checker, the absolute call type checker assignment of such a reference always changes as well.

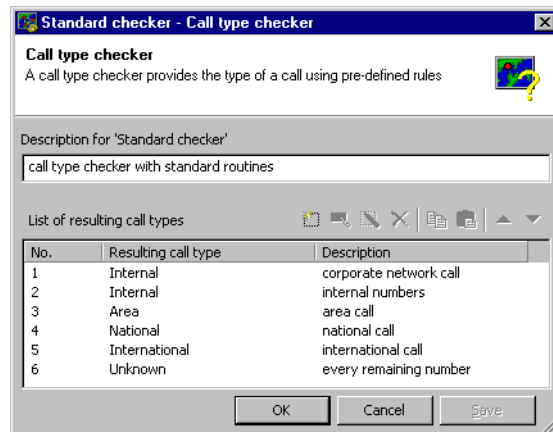
Save

Copies the modifications performed.

IMPORTANT:

As soon as you save an NCO configuration, it will become active on the relevant XPR server within the next 60 seconds. Faulty settings may **trouble** the XPR server operation.

9.9.6.1 Editing the Call Type Checker



The connection types of a selected call type checker can be edited in the call type checker configuration dialog.

The following dialog elements are available:

Add

Adds a new connection type to the list of connection types already configured.

Change Value

Sets the value of the resulting connection type in an editable state.

Edit

Opens a configuration dialog with the properties of the connection type selected in the list.

Delete

Deletes the selected connection type.

Copy

Copies the selected connection type and its assigned configuration to the clipboard.

Paste

Inserts the connection type previously **copied** to the clipboard in the list of connection types already configured.

Move up

Moves the selected connection type up by one position in the list.

Move down

Moves the selected connection type down by one position in the list.

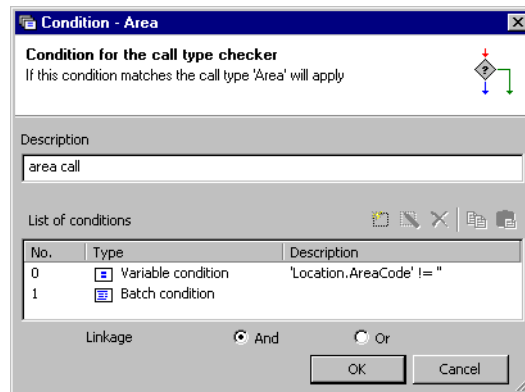
Save

Copies the modifications performed.

IMPORTANT:

As soon as you save an NCO configuration, it will become active on the relevant XPR server within the next 60 seconds. Faulty settings may **trouble** the XPR server operation.

9.9.6.2 Editing the Conditions of a Call Type



The single connection types of a selected call type checker can be edited in the call type checker condition configuration dialog. Among these settings are the conditions themselves as well as their logical links.

The following dialog elements are available:

Description

Defines a short descriptive text for the selected call type checker.

Add

Adds a new condition to the list of conditions already configured.

Edit

Opens a configuration dialog with the properties of the condition selected in the list (cf. [Section 9.9.11, “NCO Conditions”, on page 468](#)).

Delete

Removes the selected condition.

Copy

Copies the selected condition and its assigned configuration to the clipboard.

Paste

Inserts the condition previously **copied** to the clipboard in the list of conditions already defined. The indication *Copy of...* is then used for the new entry.

Paste link

Defines with which logical operator all listed conditions are linked. Possible options are:

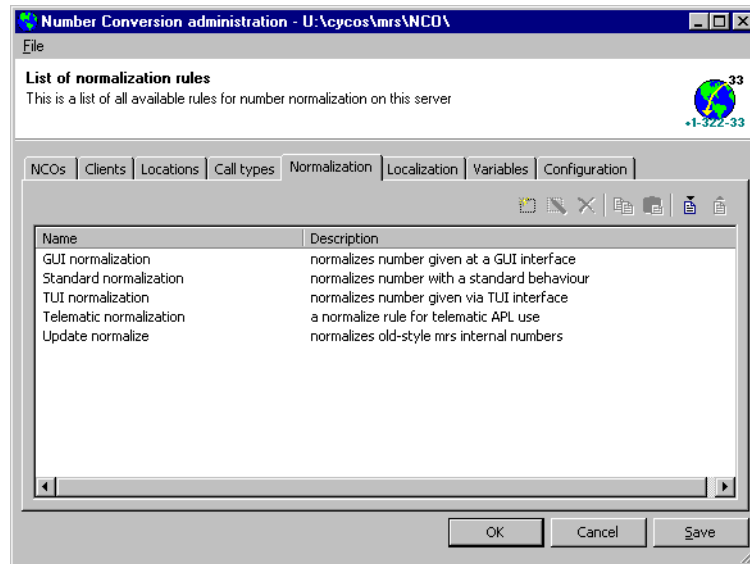
- **AND**
All listed conditions are linked to each other via the logical AND operator.

Number Conversion Object (NCO)

- OR

All listed conditions are linked to each other via the logical OR operator.

9.9.7 Normalization Rule Sets



All normalization rule sets are administered on the **Normalization** tab. The following dialog elements are available:

Add

Adds a new normalization rule set to the list of rule sets already configured.

Edit

Opens a configuration dialog with the properties of the rule set selected in the list (cf. [Section 9.9.7.1, “Rule Set Editing”, on page 461](#)).

Delete

Deletes the selected rule set.

Copy

Copies the selected rule set and its assigned configuration to the clipboard.

Paste

Inserts the rule set previously **copied** to the clipboard in the list of rule sets already defined. The indication *Copy of...* is then used for the new entry.

Import

Imports a previously exported normalization rule set configuration in the XPR server. New NCO elements are added during the import to the existing configuration. Imported NCO elements that already exist in the configuration overwrite these.

Export

Exports the selected normalization rule set configuration to a XML-based configuration file. This file can later be imported in a XPR server.

Default name for the export file is:

`<rule set name>.xml`.

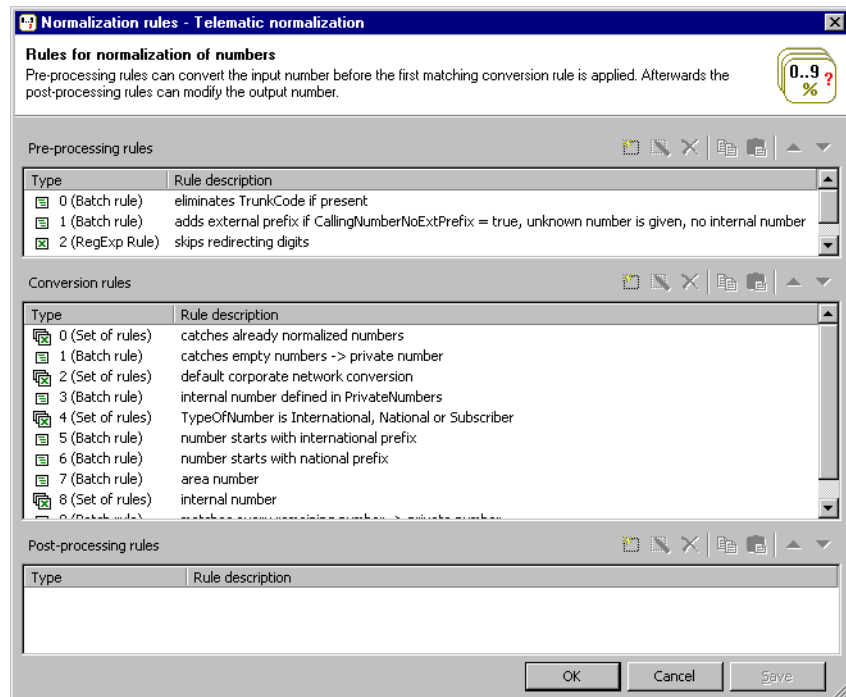
Save

Copies the modifications performed.

IMPORTANT:

As soon as you save an NCO configuration, it will become active on the relevant XPR server within the next 60 seconds. Faulty settings may **trouble** the XPR server operation.

9.9.7.1 Rule Set Editing



The settings of a selected rule set can be edited in the normalization rule set configuration dialog. Among these settings are conversion, pre- and post processing rules.

The following dialog elements are available:

Preprocessing rules

Lists all preprocessing rules of the relevant rule set (cf. [Section 9.3.7, “Localization and Normalization Rules”, on page 357](#)).

Conversion rules

Lists all conversion rules of the relevant rule set (cf. [Section 9.3.7, “Localization and Normalization Rules”, on page 357](#)).

Postprocessing rules

Lists all postprocessing rules of the relevant rule set (cf. [Section 9.3.7, “Localization and Normalization Rules”, on page 357](#)).

Add

Adds a new rule for preprocessing, converting or postprocessing to the associating list of preprocessing, conversion or postprocessing rule sets already configured.

Edit

Opens a configuration dialog with the properties of the normalization rule selected in the list (cf. [Section 9.9.12, “NCO Rules”, on page 478](#)).

Delete

Removes the selected rule.

Copy

Copies the selected rule and its assigned configuration to the clipboard.

Paste

Inserts the rule previously **copied** to the clipboard in the list of rules already defined. The indication *Copy of...* is then used for the new entry.

Move up

Moves the selected rule up by one position in the respective list.

Move down

Moves the selected rule down by one position in the respective list.

Save

Copies the modifications performed.

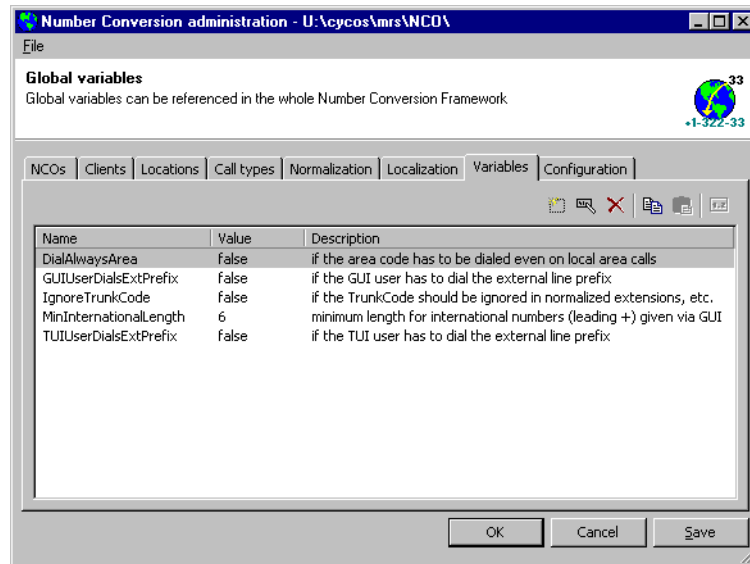
IMPORTANT:

As soon as you save an NCO configuration, it will become active on the relevant XPR server within the next 60 seconds. Faulty settings may **trouble** the XPR server operation.

9.9.8 Localization Rule Sets

The administration of localization rule sets corresponds to administering normalization rule sets (cf. [Section 9.9.7, “Normalization Rule Sets”, on page 459](#)).

9.9.9 Variables



All globally defined variables are administered on the **Variables** tab. The following dialog elements are available:

Add

Adds a new variable to the list of variables already configured.

Change Value

Sets the value of the selected variable in an editable state.

Delete

Removes the selected variable.

Copy

Copies the selected variable and its assigned configuration to the clipboard.

Paste

Inserts the variable previously **copied** to the clipboard in the list of variables already defined. The indication *Copy of...* is then used for the new entry.

Edit as Number Range

Opens a configuration dialog for entering range lists. A number range can thus be defined for the previously selected variable (cf. [Section 9.9.9.1, "Range List Editor of a Variable"](#), on page 465).

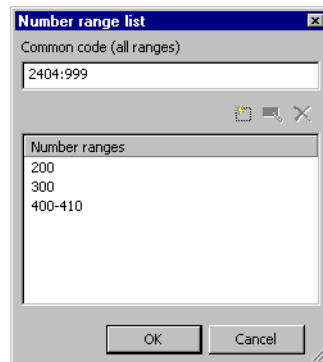
Save

Copies the modifications performed.

IMPORTANT:

As soon as you save an NCO configuration, it will become active on the relevant XPR server within the next 60 seconds. Faulty settings may **trouble** the XPR server operation.

9.9.9.1 Range List Editor of a Variable



Using the range list editor, range lists can be defined within a variable in a simple way (cf. [Section 9.3.12, “Range Lists”, on page 376](#)).

Common code (all number ranges)

Defines the optional common code in a range list in general format. This can be for example the area and subscriber code of the desired number range.

For your entries use the notation:

<Number Portion 1>:<Number Portion 2>: ... <Number Portion n>.

Number Ranges

Defines the number ranges contained in the number range list. Each entry must contain either a single extension or a coherent number range of the format *<Extension 1> – <Extension 2>.*

Add

Adds a new number range to the list of number ranges already configured.

Change Value

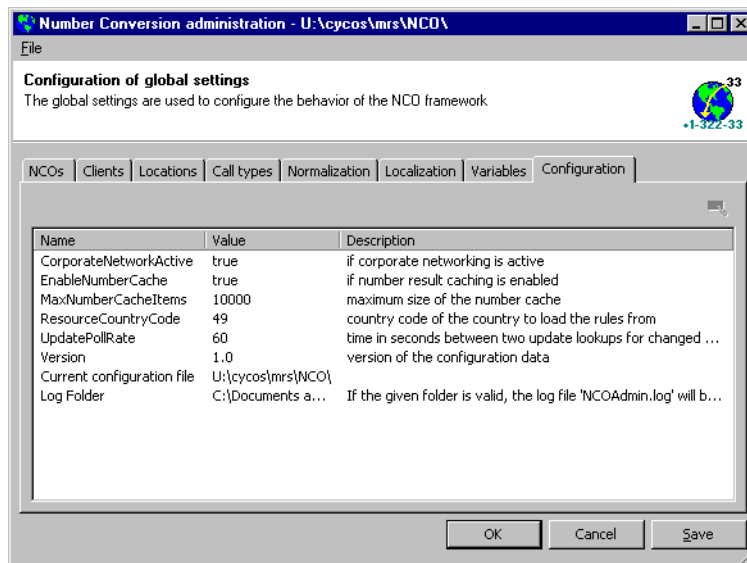
Sets the value of the selected number range in an editable state.

Delete

Deletes the selected number range.

9.9.10 Configuration

The **Configuration** tab lists various configurations that control the general NCO behavior.



The available settings are:

- **Corporate Network Active**
Defines whether the Corporate Network settings are active in NCO.

NOTE:

This option is automatically activated as soon as the XPR server recognizes the license for the *Long Distance Networking* feature.

- **Enable Number Cache**
Activates the caching mechanism for phone numbers previously defined. If, for example, a phone number with the same subconditions (variables, location etc.) is converted for the second time, the result previously saved is directly put out.
In normal operation, this switch should always be set to *true*.

IMPORTANT:

If you execute the NCO tester with activated phone number cache, phone numbers once tested are stored with their respective conversion result. If the you then change the configuration and test a previously tested phone number again, the changed configuration will not take effect. The previously stored conversion result is put out instead.

- **Max. Number Cache Items**
Defines how many phone numbers are stored in the phone number cache.
- **Resource Country Code**
Defines the NCO country behavior. Cf. [Section 9.3.14.1, “XPR Server Basic Settings”, on page 384.](#)
- **Update Poll Rate [in seconds]**
Defines the time after which each NCO client loads the current NCO configuration status.
- **Version**
Defines in which system version the configuration file used is available.
- **Current Configuration File**
Defines the share in which the NCO configuration data are stored. The specified share references to the `<XPR Install>\NCO` directory.
- **Log Folder**
Defines the folder for the log file written with the NCOAdmin during the configuration.

The following dialog elements are available in addition:

Change Value

Sets the value of the selected variable in an editable state.

Save

Copies the modifications performed.

IMPORTANT:

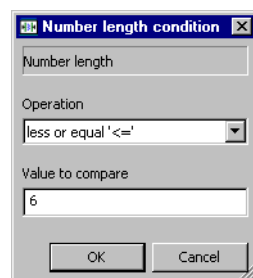
As soon as you save an NCO configuration, it will become active on the relevant XPR server within the next 60 seconds. Faulty settings may **trouble** the XPR server operation.

9.9.11 NCO Conditions

Conditions serves to check whether a defined requirement has been met. They are used in various NCO areas. On the one hand in each call type checker, on the other hand to define preconditions for normalization or localization rules. You find general information on NCO conditions in [Section 9.3.6, “NCO Conditions”, on page 353](#).

The following sections describe the various conditions types used under NCO.

9.9.11.1 Number Length Condition



This condition checks whether a phone number length matches a defined default. The following settings and dialog elements are available:

Operation

Serves to state the logical operator on the basis of which the associating comparison is to occur. Possible options are:

- greater or equal '>='
- larger '>'
- less or equal '<='
- smaller '<'
- Equal '='

Number length

Defines the comparison size for the number length to be checked.

9.9.11.2 Number range Condition

This condition checks whether a phone number falls into a defined phone number range. Cf. also [Section 9.3.12, “Range Lists”, on page 376](#).

The following settings and dialog elements are available:

Description

Defines a short descriptive text for the relevant condition.

Variable to check

Defines the variable that holds the phone number to be checked. This is in most cases the *NumberInput* variable.

Range List to check

Defines the number range into which the phone number to be checked is to fall. Three options are available for this:

- All number range lists of the location:
The phone number to be checked is checked against all defined range lists of the relevant location.
- Number range list of the variable:
The phone number to be checked is checked against a range list defined in the stated variable.
- One entry of the Range List:
The phone number to be checked is checked against the range list defined here.

Check mode

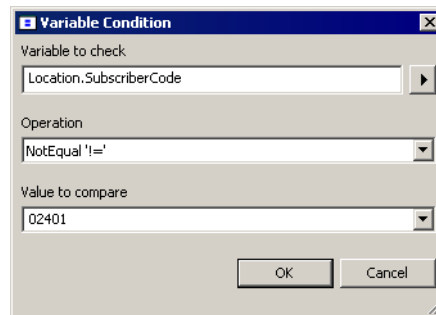
Defines in which way the phone number to be checked is compared to the specified range lists. The following four options are available for this:

- From right to left
- From left to right
- From left to right with expressions to be skipped
In this case the expression to be skipped may also be specified in the format of a regular expression.
- Allow spare digits
With this option you can perform comparisons with end-sided matches and spare digits. Comparisons are possible from left to right as well as from right to left.

Example (right to left):

The phone number 80150 does not belong to the number range 100–200 until the **Allow spare digits** option has been activated. In this case the spare digits are: 80.

9.9.11.3 Variable Check Condition



This condition checks a specific variable for containing a defined value. The following settings and dialog elements are available:

Variable to check

Defines the variable the contents of which is to be checked.

Operation

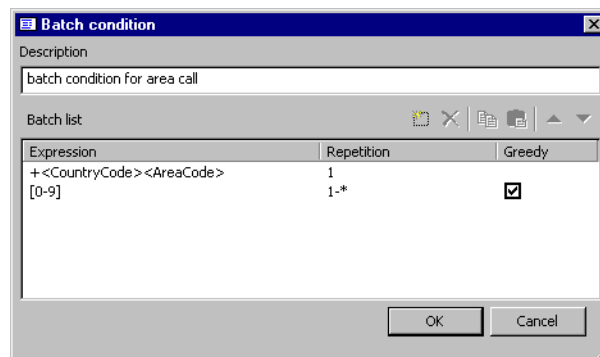
Serves to state the logical operator on the basis of which the associating comparison is to occur. Possible options are:

- Equal '='
- Not equal '!='
- (Variable) Exists
- (Variable) Not exists
- Not equal or (variable) not exists

Value to compare

Defines the value with which the variable content is to be compared.

9.9.11.4 Batch Condition



On the basis of one or several regular expression-based rules, this condition checks whether a phone number has a specific value and/or a specific structure. If several batch entries are defined in the batch list, all of these must apply to meet the entire batch condition.

For more detailed information on the batch entry structure see [Section 9.3.8, “Batch and regular Expressions”](#), on page 367.

The following dialog elements are available:

Description

Defines a short descriptive text for the relevant condition.

Batch List

Defines the single regular expression¹³-based batch entries to be used for the comparison.

Add

Adds a new batch entry to the selected rule.

Delete

Deletes the selected batch entry.

Copy

Copies the selected batch entry to the clipboard.

Paste

Inserts the batch entry previously **copied** to the clipboard in the list of batch entries already defined. The indication *Copy of...* is then used for the new entry.

Move up

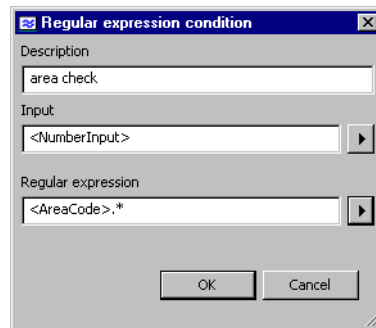
Moves the selected batch entry up by one position in the displayed list.

¹³.The regular expression syntax used by NCO corresponds to the JavaScript (ECMAScript) syntax.

Move down

Moves the selected batch entry down by one position in the displayed list.

9.9.11.5 Regular Expression Condition



Based on a regular expression this condition checks whether the phone number to be checked has a specific value and/or a specific structure. The following settings and dialog elements are available:

Description

Defines a short descriptive text for the relevant condition.

Input

Defines the expression to be evaluated with the regular one. The input is in most cases the *NumberInput* variable.

The selector icon at the end of the text field enables a menu guided entry.

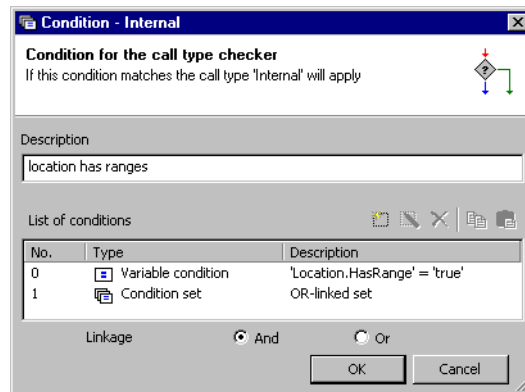
Regular expression

Defines the regular expression¹⁴ to be used for the check.

The selector icon at the end of the text field enables a menu guided entry.

14. The regular expression syntax used by NCO corresponds to the JavaScript (ECMAScript) syntax.

9.9.11.6 Set of Conditions



This condition enables the grouping of different NCO conditions which can be of the types of conditions described in this section again.

The following settings and dialog elements are available:

Description

Defines a short descriptive text for the relevant condition.

List of conditions

Shows all conditions contained in the set of conditions.

Paste link

Defines with which logical operator all contained conditions are linked. Two options exist:

- **AND**
All listed conditions are linked to each other via the logical AND operator.
- **OR**
All listed conditions are linked to each other via the logical OR operator.

A combination of these two types of linkage can be configured via nesting several sets of condition.

Add

Inserts a new condition in the selected one.

Edit

Opens a configuration dialog with the properties of the condition selected in the list.

Delete

Deletes the selected entry.

Number Conversion Object (NCO)

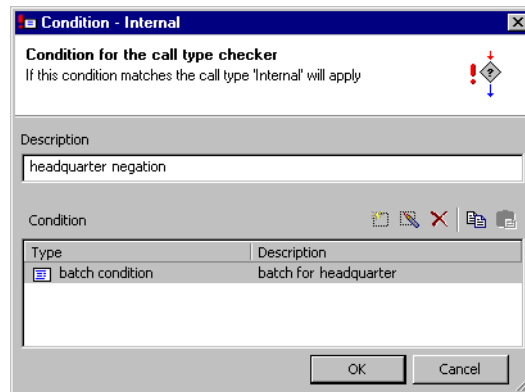
Copy

Copies the entry to the clipboard.

Paste

Inserts the condition previously **copied** to the clipboard in the list of conditions already defined. The indication *Copy of...* is then used for the new entry.

9.9.11.7 Negating Condition



This condition contains an arbitrary condition the result of which is conclusively logically negated.

The following dialog elements are available:

Description

Defines a short descriptive text for the relevant condition.

Add

Adds a new entry to the selected condition.

Edit

Opens a configuration dialog with the properties of the condition selected in the list.

Delete

Deletes the selected entry.

Copy

Copies the entry to the clipboard.

Paste

Inserts the condition previously **copied** to the clipboard in the list of conditions already defined. The indication *Copy of...* is then used for the new entry.

9.9.12 NCO Rules

Within NCO, rules are used to normalize and localize phone numbers. You find general information on this topic in [Section 9.3.7, “Localization and Normalization Rules”](#), on page 357.

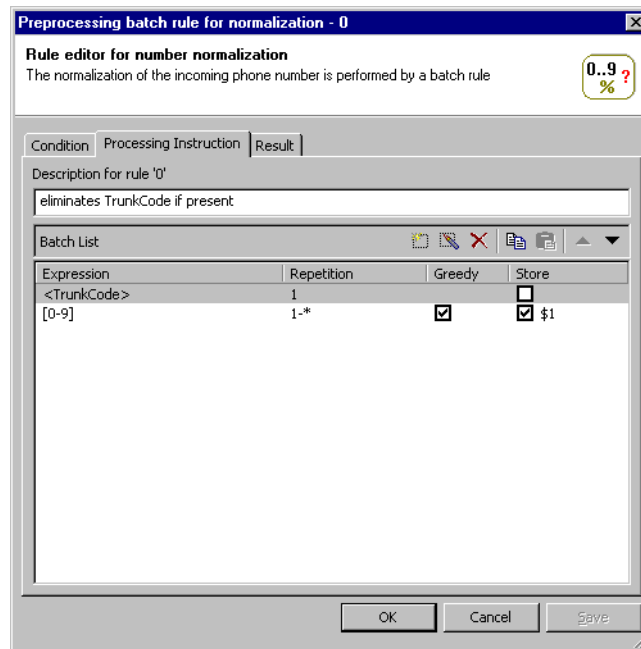
The following sections describe the various rule types used under NCO.

9.9.12.1 Batch Rule – the *Condition Tab*

The structure and function of the rule dialog's **Condition** tab corresponds to the configuration dialog of a call type checker. Cf. [Section 9.9.6.2, “Editing the Conditions of a Call Type”](#), on page 457.

Before the processing instruction of a rule is applied to a phone number, the conditions of the relevant rule are checked. Only if these conditions apply considering their linkage, the processing instruction is continued.

9.9.12.2 Batch Rule – the *Processing Instruction Tab*



The batch rule generates the conversion result for a phone number on the basis of at least one regular expression-based instruction. If several expression portions are defined in the batch list, all of these must apply to accept the entire processing instruction as match.

You find continuative information on the generation of single batch entries in [Section 9.3.8, “Batch and regular Expressions”, on page 367](#).

The following dialog elements are available:

Description

Defines a short descriptive text for the relevant rule.

Batch List

Defines the single regular expression¹⁵-based expression portions to be used for the conversion.

Repetition option

Defines how often the expression portion is to repeat itself.

Greedy option

Defines the behavior of an expression portion when phone number digits match this as well as the following expression portion.

¹⁵The regular expression syntax used by NCO corresponds to the JavaScript (ECMAScript) syntax.

Store option

Defines whether the phone number portion described by the regular expression of the respective processing instruction is buffered in a temporary system variable. Values stored in this way can later be processed in the conversion result.

If this option is active, the system variable used for the relevant buffering is displayed next to the respective check box.

Add

Adds a new entry to the selected rule.

Delete

Deletes the selected expression.

Copy

Copies the selected expression to the clipboard.

Paste

Inserts the expression previously **copied** to the clipboard in the list of entries already defined. The indication *Copy of...* is then used for the new entry.

Move up

Moves the selected expression up by one position.

Move down

Moves the selected expression down by one position.

Save

Copies the modifications performed.

IMPORTANT:

As soon as you save an NCO configuration, it will become active on the relevant XPR server within the next 60 seconds. Faulty settings may **trouble** the XPR server operation.

9.9.12.3 Batch Rule – the *Result* Tab

On the **Result** tab of a batch rule the conclusive conversion result of the rule is defined. The settings defined in this tab are only evaluated and executed if the conditions defined in the rule and the processing instruction previously applied.

The **Result** tab is different for conversion and preprocessing or postprocessing rules.

The *Result* tab for batch conversion rules

Conversion batch rule for normalization - 4

Result of a normalization rule
Assignment of the normalized number as a result and optional variables

Condition | Rule | **Result**

Resulting normalized number
Enter the resulting normalized number here.
You can use tagged expressions from the regular expression/batch expression you entered in the previous page.

+\$1

☒ International ☐ Private

☒ Advanced options

Resulting variable assignments
Enter variables with corresponding values here that shall be set if this rule matches.

Name	Value

OK Cancel Save

On the **Result** tab the following settings and dialog elements are available for conversion rules:

Resulting normalized/localized number

Defines the actual conversion result from different variables. The result can be a composition of the general NCO variables as well as of the temporal system variables set on the **Rule** tab.

The selector icon at the end of the text field enables a menu guided entry.

International option

This option furnishes the specified conversion result with a leading '+' character. The result then becomes an international phone number.

Private option

This option furnishes the specified conversion result with a leading 'p' character. The result then becomes a private phone number.

Extended Options

This option displays or hides the *Resulting Variable Assignments* portion.

Add

Adds a new variable to the list of variables already configured. This variable is allocated with the specified value after the successful execution of the relevant rule and – if necessary – previously generated as well.

Change Value

Sets the value of the selected variable in an editable state.

Delete

Removes the selected variable.

Copy

Copies the selected variable and its assigned configuration to the clipboard.

Paste

Inserts the variable previously **copied** to the clipboard in the list of variables already defined. The indication *Copy of...* is then used for the new entry.

Edit as Number Range

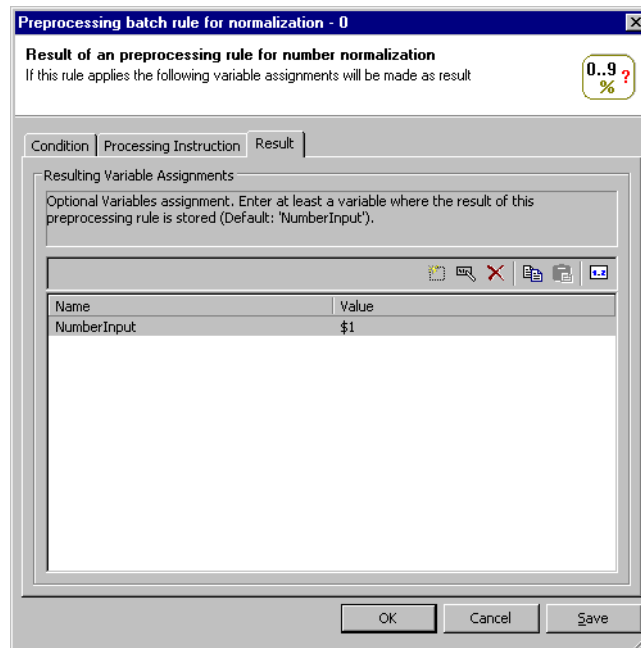
Opens a configuration dialog for entering range lists. A number range can thus be defined for the previously selected variable (cf. [Section 9.9.9.1, “Range List Editor of a Variable”, on page 465](#)).

Save

Copies the modifications performed.

IMPORTANT:

As soon as you save an NCO configuration, it will become active on the relevant XPR server within the next 60 seconds. Faulty settings may **trouble** the XPR server operation.

The *Result* tab for batch preprocessing and batch postprocessing rules

The preprocessing or postprocessing rules edit a phone number before or after the number's actual conversion. In doing so, preprocessing rules use the *NumberInput* variable and postprocessing rules use the *NumberResult* variable in most cases. Other variables can be set as result of a preprocessing or postprocessing rule as well. You find more information on this in [Section 9.3.7, "Localization and Normalization Rules", on page 357](#).

The **Result** tab contains the following dialog elements for preprocessing or postprocessing rules:

Add

Adds a new variable to the list of variables already configured. This variable is allocated with the specified value after the successful execution of the relevant rule and – if necessary – previously generated as well.

Change Value

Sets the value of the selected variable in an editable state.

Delete

Removes the selected variable.

Copy

Copies the selected variable and its assigned configuration to the clipboard.

Paste

Inserts the variable previously **copied** to the clipboard in the list of variables already defined. The indication *Copy of...* is then used for the new entry.

Edit as Number Range

Opens a configuration dialog for entering range lists. A number range can thus be defined for the previously selected variable (cf. [Section 9.9.9.1, “Range List Editor of a Variable”, on page 465](#)).

Save

Copies the modifications performed.

IMPORTANT:

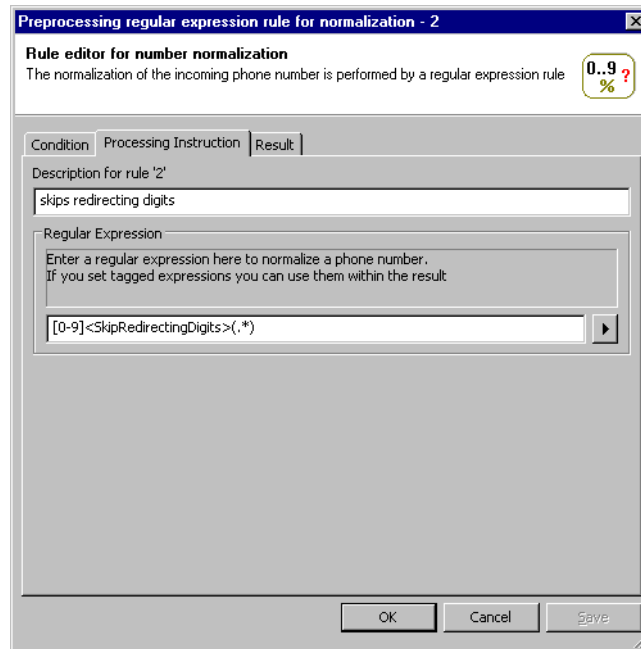
As soon as you save an NCO configuration, it will become active on the relevant XPR server within the next 60 seconds. Faulty settings may **trouble** the XPR server operation.

9.9.12.4 Regular Expression Rule – the *Conditions Tab*

The structure and function of the rule dialog's **Condition** tab corresponds to the configuration dialog of a call type checker. Cf. [Section 9.9.6.2, “Editing the Conditions of a Call Type”, on page 457](#).

Before the processing instruction of a rule is applied to a phone number, the conditions of the relevant rule are checked. Only if these conditions apply considering their linkage, the processing instruction is continued.

9.9.12.5 Regular Expression Rule – the *Processing Instruction* Tab



The regular expression rule generates the conversion result for a phone number on the basis of a single regular expression.

The following dialog elements are available:

Description

Defines a short descriptive text for the relevant rule.

Regular expression

Defines the regular expression¹⁶ to be used for the phone number conversion. The selector icon at the end of the text field enables a menu guided entry.

Save

Copies the modifications performed.

IMPORTANT:

As soon as you save an NCO configuration, it will become active on the relevant XPR server within the next 60 seconds. Faulty settings may **trouble** the XPR server operation.

¹⁶ The regular expression syntax used by NCO corresponds to the JavaScript (ECMAScript) syntax.

9.9.12.6 Regular Expression Rule – the *Result* Tab

On the **Result** tab of a regular expression rule the conclusive conversion result is defined. The settings defined in this tab are only evaluated and executed if the conditions defined in the rule and the processing instruction previously applied.

The **Result** tab is different for conversion and preprocessing or postprocessing rules.

The *Result* tab for regular expression conversion rules

Conversion regular expression rule for normalization - 1

Result of a normalization rule
Assignment of the normalized number as a result and optional variables

Condition Rule **Result**

Resulting normalized number
Enter the resulting normalized number here.
You can use tagged expressions from the regular expression/batch expression you entered in the previous page.

p\$1

☐ International ☒ Private

☒ Advanced options

Resulting variable assignments
Enter variables with corresponding values here that shall be set if this rule matches.

Name	Value

OK Cancel Save

On the **Result** tab the following settings and dialog elements are available for conversion rules:

Resulting normalized/localized number

Defines the actual conversion result from different variables. The result can be a composition of the general NCO variables as well as of the temporal system variables set on the **Rule** tab.

The selector icon at the end of the text field enables a menu guided entry.

International option

This option furnishes the specified conversion result with a leading '+' character. The result then becomes an international phone number.

Private option

This option furnishes the specified conversion result with a leading 'p' character. The result then becomes a private phone number.

Extended Options

This option displays or hides the *Resulting Variable Assignments* portion.

Add

Adds a new variable to the list of variables already configured. This variable is allocated with the specified value after the successful execution of the relevant rule and – if necessary – previously generated as well.

Change Value

Sets the value of the selected variable in an editable state.

Delete

Removes the selected variable.

Copy

Copies the selected variable and its assigned configuration to the clipboard.

Paste

Inserts the variable previously **copied** to the clipboard in the list of variables already defined. The indication *Copy of...* is then used for the new entry.

Edit as Number Range

Opens a configuration dialog for entering range lists. A number range can thus be defined for the previously selected variable (cf. [Section 9.9.9.1, “Range List Editor of a Variable”, on page 465](#)).

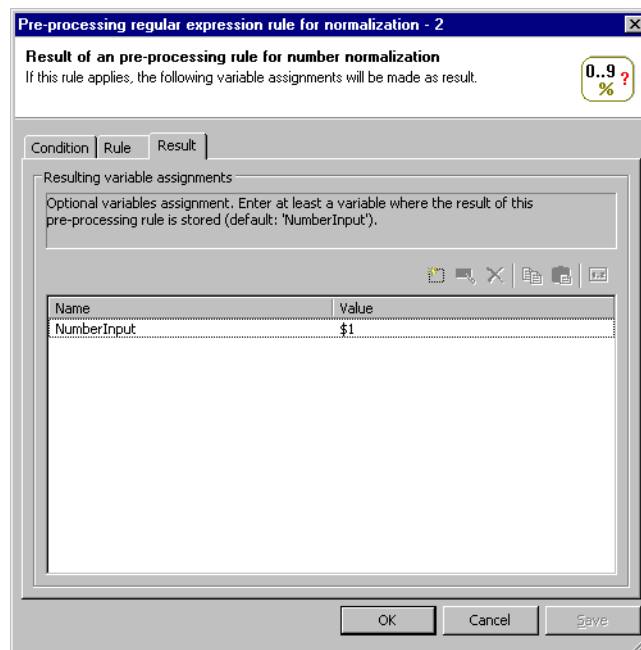
Save

Copies the modifications performed.

IMPORTANT:

As soon as you save an NCO configuration, it will become active on the relevant XPR server within the next 60 seconds. Faulty settings may **trouble** the XPR server operation.

The **Result** tab for regular expression preprocessing and postprocessing rules



The preprocessing or postprocessing rules edit a phone number before or after the number's actual conversion. In doing so, preprocessing rules use the *NumberInput* variable and postprocessing rules use the *NumberResult* variable in most cases. Other variables can be set as result of a preprocessing or postprocessing rule as well. You find more information on this in [Section 9.3.7, "Localization and Normalization Rules"](#), on page 357.

The **Result** tab contains the following dialog elements for preprocessing or postprocessing rules:

Add

Adds a new variable to the list of variables already configured. This variable is allocated with the specified value after the successful execution of the relevant rule and – if necessary – previously generated as well.

Change Value

Sets the value of the selected variable in an editable state.

Delete

Removes the selected variable.

Copy

Copies the selected variable and its assigned configuration to the clipboard.

Paste

Inserts the variable previously **copied** to the clipboard in the list of variables already defined. The indication *Copy of...* is then used for the new entry.

Edit as Number Range

Opens a configuration dialog for entering range lists. A number range can thus be defined for the previously selected variable (cf. [Section 9.9.9.1, “Range List Editor of a Variable”, on page 465](#)).

Save

Copies the modifications performed.

IMPORTANT:

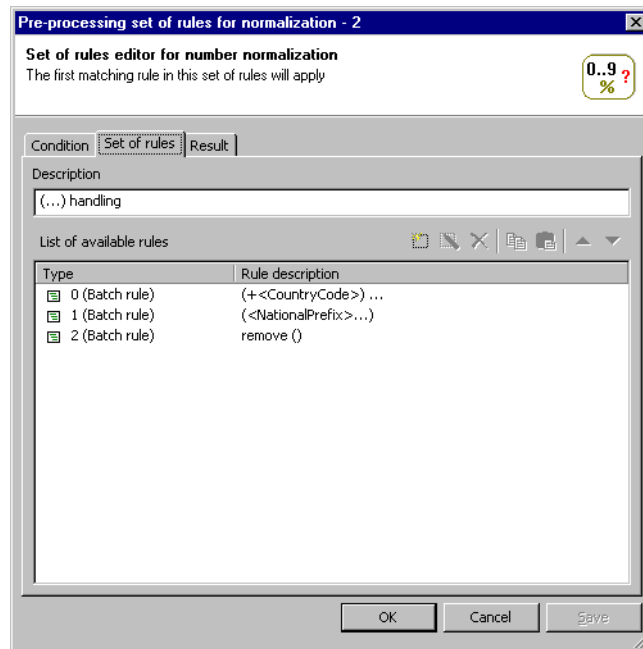
As soon as you save an NCO configuration, it will become active on the relevant XPR server within the next 60 seconds. Faulty settings may **trouble** the XPR server operation.

9.9.12.7 Rule Set Rule – the *Condition Tab*

The structure and function of the rule dialog's **Condition** tab corresponds to the configuration dialog of a call type checker. Cf. [Section 9.9.6.2, “Editing the Conditions of a Call Type”](#), on page 457.

Before the processing instruction of a rule is applied to a phone number, the conditions of the relevant rule are checked. Only if these conditions apply considering their linkage, the processing instruction is continued.

9.9.12.8 Rule Set Rule – the *Set of rules Tab*



This rule enables the summary of different NCO rules which can be of the types of rules described in this section again. In this way very comprehensive set of rules can be structured.

The following dialog elements are available:

Description

Defines a short descriptive text for the relevant rule.

List of available rules

Displays all rules contained in the rule set.

Add

Adds a new entry to the selected rule set rule.

Edit

Opens a configuration dialog with the properties of the rules selected in the list.

Delete

Removes the selected rule.

Copy

Copies the selected rule entry to the clipboard.

Paste

Inserts the rule entry previously **copied** to the clipboard in the list of elements already defined. The indication *Copy of...* is then used for the new entry.

Move up

Moves the selected rule up by one position in the displayed list.

Move down

Moves the selected rule down by one position in the displayed list.

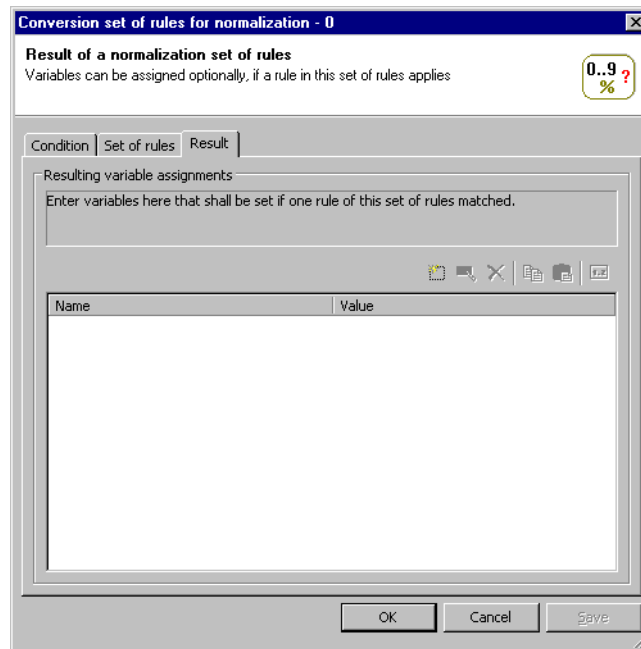
Save

Copies the modifications performed.

IMPORTANT:

As soon as you save an NCO configuration, it will become active on the relevant XPR server within the next 60 seconds. Faulty settings may **trouble** the XPR server operation.

9.9.12.9 Rule Set Rule – the *Result Tab*



On the **Result** tab of a rule set rule the conclusive conversion result of the rule is defined. The settings defined in this tab are only evaluated and executed if the conditions defined in the rule and the processing instruction previously applied.

On the **Result** tab the following elements are available:

Add

Adds a new variable to the list of variables already configured. This variable is allocated with the specified value after the successful execution of the relevant rule and – if necessary – previously generated as well.

Change Value

Sets the value of the selected variable in an editable state.

Delete

Removes the selected variable.

Copy

Copies the selected variable and its assigned configuration to the clipboard.

Paste

Inserts the variable previously **copied** to the clipboard in the list of variables already defined. The indication *Copy of...* is then used for the new entry.

Edit as Number Range

Opens a configuration dialog for entering range lists. A number range can thus be defined for the previously selected variable (cf. [Section 9.9.9.1, “Range List Editor of a Variable”](#), on page 465).

Save

Copies the modifications performed.

IMPORTANT:

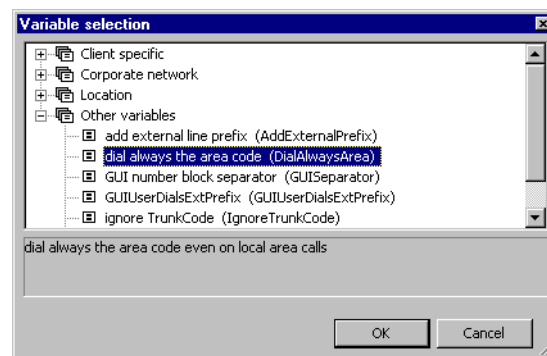
As soon as you save an NCO configuration, it will become active on the relevant XPR server within the next 60 seconds. Faulty settings may **trouble** the XPR server operation.

9.9.13 NCO Variables Reference

IMPORTANT:

NCO clients can default individual contents for NCO variables for phone number conversions. Such individual client defaults may temporarily override the content that is defined for the corresponding variable in the NCO configuration.

The following is a description of the variables already predefined by NCO. They are specified in the `VariableProposals.xml` file as suggestion list and can be selected via a dialog with entering a variable.



You find continuative information on this in [Section 9.3.2.9, “Variables”, on page 343](#).

The variables are structured as follows.

- [Variables in the Built-In Area](#)
- [Variables in the Client specific Area](#)
- [Variables in the Corporate Network Area](#)
- [Variables in the Location Area](#)
- [Variables in the Others Area.](#)

NOTE:

Where a variable may be used is not determined by the folder in which the variable is contained. This allocation serves for a better overview only.

Example:

The variable `AreaCode` is stored in the `Location` folder. That does *not* mean that it may exclusively be used in the **Locations** tab of the NCO settings. Instead, it can be used in any place of the NCO framework.

On each variable the following information will be provided on the next pages:

- **Variable name**
Defines the exact name of the relevant variable.
- **Default value**
Defines the possibly default set value of the variable.
- **Possible values**
Defines the possibly defaulted variable contents or their general format.
- **Mode**
Defines in which format the variable can be processed in the course of the conversion process.

Possible modes are:

- *in*
The variable can be transferred to NCO by the calling client or attached to the phone number to be converted.
- *write*
The variable can be generated during the phone number conversion or assigned a new value.
- *read*
The variable can be read during the phone number conversion.
- *out*
The variable can be generated during the phone number conversion and subsequently transferred to the calling client by NCO.
- *range*
The variable can be edited as number range.
- *location*
The variable can be added to the variables of a location.

9.9.13.1 Variables in the *Built-In Area*

NumberInput

Default:	–
Possible values:	Result of a conversion before the execution of the actual conversion rule.
Mode:	read , write

Contains the respective phone number to be converted until the execution of the matching conversion rule.

During a phone number conversion, rules of the areas preprocessing, conversion and postprocessing are run through in succession. **NumberInput** serves as buffer for the intermediate results during the preprocessing rule run-through.

Cf. [Section 9.3.7, “Localization and Normalization Rules”](#), on page 357.

NumberResult

Default:	–
Possible values:	Result of conversions after the execution of the actual conversion rule.
Mode:	read , write

Contains the respective phone number to be converted after the execution of the matching conversion rule.

During a phone number conversion, rules of the areas preprocessing, conversion and postprocessing are run through in succession. **NumberInput** serves as buffer for the intermediate results during the postprocessing rule run-through.

Cf. [Section 9.3.7, “Localization and Normalization Rules”](#), on page 357.

9.9.13.2 Variables in the *Client specific Area*

The Client area lists all variables that can be used by single NCO clients.

These are:

- [Variables of the CTI APL Client](#)
- [Variables of the ISC PhoneMail client](#)
- [Variables of the SAP gateways clients](#)
- [Variables of the Telematic APLs clients](#)
- [Variables of the XML APL client](#)

Variables of the CTI APL Client**AdditionalOutPrefix**

Default:	–
Possible values:	<character>
Mode:	in, read
Remark:	Is temporarily overridden by the Additional prefix to be ignored for outgoing calls option of the CTI APL settings.

Defines an additional prefix that is transferred to the CTI APL with each called number by a connected PBX.

AdditionalPrefix

Default:	–
Possible values:	<number> and/or <letter>
Mode:	in, read
Remark:	Is temporarily overridden by the Additional prefix to be ignored for incoming calls option of the CTI APL settings.

Defines an additional prefix that is transferred to the CTI APL with each calling number by a connected PBX.

AllowedNumberCharacters

Default:	1234567890*#
Possible values:	<character>
Mode:	in, read
Remark:	Is temporarily overridden by the CTI APL.

Table 15

Defines the characters allowed in a phone number.

TypeOfNumber

Default:	–
Possible values:	International – Intern. phone number format (e.g. 492404901100) National – Nation. phone number format (e.g. 2404901100) Subscriber – Code format (e.g. 901100) Unknown – Unknown phone number format (e.g. 100)
Mode:	in, read, write, out
Remark:	Is temporarily overridden by the CTI APL.

An ISDN phone number can be transmitted between two systems in different formats. **TypeOfNumber** defines in which phone number format the simultaneously transferred phone number is available.

UseTypeInternational

Default:	false
Possible values:	<i>false</i> – Phone numbers will not be transferred in the intern. format <i>true</i> – Phone numbers will be transferred in the intern. format
Mode:	in, read
Remark:	Is temporarily overridden by the CTI APL. See DontLocalize [REG_DWORD] .

Defines whether the XPR server transfers phone numbers in international format (e.g. 492404901100) to a system connected via the NCO client.

Variables of the *ISC PhoneMail* client**SrcPrefix**

Default:	–
Possible values:	<Prefix>
Mode:	in, read

In an ISC network the users' phone number information of the diverse ISC nodes are exchanged in network profiles. A received network profile may possibly not contain a phone number that can be dialed. In this case it is possible to create a number that can be dialed by simply replacing a location prefix contained in the phone number with a freely configurable one. This freely configurable prefix can e.g. correspond to a tie line that is to be dialed.

SrcPrefix defines the series of numbers that is to be replaced by the freely configurable prefix.

DstPrefix

Default:	–
Possible values:	<Prefix>
Mode:	in, read

In an ISC network the users' phone number information of the diverse ISC nodes are exchanged in network profiles. A received network profile may possibly not contain a phone number that can be dialed. In this case it is possible to create a number that can be dialed by simply replacing a location prefix contained in the phone number with a freely configurable one. This freely configurable prefix can e.g. correspond to a tie line that is to be dialed.

DstPrefix defines the series of numbers of the freely configurable prefix.

Variables of the *SAP gateways clients*

AddressType

Default:	–
Possible values:	FAX – Defines a fax number PAG – Defines a pager number
Mode:	in, read

Defines the address type for the associating phone number.

LocalizeInternalNumbers

Default:	–
Possible values:	<i>false</i> – Internal phone numbers will not be normalized <i>true</i> – Internal phone numbers will be normalized
Mode:	in, read

Defines whether internal phone numbers are to be localized.

Variables of the Telematic APLs clients**CalledNumberWithTrunkCode**

Default:	<i>false</i>
Possible values:	<i>false</i> – TrunkCode is not transmitted by the PBX <i>true</i> – TrunkCode is transmitted by the PBX
Mode:	in, read
Remark:	Is temporarily overridden by the option PBX sends Called Numbers with Trunk Code option of the Telematic APL settings.

The XPR server is in most cases linked up with the connected PBX via a tie line. **CalledNumberWithTrunkCode** defines whether the active PBX transfers the associating trunk code to the XPR server within the called number.

CallingNumberNoExtPrefix

Default:	<i>false</i>
Possible values:	<i>false</i> – External prefix is not transferred by the PBX <i>true</i> – External prefix is transferred by the PBX
Mode:	in, read
Remark:	Is temporarily overridden by the Calling Numbers of unknown type without external line prefix option of the Telematic APL settings.

In a PBX a digit for setting up external communication connections is defined in most cases. This digit is called external prefix or outside line dialing number.

CallingNumberNoExtPrefix defines whether the connected PBX transfers this external prefix to the XPR server with an originator number of the phone number format '*Unknown*'.

DirectLin

Default:	<i>false</i>
Possible values:	<i>false</i> – XPR server is not directly connected to the PSTN <i>true</i> – XPR server is directly connected to the PSTN
Mode:	in, read

Defines whether the XPR server is directly connected to the PSTN or e.g. via a PBX.

HP8000

Default:	<i>false</i>
Possible values:	<i>false</i> – Leading zero in the normalized phone number format <i>true</i> – No leading zero in the normalized phone number format
Mode:	in, read
Remark:	If the XPR server is used at OpenScape Voice, this variable must be set to value <i>true</i> for each NCO location.

When communicating with the XPR server, some PBXs use a normalized phone number format without leading zero (*Example OpenScape Voice: 492404901100*). In this case the default NCO rules for telematics connections deliver wrong normalization and localization results and need to be adapted.

To adjust the NCO rules, the NCO variable [HP8000](#) must be set to *true*.

MWIExtensionLength

Default:	–
Possible values:	< <i>number</i> >
Mode:	in, read, write, out

Defines whether a MWI phone number is reduced to the length of a fixed phone number. The number specified here defines the resulting, shortened phone number length.

SkipCalledNumberDigits

Default:	0
Possible values:	< <i>number</i> >
Mode:	in, read, write, out

Defines the number of digits to be skipped in an incoming called number with the transfer of this number.

SkipRedirectingDigits

Default:	0
Possible values:	< <i>number</i> >
Mode:	in, read

Defines the number of digits to be skipped in a 'redirecting number' with the transfer of this number.

SMSCProtocol

Default:	–
Possible values:	TAP – Enables NCO adjustments for the TAP protocol. UCP – Enables NCO adjustments for the UCP protocol. GSM – Enables NCO adjustments for the GSM protocol. IP – Enables NCO adjustments for the IP protocol.
Mode:	in, read

The XPR server can send SMS messages via one of the following APLs:

- ISDNAPL
- SMS APL

In the process each of these APLs supports only specific transmission protocols, which, in turn, make individual demands on the normalization respectively localization of SMS addresses. Such individual demands are realized by appropriate NCO adjustments.

Via the **SMSCProtocol** variable you can set which adjustments NCO is to use for the normalization respectively localization of SMS addresses.

For selecting the correct setting the following hints apply:

- TAP and UCP are used by the ISDN APL
- GSM and IP is used by the SMS APL

If you use the ISDN APL to send SMS messages you may need to clear with your SMS provider which of the possible protocols to configure.

TypeOfNumber

Default:	–
Possible values:	International – Intern. phone number format (e.g. 492404901100) National – Nation. phone number format (e.g. 2404901100) Subscriber – Code format (e.g. 901100) Unknown – Unknown phone number format (e.g. 100)
Mode:	in, read, write, out

An ISDN phone number can be transmitted between two systems in different formats. **TypeOfNumber** defines in which phone number format the simultaneously transferred phone number is available.

UseTypeInternational

Default:	<i>false</i>
Possible values:	<i>false</i> – Phone numbers will not be transferred in the intern. format <i>true</i> – Phone numbers will be transferred in the intern. format
Mode:	in, read
Remark:	Is temporarily overridden by the International Format for Called Number or International Format for Calling Number option of the Telematic APL settings.

Defines whether the XPR server transfers phone numbers in international format (e.g. 492404901100) to a system connected via the NCO client.

Variables of the XML APL client

XMLMinInternationalLength

Default:	12
Possible values:	<Phone number length>
Mode:	in, read, write, out
Remark:	Is only considered if the XMLUserDialsExternalPrefix variable has value <i>false</i> . Works in combination with XMLMinNationalLength .

If a phone number is transferred to the XPR server via the XML APL, this variable defines from which digit length NCO interprets this phone number as international number.

XMLMinNationalLength

Default:	10
Possible values:	<Phone number length>
Mode:	in, read, write, out
Remark:	Is only considered if the XMLUserDialsExternalPrefix variable has value <i>false</i> . Works in combination with XMLMinInternationalLength .

If a phone number is transferred to the XPR server via the XML APL, this variable defines from which digit length NCO interprets this phone number as national number.

XMLUserDialsExternalPrefix

Default:	<i>true</i>
Possible values:	<i>false</i> – Phone numbers will be normalized in dependency on their length <i>true</i> – Phone numbers will be normalized irrespectively of their length
Mode:	in, read

If this variable has value *true*, phone numbers for external destinations must always be transferred to the XML APL in one of the following formats:

- in normalized format
- with the leading external prefix 0.

NCO will then normalize incoming phone numbers according to the following scheme:

+	External Prefix	National Prefix	Internat. Prefix	Country Code	Area Code	Number	Normalized as ...
+						100	Internal phone number
+	0					901100	Local phone number with external prefix

+	External Prefix	National Prefix	Internat. Prefix	Country Code	Area Code	Number	Normalized as ...
+	0	0			2404	901100	National phone number with external and national prefix
+	0		00	49	2404	901100	International phone number with external and international prefix
+				49	2404	901100	Phone number already normalized

If this variable has value *false*, NCO normalizes incoming phone numbers based on the variable settings of [XMLMinInternationalLength](#), [XMLMinNationalLength](#) and [Location.MaxExtensionLength](#).

NOTE:

If in this case a leading + character is transferred with the phone number, it will be removed before the phone number normalization.

9.9.13.3 Variables in the Corporate Network Area

CNConversion

Default:	–
Possible values:	<i>true</i> – The conversion concerns two corporate network locations
Mode:	READ

Defines whether the current phone number conversion concerns the communication between two corporate network locations.

This evaluation occurs by the Corporate Network preprocessing rule used. Cf. [Section 9.7.2, “Corporate Network Rules”, on page 420](#).

CNDestPublicID

Default:	–
Possible values:	<phone number>
Mode:	READ

Defines the public ID of the Corporate Network destination location.

The allocation of this variable occurs by the Corporate Network preprocessing rule used. Cf. [Section 9.7.2, “Corporate Network Rules”, on page 420](#).

CNOrgLocationID

Default:	–
Possible values:	See description
Mode:	IN

Defines the location information the basis on which a phone number is localized.

The following two predefined values are currently supported:

- *CNUseNCOLocation*
The information of the assigned NCO location is used for localization.
- *CNNoOrgLocation*
No individual Corporate Network information is used for the localization.
The localization is performed as would be done without the existence of a Corporate Network environment.

Furthermore, individual contents of the following format can be assigned to this variable:

- *<Location Name>*
Defines the name of a configured NCO location.
- *<Phone Number>*
Defines a normalized phone number that uniquely describes an NCO location. E.g. +492404901100.

CNOrgToDestPrefix

Default:	–
Possible values:	<i><Corporate Network prefix></i>
Mode:	READ

Defines the trunk code that connects the originator location to the destination location in the desired communication direction.

The allocation of this variable occurs by the Corporate Network preprocessing rule used. Cf. [Section 9.7.2, “Corporate Network Rules”](#), on [page 420](#).

Variables under *CNOrgLocation*

CNOrgLocation.AreaCode

Default:	–
Possible values:	<Area code>
Mode:	READ

Defines the area code of the Corporate Network originator location without leading zero.

Example: 2404 for Alsdorf.

CNOrgLocation.CountryCode

Default:	–
Possible values:	<country code>
Mode:	READ

Defines the country code of the Corporate Network originator location without leading zeros or plus signs. For example 49 for Germany.

CNOrgLocation.ExtensionCode

Default:	–
Possible values:	<extension>
Mode:	READ

Defines the extension under which the XPR server can be reached at the Corporate Network originator location. **ExtensionCode** is only defined if the XPR server is not operated behind a PBX but at a point to multi-point connection.

CNOrgLocation.ExternalPrefix

Default:	–
Possible values:	<external prefix>
Mode:	READ

Defines the external prefix (*outside line dialing number*) used in the connected PBX of the Corporate Network originator location. In Germany this is in most cases digit 0.

CNOrgLocation.InternationalPrefix

Default:	–
Possible values:	< <i>international prefix</i> >
Mode:	READ

Defines the international prefix (*international separation number*) used in the connected PBX of the Corporate Network originator location. In Germany this is in most cases the two digits 00.

CNOrgLocation.MaxExtensionLength

Default:	–
Possible values:	< <i>number</i> >
Mode:	READ

Defines the maximum length of the extensions for the PBX in the Corporate Network originator location.

CNOrgLocation.Name

Default:	–
Possible values:	< <i>string</i> >
Mode:	READ

Defines the name of the Corporate Network originator location.

CNOrgLocation.NationalPrefix

Default:	–
Possible values:	< <i>national prefix</i> >
Mode:	READ

Defines the national prefix (*national separation number*) used in the connected PBX of the Corporate Network originator location. In Germany this is in most cases digit 0.

CNOrgLocation.RangeCode

Default:	–
Possible values:	<phone numbers>, colon (:), semicolon (;), hyphen (–)
Mode:	read, range

Defines the range list of a Corporate Network's originator location range code. The calling numbers thus described are then externally accessible.

If no range code is defined, all calling numbers are accessible externally.

CNOrgLocation.SubscriberCode

Default:	–
Possible values:	<subscriber code>
Mode:	READ

Defines the subscriber code of the Corporate Network originator location.

CNOrgLocation.TrunkCode

Default:	–
Possible values:	<trunk code>
Mode:	READ

Defines the trunk code under which the XPR server at the Corporate Network originator location is addressed within the PBX.

Variables under *CNDestLocation***CNDestLocation.AreaCode**

Default:	–
Possible values:	<Area code>
Mode:	READ

Defines the area code of the Corporate Network destination location without leading zero.

Example: 2404 for Alsdorf.

CNDestLocation.CountryCode

Default:	–
Possible values:	<country code>
Mode:	READ

Defines the country code of the Corporate Network destination location without leading zeros or plus signs. For example 49 for Germany.

CNDestLocation.ExtensionCode

Default:	–
Possible values:	<extension>
Mode:	READ

Defines the extension under which the XPR server can be reached at the Corporate Network destination location. **ExtensionCode** is only defined if the XPR server is not operated behind a PBX but at a point to multi-point connection.

CNDestLocation.ExternalPrefix

Default:	–
Possible values:	<external prefix>
Mode:	READ

Defines the external prefix (*outside line dialing number*) used in the active PBX of the Corporate Network destination location. In Germany this is in most cases digit 0.

CNDestLocation.InternationalPrefix

Default:	–
Possible values:	<international prefix>
Mode:	READ

Defines the international prefix (*international separation number*) used in the connected PBX of the Corporate Network destination location. In Germany this is in most cases the two digits 00.

CNDestLocation.MaxExtensionLength

Default:	–
Possible values:	<number>
Mode:	READ

Defines the maximum length of the extensions for the PBX in the Corporate Network destination location.

CNDestLocation.Name

Default:	–
Possible values:	<string>
Mode:	READ

Defines the name of the Corporate Network destination location.

CNDestLocation.NationalPrefix

Default:	–
Possible values:	<national prefix>
Mode:	READ

Defines the national prefix (*national separation number*) used in the connected PBX of the Corporate Network destination location. In Germany this is in most cases digit 0.

CNDestLocation.RangeCode

Default:	–
Possible values:	< <i>phone numbers</i> >, colon (:), semicolon (;), hyphen (–)
Mode:	read, range

Defines the range list of a Corporate Network's destination location range code. The calling numbers thus described are then externally accessible.

If no range code is defined, all calling numbers are accessible externally.

CNDestLocation.SubscriberCode

Default:	–
Possible values:	< <i>subscriber code</i> >
Mode:	READ

Defines the subscriber code of the Corporate Network destination location.

CNDestLocation.TrunkCode

Default:	–
Possible values:	< <i>trunk code</i> >
Mode:	READ

Defines the trunk code under which the XPR server at the Corporate Network originator location is addressed within the PBX.

9.9.13.4 Variables in the *Location Area*

AreaCode

Default:	–
Possible values:	<Area code>
Mode:	READ

Defines the area code of the relevant location without leading zero.

Example: 2404 for Alsdorf.

CountryCode

Default:	–
Possible values:	<country code>
Mode:	READ

Defines the country code of the relevant location without leading zeros or plus characters. For example 49 for Germany.

ExtensionCode

Default:	–
Possible values:	<extension>
Mode:	READ

Defines the extension under which the XPR server can be reached.

ExtensionCode is only defined if the XPR server is not operated behind a PBX but at a point to multi-point connection.

ExternalPrefix

Default:	–
Possible values:	<external prefix>
Mode:	READ

Defines the external prefix (*outside line dialing number*) used in the connected PBX. In Germany this is in most cases digit 0.

InternationalPrefix

Default:	–
Possible values:	<international prefix>
Mode:	READ

Defines the international prefix (*international separation digit*) used in the connected PBX. In Germany this is in most cases the two digits 00.

Location.DialAlwaysArea

Default:	<i>false</i>
Possible values:	<i>false</i> – The area code is not always transferred to the PBX <i>true</i> – The area code is always transferred to the PBX
Mode:	READ

Defines whether the area code is also transferred to the active PBX by the XPR server for communication requests in the same local network.

Location.HasRange

Default:	–
Possible values:	<i>false</i> – The location does not have a range list <i>true</i> – The location has at least one range list
Mode:	READ

Defines whether the relevant location is assigned a range list.

Location.IsCorporateNetworkSite

Default:	<i>false</i>
Possible values:	<i>false</i> – The location does not belong to an XPR corporate network <i>true</i> – The location belongs to an XPR corporate network
Mode:	READ

Defines whether a location belongs to a XPR corporate network.

Location.MaxExtensionLength

Default:	–
Possible values:	<number>
Mode:	READ

Defines the maximum length of the extensions for the PBX of the relevant location.

Location.Name

Default:	–
Possible values:	< <i>string</i> >
Mode:	READ

Defines the name of the relevant location.

Location.PrivateNumbers

Default:	–
Possible values:	< <i>phone numbers</i> >, comma (,), hyphen (–)
Mode:	read, location, range

Defines phone numbers normalized into a private phone number format as number range list.

NationalPrefix

Default:	–
Possible values:	< <i>national prefix</i> >
Mode:	READ

Defines the national prefix (*national separation digit*) used in the connected PBX. In Germany this is in most cases digit 0.

RangeCode

Default:	–
Possible values:	< <i>phone numbers</i> >, colon (:), semicolon (;), hyphen (–)
Mode:	read, range

Defines the range list of a location's range code. The calling numbers thus described are then externally accessible.

If no range code is defined, all calling numbers are accessible externally.

SubscriberCode

Default:	–
Possible values:	< <i>subscriber code</i> >
Mode:	READ

Defines the subscriber code of the relevant location.

TrunkCode

Default:	–
Possible values:	< <i>trunk code</i> >
Mode:	READ

Defines the trunk code under which the XPR server of the relevant location within the PBX is addressed.

TrunkPrefix

Default:	–
Possible values:	< <i>trunk code</i> >
Mode:	READ

Particularly networking PBXs via cross connections may require the XPR server to add a trunk code to the phone number to be dialed.

TrunkPrefix defines such a trunk code.

A trunk prefix needs to be configured only rarely.

9.9.13.5 Variables in the *Others* Area

AcceptOldNormNumber

Default:	–
Possible values:	<i>false</i> – Old phone number formats are correctly normalized <i>true</i> – Old phone number formats are not correctly normalized
Mode:	in, read, write, out

After upgrading a server to a version greater or equal XPR 4.0, external databases may still contain numbers not supported with this new version any more (e.g. 492404...). The default conversion of such numbers with the rules of the relevant NCO clients leads however to wrong results (e.g. +492404492404). The reason for this is that the NCO rules recognize these phone numbers as local network numbers.

Therefore, the *AcceptOldNormNumber* variable is automatically generated with a server upgrade and allocated with the *true* value. This results in the correct conversion of the old format phone numbers by the default rules of the relevant NCO clients.

With this setting, however, the local-network numbers of the supported new format are not correctly normalized. Therefore this variable must immediately be removed again after the resetting of the external databases.

The *AcceptOldNormNumber* variable can also be created manually and independently from the above server update, and be allocated with value *true*. Users can then use phone numbers of the old format in the XPR server GUI and TUI.

AddExternalPrefix

Default:	–
Possible values:	<i>false</i> – Does not insert an external prefix <i>true</i> – Inserts an external prefix
Mode:	in, read, write, out

Defines whether the external prefix of the location is attached to the external calling number after the localization.

DialAlwaysArea

Default:	<i>false</i>
Possible values:	<i>false</i> – The area code is not always dialed <i>true</i> – The area code is always dialed
Mode:	in, read, write, out

In some countries the associating area code must be dialed even if the connection is set up in the same local network.

DialAlwaysArea defines whether the area code is always dialed.

EnablePostDialing

Default:	<i>true</i>
Possible values:	<i>false</i> – Disables the processing of the \$ character for Fax G3 post dialing <i>true</i> – Enables the processing of the \$ character for Fax G3 post dialing
Mode:	in, read, write, out

If the telematics protocol FAX G3 post dialing is enabled for the XPR server, phone numbers may contain the \$ character. So that phone numbers with this character can be correctly localized respectively normalized, the **EnablePostDialing** variable must be set to *true*.

GUISeparator

Default:	< <i>blank</i> >
Possible values:	< <i>character</i> >
Mode:	in, read, write, out

Defines a character to separate calling numbers in case of GUI entries.

GUIUserDialsExtPrefix

Default:	<i>false</i>
Possible values:	<i>false</i> – The GUI user does not dial the external prefix <i>true</i> – The GUI user dials the external prefix
Mode:	in, read, write, out

Defines whether the GUI user dials the external prefix (outside line dialing number).

In case of a calling number conversion this variable is allocated with the content of the associating NCO_GUI_PREFIX field of the correlation database. This information can subsequently be evaluated by the conversion rules.

MaxExtensionLength

Default:	–
Possible values:	< <i>number</i> >
Mode:	in, read, write, out

Defines the maximum length of the internal calling numbers. Numbers that exceed this length are not recognized as internal calling numbers.

PurposeOfNumber

Default:	–
Possible values:	See description
Mode:	in, read

Phone numbers can have different descriptions depending on their purpose.

The valid descriptions for the phone number purpose are:

- Called
- Called.CalledParty
- Called.DiversionDestination
- Called.DivertedParty
- Called.MWIReceivingParty
- Called.CallCompletionParty
- Called.CallTransferDestination
- Called.Extension
- Calling
- Calling.CallingParty
- Calling.RedirectingParty
- Calling.DiversionActivator
- Calling.MWIActivator
- Calling.CallTransferOriginator
- Calling.ConnectedParty
- Calling.Extension
- MonitorPoint

TUIUserDialsExtPrefix

Default:	<i>false</i>
Possible values:	<i>false</i> – The TUI user does not dial the external prefix <i>true</i> – The TUI user dials the external prefix
Mode:	in, read, write, out

Defines whether the TUI user dials the external prefix (outside line dialing number).

In case of a calling number conversion this variable is allocated with the content of the associating NCO_TUI_PREFIX field of the correlation database. This information can subsequently be evaluated by the conversion rules.

UIDialAlwaysArea

Default:	<i>false</i>
Possible values:	<i>false</i> – The area code is not always dialed <i>true</i> – The area code is always dialed
Mode:	in, read, write, out

So that long internal phone numbers are differentiated from short external local network numbers, the associating area code may have to be dialed as well.

The *UIDialAlwaysArea* defines in this context whether the area code is additionally dialed at the user interfaces.

10 Telematics APL

NOTE:

The OpenScape Voice PBX used to be called HiPath 8000 before product version 3.1 R2. General OpenScape Voice information applies in this chapter also for the previous version HiPath 8000.

This chapter describes the telematics APLs made available by the XPR server.

Telematics APLs provide logical interfaces via which the XPR server communicates with PBXs. Among such APLs you find the following ones:

- ISDNAPL
- IP APL

Telematics services enabled by these XPR modules are, for example, Fax G3, Fax G4 or programmable voicemail systems such as *Ergo* or *PhoneMail*. Type and range of the provided services depend on the corresponding APL.

The information contained in this chapter is divided into the following sections:

- [General Technological Concepts](#)
- [Technological Concepts of the ISDN APL](#)
- [Technological Concepts of the IP APL](#)
- [Protocols of the XPR Server](#)
- [General Configuration of Telematics Services](#)
- [Telematics Service Configuration Example Scenarios](#)
- [Specific Solutions with the Telematics APL](#)
- [Creating a new SIP Certificate for the XPR Server](#)
- [Configuration Reference for ISDN Connections \(ISDN APL\)](#)
- [Configuration Reference for Voice-over-IP Connections \(IP APL\)](#)
- [Ending Telematics APLs “softly”](#)

10.1 General Technological Concepts

The following sections describe special technological concepts relevant for general telematics APL usage.

These are the sections:

- [Telematics Program Libraries](#)
- [Number Conversion Objects \(NCO\)](#)
- [Trusted Transfer Mode \(TTM\)](#)
- [Voice Mail Networking](#)
- [Redirecting Numbers](#)
- [Features of D-channel Protocols](#)
- [Memory Requirements for Voice Messages](#)
- [Call Attached Data \(CAD\)](#)

10.1.1 Telematics Program Libraries

10.1.1.1 The Modules *TeleReg* and *TeleReg API*

TeleReg realizes a static registry structure storing the configuration data of all telematics APLs. Furthermore, it interprets diverse reading and writing functions enabling access to this registry structure. These features are provided by the interface module TeleReg API.

For a list and description of all TeleReg registry values please refer to [Section E.20.1, “Registry Keys of the TeleReg”, on page 1860](#).

10.1.1.2 The Modules *TeleCfg* and *TeleCfg API*

The TeleReg is supplemented by the TeleCfg. It is the basis for GUI-based APL configuration and interprets the configuration features of all telematics APLs. The TeleCfg API module realizes the features for the APL configuration.

As a result, the GUI dialogs for the installation of the ISDN and IP APL look the same. This facilitates the configuration.

The configuration data are exchanged between the XPR monitor and the XPR server in compressed format. This enables a sufficiently fast remote administration also via lines with lower bandwidths.

10.1.1.3 The Modules *TeleLib* and *TeleLib API*

In addition to TeleReg and TeleCfg, TeleLib represents the third telematics program library. It interprets function calls of the different XPR server E-scripts. The TeleLib API provides the respective program functions.

10.1.2 Number Conversion Objects (NCO)

NCO describes a concept for phone number handling within the XPR server and is the successor to the previous DNO rules. It owes its name to the definition of so-called Number Conversion Objects, which form the central component for the NCO implementation.

NCO describes a quite complex part of the XPR server. For this reason we only deal with the basic NCO configuration in interaction with a telematics configuration. Additional information on the NCO concept is found in [Chapter 9, “Number Conversion Object \(NCO\)”](#).

10.1.2.1 Normalized and localized Calling Number Format

The central XPR server task is to evaluate and process the messages received by the connected systems. In this process, address and calling number information transmitted along with messages is particularly important in the telematics environment.

The phone number information format often varies with the messages structured according to the system. Therefore, a system-depending phone number conversion is required. The phone numbers received by the XPR server and subsequently converted are administered within the server in this defined format – the normalized phone number format (e.g. +492404901100 or p245) – during the following message processing.

In transmission direction the XPR server must convert a previously normalized phone number in a format that can evaluate the external target system. This process is also called localization. The result of this calling number conversion is the local calling number format.

Normalization as well as localization is always performed by the XPR server module that forms the interface to the corresponding external system. In our case by the respective telematics APL used.

In NCO the modules that perform the calling number conversions are called NCO clients.

10.1.2.2 The NCO Elements

Let us take a look at the elements defined in NCO, forming the base for calling number normalization and localization. We will provide a short overview at this point. More detailed information is available in [Chapter 9, “Number Conversion Object \(NCO\)”](#).

Number Conversion Object (NCO)

The Number Conversion Objects (NCO) are the central NCO modules. Each NCO combines the following four elements:

- A location
- A rule set for phone number normalization
- A rule set for phone number localization
- A call type checker

By defining different NCOs, calling numbers can be normalized or localized in different ways.

Location

The term location describes all necessary phone number information required to determine its exact 'position' in the international hierarchical communication network. This information is the basis for a correct phone number localization or normalization.

Location codes and location prefixes are location information elements.

Amongst others, the following standard codes are available:

- Country code
Defines the country code of the relevant location.
- Area code
Defines the area code of the relevant location.
- Subscriber code
Defines the subscriber code of the relevant location.
- Trunk code
Defines *only* the trunk code under which the XPR server is connected to a PBX. This code is passed from the PBX to the XPR server with phone number transfers if required.

The following location prefixes are available:

- **International prefix**
The international prefix informs the communication network that the upcoming calling number begins with a country code and requests an international remote connection.
- **National prefix**
The national prefix informs the communication network that the upcoming calling number begins with an area code and requests a national remote connection.
- **External prefix (outside line dialing number)**
The external prefix defines a digit dialed by a subscriber to establish an outside line connection at the PBX.
- **Trunk prefix**
Networking PBXs via cross connections may particularly require the XPR server to add a trunk prefix to the phone number to be dialed. This number can be defined under the trunk prefix.
A trunk prefix needs to be configured only rarely.

Normalization rule set

The normalization rule set defines the rules according to which the XPR server converts the phone numbers it receives.

Localization rule set

The localization rule set defines the rules according to which the XPR server converts the phone numbers it sends to external systems or assigns to a user.

Call type checker

On the basis of location information the call type checker determines the call type of a phone number transferred to it. This information can be used for checking the privileges that can be configured in the XPR server for users.

Possible connection types are *internal*, *local*, *national*, *international* and *unknown*.

NCO clients

All XPR server modules that communicate with external systems are counted among NCO clients. In this function they serve among other things for normalizing or localizing received phone numbers.

Connect points

Each NCO client provides defined, by its implementation determined connect points. These are automatically defined with the establishment of a client resource (e.g. a trunk group in case of the ISDN APL), and are thus available for further configuration. For instance, the ISDN APL automatically defines an associated connect point with the configuration of each new trunk group. The notation of its name is *<device number>.<trunk group number>*.

By the later assignment of connect point and NCO, an individual NCO can be allocated for a single NCO client resource. This NCO will then determine the format of the corresponding phone number conversion.

10.1.3 Trusted Transfer Mode (TTM)

You can connect the PhoneMail or Ergo application of an XPR server to OpenScape UC Application via the Trusted Transfer Mode. This extends the scope of the Unified Messaging features of the PhoneMail or Ergo script by the Unified Communications features of OpenScape UC Application.

Connecting an XPR server to the OpenScape UC Application system via the Trusted Transfer Mode integrates the relevant Unified Communications features of OpenScape UC Application in the PhoneMail or Ergo user menu of the XPR server. The user will not realize whether a selected feature is enabled by the OpenScape Xpressions V7 server or by OpenScape UC Application. He/she will receive the impression as if working with a Unified Communications system centrally providing all available features.

10.1.3.1 How the Trusted Transfer Mode operates

The Trusted Transfer Mode communicates via the standard protocol IP. If an XPR user dials into the PhoneMail or Ergo application and uses an OpenScape UC Application feature there, the XPR server routes the call of the XPR user to the user access of the OpenScape UC Application voice portal. There, the XPR user is automatically authenticated without any further user input. Subsequently, the XPR user will directly hear from OpenScape UC Application the voice menu appropriate for the selected feature.

The XPR server transfers various information to OpenScape UC Application with the call. The XPR server encodes this information in the originator number of the forwarded call with using the Trusted Transfer Mode phone number format (TTM phone number format) for encoding:

The TTM phone number format has the following general structure:

<Start character><Trusted Domain><Original system><User Information>

The various elements of the TTM phone number format specify:

- **Start character**

The start character is an indicator for the XPR and UC Application components to recognize the relevant phone number as TTM phone number. The start character can be, for example, the * character or any other non-numerical character

- **Trusted Domain**

Specifies the ID of the system that has created the relevant phone number. This ID is evaluated by the system that receives the information. Forwarded calls with invalid ID will not be accepted by the target system.

- **Original system**

The original system defines from which system the trusted transfer was induced.

- From the XPR server when an XPR user under PhoneMail or Ergo switches to OpenScape UC Application features.
- From OpenScape UC Application when the XPR user switches back to the PhoneMail or Ergo features.

- **User Information**

The User Information specifies:

- The original phone number of the caller (ANI)

NOTE:

The ANI is always transferred in the E.164 format. Thus normalized with country code etc.

- The voice box number of the user (user ID)
- The TUI User Entry Point in the original voicemail system
- The user language

The calling number schema defines the format for the different elements of the TTM phone number format (cf. [Section 10.1.3.2, “Calling Number Schema”, on page 534](#)).

10.1.3.2 Calling Number Schema

If a call is forwarded from the XPR server to OpenScape UC Application or vice versa as Trusted Transfer Mode, different information must be exchanged between the XPR server and OpenScape UC Application with the forwarding (cf. [Section 10.1.3.1, “How the Trusted Transfer Mode operates”, on page 532](#)). The calling number schema specifies in which format this information is exchanged.

The calling number schema consists of the start character to be used and several consecutive sections in the format:

%<Argument Index>\$<Argument Length>

The single elements of a section specify:

- **Argument Index**
A running number that serially numbers the different consecutive arguments of the user information.
- **Argument Length**
The permanent data length of the relevant argument.

Example:

Fixed phone number format:

<S><TD><ORG><ANI><UID><OTUI><LNG>

Calling number schema:

p*%1\$2%2\$1%3\$4%4\$4%5\$2%6\$1

Originator number:

*9055485548616

Decoded this results in:

- Start sign (S) : *
- Trusted Domain (TD) : 9
- Original system (ORG) : 0
- ANI : 5548

NOTE:
If the extension features different lengths, dial the longest one.

- User ID (UID) : 5548

NOTE:
The user ID corresponds to the voicebox number entered for the relevant user in the **VOICE** database field of the XPR Correlation database. In a TTM system environment, the length of this number may vary with the user. In this case the longest of possible user ID lengths must be configured for the user ID argument in the calling number schema.

- Original TUI User Entry Point (OTUI) : 61
- Language (LNG) : 6
 - If you use one of the following languages, you need to configure at least length **1** for this argument:
 - German (Trace-ID=0)
 - English (UK) (Trace-ID=1)
 - French (Trace-ID=2)
 - Italian (Trace-ID=3)
 - Spanish (Trace-ID=4)
 - Dutch (Trace-ID=5)
 - English (US) (Trace-ID=6)
 - If you use one of the following languages, you need to configure length **2** for this argument:
 - Portuguese (Portugal) (Trace-ID=10)
 - Portuguese (Brazil) (Trace-ID=11)
 - Spanish (US) (Trace-ID=12)
 - French (Canada) (Trace-ID=13)
 - Russian (Trace-ID=14)
 - Turkish (Trace-ID=15)
 - Czech (Trace-ID=16)
 - Japanese (Trace-ID=17)
 - Slovenian (Trace-ID=18)
 - Polish (Trace-ID=19)

NOTE:

If the transferred language is not available for the voice portal, the voice portal TUI is played in the language configured as default language for the relevant voice portal access.

In the example, argument length 4 has been configured for parameter 3 (%3) – the example thus works with four-digit extensions.

If you wish to use another length for the extension, you need to configure another argument length for parameters 3 and 4. In doing so please note that the total length of the phone number expression must usually not exceed a maximum length. This length is defaulted by the communications system used.

NOTE:

Maximum lengths for the phone number expression:

- OpenScape Voice: 24 characters
 - HiPath 4000: 22 characters
-

Examples of calling number schemas with different extension lengths:

Extension Length	Calling Number Schema
Three digits	p*%1\$1%2\$1%3\$ 3 %4\$ 3 %5\$2%6\$1
Four digits	p*%1\$1%2\$1%3\$ 4 %4\$ 4 %5\$2%6\$1
Five digits	p*%1\$1%2\$1%3\$ 5 %4\$ 5 %5\$2%6\$1

NOTE:

If you change the calling number schema, you need to perform this change for OpenScape UC Application as well as for the XPR server.

10.1.3.3 Trusted Transfer Mode Specials

If you use the Trusted Transfer Mode you need to consider the following points:

- The XPR server and the OpenScape UC Application must be connected to the same PBX

NOTE:

For the time being the Trusted Transfer Mode has only been approved for usage at OpenScape Voice and HiPath 4000

- The XPR server and OpenScape Voice must be interconnected via an SIP trunk
- The Trusted Transfer Mode supports only 1:1 relations between an XPR server and a UC Application system
- The Trusted Transfer Mode supports only 1:1 relations between a PhoneMail or Ergo entity and a voice portal access number
- The start character (S) in the TTM phone number format must not be removed by the PBX or a gateway between XPR server and OpenScape UC Application.
- PhoneMail or Ergo emits a beep before a user is forwarded from the XPR server to OpenScape UC Application.

10.1.3.4 Activating the Trusted Transfer Mode

Activating the Trusted Transfer Mode in the XPR server requires the following settings:

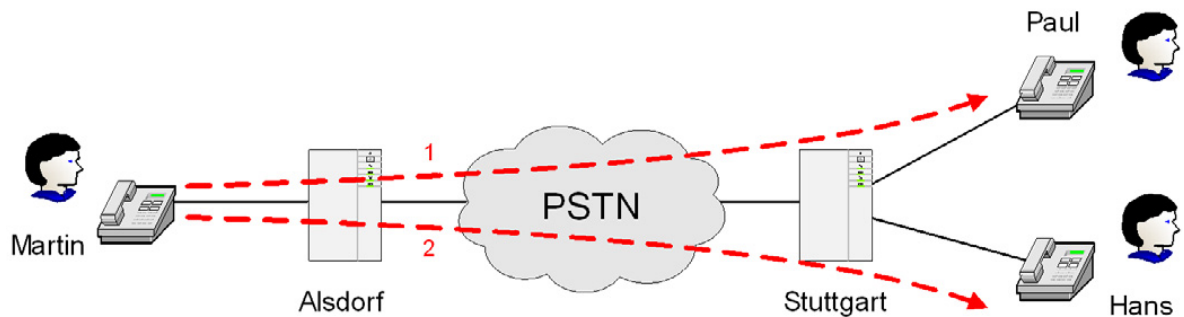
- Add the “-ttm” parameter to the PhoneMail or Ergo configuration for displaying the **OpenScape** tab.
- Close the PhoneMail or Ergo configuration and reopen it. The **OpenScape** tab is now displayed.
- On the **OpenScape** tab, under the PhoneMail or Ergo script configuration, activate the option **OpenScape integration by Trusted Transfer Mode**
- On the **OpenScape** tab, configure the Trusted Transfer Mode setting (cf. [Section 10.4.3.12, “Parameter Tab OpenScape”, on page 649](#))
- Assign all users to deploy the Trusted Transfer Mode the **Trusted Transfer Mode** privilege.

You find information about activating the Trusted Transfer Mode in OpenScape UC Application and about the released PBXs in the documentation for OpenScape UC Application.

10.1.4 Voice Mail Networking

Voice Mail Networking describes concepts for the networking of voice mail systems. Via this networking, sending newly recorded voice mails or voice mails that have been received before is enabled and optimized.

Let's have a look at a simple example:



1. Martin would like to send Paul a voice mail message. Since these two subscribers work with different voice mail systems (Alsdorf and Stuttgart), there is only one choice for Martin. He calls Paul's voice mailbox and leaves a message.

A voice mail that has already been recorded cannot be sent between the respective parties in this scenario. Since the announcement of Paul's voice mailbox would start in such a case, no faultless message transmission would be possible.

2. If Martin wants to accord Hans the same information, he has only one option: he must also call Hans' mailbox and leave the message there as well.

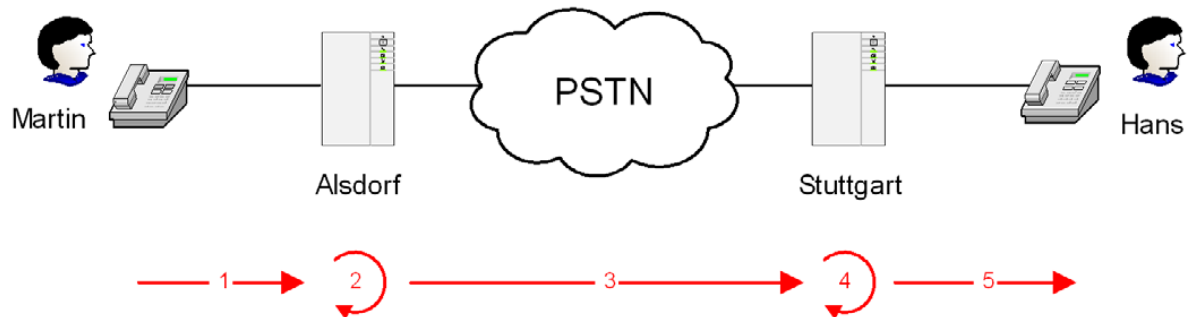
Still, often it would be desirable to send or forward voice mails spanning the locations to single subscribers or whole groups of subscribers. This is enabled via Voice Mail Networking.

Miscellaneous protocols are available for voice mail system networking. These include e.g. AMIS (Audio Messaging Interchange Specification) or VPIM (Voice Profile Internet Mail). The following paragraphs include an overview of the mode of operation of these voice mail networking protocols.

10.1.4.1 AMIS

The AMIS protocol has been developed by the Electronic Messaging Association (EMA) to exchange voice mails between voice mail systems of different manufacturers. It has been defined for analog as well as digital communication and uses the classic PSTN for the message transport.

The following figure gives an overview of the AMIS operating mode.



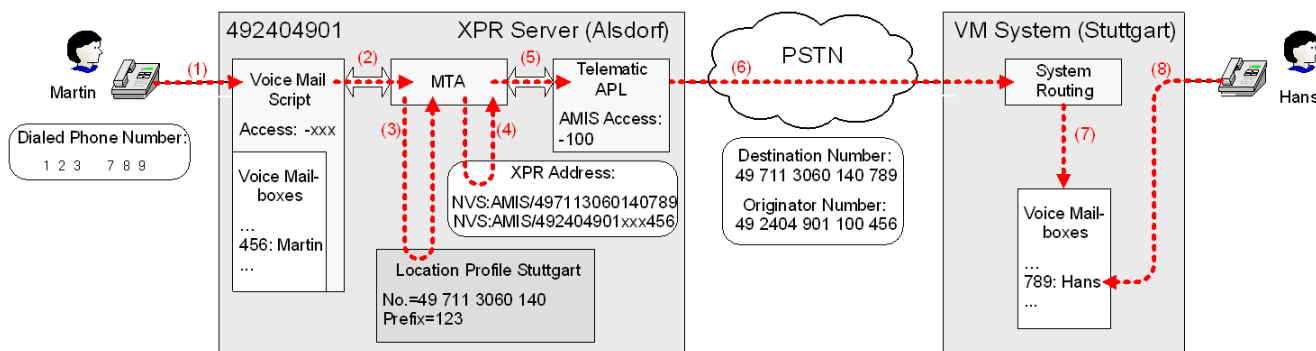
1. Martin as the sending party sets up the connection to his voice mail system. Subsequently, he starts e.g. recording a new voice mail that he wants to send to Hans, who is subscriber to another voice mail system, at a later date.
2. The voice mail system in Alsdorf records the new voice mail. After the recording has been finished, a phone number must be entered to address the recipient so that the message can subsequently be sent.
3. The voice mail system determines the voice mail system of the subscriber who is addressed on the basis of the destination number that has been entered – in our example this is the system in Stuttgart for subscriber Hans. Afterwards, it establishes the connection to the voice mail system in Stuttgart via PSTN. Then, it transmits all required phone number information of the current message via DTMF (phone number of the originator, destination number, etc.) and plays the recorded voice mail via the connection that has been established.
4. The voice mail system in Stuttgart analyzes the transmitted phone number information and records the transmitted message as it is played back. After the end of the transmission the system transmits the message to the voice mailbox of subscriber Hans who has been addressed.
5. Afterwards, Hans can listen to the newly received voice mail after he has entered his voice mailbox.

The voice mail transmission described here can take place between any voice mail systems. It only requires the AMIS protocol support. Thus, the way a system has been implemented or messages are processed internally is of no importance.

Now let us have a closer look at the addressing of the voice mailbox of another voice mail system within a XPR server context. We examine a simple networking of two voice mail systems that communicate via AMIS.

AMIS and XPR Server (Sending)

We start with sending a voice mail from the XPR server to another voice mail system.



Let us have a look at the single steps:

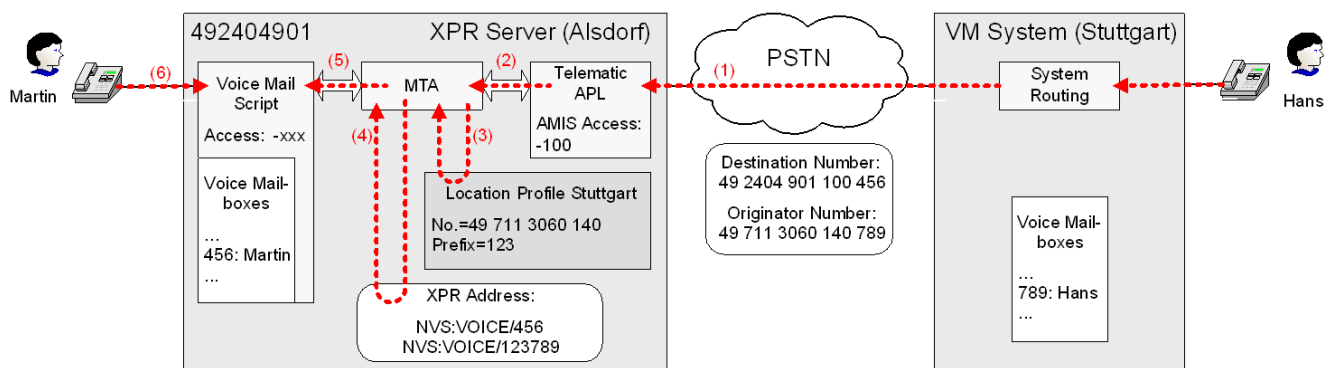
1. Martin has recorded a new voice mail via the applied voice mail script of the XPR server. He is asked who the message is to be sent to. He would like to send it to subscriber Hans at the voice mail system in Stuttgart and therefore enters the destination number **123789** at his telephone. **123** represents the prefix that uniquely identifies every voice mail system – in our case the system in Stuttgart.
In very rare cases voice mail systems can also be uniquely defined via the combination of prefix and assigned extension number range (cf. [Section 10.1.4.1, "Selection of an AMIS prefix", on page 543](#)).
2. The voice mail script now sends the voice mail together with the destination and originator address information to the XPR server MTA. In doing so, it creates the destination address information in the format **NVS:Voice/123789** and the originator address information in the format **NVS:VOICE/456**.
3. During the message transmission, the MTA recognizes by the prefix **123** that the voice mail on hand is an information exchange based on AMIS - with the voice mail system in Stuttgart.
4. The MTA then replaces the prefix **123** in the destination address with the corresponding server phone number **497113060140** – the access number of the voice mail system. Consequently, the destination address is **XNVS:AMIS/497113060140789X**. The phone number of the originator address is normalized by the XPR server. This results in our example in **NVS:VOICE/492404901100 456**.
5. Now routing via the MTA is completed and the message can be forwarded to the telematics APL that is installed for transmission.
6. The telematics APL now establishes a connection to the desired voice mail system via the public telephone network.

7. The routing of this system receives the message and delivers it to the voice mail box with the number **789**.
8. From there, Hans can retrieve it if required.

Sending a voice mail from the XPR server is now complete. Let's have a look at the case of an incoming message.

AMIS and XPR Server (Receiving)

After we have seen in the previous section how voice mails are sent from an XPR server to another voice mail system via AMIS, we will now consider the opposite case.



How is a message received by the XPR server:

1. The XPR server in Alsdorf receives an incoming call for the phone number **49 2404 901 100 456** on the telematics APL that is installed.
2. The incoming information is transmitted to the XPR server MTA for further routing.
3. As the communication comes in via the AMIS protocol (extension **100**), the XPR server searches for a correlating location profile on the basis of the access number of the sending voice mail server. It finds the profile via the prefix **123**.

4. With the help of this information the MTA converts the received originator number from **497113060140 789** to **XNVS:VOICE/123789X**. Thereby an address is created for the originator number to which the recipient Martin can easily reply later on, since it can be resolved by the MTA via the AMIS protocol (see [Section 10.1.4.1, “AMIS and XPR Server \(Sending\)”, on page 541](#)).
Furthermore, the MTA transforms the remote address from **4902404901100456** to **NVS:VOICE/456**.
5. Via this conversion, the incoming message is forwarded to the voice mail script that is configured. Here the remote address is analyzed and the message is forwarded to the mailbox with the phone number **456**.
6. From there, Martin can retrieve it if required.

Selection of an AMIS prefix

As we have seen in the above routing examples, the prefix of the location profile is a crucial parameter for message routing in a voice mail networking. The destination an outgoing voice mail is routed to depends on it. Moreover, it defines the conversion of the originator address of an incoming message.

Therefore, each AMIS-based voice mail server must be addressable uniquely via a corresponding prefix. In this case the XPR server can uniquely identify each location on the basis of its configured prefix. Thus, unique message routing is possible.

Examples of unique prefixes:

Location	Prefix	Voice box range*	Addressing is...
Alsdorf	123	2000-2500	unique
Stuttgart	234	4000-4200	unique
Munich	345	2000-2300	unique

* Corresponds to the entry field *Extension Number Range* in the location profile configuration.

In special cases, the XPR server is also able to identify a location profile because of the unique combination of prefix and addressed voice mailbox. In such a case, the address ranges of the voice mailboxes must by no means not clash between the single servers. If this happens, unique message routing is not guaranteed.

Example of wrong prefixes that are not unique:

Location	Prefix	Voice box range	Addressing is...
Alsdorf	123	2000-2500	unique
Stuttgart	345	4000-4200	not unique
Munich	345	3000-4100	not unique

Example of correct prefixes that are not unique:

Location	Prefix	Voice box range	Addressing is...
Alsdorf	123	2000-2500	unique
Stuttgart	345	4000-4200	unique
Munich	345	3000-3999	unique

IMPORTANT:

You must make sure that no prefix corresponds to the phone number start of a local voice mailbox. If this restriction is not respected, messages might be transferred incorrectly, for the voice mail script might not recognize the prefix. Instead, the message is assigned to the respective local voice mailbox.

Configuration of location profiles

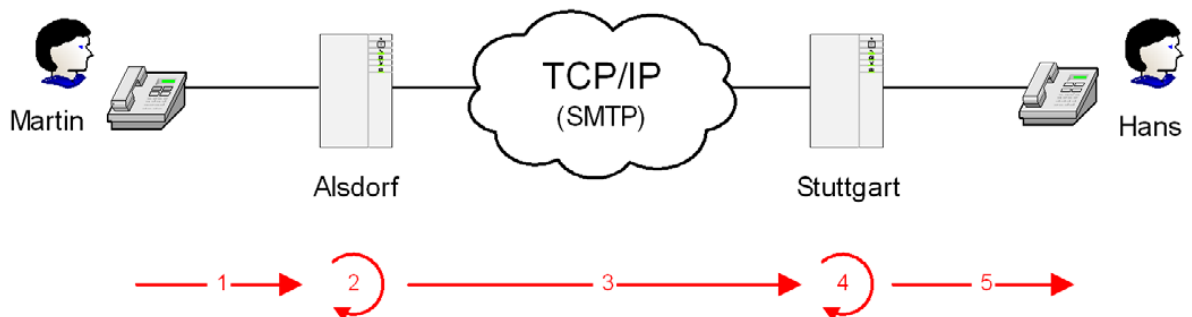
Location profiles are configured via the Web Assistant. See the descriptions in the *Web Assistant* manual on this.

10.1.4.2 VPIM

The VPIM protocol has been developed by the Internet Engineering Task Force (IETF) to exchange voice mails between voice mail systems of different manufacturers. Because of its digital and SMTP-oriented character it offers a high quality possibility for the exchange of voice mails in contrast to AMIS.

The VPIM protocol exists as RFC default. For further information on the protocol specification, please refer to <http://www.ietf.org/>.

The following figure gives an overview of the VPIM operating mode.



1. Martin, as the sending subscriber, establishes the connection to his voice mail system and starts e.g. recording a new voice mail that he wants to send to Hans at a later date. Hans is subscriber to another voice mail system.
2. The voice mail system in Alsdorf records the new voice mail. After the mail has been recorded, the system demands the entry of a recipient number to send the message.
3. The voice mail system determines the voice mail system of the subscriber who is addressed on the basis of the destination number that has been entered – in our example this is the system in Stuttgart for subscriber Hans. Subsequently, the recorded message is sent to the desired voice mail system in Stuttgart via the TCP/IP-based SMTP protocol.
4. The voice mail system in Stuttgart receives the transmitted message and forwards it to the voice mailbox of subscriber Hans who has been addressed.
5. Afterwards, Hans can listen to the newly received voice mail after he has entered his voice mailbox.

Two voice files are transferred for the message exchange via VPIM according to the standard. One contains the spoken originator name. The second file contains the spoken text of the actual message.

VPIM and XPR (sending/receiving)

For sending or receiving voice messages via VPIM, the process is as described for AMIS. Compare [Section 10.1.4.1, “AMIS and XPR Server \(Sending\)”](#), on page 541 or [Section 10.1.4.1, “AMIS and XPR Server \(Receiving\)”](#), on page 542. The only difference lies in the technology with which messages are transferred to the remote voicemail server via the transport network. AMIS uses classic telephone transmission, whereas VPIM uses the internet protocol SMTP as transport medium and thus sends the message practically as e-mail.

The address formats used differ accordingly. While AMIS uses a phone number as server address with PSTN-oriented routing, VPIM uses an SMTP and thus an e-mail address to address the target server.

NOTE:

If the optional feature of a spoken subject is to be used with VPIM, a TTS system must be installed on the XPR server.

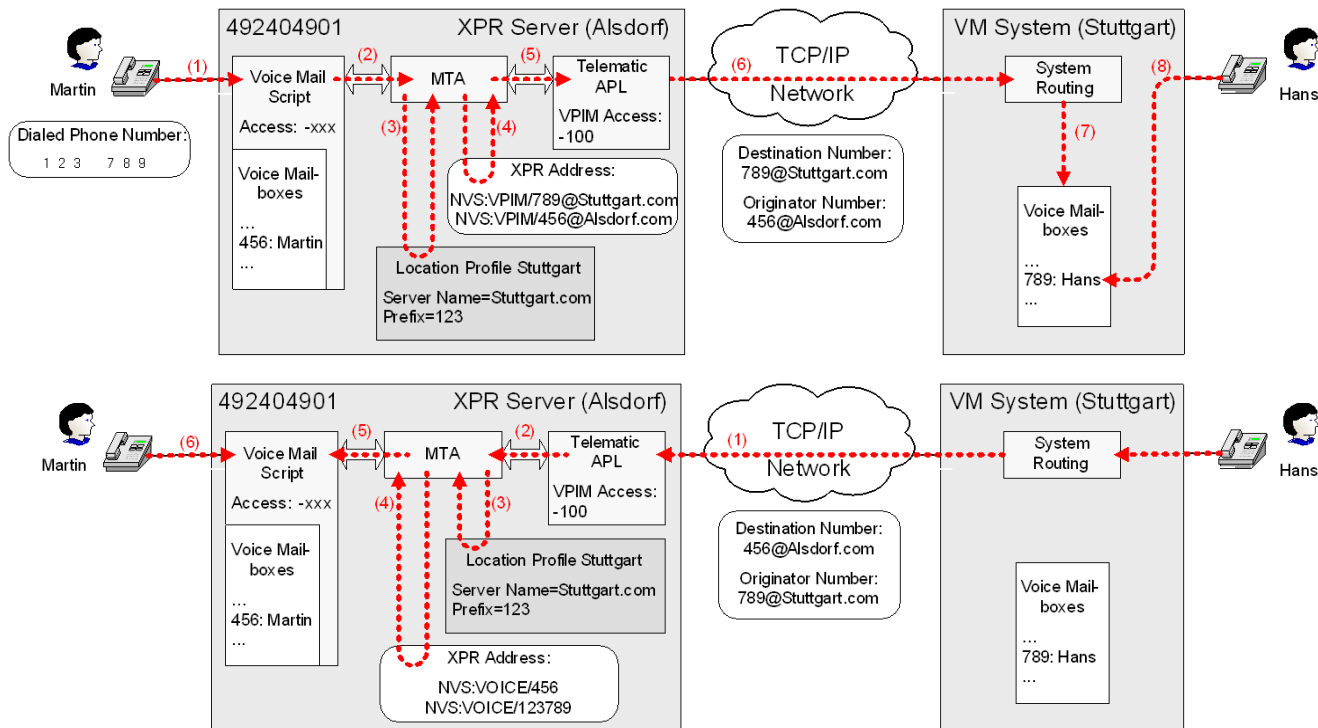
The following table shows a comparison of the address formats used.

Address	AMIS	VPIM
Prefix	<Number> <i>e.g. 123</i>	<Number> <i>e.g. 123</i>
Target Server Address	<Phone number> <i>e.g. 492404901100</i>	<SMTP address> <i>e.g. Stuttgart.com</i>
Voice mailbox (VMB)	<VMB number> <i>e.g. 456</i>	<VMB number> <i>e.g. 456</i>
Telematics address	NVS:VOICE/<tel. number><VMB number> <i>e.g. 492404901100456</i>	NVS:VOICE/<VMB number*>@<SMTP address> <i>e.g. 456@mrs.stuttgart.com</i>

Table 16 Address Formats for the AMIS and VPIM Protocols

* The voice mailbox number of the sending XPR user is always implemented in the VPIM originator number by default. But you can also add the user-individual **VPIM** field to the correlation database of the XPR server. If a different number is then configured for the sending XPR user in this field, it is implemented in the telematic address in the place of the actual voice mailbox number.

The following two figures unfold for the sending and receiving scenario:



Selection of a VPIM prefix

The same requirements apply to prefix assignment as already described for AMIS (cf. [Section 10.1.4.1, "Selection of an AMIS prefix", on page 543](#)).

Configuration of location profiles

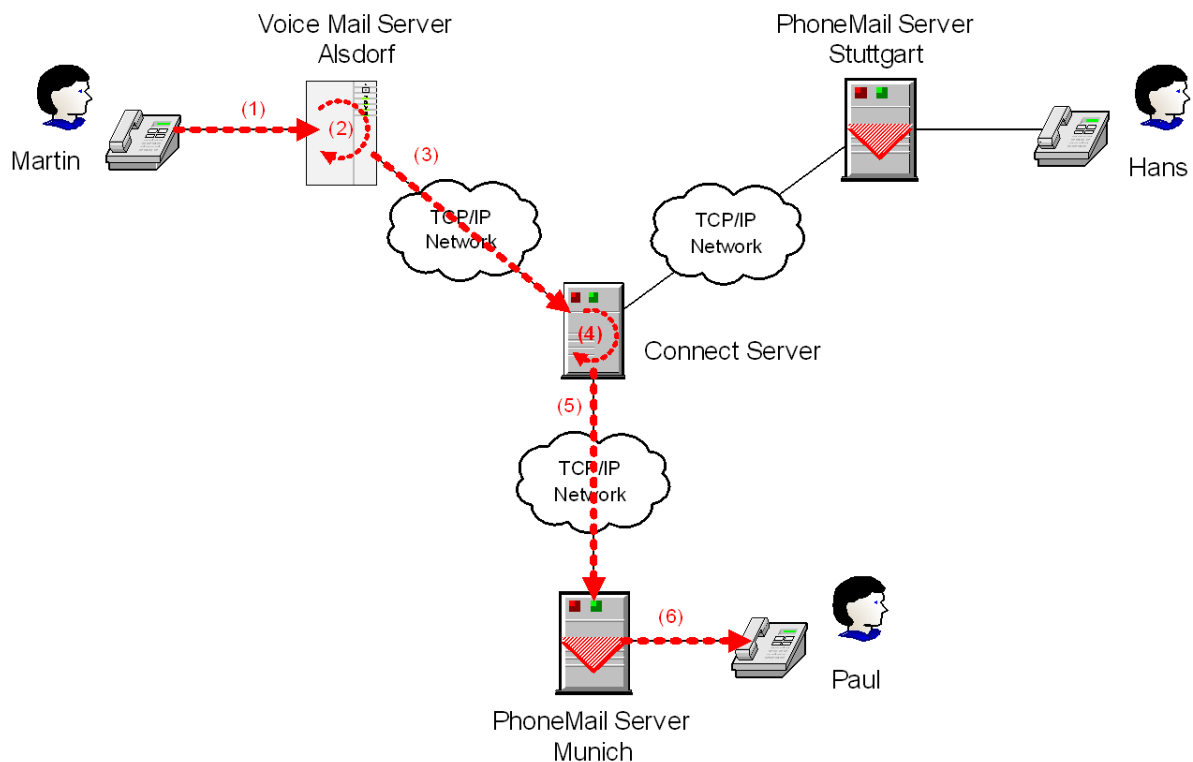
The described locations are configured via the Web Assistant. See the descriptions in the *Web Assistant* manual on this.

10.1.4.3 PhoneMail Connection (Hardware-PhoneMail)

Exchanging voice messages between *hardware-based* PhoneMail systems and an XPR server is enabled via the so-called *connect server*. This connect server is starshapedly connected to all systems that are to exchange messages with each other.

PhoneMail transmits messages between the single voice mail systems on the basis of a transport protocol similar to SMTP. The task of the connect server is to convert the sent voice mails into the WAV format and assume the central routing.

The following figure gives an overview of the functionality of a hardware-based PhoneMail connection to an XPR server. It shows the transmission of a voice message from the XPR server to the PhoneMail server.



1. Martin, as the sending party, sets up the connection to his voice mail system and starts e.g. recording a new voice mail. He wants to send this message to Paul, subscriber of a Phonemail system later on.
2. The voice mail system in Alsdorf records the new voice message. Then it requests the entry of a phone number via which the recipient can be addressed.
3. The voice mail system forwards the message as wav file to the connect server. It uses a protocol that is similar to SMTP and sends the information to be transmitted practically as e-mail.

4. The connect server converts the WAV file into the PhoneMail sound format and
5. then sends the message similarly to the PhoneMail server that has been addressed in the message – in our case the server in Munich. After having received the message, the PhoneMail server in Munich forwards the received message to the voice mailbox of the subscriber Paul who has been addressed.
6. Afterwards, Paul can listen to the newly received voice mail after he has entered his voice mailbox.

In case of the transmission of a voice message from a PhoneMail server to the XPR server, the connect server converts the incoming voice message from the PhoneMail sound format to a WAV file. This can then be sent to the XPR server.

Configuration of location profiles

Location profiles are configured via the Web Assistant. Administrative user privileges are required.

The configuration interface is displayed when you select the **Voice Mail Networking** option under *Special server settings* in the Web Assistant. In order to allow the exchange of messages between XPR users and PhoneMail users, the appropriate PhoneMail locations need to be configured on the XPR server or either a “phantom voice box” for each PhoneMail must be installed on the XPR server. A phantom voice box possesses neither PIN nor password and serves for message routing only.

Therefore, you need to enter *SMTP* in the XPR database field **Preferred**, and the database field **SMTP** must contain the address *IMCEAVOICE-
<nnnnn>@<domain>*. *<nnnnn>* corresponds to the mailbox number under PhoneMail and *<domain>* corresponds to the domain name of the connect server. This way all voice mails that are addressed to a voice mailbox number are forwarded to the connect server.

For each incoming voice mail the user database is searched for a database entry in the **Preferred** field. If *SMTP* is entered here, the voice mail is forwarded to the SMTP APL using the address entered in the *SMTP* database field. The SMTP APL finds the prefix *IMCEAVOICE* in the address and thus knows that the voice mail must be forwarded to the connect server via SMTP.

In order to enable the processing of incoming e-mails of unknown users, the following entry must be added to the routing rules in the MTA:

NVS:SMTP/IMCEAVOICE-=NVS:NIL/FAIL*

The network prefix must be configured and the following routing rule added as first rule in case of the PhoneMail locations as well as phantom voice boxes configuration:

NVS:VOICE/.=<NW>*

Selection of a PhoneMail prefix

The same requirements apply to prefix assignment as already described for AMIS (cf. [Section 10.1.4.1, “Selection of an AMIS prefix”, on page 543](#)).

10.1.5 Redirecting Numbers

10.1.5.1 What are Redirecting Numbers?

We assume that the external user A calls the XPR user B. XPR user B's telephone is currently diverted to his/her XPR voice mailbox with the phone number "C-D", though. C is the number of the XPR server and "D" the number of the corresponding voice box.

As the call diversion is set, the XPR server receives on the one hand the phone number information "A" of caller A, if his/her phone number is transmitted. On the other hand, the voice mailbox number "D" is transmitted to the XPR server. The XPR server then decides for which user the call is intended. Therefore it searches the XPR user database for an entry with the phone number "D". If the XPR server finds the respective user, caller A is connected to the corresponding voice mailbox.

The main problem of this approach is: the operator of a voice mail system with 1000 users requires in the PBX 1000 different extensions for different voice boxes.

If the PBX and the ISDN card used support Redirecting Numbers, this scenario can be optimized as follows: The XPR server receives in addition to the previously described information "A" and "D" the phone number "B" of the diverting XPR user B.

In such a context, the voice mail system can search for the desired user on the basis of his/her phone number "B" in the XPR user database. Thus, no *user-adjusted* extension "D" is needed for the voice mailboxes, but only *one* extension for *all* users diverting their telephone. Accordingly, this one extension number represents the access number of the voice mail system in the XPR server.

If the "Redirecting Numbers" feature is to be applied in an XPR context, it must be supported by *all* of the following system components:

- ISDN board
- PBX
- Voice mail script

10.1.5.2 Cascaded Forwarding

The call of a subscriber may have to be diverted several times until it eventually reaches an XPR voice mailbox.

Example:

An external subscriber A calls the XPR user B. XPR user B's telephone is currently diverted to his/her cell phone with the phone number E, though. The cell phone is, however, currently switched off and routes the call to the XPR voice mailbox with the phone number "C-D".

Which phone number shall the XPR server use as redirecting number in this case of a cascaded forwarding? The originally called phone number B or the last redirecting phone number D?

By default, the XPR server uses in case of cascaded forwardings the originally called phone number as redirecting number. In the example thus phone number B.

You can globally configure for the PhoneMail and VMS scripts that not the originally called phone number but the last redirecting phone number is used as redirecting number. In the example thus phone number D. To this, set the script parameter **-lr** in PhoneMail respectively VMS.

IMPORTANT:

If you use the IP APL, the script parameter **lr** only takes effect for SIP and CorNet IP devices.

You can configure for the Ergo script individually for users and user groups that not the originally called phone number but the last redirecting phone number is used as redirecting number. In the example thus phone number D.

To control the redirecting number behavior in Ergo, you need to add the new **USE_LAST_REDIR** database field to the user and/or user group mask of the Correl Database in the form of a text field.

NOTE:

You can perform the user respectively user group setting for the redirecting number behavior in Ergo only via the Web Assistant. This configuration is not possible in Communications.

10.1.5.3 Supporting Redirecting Numbers

Redirecting Numbers are not *always* supported by interface boards and PBXs, since the transmission of Redirecting Numbers to an application has been defined as an optional feature in the CAPI specification. Thus, it is the choice of the respective telecommunication hardware manufacturer to implement this feature.

10.1.5.4 Function Test for Redirecting Numbers

Via the following steps it is possible to verify in practice whether Redirecting Numbers are supported in an XPR context.

1. Set up a functional XPR voicemail environment with at least 2 telephone devices.
2. Make sure that it is possible to dial the test environment voice mail box from both telephone devices.
3. Configure one of the telephone devices in a way that all incoming calls are diverted to the installed voice mail system access number.
4. Create a new log window for the applied telematics APL in the XPR monitor and activate all topics.
5. Now call the diverted telephone device from the other one. You should be connected to the voice mailbox because of the call diversion.
6. Keep track of the XPR monitor logging output where you should be able to view the Redirecting Number as the phone number transmitted to the telematics APL:

```
24.16:27:10.564
IsdnApl Plci 3 Received redirected number info: len=5 ...
24.16:27:10.564
IsdnApl Plci I Redirected number <11>
```

... later on the transmission to the voice mail script:

```
24.16:27:10.694
IsdnApl VFS D MCK.main() redirected number = 11
```

(In this example the phone number of the second telephone device is 11; this corresponds to the Redirecting Number).

If these lines cannot be found in the logging output, either the PBX has not transferred the Redirecting Number to the ISDN board or the ISDN board has not transmitted the number to the telematics APL.

10.1.5.5 Known Problems with Redirecting Numbers in PBX Systems

The PBXs of type *Hicom 300/300E* do not transmit the Redirecting Number according to CAPI standard. Such systems use a proprietary method to transfer the information, which is then not evaluated by the ISDN boards.

However, if you use a Sangoma Diva(R) ISDN board with the Hicom 300E, this solution is operational. These ISDN boards transfer the information in a proprietary way to the connected application – thus the ISDN APL.

IMPORTANT:

In order to configure the ISDN APL respectively, the parameter *CheckFacility* must be set to **1** in the private settings of the corresponding device. Since this setting can currently not be configured via the XPR monitor, the configuration must be performed manually in the registry (cf. registry key **Private [REG_MULTI_SZ]**).

This solution works *only* with Sangoma Diva(R) ISDN boards at Hicom -300E PBXs. This solution has not been tested with the Hicom 300 yet.

10.1.6 Features of D-channel Protocols

The following tables give an overview of the D-channel features supported by the E-scripts ERGO, PhoneMail and VMS.

10.1.6.1 Ergo

Function (– Not supported; x supported)	D-channel protocol						
	QSIG	CorNet T	CorNet N	CorNet NQ	CorNet IP	EDSS1	SIP
Display Control	–	–	X	X	X	–	–
Receiving fax messages (Fax G3 and Fax G4)	X	X	X	X	–	X	–
Caller identification (ANI) *	X/X	X/X	X/X	X/X	X/–	X/X	X/–
Called party identification (DNIS)	X	X	X	X	X	X	X
Identification of a telephone that redirects to the XPR server	X	X	X	X	X	X	X
Identification of a reason for forwarding (required for the function “Busy Announcement”)	X	X	X	X	X	X	–
User-to-User information (detects whether a system calls itself; dynamic change of protocol)	X	X	X	X	X	X	–
Call forwarding to e.g. call the originator of a message	X	X	X	X	X	X	X

Table 17 *Ergo Features for different D-Channel Protocols*

* Uses two TeleLib functions: <TL_CallerNumberGet>/<TL_CallerSecretNumberGet>

10.1.6.2 VMS

Function (– Not supported; x supported)	D-channel protocol						
	QSIG	CorNet T	CorNet N	CorNet NQ	CorNet IP	EDSS1	SIP
Display Control	–	–	X	X	X	–	–
Receiving fax messages (Fax G3 and Fax G4)	X	X	X	X	–	X	–
Caller identification (ANI) *	X/X	X/X	X/X	X/X	X/–	X/X	X/–
Called party identification (DNIS)	X	X	X	X	X	X	X
Identification of a telephone that redirects to the XPR server	X	X	X	X	X	X	X
Identification of a reason for forwarding (required for the function “Busy Announcement”)	X	X	X	X	X	X	–
User-to-User information (detects whether a system calls itself; dynamic change of protocol)	X	X	X	X	X	X	–
Call forwarding to e.g. call the originator of a message	X	X	X	X	X	X	X
Caller identification (ANI) if called party is changed (in case a subscriber forwards the call to another device) **	–/–	X/–	X/X	X/X	X/X	–/–	–/–
Authorization of the PBX for call transfer	–	X	X	X	X	–	–
Call transfer control of the own device to another phone number via the TUI	–	–	–	X	–	–	–
Caller identification (Hicom PIN: each subscriber has a unique ID, independent of the applied device)	–	–	X	X	–	–	–
Initiate a callback in case of an unsuccessful call via the TUI (“Destination Busy” – CCBS or “Ring No Answer” – CCNR)	–	X	–	X	–	–	–

Table 18 VMS Features for different D-Channel Protocols

* Uses two TeleLib functions: <TL_CallerNumberGet>/<TL_CallerSecretNumberGet>

** Uses two TeleLib functions: <TL_HicomConnectedNumberGet>/<TL_HicomPinCodeGet>

NOTE:

The feature CCBS/CCNR is only used for the HiPath 4000 from version 2.

10.1.6.3 PhoneMail

Function (– Not supported; x supported)	D-channel protocol						
	QSIG	CorNet T	CorNet N	CorNet NQ	CorNet IP	EDSS1	SIP
Display Control	–	–	X	X	X	–	–
Receiving fax messages (Fax G3 and Fax G4)	X	X	X	X	–	X	–
Caller identification (ANI) *	X/X	X/X	X/X	X/X	X/–	X/X	X/–
Called party identification (DNIS)	X	X	X	X	X	X	X
Identification of a telephone that redirects to the XPR server	X	X	X	X	X	X	X
Identification of a reason for forwarding (required for the function “Busy Announcement”)	X	X	X	X	X	X	–
User-to-User information (detects whether a system calls itself; dynamic change of protocol)	X	X	X	X	X	X	–
Call forwarding to e.g. call the originator of a message	X	X	X	X	X	X	X
Authorization of the PBX for call transfer	–	X	X	X	X	–	–/–
Initiate a callback in case of an unsuccessful call via the TUI (“Destination Busy” – CCBS or “Ring No Answer” – CCNR)	–	X	–	X	–	–	–
Call transfer control of the own device to another phone number via the TUI	–	–	–	X	–	–	–
Determination whether a call is a callback	–		X	X	X	–	–
Caller identification (Hicom PIN: each subscriber has a unique ID, independent of the applied device)	–	–	X	X	–	–	–

Table 19 PhoneMail Features for different D-Channel Protocols

* Uses two TeleLib functions: <TL_CallerNumberGet>/<TL_CallerSecretNumberGet>

NOTE:

The feature CCBS/CCNR is only used for the HiPath 4000 from version 2.

10.1.7 Memory Requirements for Voice Messages

The memory requirements for recording voice messages or greetings depend on the telematics APL used.

10.1.7.1 ISDN APL Memory Requirements

If a user has a voice message or greeting recorded via the ISDN APL, the ISDN APL generates a sound file in WAV (8 bit) format.

Example:

A voice message with a length of **10 seconds** requires the following ISDN APL memory:

$10\text{s} \times 8000\text{Hz} \times 1\text{Byte} = \mathbf{80.000\text{Bytes}}$ (corresponds to approximately 78KB)

10.1.7.2 IP APL Memory Requirements

If a user has a voice message or greeting recorded via the IP APL, the IP APL generates a sound file in WAV (16 bit) format by default. The MTA then converts this file into a file of the format WAV (8bit). Both files are subsequently consolidated in a PMF file and stored on the XPR server computer system.

Example:

A voice message with a length of **10 seconds** requires the following IP APL memory:

$10\text{s} \times 8000\text{Hz} \times (2 + 1)\text{Byte} = \mathbf{240.000\text{Bytes}}$ (corresponds to approximately 234KB)

You can change this behavior with the registry value **VoiceRecFormat [REG_DWORD]** of the IP APL and configure one of the following alternative storage formats for voice messages:

- A-law
- μ -law

After you have configured one of these storage formats the IP APL will allocate only approximately 1/3 of the original storage space for voice messages on the XPR server computer system. Reason: In this case voice messages will not be additionally stored in the WAV format.

10.1.8 Call Attached Data (CAD)

The ISDN and IP APL support CAD. To activate this feature you need to set the registry value **UseCtiMonitorPoint** to **1** for the relevant APL. You find this value in the registry under the key:

HKLM\Software\Wow6432Node\PP-COM\MRS\<APL name>.

If you activate CAD for the ISDN APL, no phone number recognition for outbound connections must be configured in the ISDN settings. Cf. **ISDN settings > Outbound > Use following ID**.

10.2 Technological Concepts of the ISDN APL

The following sections describe special technological concepts relevant for ISDN APL usage.

These are the sections:

- [ISDN APL Telematics Services](#)
- [Supported ISDN Boards](#)
- [CorNet-N Support](#)

10.2.1 ISDN APL Telematics Services

The ISDN APL provides the XPR system with several ISDN telematics services. These are especially:

- Sending and receiving Fax G3
- Operation as fax concentrator (fax-fax conversion protocol)
- Sending and receiving Fax G4
- Sending voice files
- XPR client/server interconnection via SMI protocol
- Programmable Voice and Fax-on-Demand systems

The configuration is normally performed via the XPR monitor. Cf. [Section 10.9, “Configuration Reference for ISDN Connections \(ISDN APL\)”](#), on page 804.

10.2.2 Supported ISDN Boards

You find all supported ISDN boards in the XPR server release notes.

IMPORTANT:

In an XPR server system only ISDN boards of *one* manufacturer should be integrated, or preferably, of *one* version. Mixed operation is normally not certified. If required, new ISDN APL entities can be installed on additional server systems. The *Distributed XPR Server* created in this way can then be easily operated with miscellaneous ISDN boards. This may be necessary when the required functionality can only be achieved through the installation of ISDN boards of various manufacturers.

The server hardware should be dimensioned according to the number of ISDN boards used regarding its performance data. Otherwise the data load could not be managed.

The ISDN APL supports CAPI 2.0 as interface.

10.2.3 CorNet-N Support

For specific Sangoma Diva(R) cards possessing a vendor ID from Unify GmbH & Co. KG, the producer-specific D-channel protocol CorNet-N is supported. If an appropriate DLL exists, additional features of PBXs by Unify GmbH & Co. KG may be used. This realization option is only available for projects with Unify GmbH & Co. KG as prime contractor.

Via CorNet-N you can e.g. address telephone displays and set the associated MWIs.

NOTE:

For E-scripts, display control is automatically executed via the D-channel if it is available.

For VFS scripts, the XPR feature AclUse should explicitly be deactivated via the corresponding ISDN APL registry key to avoid using the less efficient Hicom APL. To set the mailbox LED, enter the expression "MWI/<phone number>" in the XPR database field CIT for the relevant user. The MWI protocol is meanwhile automatically installed and activated with the ISDN APL.

10.3 Technological Concepts of the IP APL

The following sections describe special technological concepts relevant for IP APL usage.

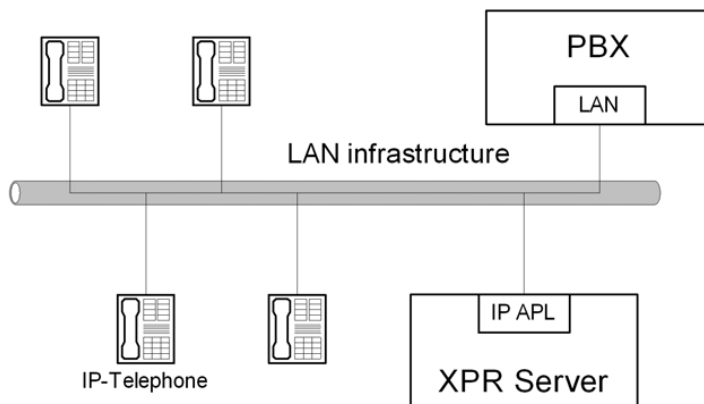
These are the sections:

- [IP APL Usage Environment](#)
- [IP APL Structure](#)
- [TAPI-based Connection](#)
- [H.323](#)
- [CorNet IP](#)
- [Session Initiation Protocol \(SIP\)](#)
- [Fax-over-IP \(T.38\)](#)
- [Transmitting DTMF Tones \(RFC 2833\)](#)
- [Quality of Service \(QoS\)](#)
- [Public Key Infrastructure \(PKI\)](#)
- [Multimedia Internet Keying \(MIKEY\)](#)
- [Encryption of the Signaling \(TLS\)](#)
- [Encryption of the RTP Communication \(SRTP\)](#)
- [IP APL at a Layer 3 Cluster of OpenScape Voice.](#)

10.3.1 IP APL Usage Environment

The IP APL implements access to telecommunication protocols like all other telematics APLs. It represents an extension of the XPR communication with regard to IP-based integration of the XPR server. The installation of IP transport services is realized by the IP APL as it is e.g. required in the voice mail context of IP telephony - the current IP APL range of use.

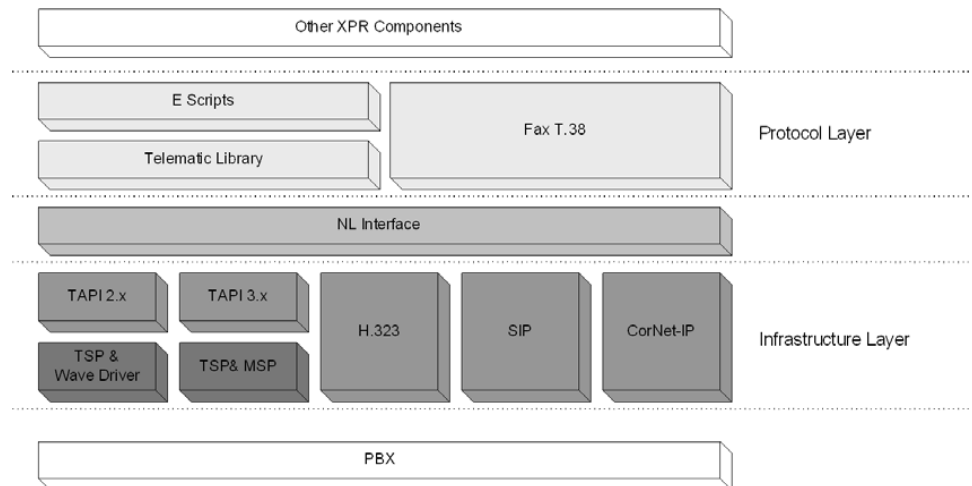
In such a voice mail scenario, an XPR server provides voice mail services via the IP APL that can be used by an IP-based PBX. The principle structure of such a solution is displayed in the following figure.



The XPR server is integrated into an IP Telephony solution via the IP APL. Thus, additional services that the connected PBX does not support at all or only insufficiently can be provided for the PBX and its telephones .

10.3.2 IP APL Structure

The following figure gives a schematic overview of the inner structure of the IP APL.



Simplified, the IP APL can be divided into three layers:

- Protocol layer
- Infrastructure layer
- NL interface.

Protocol layer

The protocol layer executes the E-scripts (e.g. Ergo) that are configured in the IP APL. In addition, it provides further protocols used by the IP APL for communicating with PBXs. At present, this is the T.38 fax protocol.

Infrastructure layer

The infrastructure layer provides all protocols used by the IP APL to access different network media.

The infrastructure layer currently supports the following communication standards:

- TAPI 3.0/3.1, TAPI 2.1 in connection with a Wave interface
- H.323

- SIP.

IMPORTANT:

Each IP APL only supports precisely one protocol of the infrastructure layer. Consequently, the IP APL does not support any parallel connection of a PBX via SIP after the configuration of T.38 via H.323.

NL interface

The Network Layer interface of the XPR server is the link between the protocol and the infrastructure layer. It enables using a protocol of the protocol layer via different protocols of the infrastructure layer.

Several IP APLs in one XPR server

The IP APL can be instantiated in an XPR server several times. This requires each IP APL to use an individual IP address. The IP address of an IP APL is stored under the respectively associated registry value **Private** in the **LISTEN** parameter.

Example:

```
HLM\Software\Wow6432Node\PP-  
COM\MRS\<IP APL>\Devices\<Device>\Private
```

See [Section 10.10.6, “Several IP APLs on one Server”](#), on page 874.

Support of features in the IP APL

The following table provides an overview of the special IP APL features depending on the protocol of the infrastructure layer.

Function	Infrastructure Protocol			
	TAPI2/3	H.323	CorNet IP	SIP
(– Not supported; x supported)				
Fax-over-IP – G.711	–	X	X	X
Fax-over-IP (T.38)	–	X	X	X
Transmitting DTMF Tones (RFC 2833)	–	X	X	X
Encryption of the Signaling (TLS) (Notification)	–	–	–	X
Encryption of the RTP Communication (SRTP) (Streaming)	–	–	–	X

Table 20 Special IP APL Features

You find a detailed description of the listed features and protocols in the following sections.

10.3.3 TAPI-based Connection

The Telephony Application Programming Interface (TAPI) is a programmable interface under the Windows operating system, enabling PC-based telephoning.

The following TAPI interfaces are currently used:

- **TAPI 3.1**

Is based on the H.323 TSP delivered by Microsoft. With TAPI 3.1 the TSP also supports the Supplementary Telephony Services described in the H.450 standard. Supplementary Telephony Services define additional services to complement the Basic Telephony Services, e.g. *Holding*, *Parking*, *Alternating* and setting up conferences.

IMPORTANT:

The Microsoft H.323 TSP is no longer supported.

- **TAPI 3.0**

In this case, the manufacturer supplies a corresponding TSP for their PBX.

IMPORTANT:

The Microsoft H.323 TSP is no longer supported.

- **TAPI 2.1 with wave interface**

Here as well the producer needs to supply a corresponding TSP. In contrast to versions 3.0/3.1, TAPI 2.1 is not H.323-based. An example of this connection is the Cisco Call Manager.

Depending on the TAPI version used, possible features may be restricted. Version 2.1, for example, does not support Fax-over-IP (T.38).

TAPI interface usage, as described above, occurs with an additional software module - the TAPI Service Provider (TSP). The TSP is the link between the hardware-independent TAPI and the communication network hardware. Thus it represents a driver for the transporting technology used. Queries posed by the TAPI to the TSP are converted by the TSP into operations to control the connected hardware.

In this function this module defines the scope of performance supported via the TAPI. Beyond that, communication- and hardware-specific details remain hidden from the application itself with this concept.

To support manufacturer-specific features with PBX systems, PBX manufacturers often deliver an individually adapted TSP along with their PBX systems. The TSP supplied along with Windows, implementing the above H.323 standard, can be used as an alternative.

10.3.4 H.323

H.323 is a universal standard of the International Telecommunication Union (ITU) for multimedia communication services in packet-switched networks. It represents a widely-used basis for Voice-Over-IP solutions in data networks.

Besides the original standard, the standard collection, in the meantime accrued to a protocol family, comprises norms for further communication services that origin in the telephony world. Such services include among others Fax-over-IP (T.38) or H.450 for supplementary telephony services such as *call transfer* or *call-hold*.

H.323 basic components are terminals, gateways, gatekeeper and Multipoint Control Units (MCU), with gateways and terminals also being called end points.

The functions of these components are:

- **Terminal**
The H.323 terminal represents the terminal device in a VoIP solution according to H.323 standard. It must support the voice service as minimum configuration. Further multimedia services such as fax or video can be integrated optionally.
- **Gateway**
The H.323 gateway is responsible for the communication between H.323 terminals and subscribers of classic PBXs. Thus it serves as interface between classic telephony and a VoIP solution and realizes the network transition with regard to transmission formats and protocols.
- **Gatekeeper**
The H.323 gatekeeper is in charge of converting service-individual addresses of the terminals and gateways into IP addresses. This concerns e.g. telephone numbers or e-mail addresses. Furthermore, it realizes a bandwidth management for the transport infrastructure and an access check for subscribers.
- **Multipoint Control Unit (MCU)**
An MCU is required for conferencing (conversation between more than two subscribers). It serves to prepare the possible communications in suitable form and subsequently to distribute them to the participating terminals.

In an H.323 solution the IP APL acts as gateway.

On establishing a connection between a terminal and the XPR server, the desired subscriber number is evaluated, and based on it the correct communication script (e.g. PhoneMail) selected. Thus the function of such a solution does not principally differentiate from a classic solution based on the ISDN APL but only in its transport technology.

Recently a new IP-based communication protocol is becoming popular that yet realizes similarly comprehensive services like the H.323 - the Session Initiation Protocol (SIP). Contrary to H.323 this protocol is no ITU standard but has been defined as RFC.

10.3.5 CorNet IP

CorNet IP is a VoIP protocol based on an H.323 communication with tunneled CorNet-NQ messages. This way the VoIP communication is not restricted to H.323 features but contains the enhanced CorNet-NQ protocol feature set.

Thus, a CorNet IP solution provides the manifold features of a CorNet-NQ-TDM solution without causing the increased costs for TDM cards.

The CorNet IP protocol is currently supported by the following PBX systems:

- HiPath 3000 from V5.0 with HG1500 module (HXG3)
- HiPath 4000 from V2.0 with HG3550 module (STMI2)
- HiPath 5000 from V5.0

You find a list of the features currently supported in the IP APL by CorNet IP in [Section 10.1.6, "Features of D-channel Protocols", on page 555](#).

Cornet IP Support in the IP APL

NOTE:

The Cornet IP of the IP APL can only be used with en-block dialing.

A connection via CorNet IP is in the IP APL configured via the H.323 device.

10.3.6 Session Initiation Protocol (SIP)

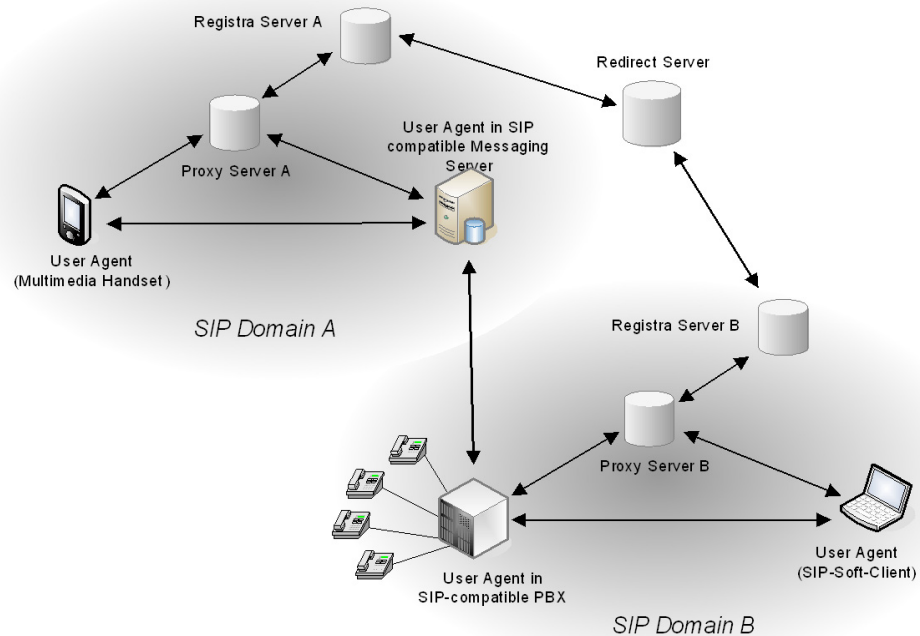
The SIP communication protocol was developed by the IETF as application layer protocol. It originally realized the signaling of IP-based voice transmission, but has in the meantime been expanded for applications in the areas video and instant messaging. Since SIP within this scope only realizes the signaling of connections, it uses various other protocols for the actual transmission of usable information. This includes e.g. the RTP protocol used for transmitting real-time data.

In the voice area, SIP enables all basic call functions such as connection set-up and shutdown, call notification or dial tone. Beyond that, further features are already implemented in SIP. Among these are the features parking, call transfer or conference switch. SIP can therefore – with reference to its features – be compared with H.323.

Contrary to H.323, the SIP communication model realizes a big part of the functions in the terminal device. This significantly differentiates it from the traditional communication concepts in which the actual intelligence lies in the network nodes.

10.3.6.1 SIP Network Components

An SIP network consists of different SIP-specific logic components. These intercommunicate in a defined way.



The logic components of an SIP network are:

- User Agent (UA)**
 The user agent represents the terminal device in an SIP network. It signals and manages SIP connections that it initiates with other user agents¹ or proxy servers. Upon logging in at an SIP network a user agent registers with the registrar server in charge.
 The user agent is logically divided into the user agent client and the user agent server. The user agent client is in charge of initiating SIP connections. The user agent server replies to connection requests.
 User agents are e.g. SIP telephones or an SIP client software.
- Registrar Server**
 Registrar servers are responsible for registering user agents. The information collected during the logging of the single user agents are transferred to the location server that administer these data for future requests.
 Registrar servers often operate on the same platform as the associated location server (see below).
- Location Server**
 Each SIP domain has a location server. This server manages among other things information on the bindings of logical and physical SIP addresses (cf. [Section 10.3.6.2, "Addressing an SIP Subscriber", on page 571](#)).

1. A communication connection between two user agents is directly established via RTP.

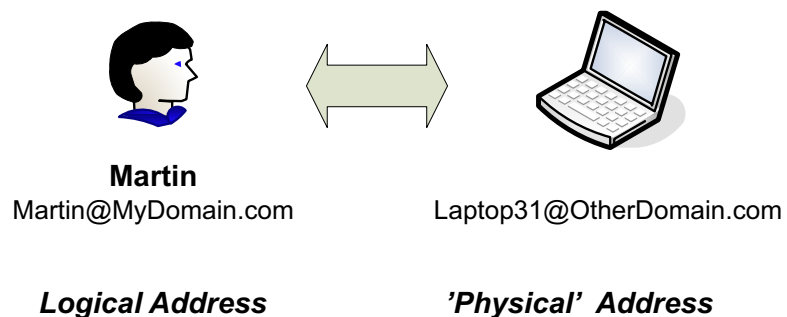
Location servers often operate on the same platform as the associated registrar server (see below).

- **Proxy Server**
 Each SIP domain has a proxy server. This server receives the connection requests by user agents or other proxy servers. The proxy server is logically divided into a client and a server component, which perform individual connection requests on behalf of user agents.
 With handling a connection request, two cases must be differentiated:
 - *The communication participants are in the same SIP domain*
 In this case only the proxy server of the domain concerned is involved in the connection establishment.
 - *The communication participant is in different SIP domains*
 In this case the two proxy servers of the domains concerned are involved in the connection establishment.
 For the resolution of SIP addresses the proxy server communicates with the associating location and redirect server.
- **Redirect Server**
 A redirect server processes proxy server requests as regards configured call reroutings for user agents. It operates domain-spanning.
 For the resolution of SIP addresses the redirect server communicates with the associated location server.

10.3.6.2 Addressing an SIP Subscriber

SIP addressing is based on a logical and a physical² SIP address. The logical address is assigned to the person "user", the physical address is allocated for the device, with which the user registers with the registrar server. The actual routing within an SIP network occurs based on the physical address.

Example:



2. The physical SIP address is not to be confused with an address of the physical OSI layer.

User Martin has in our example the logical address *Martin@MyDomain.com*. Under this address he is to be addressed in the entire SIP network. His physical address, according to which messages are routed for him in the network, depends on the terminal device with which he registers in the SIP network. In our example Martin registers with a laptop. This laptop has the physical address *Laptop31@OtherDomain.com*.

If another SIP subscriber wants to establish a communication relation to Martin, he/she addresses the connection setup with the logical destination address *Martin@MyDomain.com*. This makes sense since the SIP users do not know via which terminal device a subscriber registers. In the course of the connection setup this logical address is resolved by the location server into the current physical address.

10.3.6.3 Interaction between logical SIP Components

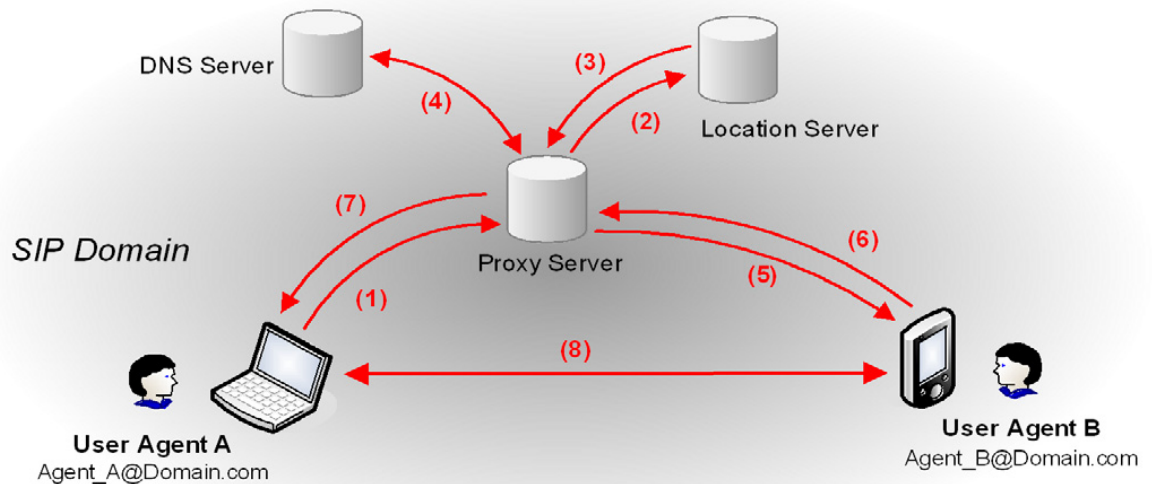
The interactions between the logical SIP components is based on various transactions. These consist of a request – sent by an SIP client to an SIP server – and an associated reply – sent by an SIP server to an SIP client each.

Let's take a look at two simple examples to describe the general interactions between the SIP components to establish a connection between two user agents. For reasons of simplification we discount the registrar and redirect server function.

The first example describes the connection establishment between two agents that are in the same SIP domain. In the second case the user agents involved are in different SIP domains.

Connection between two subscribers in one SIP domain

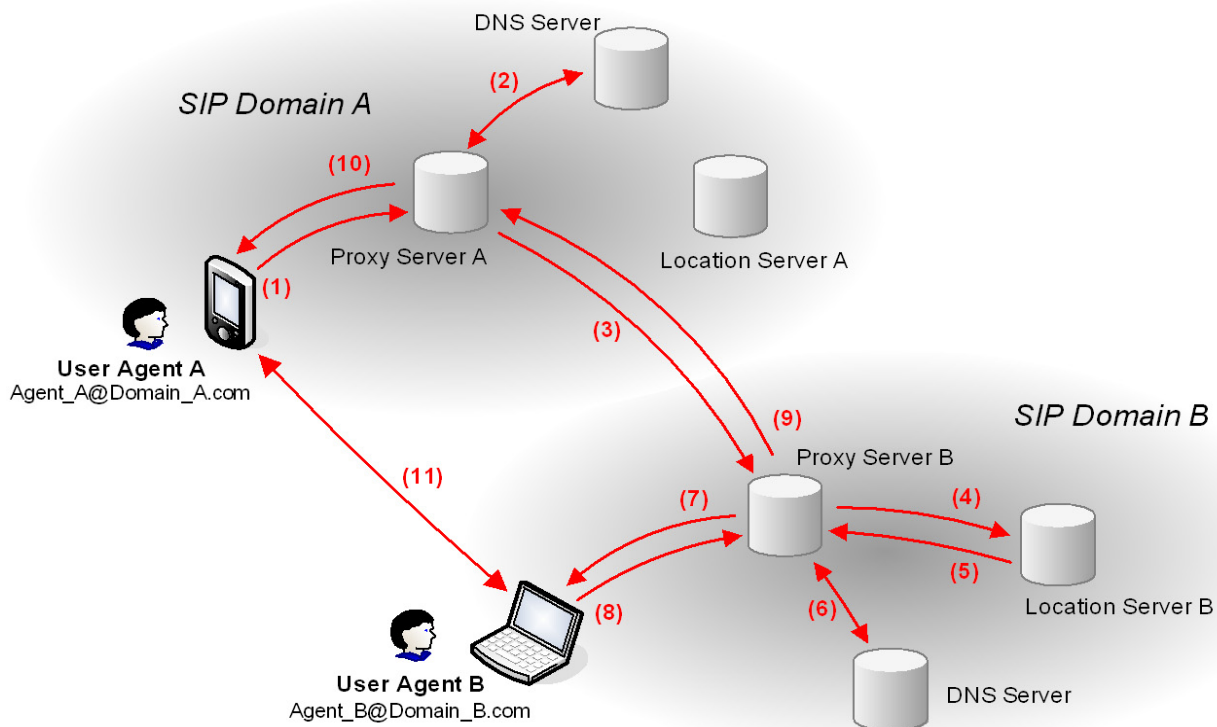
Let us see how a SIP connection is established between two SIP clients that are in the same SIP domain.



1. User agent A initiates a connection to user agent B. For this purpose he/she sends a corresponding connection request to the proxy server of the domain. The connection request contains the logical SIP address of the destination party – *Agent_B@Domain.com*.
2. The proxy server requests the registered address information of the destination subscriber from the location server.
3. The location server replies to the proxy server with the physical SIP address of the destination subscriber.
4. Subsequently, the proxy server resolves the received SIP address into an IP address via the DNS server in charge.
5. The proxy server sends an individual connection request to the IP address of user agent B.
6. User agent B replies to this request and informs the proxy server that he/she accepts the requested connection.
7. The proxy server correspondingly accepts the original connection request of user agent A (see 1).
8. User agent A then establishes a direct RTP connection to user agent B.

Connection between two subscribers in different SIP domains

The following example shows the general structure of an SIP connection between two subscribers in different domains.



1. User agent A initiates a connection to user agent B. For this purpose he/she sends a corresponding connection request to proxy server A of his/her own domain. The connection request contains the logical SIP address of the destination party – *Agent_B@Domain_B.com*.
2. By the domain name of the destination address *Domain_B.com*, proxy server A recognizes that user agent B does not belong to the own domain A. Subsequently, it queries the IP address of the proxy server responsible for domain B at the DNS server in charge. Thus the IP address of proxy server B.
3. Proxy server A sends an individual connection request to proxy server B³.
4. Proxy server B then requests the SIP address under which the destination subscriber is registered in the SIP network from the location server in charge.
5. The location server replies with the physical address of the destination subscriber.

3. Consequently, proxy server A becomes the *Outbound*-, proxy server B becomes the Inbound proxy server.

6. Subsequently, the proxy server resolves the received address into an IP address via the DNS server in charge.
7. Proxy server B now sends an individual connection request to user agent B.
8. User agent B replies to this request and informs proxy server B that he/she accepts the requested connection.
9. Proxy server B accepts the connection request by proxy server A (see 4).
10. Afterwards, proxy server A accepts the connection request by user agent A (see 1).
11. User agent A then establishes a direct RTP connection to user agent B.

You find further information on SIP in the appropriate literature or in the relevant RFC standards of the IETF (www.ietf.org).

10.3.6.4 SIP Support in the IP APL

If the SIP protocol is configured in the IP APL, the APL works as user agent. The PBX assumes the function of a proxy server and beyond that possibly also the functions of other logical SIP components – e.g. the registrar server function.

The IP APL does not dynamically register with the PBX. It is statically registered instead.

To address SIP subscribers, the IP APL only supports the address format that consists of phone number and IP address.

The following thus applies:

500@10.1.1.10	correct format
Martin@10.1.1.10	wrong format
500@MyDomain.com	wrong format
Martin@MyDomain.com	wrong format

10.3.7 Fax-over-IP (T.38)

IMPORTANT:

If you connect a HiPath 3000 or HiPath 4000 via the IP APL and want to use the fax service, the method of fax error rectifying must be identically configured in the HiPath and IP APL. If the settings differ, the number of fax transmission errors increases.

IMPORTANT:

If you connect a HiPath system with HG module via the IP APL and want to use the fax service, logging must not be activated in the HG module. If logging is active, the number of fax transmission errors increases.

IMPORTANT:

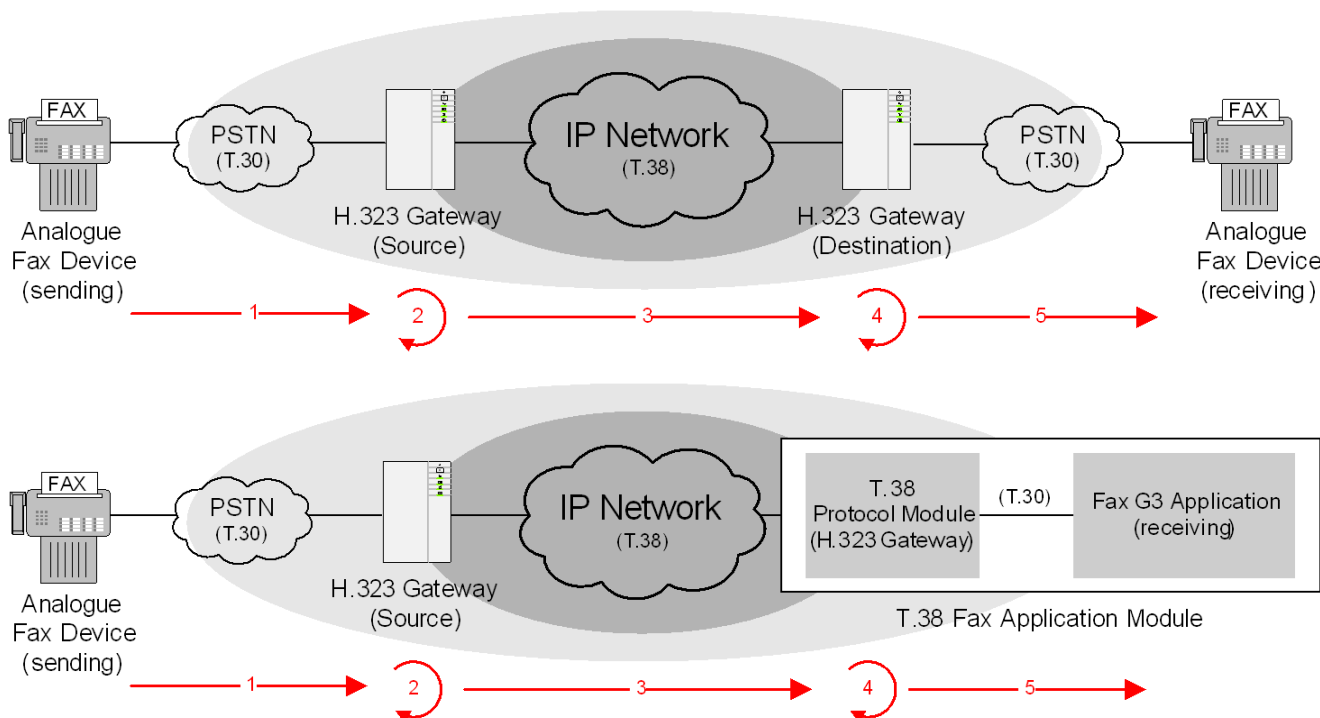
Sending and receiving of fax messages may cause disturbances in the IP APL if heavy fax traffic and the execution of maintenance script jobs coincide. Therefore, perform maintenance script jobs at times when you do not expect heavy fax traffic – e.g. at night. If the described problem arises just the same, reduce the priority for the automatic XPR server maintenance.

In an IP-based PBX environment, fax messages can always be transmitted audio-based via the G.711 codec. You can also use the digital T.38 standard as alternative.

The ITU standard T.38 defines how Fax G3 messages can be transmitted via IP networks as image data in real time. T.38 end points can here be H.323 or SIP gateways. T.38 uses the UDP protocol as transport layer.

10.3.7.1 T.38 Scenarios

The following two figures provide an overview of the T.38 scenarios *Fax Relay* and *Fax Scheduling*, if T.38 is used with H.323 gateways.



1. A fax device sends a Fax G3 message via PSTN (T.30).
2. The source gateway of the IP transport network recognizes the Fax G3 signal tone and demodulates the T.30 signal. Subsequently, it packs the received information in IP packets according to T.38 standard and
3. transmits the fax message digitally to the H.323 destination gateway. For this, a VoIP connection in the fax mode is used.
4. The destination gateway modules the information received via the IP network according to T.30 standard and
5. transmits the thus created Fax G3 message via PSTN or internally via T.30 to the desired destination fax device (fax application).

These 5 steps of a T.38 fax transmission are only a simplified description.

10.3.7.2 Fax via T.38 or G.711?

If an environment allows using T.38 as well as G.711 for fax transmission, we recommend to prefer T.38 for the following reasons:

1. Fax via T.38 uses redundancy mechanisms that improve the reliability and quality of a fax transmission.
2. You cannot use Fax via G.711 if a compression process is deployed on the way between originator and recipient – thus for example a codec such as G.729 or G.723.

As the path of a fax transmission is not always under the sovereignty of the originator or recipient, considering this restriction cannot always be guaranteed.

10.3.7.3 T.38 Fax Support in the IP APL

The IP APL currently supports T.38 for connections via

- H.323
- CorNet IP
- SIP.

10.3.7.4 Fax (G.711) Support in the IP APL

The IP APL currently supports fax over G.711 for connections via

- H.323
- CorNet IP
- SIP.

10.3.8 Transmitting DTMF Tones (RFC 2833)

The IETF recommendation RFC 2833 defines how DTMF and fax tones can be transmitted via the RTP protocol. It describes two options:

- via in-band signaling
RTP transmits DTMF and fax tones as tones in the logical transmission channel for voice information.
- via out-band signaling
DTMF and fax tones are here transmitted in an individual channel. This channel is logically independent from the voice information transmission channel.

Which of these two transmission options you should use depends mostly on one question: is voice information compressed for transmission?

Why is this question so important? Compressing affects the voice information. Consequently: voice information recovered from a compressed signal does not precisely correspond to the original information anymore. The original signal increasingly deviates from the recovered information with the degree of compressing. After its recovery, a compressed DTMF and fax tone may in the end not be correctly recognizable anymore.

DTMF and fax tones should therefore be transmitted in a separate channel (out-band signaling), if the voice information of a connection is compressed. To this, RTP uses so-called RTP events (Named Telephony Events – NTE) according to RFC 2833.

Lets us contemplate an example:

A subscriber talks on the phone, and his/her voice information is transmitted via IP and the RTP protocol. During this call, he/she pushes key 8 on the telephone keypad, for example, to control the voice mail protocol of the XPR server.



While the subscriber's voice information is transmitted in RTP as usual and possibly compressed, the RTP protocol recognizes at the sending station the DTMF tone of key 8. It consequently creates an RTP event that is transmitted to the recipient in the stream of tone information in parallel. This event contains the information: Key "8" was pushed. Since this event is not a tone information anymore, it is not affected by a possible compression.

The RTP protocol at the recipient station recognizes the transmitted event and turns it into the precise DTMF tone for key 8.

10.3.8.1 Using the RFC 2833 in the IP APL

The IP APL supports from the RFC 2833 recommendation only the out-band signaling of DTMF tones. This support is available for the following connections.

- H.323
- CorNet IP
- SIP.

The IP APL sends fax tones traditionally as audio signal withing the voice channel.

10.3.9 Quality of Service (QoS)

Voice information transmission is considered a time-critical service in networks. This means that the quality of voice transmission very much depends on the speed with which the voice information is transmitted from the sender to the recipient.

Three network parameters have a particular influence on the voice quality in this context:

- The average time the network needs to transmit the voice information from the sender to the recipient (Delay)
- The temporal delay change (Jitter)
- The loss of voice information during transmission (Loss).

If only one of these three values is too high, voice communication via the relevant network is often intolerable for the users.

To optimize the transmission of voice information via a data network, the IP APL for SIP connections can be configured in a way that it uses the QoS functionality of the Windows operating system. In this case the IP APL data are prioritized against other data with the so-called DSCP byte in the IP header of the data packets. The result is in most cases a significant increase in voice quality.

You need to perform the following settings for the IP APL to use the described QoS functionality of the Windows operating system:

- Selection of the quality classes the IP APL is to use for the traffic types signaling, voice and fax
- Setting the registry value `DisableUserTOSSetting` under `HKLM/SYSTEM/CurrentControlSet/Services/Tcpip/Parameters` to 0.

You find further information about the QoS settings in [Section 10.10.4.2, “QoS”](#), on page 871.

10.3.10 Public Key Infrastructure (PKI)

PKI describes a widespread security concept for managing so-called public keys. These keys are used for encrypting messages to be sent via an insecure transport network.

The following sections consider the basic concepts of PKI. You find further information about PKI and other security mechanisms in the appropriate literature or in the Internet.

10.3.10.1 Reasons for Encryption

Messages are usually encrypted for one or several of the following reasons:

- Confidentiality
Some messages are not for everybody to read.
- Integrity
Messages should be protected from modifications performed by third parties on the sly.
- Authenticity
A foreigner shall not be enabled to send a message under the name of another person unnoticed.

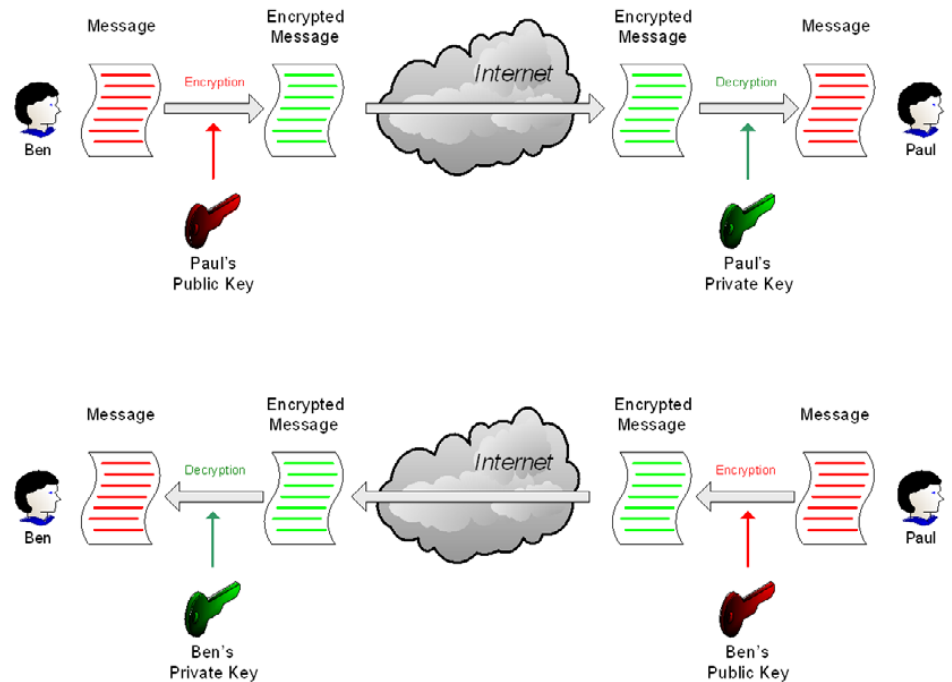
Several basic encryption methods have been developed to implement such requirements. One of them is asymmetric encryption.

10.3.10.2 Asymmetric Encryption

When this method is applied, each subscriber has a pair of keys. Such a pair of keys consists of a public key and a private key to be used to encrypt respectively decrypt messages.

The togetherness of two keys ensures that a message encrypted with a public key can only be decrypted with the associated private key.

Let us contemplate the following two figures.



In these examples, Ben and Paul want to exchange a message via the Internet and use asymmetric encryption. In the first case, Hans sends the message to Paul; in the second case the transmission direction is reversed.

We quickly recognize the basics of asymmetric encryption:

- A sender has the public key of the recipient
- A private key is not passed on by its user
- A message is always encoded with the public key of the recipient
- A message is always decoded with the private key of the recipient

10.3.10.3 Public-Key Exchange via Certificates

The example in the last section showed for asymmetric encryption: if we want to send an encrypted message to a subscriber, we need his/her public key. Therefore, this key must be exchanged before the message can be sent. In case of PKI this exchange is performed with so-called security certificates. Such certificates are to make sure that the exchanged key actually belongs to the relevant subscriber.

In most cases, certificates are issued by generally trustworthy certification centers – e.g. by Verisign.com. When a subscriber sends his/her certificate thus obtained to the communication partner, this partner checks the certificate validity by means of the certificate from the relevant certification center.

A certificate need not be issued directly from a generally trustworthy certification center. It is also possible to derive a so-called proxy certificate (temporary certificate) from a certificate by a generally trustworthy certification center. This proxy certificate is only trustworthy to a communication partner provided that also the certificate is transmitted from which the proxy certificate was derived. Only then the communication partner is able to trace the trust chain back to the original certification center and to check the proxy certificate validity.

Such mechanisms are to ensure: an intruding party cannot distribute their own key and claim that it belongs to another subscriber. Without this precaution, confidential messages could be encoded with a public key for which an intruding party has the matching private key. This would violate message confidentiality.

10.3.10.4 PKI Usage in the IP APL

NOTE:

The PKI of the IP APL is based on certificates locally stored on the XPR server. The IP APL cannot automatically load certificates from a PKI server.

In the IP APL, PKI is used for the key management when communication occurs via TLS (cf. [Section 10.3.12, “Encryption of the Signaling \(TLS\)”, on page 586](#)). In other words, it is used for the encrypted transmission of management information that is exchanged between the XPR server and the PBX.

When a TLS connection is set up, only the subscriber who accepts a connection needs to authenticate with his/her security certificate by default. The subscriber that sets up the connection only needs to authenticate if the Peer Authentication option has been activated for the relevant SIP device.

10.3.11 Multimedia Internet Keying (MIKEY)

MIKEY is a key management security protocol and thus used where keys must be managed for message encryption. It is an IETF recommendation and was developed especially for real-time applications. Because of this orientation, MIKEY is today mostly used in the environment of the SRTP and SIP protocol.

The MIKEY protocol performs the following tasks:

- Generation of keys for RTP information encryption
- Distribution of the generated keys among the involved communication partners

You find further information about the MIKEY protocol e.g. under <http://www.ietf.org/rfc/rfc3830.txt>.

Using MIKEY in the XPR server

IMPORTANT:

The MIKEY implementation of the XPR server currently only supports profile 0 of the MIKEY recommendation RFC3830. With this, MIKEY key data are merely sent uncoded. Therefore, TLS must definitely be activated to encode the MIKEY communication.

If TLS is not configured, the key data will be transmitted decrypted and thus in a legible format. This would be a security hole, which may lead to a **violation of the system integrity**.

IMPORTANT:

The MIKEY protocol may currently only be used after an individual project release.

In the XPR server, MIKEY is used for the management of keys that are used to encrypt SRTP connections. In this function it performs the following tasks:

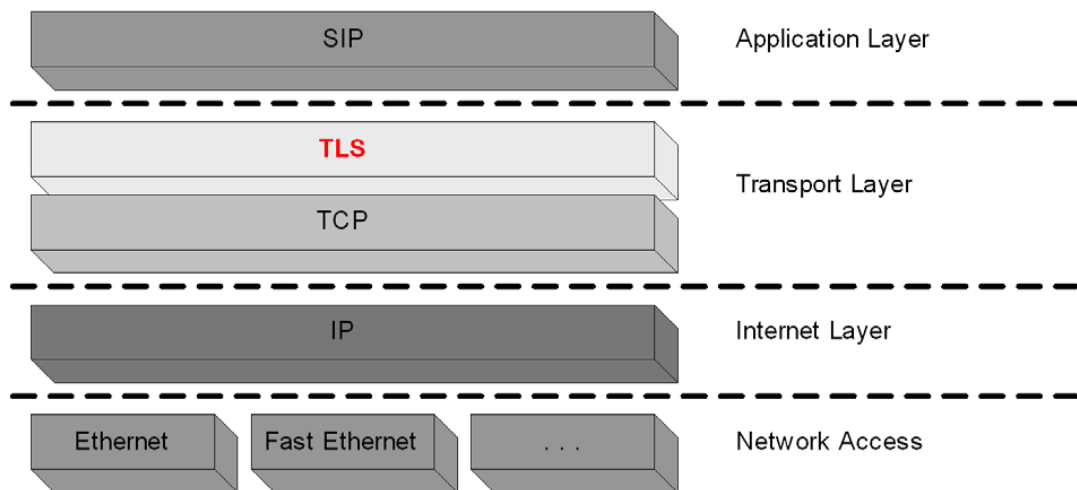
- Generation of a new key for each SRTP connection
- Distribution of the generated keys among the relevant communication partners
The keys are distributed via the signaling channel, while the connection parameters for the communication are negotiated with the connection partners.
For the actual key transmission, MIKEY uses, for example, the SDP (Session Description Protocol), which can use, for example, SIP.

10.3.12 Encryption of the Signaling (TLS)

To secure SIP signaling, the IP APL supports the open Transport Layer Security (TLS) protocol. TLS is an IETF recommendation and successor to the Secure Socket Layer (SSL) protocol, which was developed by Netscape to encrypt Internet communication.

10.3.12.1 Transport Layer Security (TLS)

The following figure shows the position of the TLS protocol in the TCP/IP layer model.



TLS is positioned directly on top of the actual transport protocol – in the representation for example directly on top of the TCP protocol. Consequently, all information of the overlying application layer, which includes SIP also, is encrypted.

TLS aims at

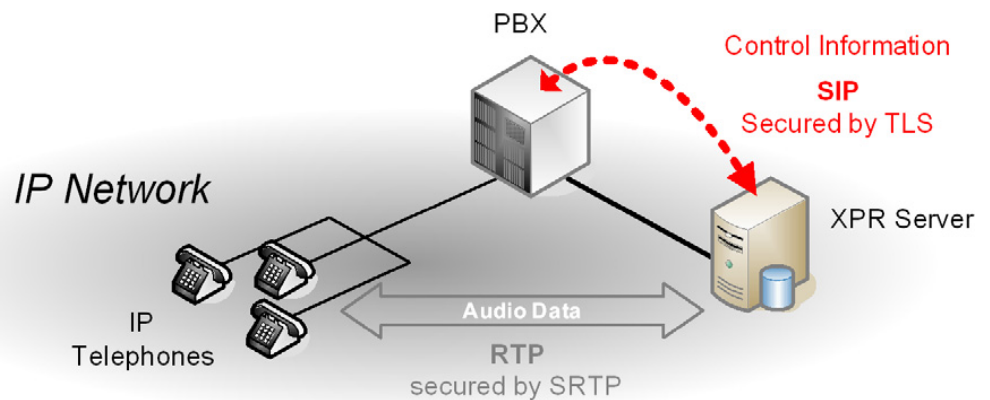
- ensuring the authenticity of a communication partner
To this, TLS uses security certificates and asymmetric encryption. Consequently, intruding parties cannot send messages the originator of which is apparently a different person.
- assuring the confidentiality of a connection
Data are encrypted before their transmission. This makes it difficult for intruding parties to read along sent messages.
- guaranteeing message integrity
Intruding parties are stopped from unnoticeably modifying messages.

You find detailed information about encrypting TLS information in [Section 10.3.10, “Public Key Infrastructure \(PKI\)”](#), on page 582.

You find further information about the TLS protocol e.g. under <http://www.ietf.org/rfc/rfc2246.txt>.

10.3.12.2 Using TLS in the XPR Server Environment

The following figure shows an example of connecting a PBX to the XPR server – via the IP APL and the SIP protocol.



In the XPR server environment, TLS secures management information that is exchanged between the XPR server and PBX.

IMPORTANT:

TLS is store-and-forward-based protocol. To ensure encryption of the SIP management information on the entire transmission network from the XPR server to the SIP terminal device, TLS must also be implemented between PBX and telephone.

NOTE:

OpenScape Voice respectively HiPath 8000 endpoints do not use TLS by default. For using TLS you need to set the **MTLS** transport protocol or the **Use Server Virtual Address** option for the relevant endpoints.

10.3.12.3 TLS Support in the IP APL

The IP APL supports TLS V1, V1.1 and V1.2 for connections via:

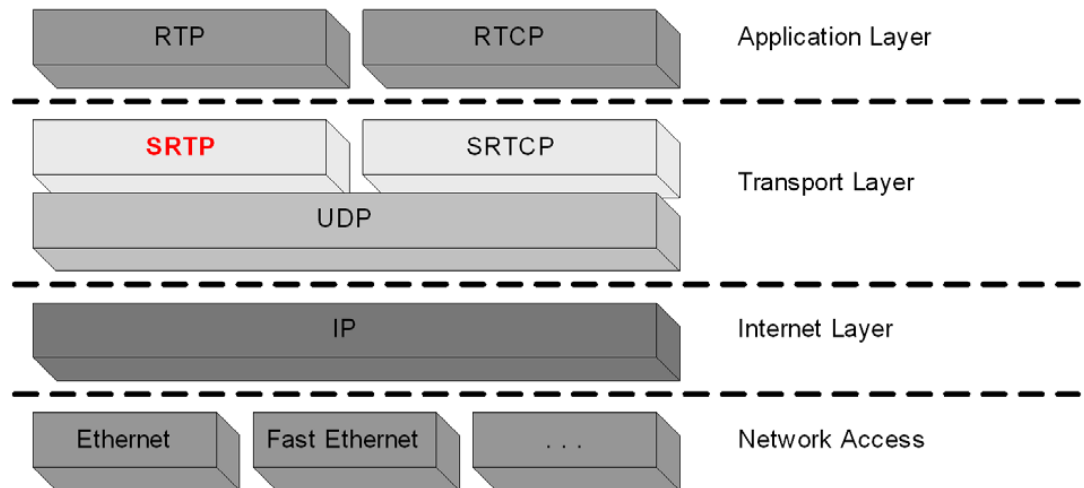
- SIP.

10.3.13 Encryption of the RTP Communication (SRTP)

To secure RTP messages, the IP APL supports the IETF protocol Secure Realtime Transport Protocol (SRTP).

10.3.13.1 Secure Realtime Transport Protocol (SRTP)

The following figure shows the position of the SRTP protocol in the TCP/IP layer model.



SRTCP mainly aims at

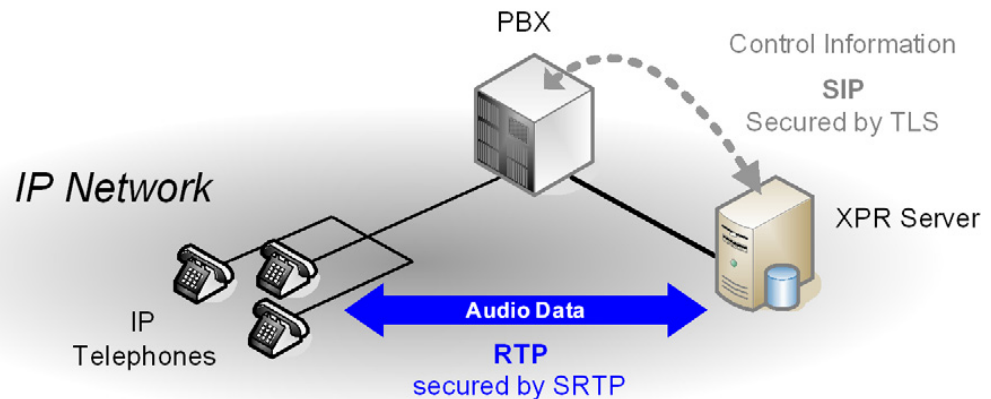
- ensuring the authenticity of a communication partner
For this purpose, communication partners usually exchange keys for each connection to encrypt the message transmission. Consequently, intruding parties cannot send messages the originator of which is apparently a different person.
- assuring the confidentiality of RTP payload
RTP data are encrypted before their transmission. This makes it difficult for intruding parties to read along sent messages.
- guaranteeing the integrity of RTP payload and header
Intruding parties are stopped from unnoticeably modifying messages.

You find further general information about the SRTCP protocol e.g. under <ftp://ftp.rfc-editor.org/in-notes/rfc3711.txt>.

You find detailed information about generating and distributing keys for SRTCP in [Section 10.3.11, "Multimedia Internet Keying \(MIKEY\)", on page 585](#).

10.3.13.2 Using SRTCP in the XPR Server Environment

The following figure shows as example the previously described connection of a PBX to the XPR server – via the IP APL and the SIP protocol.



In the XPR server environment, SRTP secures audio information that is exchanged between the XPR server and other terminal devices.

10.3.13.3 SRTP Support in the IP APL

IMPORTANT:

The SRTP protocol may currently only be used after an individual project release.

The IP APL supports SRTP for connections via

- SIP.

10.3.14 IP APL at a Layer 3 Cluster of OpenScape Voice

An OpenScape Voice Layer 3 cluster consists of several OpenScape Voice systems that are distributed among various locations and are to act like a single communication system for a connected XPR server. Such an OpenScape Voice cluster can be used to enable the following features for communication services:

- High availability
- Load distribution

So that the systems of an OpenScape Voice cluster can be addressed by the IP APL, the OpenScape Voice systems of the cluster register under a defined cluster name with at least one Domain Name System (DNS). This cluster name must also be configured in the settings of the SIP device during the configuration of the IP APL.

If the IP APL is to set up a connection via the OpenScape Voice cluster, the IP APL resolves the configured cluster name into one or several IP addresses. To this the IP APL uses the DNS, which is configured in the LAN settings of the APL's associated XPR server system. Besides IP addresses the APL receives further information: for example, whether the relevant OpenScape Voice cluster is configured for load distribution.

10.3.15 IP APL at an SIP Gateway Cluster

The IP APL can be connected to several SIP gateways of an SIP cluster for redundancy. The associated configuration is currently executed via the following parameters of the **Private** registry value:

- **CLUSTERGW1, CLUSTERGW2, CLUSTERGW3** etc.
- **CLUSTERCNT**
- **CLUSTERTIMESENS**

You find the relevant registry value **Private** under:

```
HKLM\Software\Wow6432Node\PP-COM\MRS\IpApl\Devices
```

By default, the IP APL uses the gateway that is configured via the XPR monitor to send SIP signals and MWI messages. If this connection fails, the IP APL can use other SIP gateways, which are defined via the **CLUSTERGW** parameter.

The **CLUSTERCNT** and **CLUSTERTIMESENS** parameters define when the IP APL considers a connection to an SIP gateway failed.

To find out whether the connection to an SIP gateway failed, the IP APL uses so-called failure windows. If the IP APL detects at least one SIP or MWI connection error in such a failure window, the communication within this failure window is considered failed.

CLUSTERCNT defines after how many failure windows with failed communication the IP APL considers the communication failed and uses the next SIP gateway. Every successful connection resets the current number of failure windows with failed communication to 0.

CLUSTERTIMESENS defines how long each failure window lasts. The IP APL starts the first failure window with the first connection error. Based on this connection error the communication within the first failure window is considered failed. If value **1** has been configured for **CLUSTERCNT**, the IP APL uses the next SIP gateway immediately after the first connection error and the setting of **CLUSTERTIMESENS** is irrelevant.

After a reboot the IP APL always uses the gateway deployed last.

Requirements for using an SIP gateway cluster

If you want to use the IP APL at an SIP gateway cluster, the following requirements must be complied with:

- The IP APL does not use an OpenScape Voice cluster
- The IP APL does not use TLS
- Each gateway of the SIP gateway cluster must use the same SIP configuration (e.g. the same transport protocol).

10.4 Protocols of the XPR Server

The XPR server supports a large number of protocols. These are described in this chapter in detail.

- [Evo](#)
- [Ergo](#)
- [PhoneMail](#)
- [Voicemail VMS](#)
- [Fax G3](#)
- [Fax G3 Post-Dialing](#)
- [Fax G3 Polling](#)
- [Fax G4](#)
- [Fax-on-Demand Server Script \(Fax-on-Demand\)](#)
- [Fax-Fax Converter \(Fax Forward\)](#)
- [Single Number](#)
- [SMI](#)
- [Voice](#)
- [PlayWave](#)
- [Hicom Message Waiting Indication \(MWI\)](#)
- [Message Waiting Indication \(MWI\)](#)
- [Pager](#)
- [SMS \(TAP or UCP Protocol\)](#)
- [AMIS](#)
- [CTI Computer Telephony Integration](#)
- [CTI Light](#)
- [Vogue](#)
- [Caller Guide](#)
- [Conversation Recorder](#)

10.4.1 Evo

EVO is the latest voice mail script of the XPR server. In principle, it provides the same features as Ergo. Because of its speech recognition feature, which is integrated in the TUI, it can also be controlled via voice commands.

Just like other voicemail scripts, Evo always works in a Telematic APL context. This is why you reach the Evo configuration dialogs also via the settings dialog of the Telematic APL used in the XPR monitor. You find the Evo configuration in the corresponding protocol settings (*Protocols* tab) via the **Parameters** button on the configuration tab *Script*. Subsequently, the parameter tabs that will be described in the following section are displayed.

The XPR server selects reasonable defaults for all other configuration values.

Modifications of the configuration values can be made via the global voice mail profile settings (see [Section 10.9.2, “General Voicemail Settings \(Voicemail\)”](#), on [page 811](#)) and the configuration dialogs the Evo script.

IMPORTANT:

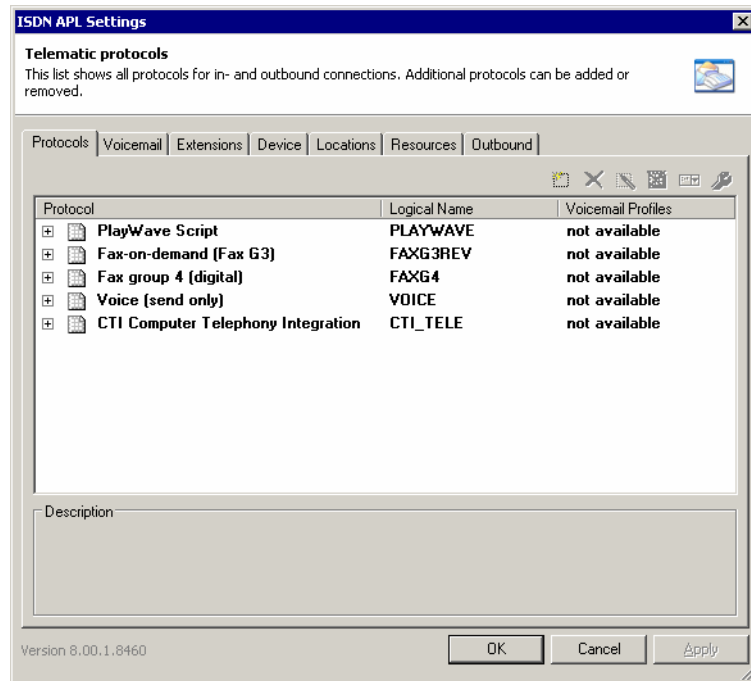
The EVO script is not installed via the XPR server default setup. Before it can be added as protocol in the setting dialog, it must have been manually installed from the product data carrier beforehand.

Start therefore the `setup.exe` file in the `XpressionsInstall\AddOn\Misc\ASR` directory. Then, a setup wizard to accompany the following installation steps opens.

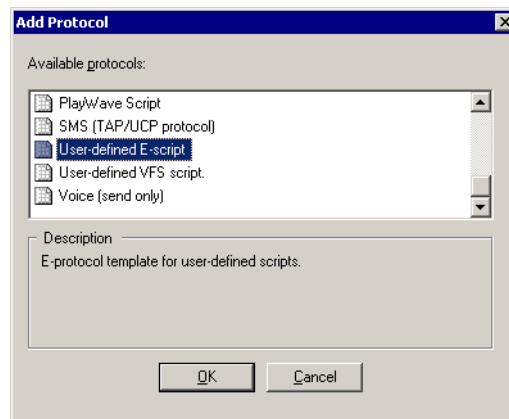
10.4.1.1 Installation of the EVO Protocol

After the installation of the Evo protocol proceed as follows to add the protocol to the current XPR environment.

1. Select the **Advanced Settings** option under the applied telematics APL in the XPR monitor.
2. Select the **Add...** button in the toolbar to add EVO to the current XPR configuration.



3. Select the **User-defined E-script** entry from the available protocols and confirm your choice with **OK**.



4. Enter a short script name in the **Name** field. We recommend to enter *EVO*.

The screenshot shows the 'E-Script Protocol Properties' dialog box with the 'General' tab selected. The 'Name' field contains 'EVO'. The 'Protocol designation' field contains 'EVO script'. The 'Description' field contains 'voice-operated voice mail script'. The 'OK', 'Cancel', and 'Apply' buttons are at the bottom.

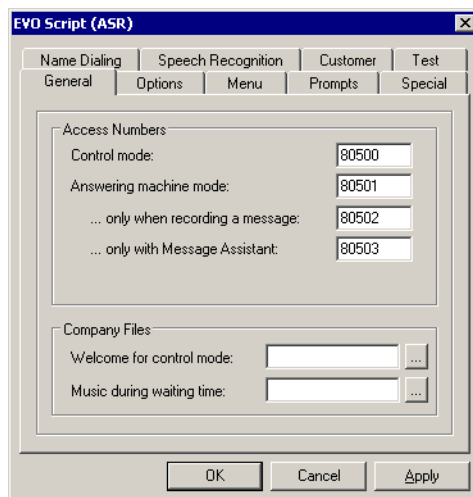
5. In the **Protocol designation** and **Description** fields also enter a “descriptive” entry.
6. Save the settings you made by clicking the **Apply** button.
7. Change to the *Script* tab and select **Evo Script (ASR)** as E-script.

The screenshot shows the 'E-Script Protocol Properties' dialog box with the 'Script' tab selected. The 'E-Script' dropdown menu is set to 'Evo Script (ASR)'. Below the dropdown are 'Parameters...' and 'Compile' buttons. The 'OK', 'Cancel', and 'Apply' buttons are at the bottom.

8. Select the **Parameters** button to install the EVO script parameters.

The EVO script has now been added to the XPR server. Let's have a look at the parameter tabs of the EVO script.

10.4.1.2 Parameter Tab *General*



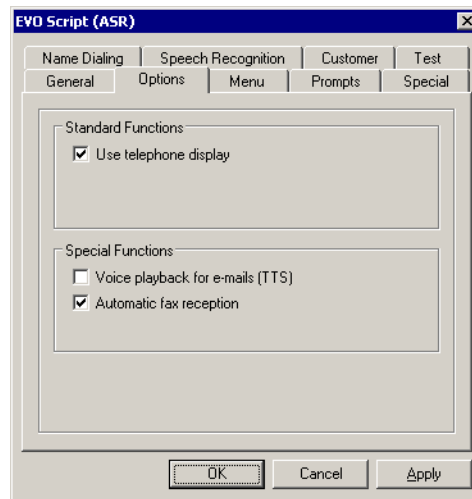
On this tab, the extension ranges for the different operation modes of the EVO script are defined in the *Access Numbers* section. In principle, determining a phone number for the **Control mode** and the **Answering machine mode** is required.

For direct access to the forwarding mode (answering machine mode after diversion to the individual mailbox) two additional access numbers can be defined. They allow access with fixed functionality, no matter which voice mail settings the user has performed. An access number can be defined that exclusively allows leaving a message and another one that merely starts the message wizard.

In the *Company Files* section you can configure a new greeting under **Welcome for control mode** that will be used instead of the default greeting. The respective PCM file must be selected via a file selection window. The system announcements are stored in the path `<XPR Install>\res\E\evo\<language>\`.

As in TUM (True Unified Messaging) environments – depending on the reply times – the response time to mailbox queries may take some time, a tune is played during waiting times. Thus the user is informed that he/she is still connected to the system and the entries are being processed. This waiting tune can be defined individually in the **Music during waiting time** field similarly to the welcome greeting.

10.4.1.3 Parameter Tab *Options*



In the *Options* parameter tab the following functions may be configured.

Use telephone display

Determines if the texts are to be sent to the displays of the connected telephone devices.

NOTE:

This feature should be deactivated, if the applied PBX does not support telephone display at the device.

Voice playback for e-mails (TTS)

Enables or disables the feature that e-mails can be played back via a speech converter when messages are retrieved for all users.

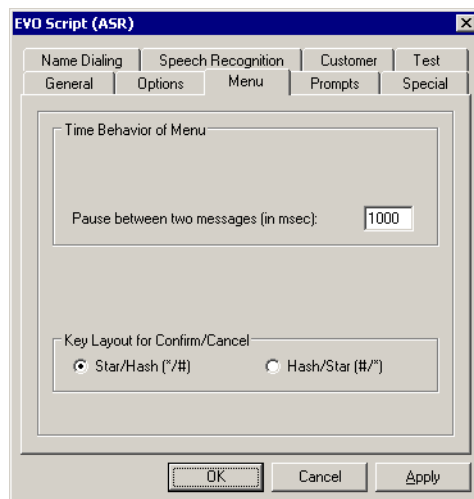
IMPORTANT:

E-mails can only be read out by the system if a license for the speech converter and a license for the XPR server feature has been purchased. The speech converter can be supplied by a third party supplier (e.g. *Speechworks Speechify*) or by your system integrator.

Automatic fax reception

If this option is activated, Evo switches in case of an incoming fax automatically to fax receiving and stores the fax in the user's mailbox. This switching requires Evo being able to recognize a fax tone.

10.4.1.4 Parameter Tab Menu



In this parameter tab settings to the menu navigation, especially time behavior in the menu navigation are made.

The following parameters are configurable:

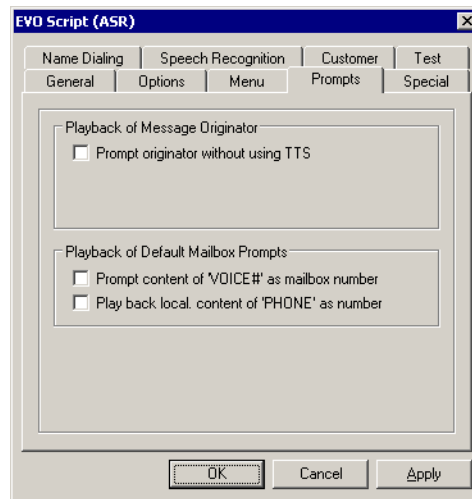
Pause between two messages

Describes the time interval from the end of the message just played back until the playback of the next message. The configuration range is between 0 and 9999 milliseconds. Default is 1000 milliseconds.

Key Layout for Confirm/Cancel

Via this option the features of the * and # key can be exchanged. Per default, all user entries can be confirmed via the * key, and the # key serves to cancel the current operating step. If the converse behavior is desired, it can be changed via this setting. Thus you can react flexibly to the usage conventions of voice mail systems that might be replaced.

10.4.1.5 Parameter Tab *Prompts*



On this parameter tab, settings are made for the announcements of the message originator and recipient. These settings only take effect when the originator or recipient has not recorded a name greeting.

The following parameters are configurable:

Prompt originator without using TTS

If the Text-to-Speech (TTS) feature is installed, the system interprets the entry of the database field **NAME** as originator announcement.

Prompt content of VOICE# as mailbox number

Defines that the content of the database field **VOICE#** is played as mailbox number. Normally, the internal extension is entered here that the XPR server transmits to the **VOICE** database field in normalized form.

Play back local. content of 'PHONE' as number

Defines if the normalized phone number in the database field **PHONE** is played localized as announcement. Localized means that the normalized calling number is reduced to the mere subscriber calling number.

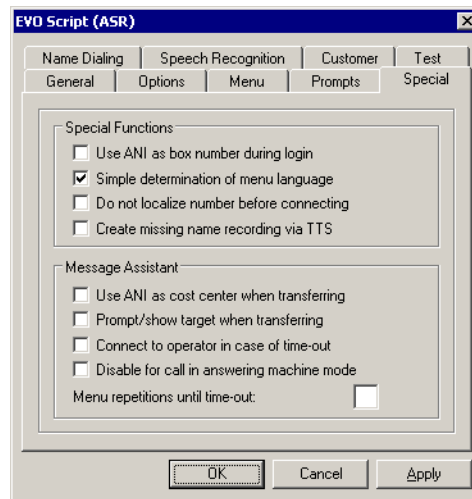
Example:

If the entry in the **PHONE** field is *49 2404 901 111*, the greeting is “111”.

NOTE:

When the user has not defined an individual name greeting or another greeting, the mailbox number is given out per default (database field **VOICE**).

10.4.1.6 Parameter Tab *Special*



On this parameter tab, some special functions can be configured.

The following settings are possible:

Use ANI as box number during login

Via this option, it is possible to determine a simplified procedure to access the individual mailbox. EVO first determines the number of the calling device (ANI). If you dial into the control mode of the voice mail system via your own telephone device, EVO searches the corresponding mailbox number of this subscriber and automatically uses it. Thus entering the mailbox number manually is omitted. In this case you only have to enter the access PIN.

NOTE:

If the user has additionally defined the calling device as trusted number, even entering the PIN becomes unnecessary. You may access the control mode directly without further inputs. Cf. [Section 10.9.2.4, “Security Settings”, on page 816](#).

Simple determination of menu language

This function allows you to determine by which criteria the menu language is selected in case of a call. If the option is activated, the default language is always used first in the control and answering machine mode for announcements. After login, EVO will switch to the language selected by the user for his/her mailbox. If the mailbox is accessed directly, the menu language configured for this mailbox is used. If no language was selected, the default setting is automatically fallen back to.

If this function is not activated, EVO will try to offer the appropriate menu language depending on the access mode or the selected mailbox. If the number of the caller is not transmitted, EVO will use the default language. If it is transmitted and can be assigned to an XPR user, EVO can connect the determined phone number with the corresponding user and thus deduce the voice settings from here. If the transmitted phone number is unknown to the XPR server, the language will be set according to the country code.

Example:

If the transmitted phone number is unknown to the XPR server and if the ANI starts with **49**, German is selected.

NOTE:

If the VOGUE script routes a caller to EVO, EVO uses for all greetings the language that the VOGUE script has already defined for the caller – for example via a national language box.

Do not localize number before connecting

Normally, all phone numbers are internally localized before they are sent as dial information. This option forces EVO to ignore this localization and to dial the number directly.

Create missing name recording via TTS

If no name recording is available, the Text-to-Speech software generates the configured user name as a file that is later used for name announcement.

NOTE:

The following settings for the behavior of the message assistant only take effect if the user configures his/her mailbox enabling the message assistant. If the mailbox is only used as answering machine, these settings are not interpreted.

Use ANI as cost center when transferring

In case of a transfer, the mailbox number is passed to the PBX as caller by default. In this way the mailbox number is used for billing.

With this option you can have a caller's phone number transferred to the PBX so that his/her number is used for billing.

Prompt/show target when transferring

Selecting this box globally suppresses the announcement and display of the target calling number. This option should be activated when for reasons of confidentiality calling numbers are not to become public.

Connect to operator in case of time-out

Callers may not be able to operate the message wizard menu – for example, when their telephone does not support DTMF. If this option is active in such a case, the relevant callers are automatically routed to the postmaster after a configurable number of menu prompts.

If this option is disabled, callers without DTMF-compatible telephone are merely prompted to leave a message.

Disable for call in answering machine mode

Defines if the message assistant is globally deactivated for all users in the answering machine mode.

Menu repetitions until time-out

Use this field to enter the number of menu repetitions until the call will be disconnected (time-out).

NOTE:

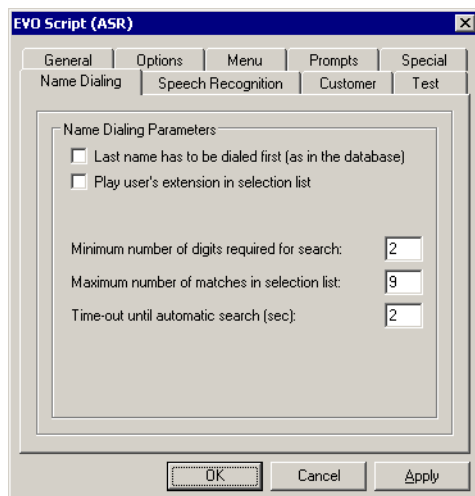
0A caller without DTMF-compatible telephone is unlikely to listen to the greeting again when he/she realizes that Ergo does not accept any entries from him/her.

10.4.1.7 Parameter Tab *Name Dialing*

This parameter tab serves for the name dialing configuration. Thus it allows Evo users to establish a telephone connection not only by entering phone numbers, but also by defining a name. The name must be entered via the keys of the telephone device, since speech recognition is not supported for name dialing (see [Section 10.4.1.8, “Parameter Tab Speech Recognition”, on page 608](#)).

If you want to enter a name via the keys of your device to establish a connection, the single letters must be entered by pressing the corresponding key once (vanity number). To allow for faster entries, not all letters of a name must be entered. The entry can be finished after the first characters with the * or # key (cf. [Section 10.4.1.4, “Parameter Tab Menu”, on page 599](#)). The EVO script will then deliver a list with all known user names starting with the character string you entered.

To optimize searching in the database on the basis of name dialing, the XPR server uses the VM_VANITY database field. In this database field the XPR server deposits a user-individual vanity number created from another database field of the respective user. You find more details on this in [Section 11.11, “Vanity Number Support”, on page 895](#).



In the parameter tab *Name Dialing* the following settings are available:

Last name has to be dialed first

This option controls the operating instruction integrated in EVO for entering name dialing by a user. For this operating instruction two options are available:

- Name dialing entry starting with the first name
- Name dialing entry starting with the last name

NOTE:

The setting **Last name has to be dialed first** only controls which operating instruction is played to the user of the EVO script. The selected option does *not* influence the search algorithm of the XPR server.

The XPR server compares the search information entered for name dialing with the entries of the **NAME** fields in the XPR database. Depending on the users being stored with leading first name or last name, the operating note **Last name has to be dialed first** must be activated or not.

Consequently, a mixture of the first and last name sequence in the **NAME** fields of the XPR database causes problems in the search algorithm.

Play user's extension in selection list

If a user receives a hit list for name dialing, each hit can be announced either with or without the corresponding extension. If this option is selected, the extension is indicated.

Minimum number of digits required for search

For name dialing not the complete name of the callee must be entered. This option defines, how many letters need to be entered at least when dialing via the telephone keys before a search will start. If you finish the name dialing with the * or # key after having entered fewer numbers than required, the EVO script prompts you to continue the entry.

Maximum number of matches in selection list

The entry made here defines the maximum length of hit lists. If a hit list with more users than defined here results from name dialing, the EVO script points this out and requests redialing. This redialing should then be performed with a qualified entry to shorten the hit list.

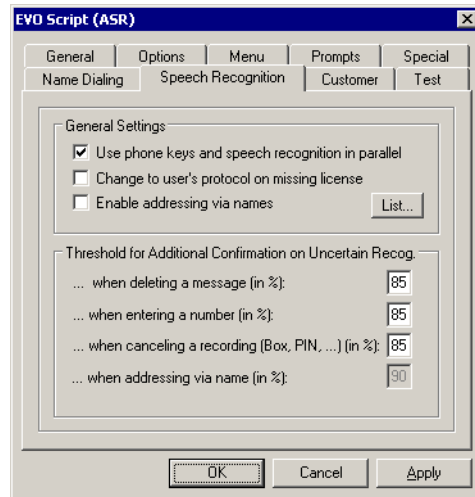
Time-out until automatic search

If no further entry is made via the telephone keys in the time interval defined here, EVO starts an automatic search for a corresponding user name. Only the characters entered until now are used for the search.

If this entry should fall below the **Minimum number of digits required for search**, the Evo script again prompts to continue the entry.

10.4.1.8 Parameter Tab *Speech Recognition*

Via this parameter tab settings for automatic speech recognition are made.



The following settings are available:

Using phone keys and speech recognition in parallel

To navigate through the Evo script menu, the user may deploy, besides speech recognition, also telephone keys for DTMF dialing. This may be required if, for example, the automatic speech recognition is unable to properly recognize voice entries owing to external influences – such as noises, low user voice etc. To release this feature, this option must be activated.

If this option has been deactivated, DTMF dialing cannot be used within EVO. In the event that the Evo script receives a DTMF tone from the user just the same, the call is diverted to the DTMF-capable voicemail script configured for the respective XPR user (e.g. PhoneMail).

This voice mail script is defined in the **VM_PROTOCOL** field of the Correlation Database, which is available for individual users as well as for complete user groups. If the EVO script receives a DTMF tone that is not permitted, the user-specific setting is applied first. If no entry exists, a setting for the respective user group is searched for. If neither entry exists here, the system continues with the EVO script.

Change to user's protocol on missing license

If all Evo licenses for the existing voice mail connections are in use, the XPR server can react to an additional caller as follows:

- Rejecting the new call, since no licenses are available
- Rerouting the call to the voicemail script that has been configured for the relevant XPR user (e.g. PhoneMail)

NOTE:

The respective voice mail script is defined in the **VM_PROTOCOL** field of the Correlation Database. This field is available for individual users as well as for complete user groups.

If no free EVO license is available for a call with this option, the user-specific setting is applied first. If no entry exists, a setting for the respective user group is searched for. If neither entry exists here, the respective call is rejected.

If the option **Change to user's protocol on missing license** has been activated, a call will be diverted to the possibly configured voice mail script when the Evo licenses do not exist. Otherwise the call would be directly rejected.

Enable addressing via names

EVO allows speech-recognizing dialing by addressing user names. For this, it compares the spoken name of the desired conversation partner per default with the unique user names available in the **Name** fields of the XPR user database.

Since it is possible that name entries of XPR users are abbreviated or encrypted (e.g. *ABC help*), this default setting can be extended (How should the user named *ABC help* be pronounced at all? *Abs help*?) Therefore you can create up to 99 additional fields in the XPR user database for any user (**VM_ASR_NAME_01 ... VM_ASR_NAME_99**). Each of these additional fields can then contain exactly one possible name pronunciation entry.

Example:

Cycos AG	– Cycos Peelsee, Cycos Public Limited Company, Cycos
ABC help	– Abeesee help, spell aid, help, hotline

The thus complemented fields are then checked in addition to the **Name** database fields for a match with the addressed user.

NOTE:

The database fields **VM_ASR_NAME_<xx>** must be added manually in the XPR database. Use the Web Assistant and add the desired fields to the **USER** mask. For detailed information on this, please refer to the appropriate user manual.

To enable addressing via names, you need to create the vocabulary required for speech recognition first. This vocabulary is composed of the entries of the database fields **Name** (and possibly **VM_ASR_NAME_<xx>**) of the XPR users, who furthermore have an entry in the database field **VOICE**. To initiate the creation of vocabulary, you need to select the **List** button after you have activated the **Enable addressing via names** option.

NOTE:

After the initial activation of the **Enable addressing via names** option or after modifying the **Name** or **VM_ASR_NAME_<xx>** database fields a name list must be generated. This occurs automatically in the first case.

Threshold for Additional Confirmation on Uncertain Recognition ...

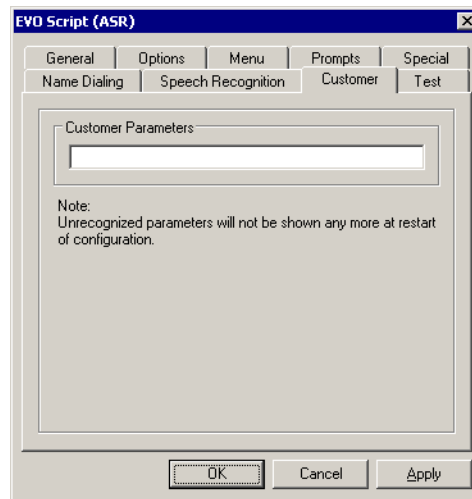
The speech recognition used with EVO returns a value in percent after each speech-based entry to indicate the entry's recognition quality. This value describes how certain the assignment of entry and associated entry of the known vocabulary is.

Depending on the size of the defined threshold value you can define if additional verification of the match by users is to take place. During this verification EVO asks the user if the found match corresponds to his/her choice. If no verification is effected since the recognition quality value is higher than the defined threshold, the found match is automatically accepted as correct and executed.

Thresholds need to be configured for the following actions:

- **... when deleting a message**
Defines a threshold (in percent) for speech recognition when a message is deleted
- **... when entering a number**
Defines a threshold (in percent) for speech recognition when recordings are canceled
- **... when canceling a recording (Box, PIN, ...)**
Defines a threshold (in percent) for speech recognition when numbers are entered (voicebox, PIN etc.)
- **... when addressing via name**
Defines a threshold (in percent) for name recognition in addressings.

10.4.1.9 Parameter Tab *Customer*



In the parameter tab *Customer* you can enter special, customer-specific parameters.

The following parameter settings are available at the moment:

- `-fewv`
- `-pga`
- `-rmtopic.`

Beyond that, the following five parameters (silence detection parameters), via which the Evo silence detection can be adjusted, exist.

- `recplen=`
- `recplvl=`
- `recslen=`
- `recslvl=.`

If several parameters are to be used simultaneously, they are entered in the entry row, separated by a blank. Invalid parameters are ignored and no longer shown when this configuration page is called again.

Let's have a closer look at the functions of these parameters.

-fewv (Forward Email with Voice Annotation)

By default, an annotation can only be recorded for voice mails to be forwarded.

With this parameter, the annotation function can also be activated for e-mails to be forwarded.

-pga (Pre-Greeting-Announcement)

With this parameter string you can implement an additional welcome message for external, inbound calls. In this way you can have e.g. a company greeting played before the EVO voice mail system answers the call. This can be required to inform customers that they are connected to the right extension. The associated greeting specific to a company is not included in the Evo scope of delivery. If required, such a greeting must be recorded individually.

Some important remarks on this:

- The greeting file to be implemented must be generated in the PCM format
- Its name must be `pregreetingann.pcm` since only a greeting file with this name is played at this point.
- The directory in which this greeting file must be stored is `<XPR Install>\res\E\evo\` and there in the folder according to the currently selected language (*Example: american or british*).

-rmtopic (Remove XPR Monitor Topic)

If the XPR server is set up completely, it may happen that no topic entry for Evo monitoring can be created in the modules window of the XPR monitor as their number per APL is limited (max. 64). With the help of this parameter string the XPR monitor can be configured in a way that some existing topics can be removed from the branch of the applied telematics APL and EVO can be inserted as topic.

recplen, recplvl, recslen and recslvl

As the electronic password depends on the volume of the applied recording/playback components in a recording, it might be necessary to adapt the volume. The impulse length that must at least be available for starting a recording can be additionally influenced.

The following four parameters are used to detect speaking or silence for starting or stopping a recording. In this way recording times are limited so that no unnecessarily large recording files are generated. The problem is to select the level that clearly recognizes speech but still interprets line and background noise as silence, for example. The thresholds for length and peak level, required to detect breaks, can be adapted here.

recplen=<value> (Record Peak Length)

Defines in milliseconds the minimum pulse length of a signal in order to be detected as such.

Default: 64

Value range: 0 to 4000

recplvl=<value> (Record Peak Length)

Defines the minimum peak level of a signal for starting a recording. The higher the “peak level” is selected, the louder a person must speak to start a recording. When the entry value is divided by 40, you receive the level value in percent (in relation to the maximum value).

Default: 32

Value range: 0 to 4000

recslen=<value> (Record Peak Length)

Defines in milliseconds the minimum impulse length a break must have for stopping a recording.

Default: 3000

Value range: 0 to 4000

recslvl=<value> (Record Peak Length)

Defines the minimum peak level a break must have for stopping a recording. The higher the “peak level” is selected, the louder a person must speak for the recording not to be stopped. When the entry value is divided by 40, you receive the level value in percent (in relation to the maximum value).

Default: 32

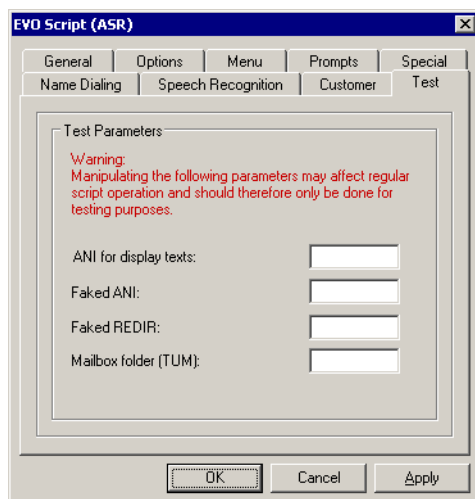
Value range: 0 to 4000

10.4.1.10 Parameter Tab Test

This parameter tab serves for entering test parameters.

IMPORTANT:

In a customer system, no parameters may be entered here. Nonsensical entries may hamper regular EVO operation, or make it even impossible.



The functions of the entry fields are as follows:

ANI for display texts

You can enter a telephone number in this field, to which all display text will then be diverted. This option is only designed for a general feature check.

Faked ANI

For testing purposes an arbitrary number, automatically interpreted by the system as recognized calling number for every further call, can be entered here.

Faked REDIR

Another field for testing purposes in which you can specify – similar to the **Faked ANI** – a redirected number for call rerouting.

Mailbox folder (TUM)

Here you can explicitly define the output mailbox folder for True Unified Messaging (TUM) by entering its name.

10.4.1.11 Adjusting the XPR Routing Rules

Scenario:

Let us contemplate an Exchange or Lotus Notes integration without True Unified Messaging and without inbox replication. Voice mails remain on the XPR server and are exclusively polled via EVO. Only fax messages are delivered to the foreign system and with voice mails a corresponding notification report is sent in most cases.

Since Evo tries to access the messages via the TUM interface and would access the foreign system on the basis of the data from the user database (database field **PREFERRED**), the routing rules need to be customized.

The following rule must be inserted before the first rule entry, while *<Server Name>* needs to be replaced with the XPR server name:

```
NVS : <Server Name> /* [TYPE=TRANS] =NVS:MAILBOX/* [ABORT=1]
```

Thereby all transactions by Evo are routed to the Mail APL which acts as TUM Backend for access to the XPR-own database. Furthermore, the preferred rule must be modified so that it does not cancel out the alteration made above:

```
NVS : * . * /* [ABORT=0] = <PREFERRED>
```

In the registry, the HKLM\Software\Wow6432Node\PP-COM\MRS\MailApl\TumBackend value should either not exist or be set to **1** so that the TUM functionality of the Mail APL is active.

NOTE:

In this scenario the corresponding TUM APL for access to user inboxes must be installed just the same if you want to generate notifications via the Notification APL by Web Administrator.

For the Evo operation the user manual *Evo* is available.

10.4.2 Ergo

Ergo is a powerful voice mail system of the XPR server that reads and writes messages via the TUM interface. Within the XPR server there are diverse APLs for access via the TUM interface to Microsoft Exchange, Lotus Notes and the individual XPR database.

The Ergo script operates as protocol always in a Telematic APL context. This is why you reach the Ergo configuration dialogs via the settings dialog of the Telematic APL used in the XPR monitor. You will find the ERGO configuration in the corresponding protocol settings (*Protocols* tab) via the **Parameters** button on the configuration tab *Script*. Subsequently, the parameter tabs that will be described in the following section are displayed.

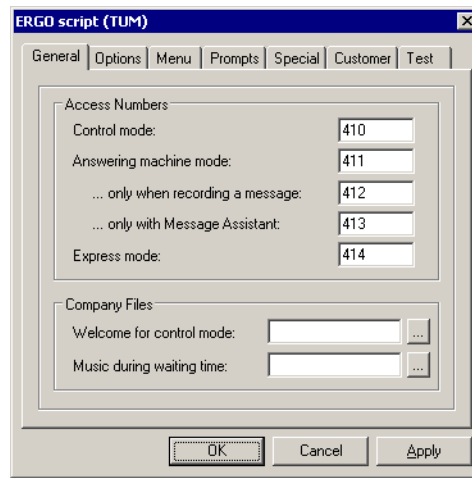
The access numbers for the *Control mode*, *Answering machine mode* and *Express mode* are automatically assigned during the installation from the first three numbers of the configured extension number range.

For all other configuration values reasonable defaults are used.

Modifications of the configuration values can be made via the global voice mail profile settings (see [Section 10.9.2, “General Voicemail Settings \(Voicemail\)”, on page 811](#)) and the configuration dialogs of the Ergo script.

Let's have a closer look at the configuration dialogs of the Ergo scripts.

10.4.2.1 Parameter Tab *General*



In the **Access Numbers** section you can configure the phone numbers for the single ERGO operating modes: the phone numbers for the *Control mode*, *Answering machine mode* and *Express mode*. The first three phone numbers of the extension range defined for ERGO are already automatically preconfigured as ERGO access numbers during the server setup.

All access numbers must be specified in one of the following phone number formats:

- As extension
Example: 100
- As normalized phone number with leading plus sign
Example: +492404901100.

IMPORTANT:

The XPR server does not check whether the entries made are correct. Wrong entries lead to ERGO malfunctions.

In principle, a definition of calling numbers for the control, answering machine and express mode is required when redirected numbers are used. In this case users are assigned their telephone number as voice mail number and redirect their telephone to the number of the answering machine mode. When extension ranges are available this is only required for the express mode since each user has a separate calling number for their mailbox and can also switch to the control mode from the thus accessible answering machine mode.

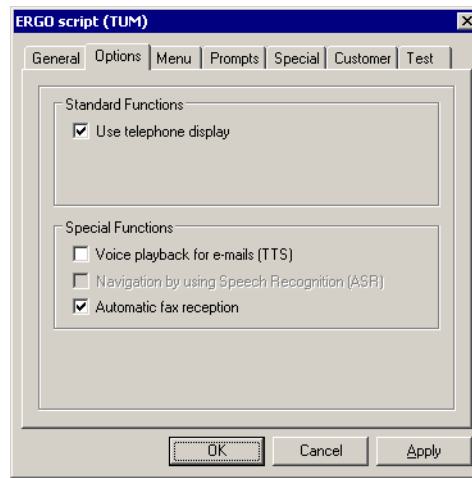
For direct access to the forwarding mode (answering machine mode after diversion to the individual mailbox) two additional access numbers can be defined. They allow access with fixed functionality, no matter which voice mail

settings the user has performed. An access number can be defined that exclusively allows leaving a message and another one that merely starts the message wizard.

In the *Company Files* section you can configure a new greeting under **Welcome for control mode**, which will be used instead of the default greeting. The respective PCM file must be selected via a file selection window. The system announcements are stored in the path `<XPR
Install>\res\E\ergo\<language>\.`

As in TUM (True Unified Messaging) environments – depending on the reply times – the response time to mailbox queries may take some time, a tune is played during waiting times. Thus the user is informed that he/she is still connected to the system and the entries are being processed. This waiting tune can be defined individually in the **Music during waiting time** field similarly to the welcome greeting.

10.4.2.2 Parameter Tab *Options*



In the *Options* parameter tab the following functions may be configured.

Use telephone display

Determines if the texts are to be sent to the displays of the connected telephone devices.

NOTE:

This function should be deactivated when a PBX not supporting a display is used.

Voice playback for e-mails (TTS)

Enables or disables the feature that e-mails can be played back via a speech converter when messages are retrieved for all users.

IMPORTANT:

E-mails can only be read out by the system if a license for the speech converter and a license for the XPR server feature has been purchased. The speech converter can be supplied by a third party supplier (e.g. *Speechworks Speechify*) or by your system integrator.

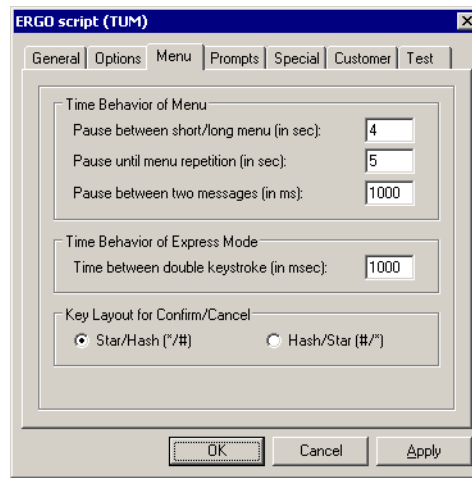
Menu navigation by Speech Recognition (ASR)

For the future implementation of menu navigation by speech recognition (Automatic Speech Recognition). This feature activates or deactivates menu operation per voice input for all users. Functions are then triggered through speaking the desired command instead of pressing a key (DTMF command).

Automatic fax reception

If this option is activated, Ergo switches in case of an incoming fax automatically to fax receiving and stores the fax in the user's mailbox. This switching requires Ergo being able to recognize a fax tone.

10.4.2.3 Parameter Tab *Menu*



In this parameter tab settings to the menu navigation, especially time behavior in the menu navigation are made.

The following parameters are configurable:

Pause between short/long menu

After the complete output of system greetings in a menu, a more detailed system greeting is automatically switched to after the pause you have specified here. The configuration range is between 1 and 99 seconds. Default is 4 seconds.

Pause until menu repetition

Once the short and subsequently the long menu have completely been played, the output procedure starts all over again after a break. The time between repetitions can be modified here. The configuration range is between 1 and 99 seconds. Default is 5 seconds.

Pause between two messages

Describes the time interval from the end of the message just played back until the playback of the next message. The configuration range is between 0 and 9999 milliseconds. Default is 1000 milliseconds.

Time Behavior of Express Mode

In express mode you can press an arbitrary key during message output to skip to the next message. With two keystrokes in succession (in a specific interval), a connection to the originator is immediately established.

To distinguish both types of entry, the first one is followed by a short waiting period. If not, the function first mentioned is triggered. The configuration range is between 0 and 9999 milliseconds. Default is 1000 milliseconds.

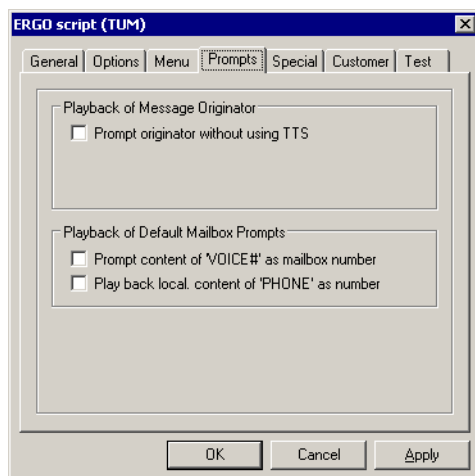
NOTE:

If this value is set to **0** no connection can be established to the originator. When you press a key the next message is immediately switched to.

Key Layout for Confirm/Cancel

Via this option the features of the * and # key can be exchanged. Per default, entries are confirmed via the * key, and the # key serves to cancel the current operating step. If the converse behavior is desired, it can be changed via this setting. Thus you can react flexibly to the usage conventions of voice mail systems that might be replaced.

10.4.2.4 Parameter Tab Prompts



On this parameter tab, settings are made for the announcements of the message originator and recipient. These settings only take effect when the originator or recipient has not recorded a name greeting.

The following parameters are configurable:

Prompt originator without using TTS

If the Text-to-Speech (TTS) feature is installed, the system interprets the entry of the database field **Name** as originator announcement. Via this option you can switch off this default.

Under **Playback of Default Mailbox Prompts** the following settings can be made:

NOTE:

When the user has not defined an individual name greeting or another greeting, the mailbox number is given out per default (database field **VOICE**).

Prompt content of VOICE# as mailbox number

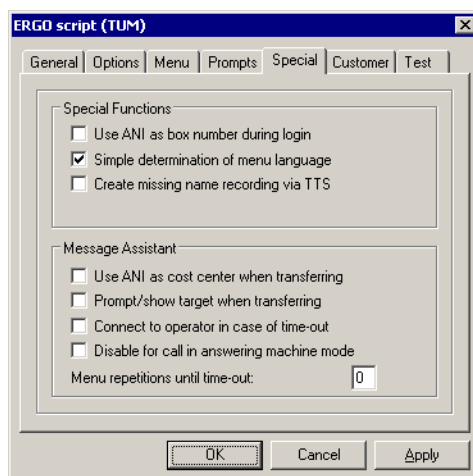
Defines that the content of the database field **VOICE#** is played as mailbox number. Normally, the internal extension is entered here that the XPR server transmits to the **VOICE** database field in normalized form.

Play back local. content of 'PHONE' as number

Defines if the normalized phone number in the database field **PHONE** is played localized as announcement. Localized means that the normalized calling number is reduced to the mere subscriber calling number.

Example: If 49 2404 901 111 is entered in the **PHONE** field, the greeting **111** occurs.

10.4.2.5 Parameter Tab *Special*



On this parameter tab, some special functions can be configured.

Under **Special Functions** the following settings can be made:

Use ANI as box number during login

Via this option, it is possible to determine a simplified procedure to access the individual mailbox. Ergo first determines the number of the calling device (ANI). If you dial into the control mode of the voice mail system via your own telephone, Ergo searches the corresponding mailbox number of this subscriber and uses it automatically. Thus entering the mailbox number manually is omitted. Only the access PIN has to be entered.

NOTE:

If the user has additionally defined the calling device as trusted number, even entering the PIN becomes unnecessary. You may access the control mode directly without further inputs.

Simple determination of menu language

This function allows you to determine by which criteria the menu language is selected in case of a call. If the option is activated, the default language is always used first in the control and answering machine mode for announcements. After login, Ergo will switch to the language selected by the user for his/her mailbox. If an extension range has been configured and you dial directly the corresponding extension of a mailbox, the language set for this mailbox is known and the menu language configured for this mailbox is immediately used. If no language was selected, the default setting is automatically fallen back to.

If this function is not activated, Ergo will try to offer the appropriate menu language depending on the access mode or the selected mailbox. If the number of the caller is not transmitted, Ergo will use the default language. If it is transmitted and can be assigned to an XPR user, Ergo can connect the determined phone number with the corresponding user and thus deduce the voice settings from here. If the transmitted phone number is unknown to the XPR server, the language will be set according to the country code.

Example:

If the transmitted phone number is unknown to the XPR server and if the ANI starts with **49**, German is selected.

NOTE:

If the VOGUE script routes a caller to ERGO, ERGO uses for all greetings the language that the VOGUE script has already defined for the caller – for example via a national language box.

Create missing name recording via TTS

If no name recording is available, the Text-to-Speech software generates the configured user name as a file that is later used for name announcement.

Under **Message Assistant** the following settings can be made:

NOTE:

The following settings for the behavior of the message assistant only take effect if the user configures his/her mailbox enabling the message assistant. If the mailbox is only used as answering machine, these settings are not interpreted.

Use ANI as cost center when transferring

In case of a transfer, the mailbox number is passed to the PBX as caller by default. In this way the mailbox number is used for billing. With this option you can have a caller's phone number transferred to the PBX so that his/her number is used for billing.

Prompt/show target when transferring

Selecting this box globally suppresses the announcement and display of the target calling number. This option can only be selected when for reasons of confidentiality calling numbers are not to become public.

Connect to operator in case of time-out

Callers may not be able to operate the message wizard menu – for example, when their telephone does not support DTMF. If this option is active in such a case, the relevant callers are automatically routed to the postmaster after a configurable number of menu prompts. If this option is disabled, callers without DTMF-compatible telephone are merely prompted to leave a message.

Disable for call in answering machine mode

Defines if the message assistant is globally deactivated for all users.

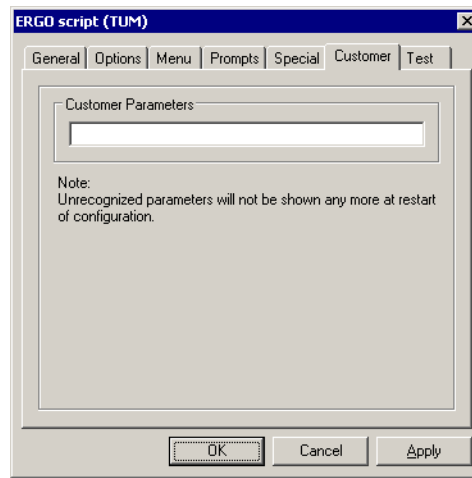
Menu repetitions until time-out

Use this field to enter the number of menu repetitions until the call will be disconnected (time-out).

NOTE:

Keep the default **0** for this value. A caller without DTMF-compatible telephone is unlikely to listen to the greeting again when he/she realizes that Ergo does not accept any entries from him/her.

10.4.2.6 Parameter Tab *Customer*



In the parameter tab *Customer* you can enter special, customer-specific parameters.

The following parameter settings are available at the moment:

- -adg
- -bga
- -chkloop
- -extended
- -fewv
- -madga
- -map
- -mapct
- -nocalendar
- -nocon
- -npda
- -pga
- -plfn
- -quotamode
- -rmtopic
- -rwb
- -ttm

- `-uao`
- `-ucid`
- `-ugnf`

Beyond that, the following parameters (silence detection parameters), via which the Ergo silence detection can be adjusted, exist.

- `recplen`
- `recplvl`
- `recslen`
- `recslvl`

If several parameters are to be used simultaneously, they are entered in the entry row, separated by a blank. Invalid parameters are ignored and no longer shown when this configuration page is called again.

Let's have a closer look at the functions of these parameters.

-adg

Ergo offers the option to quickly record or process a welcome greeting for the current day. So that this feature can be used, activate this parameter.

-bga

Ergo offers the option to play the voicebox default welcome greeting in two languages. After this option has been activated the caller will first hear the default welcome greeting in the language that the appropriate Ergo user has configured as private voice mailbox language. Subsequently, the default welcome greeting is put out in the second language, which can be configured individually for users or user groups.

NOTE:

If an Ergo user records a private welcome greeting for his/her voice mailbox, this greeting will only be played in the language that the relevant Ergo user has configured as private voice mailbox language.

With the **-bga** parameter you activate the bilingual playback of the default welcome greeting.

To configure the second playback language, you also need to add the new **SEC_LANGUAGE_ID** database field to the user and/or user group mask of the Correl Database in the form of a text field.

-chkloop

When a call comes in of which the originator number (ANI) and the *Redirected Number* are the same, Ergo does not accept this call. This is usually the case when Ergo wants to inform about new messages by *User Outcall*. In most cases the loop is already recognized by the *User-User-Info* on ISDN level and call is not accepted. If this is not the case, you can use this switch to prevent the generation of this loop.

-extended

This parameter activates the setting options of the extended mode for all users. In this mode you can execute comprehensive mailbox options via keyboard, if at the relevant workstation no client is available.

-fewv (Forward Email with Voice Annotation)

By default, an annotation can only be recorded for voice mails to be forwarded. With this parameter, the annotation function can also be activated for e-mails to be forwarded.

-madga (Message Assistant Disabled in Guest Access)

This option deactivates the message assistant in answering machine mode. Message recording starts immediately.

NOTE:

This option is only active if the message assistant is active.

-map (Message Assistant to Postmaster)

If the user activates the message assistant and the caller does not select an option in the set time, he/she will be connected to the postmaster. Without this option, a message would be recorded.

NOTE:

This option is only active if the message assistant is active.

-mapct (Message Assistant Prompt Connection Target)

Activates the option to enter a connection target in the message assistant.

NOTE:

This option is only active if the message assistant is active.

-nocalendar

This parameter deactivates the greeting of the calendar option in the Ergo menu.

-nocon

Ergo usually behaves as follows:

1. The send time of a voicemail is set to the time at which this call was accepted by PhoneMail. This enables *OpenScape Web Client* to associate the voicemail to the corresponding entry in the CTI journal if the telephone was redirected to the mailbox.
2. Ergo sends a transaction to *OpenScape Web Client* with the caller's phone number. If possible, *OpenScape Web Client* returns the caller's name. This name is then written in the voicemail subject. *OpenScape Web Client* can later extract the name of the caller from the subject again.

If *OpenScape Web Client* is not used, the above transaction leads to a warning in the log. This parameter deactivates this behavior.

-npda

This parameter deactivates the greeting of the *VoiceBoxNotFound* prompt if Ergo is addressed in the control mode by Redirected Number.

-pga (Pre-Greeting-Announcement)

With this parameter string you can implement an additional welcome message for external, inbound calls. In this way you can have e.g. a company greeting played before the Ergo voice mail system answers the call. This can be required to inform customers that they are connected to the right extension. The associated company-specific greeting is not included in the Ergo scope of delivery. If required, you need to create such a recording yourself.

Some important remarks on this:

- The greeting file to be implemented must be generated in the PCM format
- Its name must necessarily be `pregreetingann.pcm` since only a greeting file with this name is played at this point.
- This greeting file must be stored in the following directory: `<XPR Install>\res\E\ergo\<language>`.
`<language>` represents the currently selected language – for example `american` or `british`).

-p1fn (Prevent Loop For Notification)

If a mailbox is called via a *User Outcall* of the Notification APL, then this should be recognized and this call should by no means induce another call by the Notification APL. In case of ISDN this is possible without any problems and the call is therefore not accepted. In case of VoIP this is not possible. A DTMF tone is therefore played via this switch. This tone is recognized by Ergo and immediately rung off.

-quotamode

A caller can usually leave a message even with activated user quotas. You can activate a different behavior for Ergo via a parameter. When user quotas are active and a user has exceeded his/her quota, Ergo then switches automatically to the Info Mode for the corresponding mailbox. A greeting is then played to the caller, but he/she cannot leave a message.

-rmtopic (Remove XPR Monitor Topic)

If the XPR server is set up completely, it may happen that no topic entry for Ergo monitoring can be created in the modules window of the XPR Monitor. One of the reasons is that the number of topic entries is limited to 64 per APL. With the help of this parameter string the XPR monitor can be configured in a way that some existing topics can be removed from the branch of the applied telematics APL and Ergo can be inserted as topic. The Ergo activities can now be monitored in a logging window.

-rwb (Reject Without Box)

Calls to numbers not assigned to any user are rejected.

-ttm (Trusted Transfer Mode)

Activates the display of the **OpenScape** tab in the Ergo configuration. After you have set this parameter you need to close and reopen the Ergo configuration for the parameter to take effect.

-uao (Use ANI as Originator)

If a caller who is known to the system via the ANI and who has a mailbox on the system leaves a message in *answering machine mode*, the message will also be stored in his/her mailbox in the *Sent Items* folder.

-ucid (Use Caller-ID)

The redirecting numbers feature is applied for optimized voicemail-system use (cf. [Section 10.1.5, "Redirecting Numbers", on page 551](#)).

However, not all PBXs transfer the redirecting number to the XPR server as independent number. Specific PBXs transfer the redirecting number instead of the original caller ID. Such systems include e.g. the H.323 NEO gateways. So that the XPR server uses the correct redirecting number in such a case, Ergo can be configured with the **-ucid** parameter in a way that the caller ID is used as redirecting number.

-ugnfi (Use GSM Number First)

The cell phone number of the called user is normally taken from the *SMS* field. Via this switch you can change this to the *GSM* field.

recplen, recplvl, recslen and recslvl

As the electronic password depends on the volume of the applied recording/playback components in a recording, it might be necessary to adapt the volume. The minimum impulse length that must at least be available for starting a recording can be additionally influenced.

The following four parameters are used to detect speaking or silence for starting or stopping a recording. In this way recording times are limited so that no unnecessarily large recording files are generated. The problem is to select the level that clearly recognizes speech but still interprets line and background noise as silence, for example. The thresholds for length and peak level, required to detect breaks, can be adapted here.

The default values for these parameters usually depend on whether the IP APL or ISDN APL is used. If the ISDN APL is used, the default values also vary with the language format selected upon the XPR server installation.

To activate the default value for a parameter, value **4294967295** must be configured for the relevant parameter.

recplen=<value> (Record Peak Length)

Defines in milliseconds the minimum pulse length of a signal in order to be detected as such.

Default:

- 10[ms] for ISDN APL with A-Law
- 16[ms] for ISDN APL with μ -Law
- 32[ms] for IP APL

Value range: 0 to 300000[ms]

recplvl=<value> (Record Peak Length)

Defines the minimum peak level of a signal for starting a recording. The higher the “peak level” is selected, the louder a person must speak to start a recording. When the entry value is divided by 40, you receive the level value in percent (in relation to the maximum value).

Default:

- 24[ms] for ISDN APL with A-Law
- 20[ms] for ISDN APL with μ -Law
- 20[ms] for IP APL

Value range: 0 to 4000

recslen=<value> (Record Peak Length)

Defines in milliseconds the minimum impulse length a break must have for stopping a recording.

Default: 5000[ms]

Value range: 0 to 300000[ms]

recslvl=<value> (Record Peak Length)

Defines the minimum peak level a break must have for stopping a recording. The higher the “peak level” is selected, the louder a person must speak for the recording not to be stopped. When the entry value is divided by 40, you receive the level value in percent (in relation to the maximum value).

Default:

- 32[ms] for ISDN APL with A-Law
- 20[ms] for ISDN APL with μ -Law
- 20[ms] for IP APL

Value range: 0 to 4000

10.4.2.7 Parameter Tab *OpenScape*

The parameter tab *OpenScape* contains the settings for the Trusted Transfer Mode. This mode is used to connect the PhoneMail script of the XPR server with the Unified Messaging features of OpenScape UC Application. The customer parameter “-ttm” must have been set for displaying this tab. See also [Section 10.1.3, “Trusted Transfer Mode \(TTM\)”, on page 532](#).

IMPORTANT:

All users to deploy the Trusted Transfer Mode must be assigned the **Trusted Transfer Mode** privilege.

The option **OpenScape integration by Trusted Transfer Mode** activates the Trusted Transfer Mode in the XPR server.

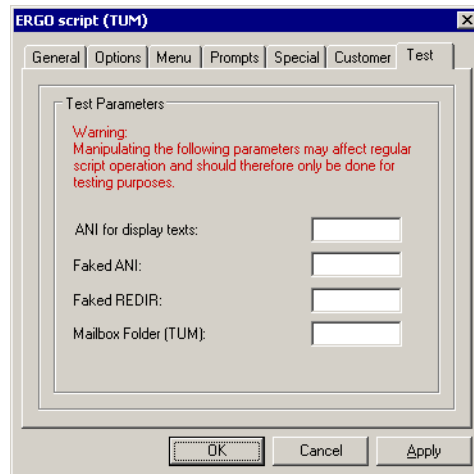
See [Section 10.4.3.12, “Parameter Tab OpenScape”](#) for information on the parameters.

10.4.2.8 Parameter Tab Test

This parameter tab serves for entering test parameters.

IMPORTANT:

In a customer system no parameters should ever be entered here. Nonsensical entries may hamper regular ERGO operation or make it even impossible.



The following entry fields exist:

ANI for display texts

You can enter a telephone number in this field, to which all display text will then be diverted. This option is only designed for a general feature check.

Faked ANI

For testing purposes an arbitrary number, automatically interpreted by the system as recognized calling number for every further call, can be entered here.

Faked REDIR

Another field for testing purposes in which you can specify – similar to the **Faked ANI** – a redirected number for call rerouting.

Mailbox folder (TUM)

Here you can explicitly define the output mailbox folder for True Unified Messaging (TUM) by entering its name.

10.4.2.9 Adjusting the XPR Routing Rules

Scenario:

Let us contemplate an Exchange or Lotus Notes integration without True Unified Messaging and without inbox replication. Voice mails remain on the XPR server and are exclusively polled via Ergo. Only fax messages are delivered to the foreign system and with voice mails a corresponding notification report is sent in most cases.

Since Ergo tries to access the messages via the TUM interface and would access the foreign system on the basis of the data from the user database (database field **PREFERRED**), the routing rules need to be customized.

The following rule must be inserted before the first rule, with *<Server Name>* to be replaced with the XPR server name:

```
NVS : <Server Name> /* [TYPE=TRANS] = NVS:MAILBOX/* [ABORT=1]
```

Thereby all transactions by Ergo are routed to the Mail APL which acts as TUM Backend for access to the XPR-own database. Furthermore, the preferred rule must be modified so that it does not cancel out the alteration:

```
NVS : *.*/* [ABORT=0] = <PREFERRED>
```

In the registry, the HKLM\Software\Wow6432Node\PP-COM\MRS\MailApl\TumBackend value should either not exist or be set to **1** so that the TUM functionality of the Mail APL is active.

NOTE:

In this scenario the corresponding TUM APL for access to user inboxes must be installed just the same if you want to generate notifications via the Notification APL by Web Administrator.

For the Ergo operation the user manual *Ergo* is available.

10.4.3 PhoneMail

PhoneMail is a voice mail script which is used to access the mailbox via telephone. Voice, fax and e-mail messages can be polled, voice mails can be recorded and sent and mailbox options can be set.

If display messages are to be sent to terminals by PhoneMail via CorNet, then the script *CIT Hicom Device Display* should also be activated.

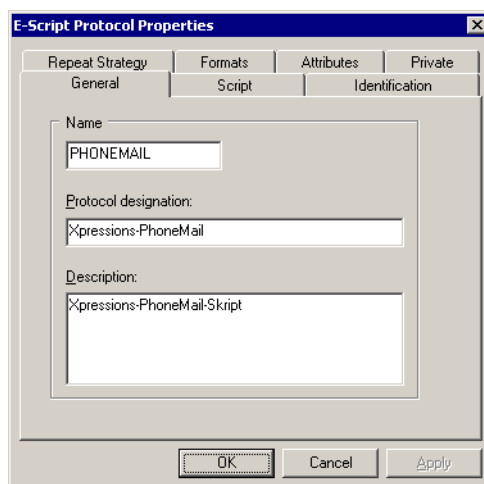
If the voice mail scripts PhoneMail and VMS are used in an XPR system in parallel, please note the following:

- A user can select the voicemail system he/she prefers in the Web Assistant. As the caller has already been identified when he/she uses the Call Back Access Mode by the access number transferred in the process (ANI), the relevant voice mail system can be started correctly, even if the access number of the other voice mail system was called.
- For external callers, this means that the voice mail system is not switched.
- The access numbers must originate in the assigned extension range which naturally must **not** overlap for PhoneMail and VMS.

You find further information about how to operate the voice mail scripts PhoneMail and VMS in parallel in [Section 10.4.5, "Using the PhoneMail and VMS Protocols in parallel", on page 699](#).

Let's have a look at the configuration tabs of the protocol settings.

10.4.3.1 Configuration Tab *General*



The elements displayed here comprise the logical protocol name (**Name**), over which the PhoneMail protocol to be configured is addressed, a descriptive **Protocol designation**: used for display in the XPR monitor, and a short **Description**: of the protocol, which appears in the configuration tab when this protocol is selected.

IMPORTANT:

So that the PhoneMail protocol can operate trouble-free, it must be assigned the logical name *PHONEMAIL*.

The logical protocol name serves as reference for the assigned protocol and is evaluated by modules that communicate with the telematics APL.

10.4.3.2 Configuration Tab *Identification*

The *Identification* tab for PhoneMail corresponds to the one of the Fax G3 protocol. Compare [Section 10.4.6.2, “Configuration Tab Identification”, on page 705](#).

10.4.3.3 Configuration Tab *Repeat Strategy*

The *Repeat Strategy* tab for PhoneMail corresponds to the one of the Fax G3 protocol. Compare [Section 10.4.6.4, “Configuration Tab Repeat Strategy”, on page 707](#).

10.4.3.4 Configuration Tab *Formats*

The *Formats* tab for PhoneMail corresponds to the one of the Fax G3 protocol. Compare [Section 10.4.6.6, “Configuration Tab Formats”, on page 709](#).

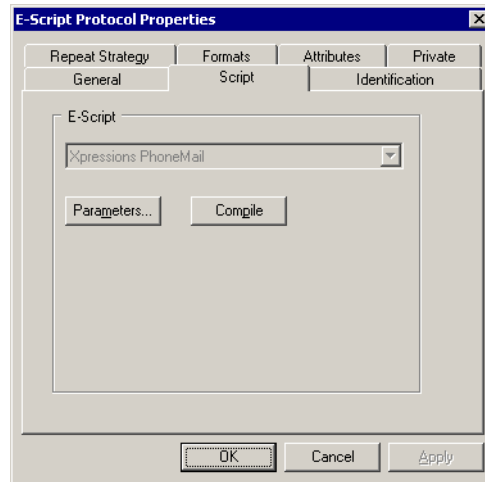
10.4.3.5 Configuration Tab *Attributes*

The *Attributes* tab for PhoneMail corresponds to the one of the Fax G3 protocol. Compare [Section 10.4.6.7, “Configuration Tab Attributes”, on page 710](#).

10.4.3.6 Configuration Tab *Private*

The *Private* tab for PhoneMail corresponds to the one of the Fax G3 protocol. Compare [Section 10.4.6.5, “Configuration Tab Private”, on page 708](#).

10.4.3.7 Configuration Tab *Script*



In the E-Script field the desired script entry can be selected or a concrete name is already entered.

IMPORTANT:

If the protocol was selected by name after clicking the **Add** button, the **E-Script** field is defaulted. If the entry **User-defined Script** has been selected instead of a protocol by name, the desired protocol name can now be defined in the **E-Script** field (cf. [Section 10.9.1, “Scripts”, on page 806](#)).

If you click the **Parameters** button, you will come to the actual protocol configuration. Via **Compile** you can compile the actual script. This is only required when you have developed new scripts yourself which are thus present in the source. In most cases an already compiled object file is available which can be executed by the XPR server.

The configuration tab *Attributes* is part of the Advanced settings. No modifications should be made here for PhoneMail.

Let's have a look which options are available for the actual protocol installation via the **Parameters** button on the configuration tab *Script*.

10.4.3.8 Parameter Tab *General*

Service Access Numbers	
Direct Access:	530
Guest/Forward Access:	531
Callback Access:	532
Fax Access:	533
Transfer Access:	534
Universal Access:	535

The phone numbers for telephone access with the access types *Direct Access*, *Guest/Forward Access*, *Callback Access*, *Fax Access*, *Transfer Access* and *Universal Access* are to be entered on the *General* parameter tab. The corresponding access numbers must be configured in the PBX in a way that calls to these numbers are automatically forwarded to the XPR server. Furthermore, they must be within the extension number range that is connected to the PhoneMail script.

The following basic questions must be clarified before you define the number range:

- Is the CorNet-N protocol supported both by the XPR server and the connected PBX?
- Should the mailbox number and telephone number be identical?
- Should it be possible to assign a mailbox to more than one subscriber (collection mailbox)?

Depending on the answer, it may be necessary to link additional extension ranges to the PhoneMail script in addition to the access numbers described above. Refer to the following table for information on possible configurations.

CorNet N	Numbers identical?	Mailbox for several subscribers?	
Yes	Yes	No	Binding of additional extension number ranges is not necessary. Call forwarding is always set to the Forward Access Number (or Fax Access Number for Fax-CF)
Yes	yes, if possible	Yes	Bindings of additional extension number ranges is necessary because call forwarding to a mailbox number is to be set instead to the Forward Access Number. Each mailbox number (provided these are used by more than one subscriber) must be included in the extension number range.
Yes	No		Bindings of additional extension number ranges is necessary because call forwarding to a mailbox number is to be set instead to the Forward Access Number. Each mailbox number must be included in the extension number range.
No			Bindings of additional extension number ranges is necessary because without CorNet-N, call forwarding cannot be set to the Forward Access Number but must be set individually to a mailbox number. Each mailbox number must be included in the extension number range.

Description of access types:

- **Direct Access**

You can poll and administer your own mailbox from any telephone by dialing the phone number defined here. If this number is used, the caller must enter his/her mailbox number and PIN at the XPR server for identification purposes

- **Guest Access**

The phone number defined here can be used to leave a voice message for another mailbox owner from any telephone. A caller must enter the mailbox number of the desired conversational partner to address his/her message.

- **Forward Access**

The phone number used here must be set in the PBX as the call forwarding destination if calls are to be routed to the XPR server by means of call forwarding or call forwarding no answer. To set up a call, this access type requires the phone number of the extension that activated call forwarding (redirecting number) to be transferred. If the PBX does not support their transmission, this access type is only possible via extension ranges.

- **Callback Access**

Access with this number corresponds to Direct Access, except that the user's own phone number no longer needs to be entered because the terminal's phone number is used. It also means that this access type can only be used from a user's own telephone or after identification vis-à-vis the PBX. Moreover, this phone number is utilized when rapid access to the XPR server is used with the help of the *Mailbox - Output* key combination or a corresponding menu selection.

IMPORTANT:

This feature requires corresponding skills in the applied devices and the applied PBX.

- **Fax Access**

This phone number is a Forward Access exclusively for fax service. Here as well the destination mailbox is analyzed via the Redirecting Number.

- **Transfer Access**

If a caller calls a postmaster account, the postmaster can forward the caller to the Transfer Access and specify the required mailbox number before transferring it. This form of access is identical to guest access except that the caller is informed by the operator that he/she is connected to a voice mail system and will therefore hear a specially created announcement.

- **Universal Access**

This access corresponds to the Guest Access but with an additional option for switching to Direct Access (press the **0** key).

In the case of Flexrouting, a Hicom ACD connection shortcoming is treated by default as a special feature of the PhoneMail script. Every callback access that contains a redirecting number is automatically executed as forward access. If this behavior is not desired, it can be deactivated via the *Customer* tab (see below).

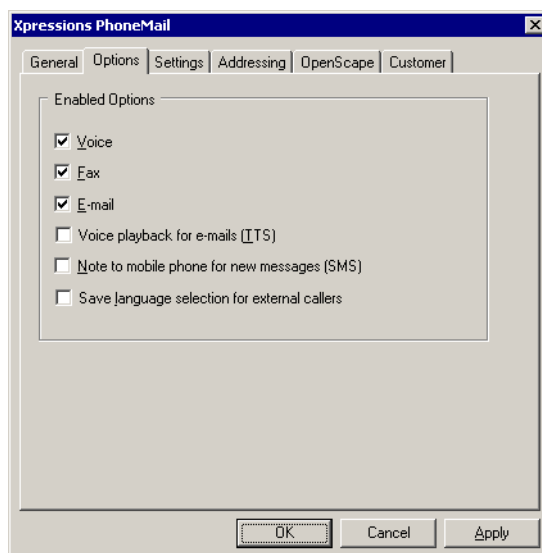
Configuring a group mailbox

The following steps should be performed to allow multiple users share a mailbox:

1. Set up another extension range in addition to the access numbers.
2. Specify one of the numbers in the group as the mailbox number.
3. The group members forward their telephone directly to this mailbox number and not to the Forward Access option.
4. Notifications (MWI) should be configured in the Web Assistant in such a way that the mailbox LED is connected to the group members' devices. For further information please refer to the *Web Assistant* user manual.

A locking mechanism has been implemented, so that always only one group member may query the mailbox. Only one version of name announcements and greetings is available. The times at which changes are made should therefore be agreed by all group members.

10.4.3.9 Parameter Tab *Options*



The services to be activated/deactivated for telephone access can be set in the *Options* tab. Deactivated message types are not signaled when polling via the telephone access.

The following options are available:

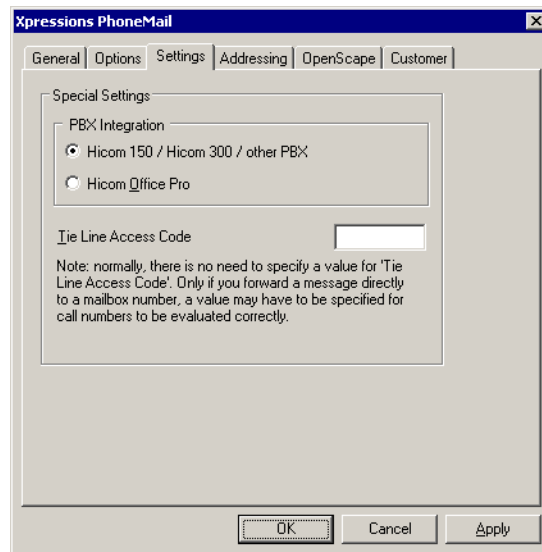
- Voice: Voicemails are signaled to users.
- Fax: Fax messages are signaled to users.
- E-mail: E-mails are signaled to users.
- Voice playback for e-mails (Text-to-Speech)
e-mails are converted into voice mails by means of a Text-to-Speech application and read out.

IMPORTANT:

For using this feature, the respective software must be installed and the Text-to-Speech (TTS) feature must be released in the XPR server.

- Note to mobile phone for new messages (SMS): With new messages in the mailbox, the user can decide whether he/she wants to receive SMS messages.
- Save language selection for external callers
The language setting for external callers is saved so that the caller hears the selected language during the next call (only relevant in case of multilingual installations).

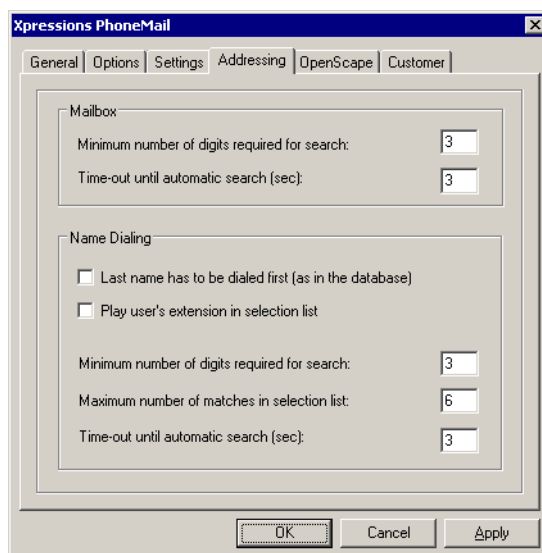
10.4.3.10 Parameter Tab *Settings*



Specific settings necessary for correct interaction with the connected PBX can be made in the *Settings* parameter tab. Normally, it is assumed that call forwarding to the Forward Access number or Fax Access number are set and no collective mailboxes are used. Different settings may be necessary in the case of deviation from this standard configuration.

The **Tie Line Access Code** may be required when using extension ranges, so that correct internal fax originators can be displayed.

10.4.3.11 Parameter Tab Addressing



In the *Addressing* parameter tab, settings for mailbox and name selection are performed.

In the *Mailbox* section the following options are available:

When dialing a mailbox, its complete phone number need not necessarily be specified. Under the following conditions dialing the first digits of a mailbox is sufficient:

- The number of digits defined in the **Minimum number of digits required for search** field must at least have been dialed.
- The associated destination mailbox could already be determined from the dialed digits.

This option can accelerate routing to a mailbox.

If no entry is made in the **Time-out until automatic search** field via the telephone keypad, PhoneMail starts the automatic search for the associated mailbox. The digits entered until then are used for the search.

This option saves pushing the # key to complete the phone number entry for a mailbox.

In the *Name Dialing* section the following options are available:

NOTE:

To optimize searching in the database on the basis of name dialing, the XPR server uses the `VM_VANITY` database field. In this database field the XPR server deposits a user-individual vanity number created from another database field of the respective user. You find more details on this in [Section 11.11, “Vanity Number Support”](#), on page 895.

Last name has to be dialed first controls the PhoneMail-integrated user note for the entry of name dialing by the user. For this operating instruction two options are available:

- Name dialing entry starting with the first name
 - Name dialing entry starting with the last name
-

IMPORTANT:

The setting **Last name has to be dialed first** only controls which operating instruction is played to the user by the PhoneMail script. The selected option does *not* influence the search algorithm of the XPR server.

The XPR server compares the information entered for name dialing with the entries of the **Name** fields of the XPR database. Depending on the users being stored with leading first name or last name, the operating note **Last name has to be dialed first** must be activated or not.

Consequently, a mixture of the first and last name sequence in the **NAME** fields of the XPR database causes problems in the search algorithm.

If a user receives a hit list for name dialing, each hit can be announced either with or without the corresponding extension. **Play user's extension in selection list** defines whether the extension is specified as well.

For name dialing not the complete name of the callee must be entered. **Minimum number of digits required for search** defines the minimum number of letters to be entered via telephone keys before a search for matches can start. If you finish the name dialing with the # key after having entered fewer digits than required, the PhoneMail script prompts you to continue the entry.

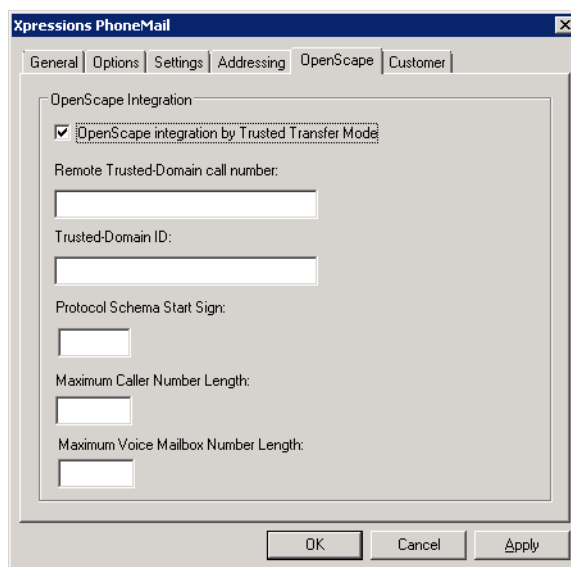
Maximum number of matches in selection list defines the maximum length of match lists. If a match list with more users than defined here results from name dialing, the PhoneMail script points this out and requests redialing. This redialing should then be performed with a qualified entry to shorten the hit list.

If no entry is made in the **Time-out until automatic search** field via the telephone keypad, PhoneMail starts the automatic search for matching user names. Only the characters entered until now are used for the search.

NOTE:

Name dialing can be deactivated by the PhoneMail parameter **disablenamedialing**.

10.4.3.12 Parameter Tab *OpenScape*



The parameter tab *OpenScape* contains the settings for the Trusted Transfer Mode. This mode is used to connect the PhoneMail script of the XPR server with the Unified Messaging features of OpenScape UC Application. See also [Section 10.1.3, “Trusted Transfer Mode \(TTM\)”, on page 532](#).

IMPORTANT:

All users to deploy the Trusted Transfer Mode must be assigned the **Trusted Transfer Mode** privilege.

The option **OpenScape integration by Trusted Transfer Mode** activates the Trusted Transfer Mode in the XPR server.

If OpenScape Xpressions V7 transfers a call to the Voice Portal of OpenScape UC Application or vice versa, various information must be exchanged. This information is coded in the transferred phone number (cf. [Section 10.1.3.1, “How the Trusted Transfer Mode operates”](#)). The following settings then result in this TTM phone number format for forwarding.

The following settings are required for the Trusted Transfer Mode to operate smoothly:

- **Remote Trusted-Domain call number**
Specifies the phone number to which the XPR server forwards a TTM call for OpenScape UC Application. This phone number thus corresponds to the appropriate access number of OpenScape UC Application
- **Trusted-Domain ID**
Specifies the ID of the trusted domain that is or will be configured as local trusted domain in OpenScape UC Application.
If the XPR server receives a forwarded TTM call from OpenScape UC Application, it checks the domain ID forwarded with the call. If this forwarded domain ID does not correspond to the one configured here, the call will be rejected as unauthorized.

NOTE:

The domain ID must not comprise more than two digits

- **Protocol schema start character**
Start character in the protocol schema of the TTM phone number format (cf. [Section 10.1.3.1, “How the Trusted Transfer Mode operates”](#)).
- **Calling number Maximum Length**
Maximum length of the caller number (user information) in the protocol schema of the TTM phone number format (cf. [Section 10.1.3.1, “How the Trusted Transfer Mode operates”](#)). Shorter numbers are completed accordingly upon the transmission. If longer numbers may occur, set the -suppressLongANI parameter for PhoneMail.

NOTE:

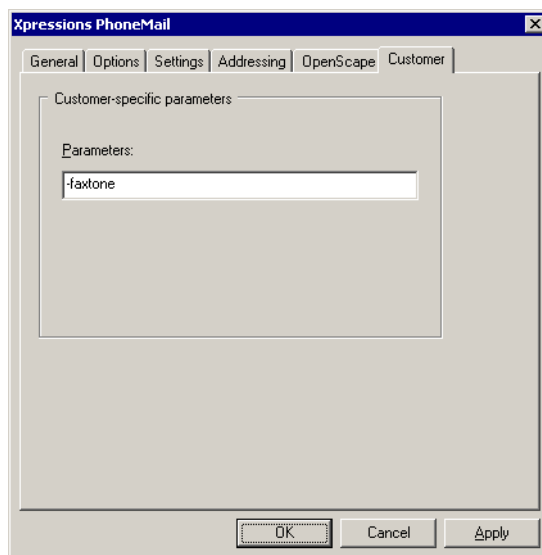
The ANI is always transferred in the E.164 format. Thus normalized with country code etc. This should be accordingly considered for this specification. E.164 allows a maximum of 15 digits. However, depending on the country, the maximum number may deviate from this value or does not always have the same length.

- **Voicebox number Maximum Length**
Maximum length of the user's voicebox number (user information) in the protocol schema of the TTM phone number format (cf. [Section 10.1.3.1, “How the Trusted Transfer Mode operates”](#)). Shorter numbers are completed accordingly upon the transmission.

The length of the voicebox number corresponds to the number of digits as they are entered for the relevant user in the **VOICE#** database field of the XPR Correlation database. In a TTM system environment, the length of this number may vary with the user. In this case the greatest of possible user ID lengths must be configured here.

This information forms the internal calling number schema as it is described in [Section 10.1.3.1, “How the Trusted Transfer Mode operates”](#).

10.4.3.13 Parameter Tab *Customer*



Any system settings can be made in the *Customer* parameter tab. The customer-specific customization of the PhoneMail script is a mandatory requirement here.

Features can also be enabled on a project-specific basis by entering the relevant parameters. The following general switches or options are thus available at present. During your entry, you must separate them from each other by blanks:

- “-adrconf”
In the short user guidance each address must only be confirmed once with the # key during the address entry by default.

Example:

`...<Address 1>#<Address 2>#<Address 3>#...`

If the **-adrconf** parameter is active, each address can be corrected after its entry. To correct an address, you need to additionally push the * key after entering `Address>#`. To copy the address as it is, push the # key after entering `Address>#` in addition.

Example:

```
...<Address 1>#*<Correction Address 1>##<Address 2>##<Address 3>##...
```

- “-allowZeroInFAM”
Allows the user to use the key '0' case his forward access menu has the key '0' configured for 'Dial the Number'. Such parameter would allow the use of the Key '0' even if the **-disabletransferout** is enabled.
- “-altoverrides”
Each PhoneMail user may record the following individual greetings:
 - Greeting when busy
 - Internal greeting
 - External greeting
 - After hours greeting

If a user additionally records the *alternative greeting*, the first three greetings of the above list will be replaced with the *alternative greeting*. Merely the *after hours greeting* will be retained as defined.

If the **-altoverride** parameter is activated, a recorded *alternative greeting* replaces all listed greetings – thus the *after hours greeting* as well.

NOTE:

This parameter takes effect in the extended mode only.

- “-cdi”
Each PhoneMail user may configure a personal forwarding menu in the Web Assistant. If the user does not define an action for the 0 key in the forwarding menu, the PhoneMail script by default closes the connection to a caller who pushes the 0 key in a voice mail box in infobox mode.
If the **-cdi** parameter is activated, a user can be connected to another subscriber via the 0 key in the above situation. The PhoneMail script asks the user for the new destination number after he/she has pushed the 0 key.
- “-con”
You need to activate this parameter if you want to access PhoneMail via the *OpenScope Web Client* or, in the scope of *Unified Communications Act Now*, via the *ComAssistant* client. This parameter changes the following:

1. The send time of a voicemail is set to the time at which this call was accepted by PhoneMail. This enables the *OpenScape Web Client* to associate the voicemail to the corresponding entry in the CTI journal if the telephone was redirected to the mailbox.
 2. PhoneMail sends a transaction to the *OpenScape Web Client* with the caller's phone number. If possible, the *OpenScape Web Client* returns the caller's name. This name is then written in the voicemail subject. The *OpenScape Web Client* can later extract the name of the caller from the subject again.
- “-defOperatorKey”
A subscriber who calls a PhoneMail voicebox dials by default **0#** to reach the preferred phone that the mailbox owner can customize for his/her mailbox. If the mailbox owner has not defined a preferred phone, dialing **0#** does not set up a connection. Furthermore, the caller can dial **00#** to be connected to the operator. For this purpose, PhoneMail searches the following PhoneMail settings in the given sequence for an operator number:
 - User group profile
 - System profile

If the **-defOperatorKey** is activated, the caller can dial **0#** to be connected to a defined phone number. PhoneMail determines this phone number by searching the following PhoneMail settings in the given sequence:

 - Preferred telephone in the individual voicebox settings
 - Operator number in the user group profile
 - Operator number in the PhoneMail system settings.
 - “-disablecallbacks”
After a user has played a message, PhoneMail enables him/her to connect to the message originator by default.
If the **-disablecallbacks** parameter is activated, the user cannot exercise this option in the PhoneMail menu anymore.
 - “-DisableConfirmation”
In PhoneMail message addresses are entered in the following format by default:
 ...<Address 1>#*<Correction Address 1>###<Address 2>##... <Address n>###...
 The example shows:
 The entry of each address is completed with the # key. Subsequently, the address entered last is corrected via the * key or confirmed as correct via the # key. The entire address entry is completed once more with the # key.

If the **-DisableConfirmation** parameter is active, the user must not push the # key again to confirm an address as correct. After pushing the # key the user must therefore either push the * key to correct the last address or start entering the next address:

...<Address 1>#*<Correction Address 1>##<Address 2># ... <Address n>##...

IMPORTANT:

If **-DisableConfirmation** is activated, the parameters **-adrconf** and **-Search-ByNameDirectly** must also be activated.

- “-disablenamedialing”
Deactivates name dialing for PhoneMail.
- “-disabletransferout”
If a caller accesses his/her PhoneMail mailbox via the forward, guest or universal access, he/she can be connected to a subscriber while recording a message by default.
If the **-disablecallbacks** parameter is activated, the user cannot exercise this option in the PhoneMail menu anymore.
- “discreccut”
If recording a message is finished owing to a cut connection, a portion is cut off of the message's end. **discreccut** specifies the length of cut portion. The **discreccut** value is interpreted in milliseconds; its default is **0ms**.
- “-faxtone”
enables automatic fax tone recognition
- “-EnableGAToXprSite”
A caller in the local Guest Access can send a message to a user on another XPR server that is connected by System Networking.
- “force_lang”
Determines an individual TUI language for this PhoneMail entity. If this parameter is not specified, the XPR server default language or the language set for “lang” is used for the PhoneMail TUI. When this parameter is used, the language set here is always deployed, independent from other settings.

Possible values for this parameter are:

– 1031: German	– 1055: Turkish
– 1033: English (USA)	– 2057: English (UK)
– 1036: French	– 2058: Spanish (USA)
– 1040: Italian	– 2070: Portuguese
– 1043: Dutch	– 3082: Spanish
– 1046: Brazilian	– 3084: Canadian

– 1049: Russian

- “-fsi”
force stand-in, shows option to set stand-in (mailbox-deputy) even if the user is user is TUM-enabled (PREFERRED-entry in LN or EXCH), to be used with special routing-rules only:
NVS:<server name>/SYSTEM[TYPE=TRANS]=NVS:MAILBOX/
*[ABORT=1]
NVS:<server name>/[TYPE=TRANS;ABORT=0]=NVS:<LN or EXCH>/
[ABORT=1]
NVS:<server name>/*[ABORT=0]=<PREFERRED> (replaces old PREFERRED-rule)
- “fwdt”
Effects a delayed output of the first greeting in Forward Access. This may be useful for ensuring that the announcement is not output twice in ACD applications. The **fwdt** value is interpreted in milliseconds; its default is **0ms**.
- “-hefa”
If a caller is connected with the voice mailbox of a PhoneMail user, the PhoneMail script announces the name and phone number of the respective PhoneMail user. It is possible to suppress the announcement of the phone number with this parameter.
- “-headersender”
Before a message is played, its complete message header is always put out first by default.
Activating this parameter reduces the message header information put out to the message number, originator name and originator call number. If users wish to listen to the hidden header information after message playback, they can do so by entering the digits 74.
- “-headersimple”
Before a message is played, its complete message header is always put out first.
Activating this parameter reduces the message header information put out to the message number. If users wish to listen to the hidden header information after message playback, they can do so by entering the digits 74.
- “-hidepmp”
For all users who have the short prompting configured for PhoneMail, the announcements of TUI menu tree portions are restricted with this parameter. This means that for the available options of the relevant menus only the names of the options contained therein with their assigned keys are announced. With this setting the menu introduction is not put out any more. The restriction concerns the following menu branches:
 - Playback menu after recording of a message.

- Reply menu after playing a message.
After activating the parameter the 'save' and 'delete' options will not be announced any more either.
- “-IgnoreHP8KMaxLen”
In the Trusted Transfer Mode between OpenScape UC Application and OpenScape Xpressions the maximum length of the userinfo field is ignored. Furthermore, the mailbox number is sent in the E.164 format without leading +-sign.
This parameter works only if
 - if no OpenScape Voice but for example an OpenScape 4000 is used.
 - the user info string does not exceed 30 characters when using an OpenScape Voice.
- “lang”
Determines an individual TUI language for each PhoneMail entity. If this parameter is not specified, the XPR server default language is used for the PhoneMail TUI. If required, the users may set another language. See also “force_lang”.

NOTE:

If a user has not yet selected a language in the Web Assistant under **Language selection**, the Web Assistant GUI language and the PhoneMail TUI language may differ for the relevant user.

Possible values for this parameter are:

– 1031: German	– 1055: Turkish
– 1033: English (USA)	– 2057: English (UK)
– 1036: French	– 2058: Spanish (USA)
– 1040: Italian	– 2070: Portuguese
– 1043: Dutch	– 3082: Spanish
– 1046: Brazilian	– 3084: Canadian
– 1049: Russian	

IMPORTANT: As of V7R1, this setting can be overridden in a multi-tenancy environment by the tenant configurations in the Web Assistant. As a result, a PhoneMail entity per language is no longer required as this assignment is determined by the languages assigned to the tenants.

- “-locationByUser”

When Xpressions is used in a multi-location environment and the Voicemail setting is configured to allow calls from internal to external, by default, the global settings (Voicemail profile) use the device location, and not the user location.

If the `-locationByUser` is active, the user location is used instead of the device one.

- “`-lr`”
By default, PhoneMail uses in case of cascaded forwarding always the first redirecting phone number as redirecting number. If you activate this option, PhoneMail uses in case of a cascaded forwarding always the last redirecting phone number as redirecting number instead (cf. [Section 10.1.5.2, “Cascaded Forwarding”, on page 552](#)).

IMPORTANT:

If you use the IP APL, the script parameter `-lr` only takes effect for SIP and CorNet IP devices.

- “`MaxVoiceMsg=<MaxMsgs>`”
Lets you restrict the maximum number of messages a user may receive. This requires the system to be Voice-only, so that voicemails are exclusively managed via the Mail APL internally. In case of handing voicemails over to an external system such as Microsoft Exchange this restriction is not possible. If this parameter is set you can add the `MAX_VOICE_MSG` database field. Depending on how it is implemented in the mask, an administrator can then set the maximum number of messages for user groups or single users. The setting in the user group or for the single user is prioritized over the value set here by parameter.
Example: `MaxVoiceMsg=20`
- “`-mmrc`”
Messages played back in the continuous message mode can be automatically marked as read. This option is deactivated by default and is activated via this parameter.
- “`mwtd`”
Normally, the MTA automatically deletes voice mails from the voice mailboxes of the XPR users after a period to be defined (cf. MTA settings). To point out the deleting processes to the respective users, a warning message can be activated via this parameter. This warning message may be displayed to the user immediately after he/she has accessed his/her voice mailbox.
The value configured for this parameter defines the time in days after which

the user is warned before one of his/her messages is deleted. Valid values for this parameter are **0** up to **99**. The setting **0** deactivates the warning. The default is **7** days.

IMPORTANT:

This does not concern True Unified Messaging users.

NOTE:

The warning does not indicate which messages will be deleted. The system only distinguishes between deleting read and unread messages.

- “**ndc**”
With name dialing, PhoneMail checks after each key entry whether the specifications made so far can be assigned a unique subscriber. If this is the case, routing is initiated. **ndc** defines the time between the key entry and the match check. The **ndc** value is interpreted in 1/10 seconds; its default is **3/10s**.
- “**-nfma**”
A significantly shortened announcement is configured for voice only users in PhoneMail. In this setting only the message text and not the header of a message is played back via the TUI. It is possible to deactivate this shortened announcement via the parameter **-nfma**.

NOTE:

Voice only users are the users who only have selected the **voice mails** option in their personal filter settings for the voice mail system.

- “**-nocc**”
Deactivates the additional connection confirmation for a connection request via the # key. Via this option the desired connection will be established immediately after you have finished entering the phone number.
- “**-noctn**”
If the PhoneMail protocol callback access is dialed from a trusted number, continuous messages output is active by default. If this parameter is activated, common message playback is used with this type of dialing in.
- “**-nodelorig**”
Sent PhoneMail messages are deleted in the originator's folder by default. If this option is set, sent messages are kept in the originator's folder.
- “**-NoGAToPhSite**”
A caller in the local Guest Access can usually send a message to a user on another PhoneMail server that is connected by System Networking. The

PhoneMail server is not an XPR system. You can use this parameter to deactivate this function.

- “-noheader”
Before a message is played, its message header is always put out first by default.
This parameter deactivates the automatic header playback when messages are put out. If users wish to listen to the hidden header information after message playback, they can do so by entering the digits 74.
- “-noflexrout”
Deactivates the default Flexrouting mechanism (see [Section 10.4.3.8, “Description of access types:”, on page 642](#)).
- “-nondr”
If a PhoneMail user sends a fax or voice message, the XPR server generates an associated delivery report in e-mail format. Such an e-mail report describes whether the message could be delivered and it is stored in the PhoneMail box of the message originator. When a user listens to his/her PhoneMail box, the e-mail reports are announced by default. It is irrelevant here whether the user has enabled or disabled the TUI greeting for e-mails. If this parameter is set, e-mail reports are only announced to a user if he/she has enabled the TUI greeting for e-mails.
- “-noprintfax”
Disables the option to print out a fax on a fax machine. This parameter setting is recommended when no fax licenses are available.
- “-nopw”
Deactivates the password prompt when using Direct or Callback Access from your own telephone.
- “-nosendtodraft”
Normally messages are sent to recipients who have already been entered if the connection to the XPR server is closed whilst a recipient list is entered. When this option is activated, the recipient list must be specifically confirmed before the message will be sent.
- “-nopw”
Deactivates the password prompt when using Direct or Callback Access from your own cellphone. The cellphone number must be transferred when the connection is set up and must be entered with the user data in the **SMS** field of the XPR user database.
- “-notodr”
Users can cancel the recording of a voice message with key 0 by default. After such a cancellation, the user is enabled to connect to the operator or to another PhoneMail user. If this switch is activated, record cancellation is no longer possible in this form.

- “-octelmenu”
Activates some adjustments that make PhoneMail behave similar to an Octel TUI. These adjustments are available in English (US) only. When you set this parameter you need to additionally replace the `menu_config.ini` file with the `octel_default_menu_config.ini` file. Save the original file and then rename the file valid for this menu adjustment accordingly. See the *PhoneMail Function Tree Octel-like-Menu*.
- “-oof”
PhoneMail users can use their mailbox options to define in which sequence the messages in their mailbox shall be announced. This setting usually only affects the announcement sequence for received messages.
If the **-oof** parameter is activated, this mailbox option also changes the announcement sequence for sent messages.
- “-opbone”
Enables the option to leave a message that has been played back via key 1 and to change to the reply of the respective message. The key entry is only accepted while a message is played back.
- “-opbtwo”
Enables the option to skip a message playback via key 2 and continue with the playback of the next message. The key entry is only accepted while a message is played back.
- “-opbthree”
Enables the option to play back a message again by pushing key 3. The key entry is only accepted while a message is played back.
- “-opbfour”
Enables the option to save a message via key 4. The key entry is only accepted while a message is played back.
- “-opbfive”
Enables the option to leave a message that has been played back via key 5 and to change to the forwarding of the respective message. The key entry is only accepted while a message is played back.
- “-opbsix”
Enables the option to delete a message via key 6. The key entry is only accepted while a message is played back.
- “-opball”
Activates the parameters **-opbone**, **-opbtwo**, **-opbthree**, **-opbfour**, **-opbfive** and **-opbsix** (see above).
- “-opd”
In PhoneMail you can activate a shortened function menu that PhoneMail users can employ merely during message playback (cf. parameter **-opbone**

to **-opbsix**). **opd** defines a period after message playback, in which the shortened function menu can still be used. The **opd** value is interpreted in milliseconds; its default is **1750ms**.

- “psd”
Defines a delay for playing a greeting. The **psd** value is interpreted in milliseconds; its default is **0ms**.
- “reccut”
Defines a time span that is removed from the end of a recording in order to prevent the recording of DTMF tones that will create a pause. The **reccut** value is interpreted in milliseconds; its default is **0ms**.
- “rejectani”
Defines an extension list of originator numbers, whose calls are ignored by PhoneMail. The individual extensions in the list are separated by commas. If users are informed about certain events in the XPR server by notifications, the extensions of the script used for this should be defined in this list. Thus you can avoid that notifications are processed by the PhoneMail script in case of a redirection to the PhoneMail box.
- “-ReplyForwInSeq”
After a PhoneMail user has forwarded or replied to a received message, he/she always returns to the received messages list by default.
If the **-SearchByNameDirectly** parameter is activated, a user may forward and/or reply to a message also several times without returning to the messages list each time in between.
- “rw”
Defines a time before the recording end when a warning about the upcoming end of the recording is issued. The **rw** value is interpreted in seconds; its default is **15s** whereby **15** is **hardcoded** and setting **rw** to **0** means that the **announcement** is **disabled**.
- “-SearchByNameDirectly”
If a PhoneMail user wants to address a message via name dialing, he/she needs to push the * key before the actual name dialing. If the **-SearchByNameDirectly** parameter is activated, the * key need not be pushed any more.
- “-SimplifiedInfobox”
If this parameter is active, the subscriber who calls a voicebox is not provided with an option selection when the Infobox mode has been configured for this voicebox. In this case the connection between caller and voicebox is thus immediately closed after the greeting playback.
- “-SimplifiedMenuTree”
Activates a simplified PhoneMail in which many options are no longer active. This option deactivates among other things the menu for toggling different greetings. Insofar, only use the extended greetings. Furthermore we assume that no *Web Assistant* is used. If the *Web Assistant* is used just the

same, the [SimplifiedMenuTree](#) parameter in the param.xml must be set to True. Please refer to the corresponding function tree *Simplified PhoneMail* on this.

- “-skipmsgplaybackout”
A PhoneMail user can listen to messages found in his/her *Outgoing messages* message group. By default, the user needs to listen to the entire message before he/she can continue in the PhoneMail menu.
If the **-skipmsgplaybackout** parameter is activated, the PhoneMail user may skip playing a message by pushing the # key while the message is put out. Instead of the # key another key may also be allocated for this feature. This allocation is performed in the configuration file *MenuConfig.ini* under the menu ID [MailboxMenu_DuringHeaderPlayback] (cf. [Section 10.4.3.16, “The MenuConfig.ini configuration file”, on page 666](#)).
- “-sra”
Activates a shortened greeting for leaving messages. In this case the file *WhenFinishedPushStarPushPound.pcm* will not be put out.
- “-suppressLongANI”
If the number of a caller in Trusted Transfer Mode to OpenScape UC Application exceeds the maximum length set, “*” is transmitted instead of the number. The behavior is then just as with a suppressed phone number.
- “tbd”
Defines a period up to which you can reconnect to another subscriber in advisory mode. The **tbd** value is interpreted in seconds; its default is **5s**.

IMPORTANT:

This setting has no effect when a user has configured a telephone deputy.

- “tenant”
Defines a default-tenant-ID, which is used for name dialing in a multi-tenant solution.
If a user logs on to the PhoneMail script, only those users who belong to the same tenant like himself/herself may given out to him/her as search result of a name dialing. This is not possible if a user cannot be identified when he/she logs on. In this case only those users are given out to him/her who belong to the tenant defined in **tenant**. Insofar, a user can only log on if he/she has also been assigned the tenant ID defined here.

IMPORTANT: As of V7R1, this setting can be overridden in an SIP-based multi-tenancy environment by the tenant configurations in the Web Assistant. As a result, a PhoneMail entity per tenant is no longer required as this assignment is determined by the extension ranges assigned to the tenants.

- “timeout”
defines a period in which the menu options will be played again if no key combinations have been pushed. The **timeout** value is interpreted in seconds; its default is **5s**.
- “tmts”
PhoneMail administers received status reports in separate message queues of each mailbox – for example in the *Read* or *Unread* queue. If such queues contain messages, PhoneMail informs the user accordingly with queue-individual greetings when he/she plays his/her messages.
If a user wants to listen to the status reports of one of these queues, he/she needs to push key 3 on the telephone keypad while the relevant greeting is played.
Via **tmts** you can specify whether a break shall interrupt the greetings for the different message queues. If **tmts** is not defined or set to 0, PhoneMail will not take any breaks between the greetings. If a value is defined in **tmts**, PhoneMail will take a break between the single greetings in accordance to this value in seconds.
The value chosen for the **tmts** definition should give users sufficient time for pushing key 3.

IMPORTANT:

This setting does not take any effect when parameter **-nfma** has been set.

- “-ttm”
Activates the display of the **OpenScope** tab in the PhoneMail configuration. After you have set this parameter you need to close and reopen the PhoneMail configuration for the parameter to take effect.
- “-ttmNormANI”
Sees to a normalized ANI being used without leading +-sign in the Trusted Transfer Mode.
- “TUICP”
Like all XPR server TUIs, PhoneMail uses the NCO client **TUI** by default to normalize and localize phone numbers. Thus the same location applies for all TUIs and for all TUIs the same NCO rules for normalization and localization of phone numbers apply.
With **TUICP** you can specify for the relevant PhoneMail protocol that it uses an individual connect point. This connect point may then refer to an individual location and to individual NCO rules for normalization and localization of phone numbers.
In this way you can define another NCO location and other NCO rules for a PhoneMail protocol than for other configured TUIs.

- “wlcst”
Defines a delay, after which a caller receives a welcome greeting. The **wlcst** value is interpreted in 1/10 seconds; its default is **5/10s**. If you set this value to 0, the **Delay of the first Prompt played** option in the voicemail settings is used. The delay set here applies otherwise.
- “-nodispcaled”
Defines if a called number is not displayed (phone display) in case the call is not completed.

10.4.3.14 PhoneMail Language Settings

Each PhoneMail user can set a language for his/her mailbox, which PhoneMail then uses for all mailbox greetings.

NOTE:

If the VOGUE script routes a caller to PhoneMail, PhoneMail uses for all greetings the language that the VOGUE script has already defined for the caller – for example via a national language box.

10.4.3.15 Company-specific Greetings

You can create global company-specific greetings in the Web Assistant or via the telephone user interface (TUI). To do this, you must log on to the Web Assistant with administrator privileges and configure the company greeting there. These greetings are internally assigned to the user *Company*. In the case of configuration via TUI, you must log on under this user account; you can then configure the greetings. To this you need the *Company* user ID with the corresponding PIN. In the as-delivered status this special user has **no** PIN and **no** mailbox number.

If you want to replace the welcome greeting in PhoneMail with a customer-specific greeting, you need to record the desired text in a WAV file with 8000 Hz, 8 bit, mono, A-law (for Europe; μ -law for the US) or 8000 Hz, 16 bit, mono. 16 bit is the preferred format. This can be done with conventional software. The existing default prompt *WelcomeToXpressions.pcm* under
`<XPR-Install>\res\e\Phonemail\German\Long` must be replaced with the file generated in this way with the same name.

IMPORTANT:

These steps must be performed for each required language. For security reasons the old PCM files should be backed up.

10.4.3.16 Company-specific Menu Adjustments

The PhoneMail menu structure may be adjusted to a company's requirements within defined limits. In this way it is possible to change the keys for selecting the various PhoneMail features. In the scope of such company-specific adjustments, it is neither possible to modify the existing PhoneMail menu structure, nor can existing features be removed from PhoneMail or new ones be added though.

The MenuConfig.ini configuration file

All menu settings that may be adjusted in PhoneMail are specified in the MenuConfig.ini configuration file, which is stored in the

<XPR-Install>\res\e\Phonemail

directory and which is already preconfigured with the PhoneMail default settings.

The key assignments of the following PhoneMail menus can be individually adjusted via this configuration file:

Menu ID in Configuration File	Short Menu Description
[MainMenu]	PhoneMail main menu
[MailboxMenu_NewMessages]	Main menu of the <i>Incoming messages</i> message group.
[MailboxMenu_EMailFaxMessages]	Menu for e-mail and fax message playback.
[MailboxMenu_EMailFaxPrint]	Menu for e-mail and fax message output on a printer or fax device.
[MailboxMenu_OldMessages]	Menu for playing old messages in the <i>Incoming messages</i> message group.
[MailboxMenu_Outgoing]	Main menu of the <i>Outgoing messages</i> message group.
[MailboxMenu_PausePlayback]	Menu while message playback is interrupted.
[MailboxMenu_DuringPlayback]	Menu during message playback.
[MailboxMenu_DuringHeaderPlayback]	Menu while a message header is played.
[MailboxMenu_ListenAgain]	Menu after selection of the <i>Listen to message again</i> feature, which follows the playback interruption.
[MailboxMenu_PlayRecipient]	Menu while the message recipients are put out.
[MailboxMenu_FurtherOptions]	Menu after selection of the <i>Further options</i> feature, which follows the playback interruption.
[MailboxMenu_AfterPlayback]	Menu after playing a message in the <i>Incoming messages</i> message group.
[MailboxMenu_AfterPlaybackOutGoingMsg]	Menu after playing a message in the <i>Outgoing messages</i> message group.
[MailboxMenu_ChangeDestination]	Menu for changing a recipient address.
[RecordMenu]	Menu during message recording.
[RecordMenu_PauseRecording]	Menu after stopping message recording.
[RecordMenu_Delete]	Menu if the <i>Delete message</i> option is selected after stopping the recording.
[RecordMenu_ListenRecording]	Menu after selection of the <i>Play recording to review</i> feature, which follows the recording stop.
[RecordMenu_Addresssing]	Menu for entering the recipient's of a message.
[RecordMenu_Sendoptions]	Send options menu.
[TTM_Options]	Menu for Trusted Transfer Mode.

Table 21 Menu IDs for the PhoneMail Configuration File MenuConfig.ini

In the following we will exemplify the entry structure in the configuration file and how individual modifications can be performed on the basis of the PhoneMail main menu.

Example: [MainMenu]

```

...
[MainMenu]
Record=1
Mailbox=3
Connect=7
Replyoptions=8
Mailboxoptions=9
...

```

The entries in the configuration file for the menu ID *[MainMenu]* have the following significance:

- *[MainMenu]*
Specifies that the following entries define the settings for the PhoneMail main menu.
- *Record=1*
Specifies that a user may select the main menu option *Record* with telephone key **1**.
- *Mailbox=3*
Specifies that a user may select the main menu option *Mailbox* with telephone key **3**.
- *Connect=7*
Specifies that a user may select the main menu option *Connect* with telephone key **7**.
- *Replyoptions=8*
Specifies that a user may select the main menu option *Replyoptions* with telephone key **8**.
- *Mailboxoptions=9*
Specifies that a user may select the main menu option *Mailboxoptions* with telephone key **9**.

If these default settings are to be adjusted in a way that a user can, for example, record a message in the main menu with telephone key **1** instead of **2**, the configuration file needs simply to be adapted as follows:

```

...
[MainMenu]
Record=2
...

```

When changing the configuration file settings, please heed the following:

- In the configuration file
 - you must not remove existing menus or options
 - you must not add new menus or options

- You need to specify different telephone keys for the various menu options. In this context, the XPR server will not check the configuration file for wrong settings.
- If the same telephone key is allocated for several menu options, the PhoneMail protocol will malfunction.
- For the options of all menus except *MailboxMenu_DuringPlayback*, only single telephone keys may be specified. To use the options of the *MailboxMenu_DuringPlayback* menu you may also enter key sequences.
- If you change the key setting for a menu, the associated menu prompt of the PhoneMail protocol has to be accordingly adjusted as well.
- The producer documentation describes the PhoneMail default behavior – thus the behavior as defined in the shipped version of the `MenuConfig.ini` file.

Activating modifications to the configuration file

The contents of the configuration file is only evaluated during the start of the telematics APL used. Therefore, you need to reboot the telematics APL to activate modifications to the configuration file in PhoneMail.

10.4.3.17 Connecting to a Message Originator with Hicom 150E Office

The PhoneMail script must be configured in order to take advantage of the telephone feature. This is done via disabling the option **Call transfers via PBX** on the *Call Transfer Settings* tab of the general voice mail settings. Cf. [Section 10.9.2.5, “Call Transfer Settings”, on page 819](#).

IMPORTANT:

This setting should only be used in special cases, however, because this function occupies two B-channels on the Hicom 150.

To use this feature with the Outlook Extensions as well, the *ctilight.e* script (logical name: CTILIGHT) and the PhoneMail script need to be configured.

10.4.3.18 Repeat Strategy for User Outcall

The repeat strategy set for the PhoneMail protocol applies to User Outcall. The default settings are 3 times with 60 seconds interval, 2 times with 120 seconds interval and once with 300 seconds interval.

If practical use reveals that users do not receive new-message notifications, the individual values should be changed to allow more attempts and/or to set longer periods between attempts.

For the PhoneMail operation the user manual *PhoneMail* is available.

10.4.3.19 Default Allocation for Shortcuts

In PhoneMail, shortcuts can be used to quickly navigate to specific PhoneMail menu options – for example the option to record a new message. Shortcuts can be individually defined by each user via the Web Assistant, but the administrator needs to specify a default allocation first.

Specifying default menu-shortcuts for all users

In the following we describe how to configure such a default allocation for all XPR users of a defined user group.

1. Configure the shortcuts for an arbitrary XPRuser according to the desired default allocation. Use the Web Assistant for this purpose.

NOTE:
In the following steps we assume that the XPRuser chosen here has the user ID *TEMPLATE*. If you want to appoint a user with another ID, replace *TEMPLATE* with this user's ID in the course of the further description.

2. Open a Windows command prompt and switch to the directory
`<XPR-Install>\SDKTools`
3. Enter the following command in the Windows command prompt to export the correlation database contents to the `cor.txt` file:

`infotool export rec=correl file=cor.txt`

The `cor.txt` file is stored in the following directory:

`<XPR-Install>\SDKTools`

NOTE:
Since the InfoTool accesses the server via Named Pipes you have to be local administrator on the computer the XPR server is running on for each call.

4. Open the `cor.txt` file in a text editor – for example NotePad.
5. In the `cor.txt` file look for the word *TEMPLATE* and find the line that reads `VM_SC_DESC_41`.

Example:

<code><Server></code>	USER	TEMPLATE	VM_SC_DESC_41	<code><Description></code>

NOTE:
The entries for `<Server>` and `<Description>` depend in your file on the XPR server configuration.

Delete all lines between this entry and the following line at the beginning of the `cor.txt` file.

DOMAIN	CLASSNAME	CLASS	KEYNAME	KEY

6. In the `cor.txt` file look for the line that reads `VM_SC_KEYS_49`.

Example:

<code><Server></code>	USER	TEMPLATE	VM_SC_KEYS_49	<code><Key></code>

NOTE:

The entries for `<Server>` and `<Key>` depend in your file on the XPR server configuration.

7. Delete all lines after this entry.
8. Your `cor.txt` file must now only contain the following lines:

Example:

DOMAIN	CLASSNAME	CLASS	KEYNAME	KEY
<code><Server></code>	USER	TEMPLATE	VM_SC_DESC_41	<code><Description></code>
<code><Server></code>	USER	TEMPLATE	VM_SC_DESC_42	<code><Description></code>
...				
<code><Server></code>	USER	TEMPLATE	VM_SC_DESC_49	<code><Description></code>
<code><Server></code>	USER	TEMPLATE	VM_SC_KEYS_41	<code><Key></code>
<code><Server></code>	USER	TEMPLATE	VM_SC_KEYS_42	<code><Key></code>
...				
<code><Server></code>	USER	TEMPLATE	VM_SC_KEYS_49	<code><Key></code>

9. Replace the expression TEMPLATE with USER.

Example:

DOMAIN	CLASSNAME	CLASS	KEYNAME	KEY
<Server>	USER	USER	VM_SC_DESC_41	<Description>
<Server>	USER	USER	VM_SC_DESC_42	<Description>
...				
<Server>	USER	USER	VM_SC_DESC_49	<Description>
<Server>	USER	USER	VM_SC_KEYS_41	<Key>
<Server>	USER	USER	VM_SC_KEYS_42	<Key>
...				
<Server>	USER	USER	VM_SC_KEYS_49	<Key>

NOTE:

With the USER expression you define that the described shortcut settings apply later for all XPR users of the USER group – such users are in most cases all XPR users except the administrator.

If you want to assign the shortcut settings to users of another user group, simply replace TEMPLATE with the desired group name.

10. Save the `cor.txt` file.

IMPORTANT:

The columns in the file are separated from each other by a tabulator. Be sure to keep it like that. If you inadvertently delete one of the tabulators or replace it with a blank, the file will become corrupt.

11. Enter the following command in the Windows command prompt to export the modified contents of the `cor.txt` file to the correlation database:

```
infotool import rec=correl file=cor.txt
```

NOTE:

Writing operations on the database require a password. Only service personnel know this password for security reasons.

You have thus configured the shortcuts specified in step 1 for all XPR users of the USER group. These settings are immediately valid after the import into the Correlation Database. Neither the XPR server nor one of its components needs to be rebooted.

If users are not happy with the shortcuts configured in this way, the settings may be individually adjusted in the Web Assistant by each XPR user.

Making the shortcut default allocation permanent

If the XPR users are not to individually adjust the configured shortcut settings, the page for setting shortcuts must be removed from the Web Assistant. Proceed as follows:

1. Open the Windows Explorer and switch to the directory
`<XPR-Install>\res\WebApl\WebAdmin\html`
2. In this directory find the `usrsettings.htm` file and make a backup.
3. Open the original `usrsettings.htm` file in a text editor – for example NotePad.
4. In the `usrsettings.htm` look for the line that reads
`<!-- programmable short cuts -->`
5. Cut the `-->` characters from the end of the found line. The line thus only reads
`<!-- programmable short cuts`
6. Approximately 10 lines further below look for the line that reads
`</xp_if>`
7. Attach the just cut characters to the end of this line. The line now reads
`</xp_if> -->`
8. Save the `usrsettings.htm` file in the directory
`<XPR-Install>\res\WebApl\WebAdmin\html`

You have thus removed the shortcut settings from the Web Assistant. XPR users are now disabled to change the defaulted shortcut settings.

If you want to display the shortcut settings in the Web Assistant again, restore the original content of the `usrsettings.htm` file from the backup.

10.4.3.20 Out-of-Office Greetings

PhoneMail users may configure an individual out-of-office greeting in the PhoneMail TUI or in the Web Assistant for their mailbox. In doing so the PhoneMail users may individually set up to which date the out of office greeting is to be active.

The out office greeting will be played during the configured time range and overrides all user greeting !

In case that an Xpressions user sends a message via Phonemail (Direct Address) to an user with an out of office greeting it reacts in the following way:

- Phonemail stores the incoming message
- Phonemail sends a replay that contains the original message and the configured out of office greeting to the message originator.

Activating out of office greetings

So that PhoneMail users can configure out of office greetings you need to add the **VM_OUT_ANN_T** database field to the **USER** mask of the correlation database. In doing so, use the attributes **CHAR** and **UPPER** and a data field length of at least **15** characters.

Subsequently, all PhoneMail users can deploy the settings in the PhoneMail TUI and in the to configure an individual out of office greeting for their mailbox.

10.4.3.21 Company-internal Messages

PhoneMail supports the company-internal message type. Messages of this type feature the following special properties.

- Company-internal messages can only be sent via the PhoneMail TUI
- Company-internal messages are displayed in the Web Assistant grayed out and cannot be opened there
- Company-internal messages are always played twice for the PhoneMail user before they can be deleted or saved
- Company-internal messages cannot be forwarded until they have been saved
- Company-internal messages are administered by PhoneMail in two separate message queues. In a queue for urgent and in a queue for not urgent company-internal messages. The messages in these two message queues are announced in the TUI before all other messages
- While a company-internal message is being played, PhoneMail does not accept any DTMF commands
- If the PhoneMail user leaves his/her mailbox without deleting or saving the company-internal message, it will be announced as new company-internal message next time the user logs in
- If the PhoneMail user saves a company-internal message, it will be saved as a standard voice message.

Activating company-internal messages

So that a PhoneMail user can send company-internal messages, you need to assign the **Send Enterprise Broadcast Message** privilege to his/her user account.

Company-internal messages can be received by every PhoneMail user.

10.4.3.22 Guest Mailbox

PhoneMail offers its users the option to configure up to nine mailboxes for each user-individual guest via the Web Assistant. The configuring PhoneMail user can specify an individual PIN for each guest mailbox.

PhoneMail generates the numbers of guest mailboxes and the user IDs for the mailbox access from

- the mailbox number of the PhoneMail user who has configured the guest mailbox and
- a consecutive digit attached to the mailbox number of the PhoneMail user.

Example:

A PhoneMail user with the mailbox number 1000 creates four guest mailboxes. For the guest mailboxes PhoneMail then uses as numbers and user IDs the numbers: 10001, 10002, 10003 and 10004.

IMPORTANT:

When creating a new guest mailbox, the number of the guest mailbox may clash with the mailbox numbers of the regular PhoneMail mailboxes (cf. [Section 10.4.3.22, “Clashing mailbox numbers”, on page 676](#)).

Guest mailboxes have the following properties.

- A guest may access his/her guest mailbox via the PhoneMail TUI only.
- Guest mailboxes may only be accessed via the PhoneMail Direct Access. Access via the Guest or Forward Access is not possible.
- Via guest mailboxes, messages can only be sent, received, answered, deleted and saved. Further features such as notifications or time profiles are not available
- From a guest mailbox, messages can only be sent to the following persons:
 - To the PhoneMail user who has configured the relevant guest mailbox.

- To all other guest mailboxes that have been created by the same PhoneMail user.
- In a guest mailbox, messages can only be received by the following persons:
 - By the PhoneMail user who has configured the relevant guest mailbox
 - By all other guest mailboxes that have been created by the same PhoneMail user.

NOTE:

Other PhoneMail users may address messages to guest mailboxes via distribution lists but these messages are not forwarded to the guest mailboxes by the MTA. Instead, the originator is notified that the sent message cannot be delivered to a guest mailbox.

- Not trusted numbers can be configured for guest mailboxes
- No short cuts can be configured for guest mailboxes.

Clashing mailbox numbers

The automatically created mailbox number of a guest mailbox may have been allocated for the regular mailbox of an XPR user already. It may also happen that you create a new regular mailbox and specify a mailbox number that is already allocated for a guest mailbox.

In these cases the XPR server behaves as follows.

1. If an XPR user wants to create a new guest mailbox but the automatically assigned mailbox number exists for a regular mailbox already, the XPR server will reject the creation of the new guest mailbox.
An error message will point out that the desired mailbox number already exists.
2. When you create a new regular mailbox, but the specified mailbox number exists already for a guest mailbox, the XPR server creates the new regular mailbox.
An error message will point out that the desired mailbox number already exists, though.
So that no message addressing problems arise, the **Voice#** field of the new regular mailbox remains empty and you need to assign a unique mailbox number manually.

Activating guest mailboxes

How to activate the use of guest mailboxes in PhoneMail.

1. Set the NCO variable **EnablePostDialing** to **true**.
2. Add the following rule to the MTA routing rules at the beginning:

```
"NVS:VOICE<(\. .+) ?>/<. +>$<[1-9]>"=NVS:VOICE%1/  
%2 [FOLDER=$hidden/Guest%3]
```
3. So that a PhoneMail user may configure guest mailboxes, you need to assign the **Guest Mailbox** privilege to his/her user account.

10.4.4 Voicemail VMS

VMS is in addition to PhoneMail another telephone user interface of the XPR server, which allows you to retrieve and administer voice mails, fax messages and e-mails. This TUI can also be used to record and send voice mails for other subscribers.

If display messages are to be sent to phone devices by VMS via CorNet, then the script *CIT Hicom Device Display* should also be activated. VMS is configured in the same way as PhoneMail.

If the voice mail scripts PhoneMail and VMS are used in an XPR system in parallel, please note the following:

- A user can select the voicemail system he/she prefers in the Web Assistant. As the caller has already been identified when he/she uses the Call Back Access Mode by the access number transferred in the process (ANI), the relevant voice mail system can be started correctly, even if the access number of the other voice mail system was called.
- For external callers, this means that the voice mail system is not switched.
- The access numbers must originate in the assigned extension range which naturally must **not** overlap for PhoneMail and VMS.

You find further information about how to operate the voice mail scripts PhoneMail and VMS in parallel in [Section 10.4.5, “Using the PhoneMail and VMS Protocols in parallel”, on page 699](#).

Let's have a look at the configuration tabs *General* and *Script* in the protocol settings.

10.4.4.1 Configuration Tab *General*

The screenshot shows the 'E-Script Protocol Properties' dialog box with the 'General' tab selected. The 'Name' field contains 'VMS'. The 'Protocol designation' field contains 'Xpressions VMS'. The 'Description' field contains 'Xpressions VMS Script'. The 'OK', 'Cancel', and 'Apply' buttons are visible at the bottom.

Displayed elements are comprised of the protocol name (**Name**) (over which the protocol is addressed), **Protocol designation**: (used for display in the XPR monitor), and a detailed **Description**: of the protocol and its functions which appears in the configuration tab when selected.

IMPORTANT:

So that the VoiceMail protocol can operate trouble-free, it must be assigned the logical name *VMS*.

The logical protocol name serves as reference for the assigned protocol and is evaluated by modules that communicate with the telematics APL.

10.4.4.2 Configuration Tab *Identification*

The *Identification* tab for PhoneMail corresponds to the one of the Fax G3 protocol. Compare [Section 10.4.6.2, “Configuration Tab Identification”, on page 705](#).

10.4.4.3 Configuration Tab *Repeat Strategy*

The *Repeat Strategy* tab for PhoneMail corresponds to the one of the Fax G3 protocol. Compare [Section 10.4.6.4, “Configuration Tab Repeat Strategy”, on page 707](#).

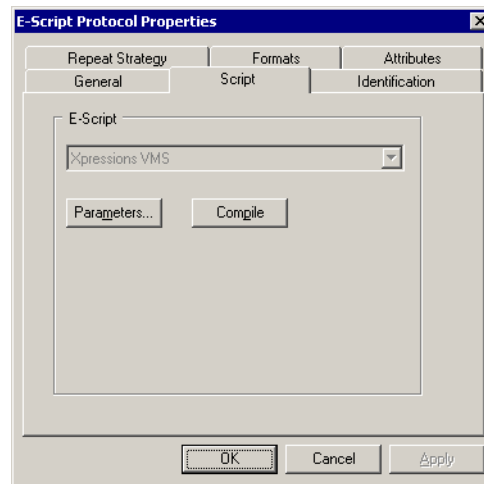
10.4.4.4 Configuration Tab *Formats*

The *Formats* tab for PhoneMail corresponds to the one of the Fax G3 protocol. Compare [Section 10.4.6.6, “Configuration Tab Formats”, on page 709](#).

10.4.4.5 Configuration Tab *Attributes*

The *Attributes* tab for PhoneMail corresponds to the one of the Fax G3 protocol. Compare [Section 10.4.6.7, “Configuration Tab Attributes”, on page 710](#).

10.4.4.6 Configuration Tab *Script*



In the E-Script field the desired script entry can be selected or a concrete name is already entered.

IMPORTANT:

If the protocol had been selected by name from the list after clicking the **Add** button, the **E-Script** is the default. If the entry **User-defined Script** has been selected instead of a protocol by name, the desired protocol name can now be defined in the **E-Script** field (cf. [Section 10.9.1, “Scripts”, on page 806](#)).

If you click the **Parameters** button, you will come to the actual protocol configuration. Via **Compile** you can compile the actual script. This is only required when you have developed new scripts yourself which are thus present in the source. In most cases an already compiled object file is available which can be executed by the XPR server.

Let's have a look which options are available for the actual protocol installation via the **Parameters** button on the configuration tab *Script*.

10.4.4.7 Parameter Tab *General*

The screenshot shows the 'Xpressions VMS' window with the 'General' tab selected. Under the 'Service Access Numbers' section, there are four input fields with the following values:

Access Type	Access Number
Own voice mailbox (Direct Access):	81299
Other user's mailbox (Guest Access):	82298
Other user's mailbox (Universal Access):	82297
Mailbox (Callback Access):	82296

At the bottom of the window are buttons for 'OK', 'Cancel', and 'Apply'.

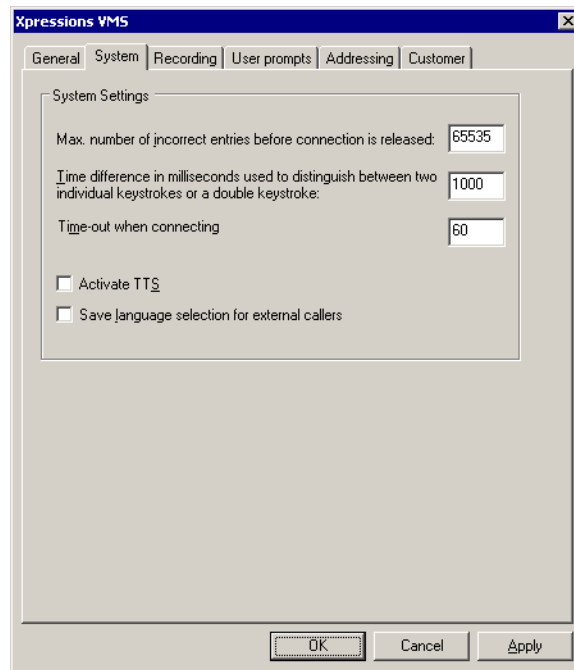
In the parameter tab *General* the phone numbers for telephone access via the access modes *Direct Access*, *Universal Access*, *Guest Access* and *Callback Access* are defined. The corresponding access numbers must be configured in the PBX in a way that calls to these numbers are automatically forwarded to the XPR server. The access numbers must be within the extension number range that is connected to the VMS script.

Description of access types:

- **Direct Access (DA)**
Corresponds to *Own voice mailbox* access. The system checks the user's ID on the basis of his/her telephone password and sends the user to the main mailbox menu.
- **Guest Access (GA)**
Corresponds to *Other user's mailbox* access. This access, also known as *polled prefix dialing*, is addressed to leave a message in another mailbox. The user can also change to the Direct Access when he/she presses the keys 0 and *. This starts the login, which leads to the main menu after a respective identification check.
- **Universal Access (UA)**
Answering machine mode. This mode is addressed as soon as a Redirecting Number (RN) is transferred during the connection setup to the VMS.
- **Callback Access (CA)**
Corresponds to *Mailbox* access. In this case, VMS starts with the new inbound messages after identification rather than in the main menu.

The server uses four different access numbers on the XPR server to distinguish the individual access types. A different number is assigned to each of the modes, Callback Access, Direct Access and Guest Access. If a redirecting number should be transmitted when a connection is established, the connection takes place via Universal Access. The parameters for the numbers called on the XPR server are mandatory.

10.4.4.8 Parameter Tab *System*



In the parameter tab *System* several settings for the behavior of the XPR server can be made.

If **Max. number of incorrect entries before connection is released** is selected, the connection is cleared down after the specified number of incorrect script entries. This is necessary, for example, to avoid maintaining connections with other automated devices for too long.

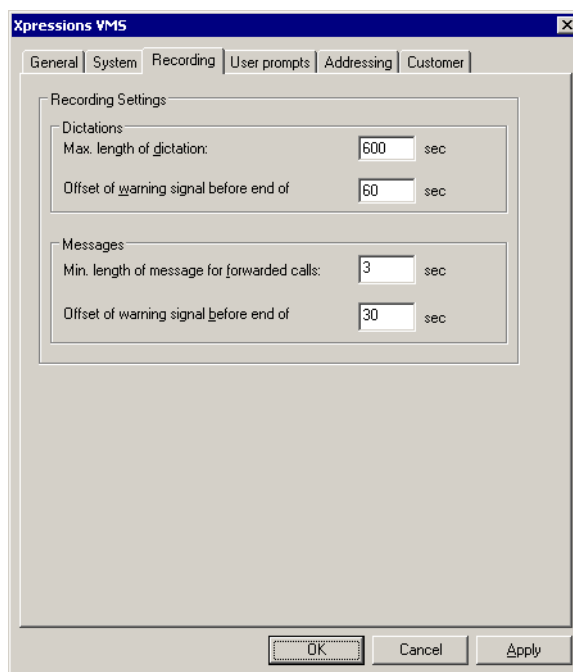
The **Time difference in milliseconds used to...** serves for distinguishing between two single keystrokes or a double keystroke. This is needed for [44] and [66] commands during message processing.

The **Time-out when connecting** value specifies the number of seconds allowed to elapse before the connection attempt is canceled.

If the **Activate TTS** option is active, users may have messages read out via text-to-speech. The user needs the `TTS Capabilities` privilege for this.

The **Save language selection of external callers** option saves the language settings of external calls, so that the caller hears the selected language for the next call. This setting is only relevant in the case of multilingual installations.

10.4.4.9 Parameter Tab *Recording*



In the parameter tab *Recording* recording settings for dictations and messages can be configured.

You can define the *Max. length of dictation* in the **Dictations** area. The parameter **Offset of warning signal before end of recording** defines the length of time between the warning and the actual termination of the recording. As the recording time is longer for dictations than for messages, we recommend to warn the user on time. If you want to dictate a 30-minute letter, you will not want to receive a warning when you have only 30 s left. A warning 2 minutes before the end of recording would be much better in this case.

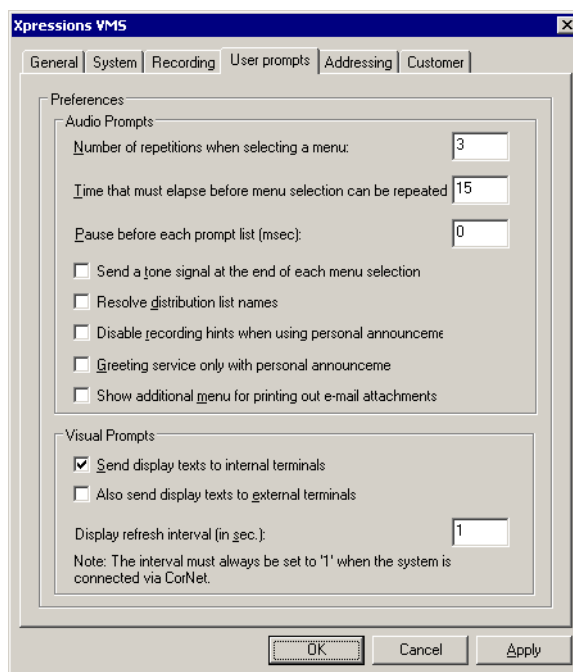
You can define the ***Min. length of messages for forwarded calls*** in the **Messages** area. You can set the length (in seconds) that the messages must have for them to be accepted and saved. Because some users just hang up when they find that the called party is an answering machine, this option is intended to prevent the generation of messages containing nothing but the sound of the handset being replaced. This parameter only applies to messages which are recorded as part of a call forwarding operation and which are terminated by handset replacement.

NOTE:

If a message recording is completed with the * key, the XPR server saves a shorter message as well.

The parameter **Offset of warning signal before end of recording** is used for recording messages. It defines the time between the warning that the caller hears and the actual end of the recording time.

10.4.4.10 Parameter Tab *User prompts*



Special acoustic and visual options for simplifying user prompting can be set in the *User prompts* parameter tab.

The option **Number of repetitions when selecting a menu** refers to the number of times a menu is offered for selection.

Example:

For **Number of repetitions when selecting a menu**, value **3** is set. In this case, the menu is output to the user once and then repeated three times.

The **Time that must elapse before menu selection can be repeated** refers to the length of time that a user who has made an incorrect entry must wait before he/she can repeat menu selection. This value should not be less than 15 seconds.

Pause before each prompt list (msec) specifies how long the system should pause before a prompt list is played back.

The **Send a tone signal at the end of each menu selection** option is used to send a tone after each completed menu selection to indicate that the selection offered is finished.

Resolve distribution list names means that the distribution list names are resolved and individual addresses are represented in the case of status queries.

Disable recording hints when using personal announcements means that a caller only hears a personal announcement played, and cannot leave a message.

If the **Greeting service only with personal announcements** option is set, the Greeting only service (infomode) can only be combined with a personal greeting and not with standard announcements. This means that only personal greetings are sent to Greeting only services.

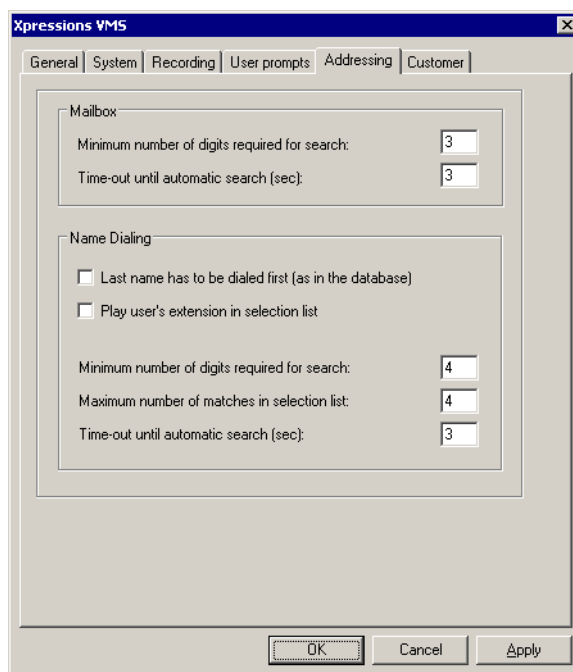
Show additional menu for printing out e-mail attachments allows the user to print out an e-mail attachment at a printer via an additional menu.

Send display texts to internal terminals is an option for sending displays for user prompts to the internal terminals used.

Also send display texts to external terminals is used for sending displays to external telephone devices. This option cannot be used unless **Send display texts to internal terminals** is activated. This setting can be necessary in the case of Virtual Private Networks (VPN).

The **Display refresh interval (in sec.)** option applies to the frequency at which displays are updated during message recording or playback. For connecting Hicom PBXs via CorNet-N this value should always be set to **1**.

10.4.4.11 Parameter Tab Addressing



In the *Addressing* parameter tab, settings for mailbox and name selection are performed.

In the *Mailbox* section the following options are available:

When dialing a mailbox, its complete phone number need not necessarily be specified. Under the following conditions dialing the first digits of a mailbox is sufficient:

- The number of digits defined in the **Minimum number of digits required for search** field must at least have been dialed.
- The associated destination mailbox could be determined from the dialed digits.

This option can accelerate routing to a mailbox.

If no entry is made in the **Time-out until automatic search** field via the telephone keypad, PhoneMail starts the automatic search for the associated mailbox. The digits entered until then are used for the search.

This option saves pushing the # key to complete the phone number entry for a mailbox.

In the *Name Dialing* section the following options are available:

NOTE:

To optimize searching in the database on the basis of name dialing, the XPR server uses the `VM_VANITY` database field. In this database field the XPR server deposits a user-individual vanity number created from another database field of the respective user. You find more details on this in [Section 11.11, “Vanity Number Support”](#), on page 895.

Last name has to be dialed first controls the PhoneMail-integrated user note for the entry of name dialing by the user. For this operating instruction two options are available:

- Name dialing entry starting with the first name
 - Name dialing entry starting with the last name
-

IMPORTANT:

The setting **Last name has to be dialed first** only controls which operating instruction is played to the user by the PhoneMail script. The selected option does *not* influence the search algorithm of the XPR server.

The XPR server compares the information entered for name dialing with the entries of the **Name** fields of the XPR database. Depending on the users being stored with leading first name or last name, the operating note **Last name has to be dialed first** must be activated or not.

Consequently, a mixture of the first and last name sequence in the **NAME** fields of the XPR database causes problems in the search algorithm.

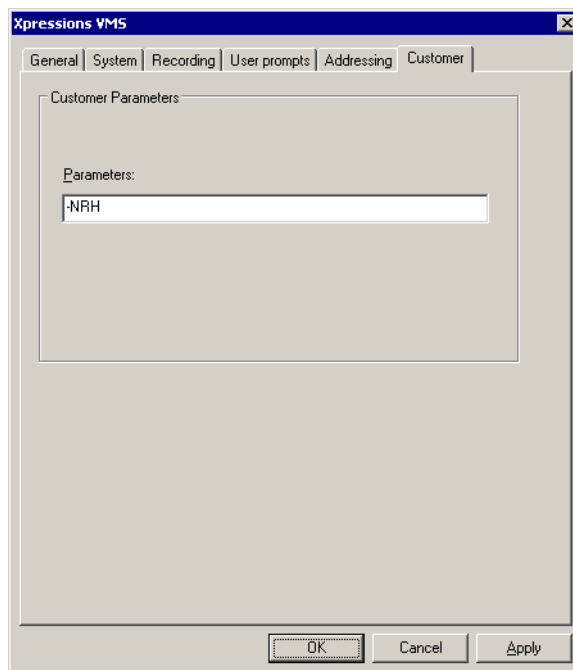
If a user receives a hit list for name dialing, each hit can be announced either with or without the corresponding extension. **Play user's extension in selection list** defines whether the extension is specified as well.

For name dialing not the complete name of the callee must be entered. **Minimum number of digits required for search** defines the minimum number of letters to be entered via telephone keys before a search for matches can start. If you finish the name dialing with the # key after having entered fewer digits than required, the PhoneMail script prompts you to continue the entry.

Maximum number of matches in selection list defines the maximum length of match lists. If a match list with more users than defined here results from name dialing, the PhoneMail script points this out and requests redialing. This redialing should then be performed with a qualified entry to shorten the hit list.

If no entry is made in the **Time-out until automatic search** field via the telephone keypad, PhoneMail starts the automatic search for matching user names. Only the characters entered until now are used for the search.

10.4.4.12 Parameter Tab *Customer*



Any system settings can be made in the *Customer* parameter tab. The customer-specific customization of the VMS script is a mandatory requirement here.

Features can also be enabled on a project-specific basis by entering the relevant parameters. The following general switches are available at present. During your entry, you must separate them from each other by blanks:

NOTE:

Parameters with a minus sign before them are option switches that can be activated as needed. Parameters without a minus sign before them require a value input in order to create the corresponding behavior.

- **-DISABLECALLCOMPLETION**
VMS offers the option to directly call back a voicemail originator from VMS. If the telephone of the relevant originator is busy during such a return call, or the originator does not accept the call, VMS supports the activation of an automatic return call. This requires the PBX used to also support this feature. If the **DISABLECALLCOMPLETION** parameter is set, the activation of a return call in case of a busy or unanswered phone is disabled.
- **-FD (Full Duplex)**
If this option is activated, the voice recording continues even during the warning tone that comes near the end of the recording time.
Default: Off

- `force_lang`
Determines an individual TUI language for this VMS entity. If this parameter is not specified, the XPR server default language is used for the VMS TUI. When this parameter is used, the language set here is always deployed, independent from other settings.

Possible values for this parameter are:

– 1031: German	– 1055: Turkish
– 1033: English (USA)	– 2057: English (UK)
– 1036: French	– 2058: Spanish (USA)
– 1040: Italian	– 2070: Portuguese
– 1043: Dutch	– 3082: Spanish
– 1046: Brazilian	– 3084: Canadian
– 1049: Russian	

- `HPQueryDisabled`
Deactivates the Hicom PIN query in Callback Access, if the user calls from his/her own terminal device.
Default: Off
- `-IDVP`
Suppresses the use of the default PIN (see [Security Settings](#) in [Section 10.9.2, “General Voicemail Settings \(Voicemail\)”, on page 811](#)). Users log on to VMS with their Hicom PIN. This option exempts users from having to enter the additional telephone password. If the user specifies a telephone password, this must be entered.
- `-lr`
By default, VMS uses in case of cascaded forwarding always the first redirecting phone number as redirecting number. If you activate this option, VMS uses in case of a cascaded forwarding always the last redirecting phone number as redirecting number instead (cf. [Section 10.1.5.2, “Cascaded Forwarding”, on page 552](#)).

IMPORTANT:

If you use the IP APL, the script parameter `lr` only takes effect for SIP and CorNet IP devices.

- `-NDOFF`
Deactivates the name dialing for all VMS users.
- `-noconnect`
While playing a message the VMS user can have a connection established to a subscriber by default. If the `noconnect` parameter is active, such a connection to a subscriber cannot be set up.

- `-norestartonchangedpartner`

In the access modes Guest Access and Universal Access the telematics APLs do not restart the VMS script by default, when the connection partner changes. If such a reboot is desired, this parameter must be disabled.

Example:

Subscriber A calls subscriber B. Subscriber B accepts the call and wants to reroute it to a VMS mailbox. He/she initiates a consultation to the VMS Guest Access. The VMS script asks B for the mailbox number to which A is to be routed. B enters the desired mailbox number. Then, he/she hangs up and A is connected to the specified mailbox.

If the `norestartonchangedpartner` parameter is disabled, the VMS script reboots after subscriber A has been transferred to the VMS script. Subscriber A would then be asked for the desired mailbox number again, which, as a matter of rule, is not desired, since he/she does not necessarily know the required mailbox number.

Default: **On**

- `-NOTDSPCOUNTER` (Not Display Counter)

Activating this switch suppresses the progress indicator during message playback (time display).

Default: **On**

- `-NRH`

suppresses the user prompt "Please start speaking after the tone" at the end of a personal greeting (only applies to Forward Access)

- `-OldFA`

You can change the Direct Access or Guest Access behavior via this parameter. A mailbox number is usually queried if the number of the phone redirected to the Guest Access is not assigned to any user. Instead, this parameter enables playing the information that the user does not have a mailbox. In case of a call coming from a rerouted telephone, the Direct Access behaves like the Guest Access. Therefore, this adjustment applies for the Direct Access as well.

- `R_WS=<value>`

This parameter allows the time span for forward and backward jumps during message playback to be changed. The value is given in seconds. Entering value **0** enforces the default of **10** seconds

- `r_plen, r_plev, r_slen and r_slev`

Since the electrical characteristic for the recording volume depends on the recording/playback components (respectively on their drivers) used, the volume may have to be adjusted.

The impulse length that must at least be available for starting a recording can be additionally influenced.

These parameters help to better recognize whether or not someone is speaking in order to start or stop recording. In this way recording times are limited so that no unnecessarily large recording files are generated. The problem is to select the level that clearly recognizes speech but still interprets line and background noise as silence, for example. The thresholds for length and peak level, required to detect breaks, can be adapted here.

- **R_PLEN=<value> (Record Peak Length)**
 Defines in milliseconds the minimum pulse length required to begin recording.
Default: 64
Value range: 0 to 4000
- **R_PLEV=<value> (Record Peak Level)**
 Defines the minimum pulse level a signal needs to have to begin recording. The higher the “peak level” is selected, the louder a person must speak to start a recording. The values you can enter range from 0 to 4000. When the entry value is divided by 40, you receive the level value in percent (in relation to the maximum value).
Default: 32
Value range: 0 to 4000
- **R_SLEN=<value> (Record Silence Length)**
 Defines in milliseconds the pulse length a recording pause must have to stop recording.
Default: 3000
Value range: 0 to 4000
- **R_SLEV=<value> (Record Silence Level)**
 Defines the minimum pulse level a recording pause must have to stop recording. The higher the “peak level” is selected, the louder a person must speak for the recording not to be stopped. The values you can enter range from 0 to 4000. When the entry value is divided by 40, you receive the level value in percent (in relation to the maximum value).
Default: 32
Value range: 0 to 4000
- **RC=<Cut end of recording in milliseconds>**
 In the case of signaling via DTMF, the tone for ending a recording may also be recorded. To avoid this, a portion (in milliseconds) can be automatically cut off of the end of the recording. RC (Record Cut) sets the length in ms.
Default: 300ms

 In CorNet-N connections, control is performed in the D-channel. Consequently, it is generally not necessary to cut anything here (RC=1).
- **-REDUCEDFUNCTIONS**
 Deactivates the following VMS functions for all VMS users.
 - Changing the mailbox deputy
 - Changing the referral extension

- Changing the playback options
- Activating/deactivating the call transfer
- Labeling messages as “unread”.
- **-RMTOPIC** (Remove XPR Monitor Topic)
If the XPR server is set up completely, it may happen that no topic entry for VMS monitoring can be created in the modules window of the XPR monitor. One of the reasons is that the number of topic entries is limited to 64 per APL. With the help of this parameter string the XPR monitor can be configured in a way that it removes existing topics from the branch of the applied telematics APL and inserts VMS as topic. The VMS activities can now be monitored in a logging window.
- **UAH=<value>** (User Address Error Hang Up)
Defines the maximum number of failed user entry attempts allowed for connecting to a telephone or fax number before the connection is cleared.
Default: 65000 (this means that the user is practically unrestricted in his/her attempts).

10.4.4.13 Company-specific Greetings

You can create global, company-specific greetings in the Web Assistant or via the telephone user interface (TUI). To do this, you must log on to the Web Assistant with administrator privileges and configure the company greetings there. These greetings are internally assigned to the user *Company*. In the case of configuration via TUI, you must log on under this user account; you can then configure the greetings. To this you need the *Company* user ID with the corresponding PIN. In the as-delivered status this special user has **no** PIN and **no** mailbox number.

10.4.4.14 VMS Language Settings

The VMS script contains a number of points at which a decision must be taken regarding the language used. Before the user logs in, the script is unaware of the user's preferred language. The script consequently uses the system language set during installation. If the user does not understand this language and therefore does not press any buttons, the script displays a language list from which the user can choose a language. Once the user has successfully logged in, the language set is applied.

NOTE:

If the VOGUE script routes a caller to VMS, VMS uses for all greetings the language that the VOGUE script has already defined for the caller – for example via a national language box.

10.4.4.15 VMS Database Fields

VMS uses the following XPR database fields:

Field	Meaning
USER	XPR user name; for example <i>John</i> . This is used for internal assignment and must be unique.
PIN	Defines the user-defined password in the VMS context. It is saved in encrypted format.
NAME	Actual name of a user; for example <i>Miller Harold</i> . This entry is used for displays.
VOICE#	The phone number of a user and the address of a user's info box.

Table 22 XPR Database Fields for VMS

VMS uses a range of additional database fields that are only used by VMS (VMS is therefore placed first).

10.4.4.16 Distribution Lists

There are three different types of distribution lists: broadcast distribution list, central distribution list and personal distribution list.

- Broadcast Call distribution list

These distribution lists can only be administered by the user *SYSTEM*. When this user is editing the central distribution list in the address book, he/she is working with so-called broadcast distribution lists. You can administer these distribution lists also with the Web Assistant or with the Communications client. Administration is also possible via HDMS.

Sample format:

Value range	Class name	Class	Key name	Key
MRS DUBLIN	GLIST	R_11	1	NVS:RUNDRUF/4930227123456
MRS DUBLIN	GLIST	R_11	2	NVS:RUNDRUF/4930227123457
MRS DUBLIN	GLIST	R_11	3	NVS:RUNDRUF/4930227123458
MRS DUBLIN	RUND	R_11	GLIST	

Table 23 VMS Broadcast Distribution List in the XPR Database

- Central (server-wide) distribution list

These distribution lists can be administered by VMS users who have the VMS administrator privilege. These users are permitted to edit the central distribution list in the address book. These lists can also be administered with the Web Assistant or with the *Communications* client. Administration is also possible via HDMS.

Sample format:

Value range	Class name	Class	Key name	Key
MRS DUBLIN	GLIST	11	1	NVS:VOICE/4930227123456
MRS DUBLIN	GLIST	11	2	NVS:VOICE/4930227123457
MRS DUBLIN	GLIST	11	3	NVS:VOICE/4930227123458
MRS DUBLIN	RUND	11	GLIST	

Table 24 VMS Central Distribution List in the XPR Database

- Personal (private) distribution list

These distribution lists can be defined by any VMS user. A private distribution list can have the same name as a public distribution list and has higher priority. Highest priority is always held by a mailbox number. These distribution lists cannot be administered with the XPR client and can only be used by the VMS script.

Sample format:

Value range	Class name	Class	Key name	Key
MYSERVER/<useralias>	GROUP	11	1	NVS:VOICE/4930227123458
MYSERVER/<useralias>	GROUP	11	2	NVS:VOICE/4930227123457

Table 25 VMS Private Distribution List in the XPR Database

The *useralias* is in this case determined by an internal database function.

10.4.4.17 Notification for User Outcall

During the installation of a XPR server automatically all prerequisites are created to use the *Notification* feature. The necessary prerequisites are given below as a checklist or for manual administration:

- The VMS script must be installed with the protocol name `VMS`.
- The user-defined routing rule for `PREFERRED` must be
- `NVS:.*/*[FLAG!=NOPREFERRED]=<PREFERRED>`
- The authorized user must have the appropriate call privilege (local, national, international)

Repeat strategy for user outcall

The repeat strategy set for the VMS protocol also applies to user outcall. The default settings are 3 times with 60 seconds interval, twice with 120 seconds interval and once with 300 seconds interval.

If practical use reveals that users do not receive new-message notifications, the individual values should be changed to allow more attempts and/or to set longer periods between attempts.

For operating VMS the *VMS* user manual is available.

10.4.5 Using the PhoneMail and VMS Protocols in parallel

The two voice mail systems, PhoneMail and VMS, can be configured in parallel on the same XPR server and can be used by specific subscribers. It is important that scripts and subscribers be correctly configured.

10.4.5.1 Configuring Scripts

Both scripts are installed via the applied telematics APL of the XPR server as already described above. With the exception of callback access, each script must be assigned unique phone numbers ranges for its access codes, enabling it to be individually addressed. This is sometimes desirable because the two scripts have a different scope of functions. Callback access is only assigned to the script most subscribers are expected to work with. When extension number ranges are assigned, again, the script assigned should be the one which most people use. All the necessary switch-overs between the scripts take place automatically.

The following table provides an overview of which script responds in which language for a specific selection. The following abbreviations are used:

DA – Direct Access	CA – Callback Access
GA – Guest Access	A – Phone number of the calling device
UA – Universal Access	B – Number called by A
FA – Forward Access	

	With Redirected Number		Without Redirected Number	
	A recognized	A unknown	A recognized	A unknown
DA	As for FA		Script DA-dependent. Language of A. Switch-over to caller's language after identification if necessary.	Script DA-dependent. Start with system language. Switch-over to caller's language after identification if necessary.
(GA)	As for FA		Script GA-dependent. Language of A. Switch-over to caller's language after time-out if necessary.	Script GA-dependent. Start with system language, switch-over to caller's language after time-out if necessary.

	With Redirected Number		Without Redirected Number	
	A recognized	A unknown	A recognized	A unknown
UA	As for FA		Script UA-dependent. Language of A. Switch-over to caller's language after time-out if necessary.	Script UA-dependent. Start with system language. Switch-over to caller's language after time-out if necessary.
FA	Script of B. Language of A.	Script of B. System language.	As for UA (if available, otherwise GA).	
	Switch-over to caller's language after time-out if necessary.			
Independent extension range	As for FA, redirected number is not evaluated.			
CA	As for FA		Script of A. Language of A.	As for DA

The table also shows that you can use forward access with all the access codes configured if a redirected number is supplied by the PBX.

Example:

In our example, PhoneMail is the script mostly used. All internal phone numbers are five-digit and range from 20000 to 69999. Guest Access is not used but Universal Access instead. In the PBX, the phone number of the XPR server is suppressed except for the last digit.

Extensions	PhoneMail	VMS
Direct Access	8	7
Guest Access	–	–
Universal Access	98	97
Callback Access	90	–
Fax Access	99	–
Transfer Access	91	–
Independent extension range	20000-69999	–

In this constellation, all extension numbers with a leading **0** or **1** can be used for other purposes, such as Fax-on-Demand or Automated Attendant.

Configuring subscribers

All subscribers should be assigned to a user group (e.g. *VMS_GROUP* or *PM_GROUP*) that already contains an entry for one of the two scripts. Thus, this script can be used as default setting for new users. This default setting should take the most frequently used script into account so that the necessary script switch-over does not have to be initiated for each connection.

Furthermore, users may be requested to set their required script via the Web Assistant.

10.4.6 Fax G3

NOTE:

The Fax G3 protocol sends fax messages up to a maximum length of 200 pages. If the **Chaining of documents enabled** option is active, this maximum message length applies for the entire send job.

The Fax G3 protocol enables the exchange of analog fax messages.

The **FAXG3#** field must be filled with the individually assigned extension in the XPR user database for each user. Use the international phone number format so that incoming fax messages can automatically be forwarded. This number is internally normalized and transcribed to the field **FAXG3** for use by the XPR server.

Example:

+49-1234-5678-90 would internally be converted into 491234567890.

You can select the same extension number range for the Fax G3 protocol as for Fax G4, as the XPR server can distinguish between these services with the help of the ISDN Service Indicator.

NOTE:

The Fax G3 protocol also recognizes a redirected phone. If a call arrives on a number that was not assigned to any user, the *Redirecting Number* is used to determine the correct recipient (cf. [Section 10.1.5, “Redirecting Numbers”, on page 551](#)).

In addition to the Fax G3 protocol the XPR server provides with *FoD.e* a fax polling script (see [Section 10.4.10, “Fax-on-Demand Server Script \(Fax-on-Demand\)”, on page 719](#)).

In all XPR clients, transmission is possible via entry of the destination number with simultaneous selection of the service Fax G3 in the send dialog. It is also possible to select the *E-Mail* service and enter the dial information FAXG3/ <destination number>.

Examples:

- 491234567890
- FAXG3/491234567890
- NVS:FAXG3/491234567890

The last example describes the complete address in the XPR format. This format is created, for example, by a mail gateway if it wants to send a Fax G3 document.

NOTE:

All viewers based on Windows Graphics Device Interface (GDI+) may display a TIFF fax page completely black. You find more information about this malfunction in <http://support.microsoft.com/kb/329270>. In such a case we recommend to use either one of the supplied clients or another viewer such as IrfanView, for example.

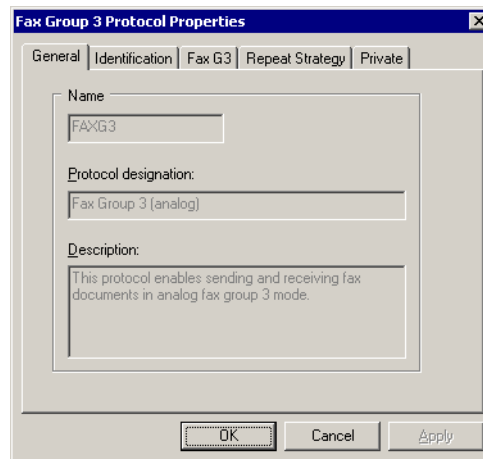
Let's have a look at the configuration tabs of the protocol settings.

10.4.6.1 Configuration Tab *General*

IMPORTANT:

For a default protocol the elements displayed here are only displayed and cannot be modified.

After a default protocol has been added to the XPR server once, it can be added again with a new name so that it can be provided with different properties. In this case the elements are to be edited.



Displayed elements are comprised of the protocol name (**Name**) (over which the protocol is addressed), **Protocol designation:** (used for display in the XPR monitor), and a detailed **Description:** of the protocol and its functions which appears in the configuration tab when selected.

10.4.6.2 Configuration Tab *Identification*



The image shows a Windows-style dialog box titled "Fax Group 3 Protocol Properties". It has five tabs: "General", "Identification", "Fax G3", "Repeat Strategy", and "Private". The "Identification" tab is selected. Inside the dialog, there are two text input fields. The first is labeled "Identification for fax transmissions" and contains the text "+49 1234 56789". The second is labeled "Page header for fax transmissions" and contains the text "Company". At the bottom of the dialog are three buttons: "OK", "Cancel", and "Apply".

With the indications *Identification for fax transmissions* and *Page header for fax transmissions* settings are defined that can be used instead of the Fax G3 identification and header globally configured in the XPR server. Up to 50 characters are permitted for the header.

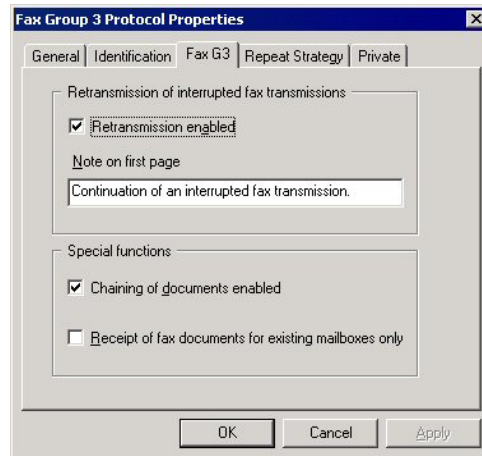
IMPORTANT:

The identification must correspond to the T.30 standard. This allows only digits, blanks and plus signs.

NOTE:

If an identification and header has been assigned to a user in the XPR user database, the personalized setting is used instead of the definition entered here.

10.4.6.3 Configuration Tab *Fax G3*



If in the configuration tab *Fax G3* the option **Retransmission enabled** is selected, the document will be sent at the next transmission from the page where the previous transmission had stopped .

The text entered in the **Note on first page** field is transmitted as note for the first page of the continued fax document.

When the option **Retransmission enabled** remains disabled, the complete document is after a connection shut-down always sent until it is transmitted correctly or the maximum number of repeats has been reached (cf. [Section 10.4.6.4, "Configuration Tab Repeat Strategy", on page 707](#)).

Via **Chaining of documents enabled**, up to 10 several fax messages can be sent to one destination address at the same time when a connection is established. The requirement is that originator, recipient and the applied fax resolution match. The maximum length 200 pages applies here for the chained message.

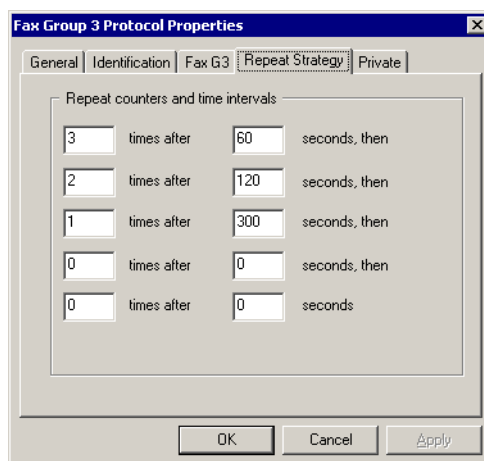
NOTE:

The IP APL does not support the **Chaining of documents** option.

Via the **Receipt of fax documents for existing mailboxes only** option it is possible to limit fax receiving so that the XPR server accepts incoming fax messages only for existing mailboxes. This option has various advantages:

- If an incoming fax document is destined for an unknown mailbox, the XPR server does not accept the message. This prevents unnecessary costs for the originator of the document.
- Since fax messages that cannot be assigned are not accepted at all, it is not possible to search for the unknown originator later on.
- System resources are saved since fax messages that cannot be delivered are not accepted at all.

10.4.6.4 Configuration Tab *Repeat Strategy*



Here the number of transmission attempts and the breaks between these attempts are specified. In the column on the left hand side you specify the number of repeats executed in the associated interval stated opposite.

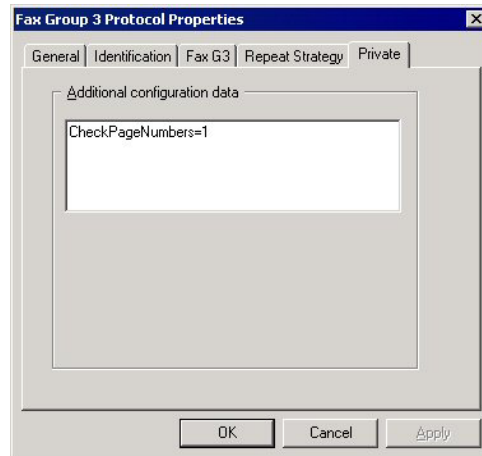
Up to five different counters with varying intervals to be executed in succession can be specified.

If all configured repeats for sending a message have been performed but the send job could not be executed successfully, the delivery attempts are stopped. The originator is informed about this in a corresponding status report.

NOTE:

The settings on the *Repetitions* tab are not used for the MWI protocol.

10.4.6.5 Configuration Tab *Private*



The configuration tab *Private* includes individual configuration data regarding the respective protocol. The settings made here correspond to an INI configuration file known from the operating system Windows 3.1.

One protocol-specific entry is made per line in the format *Label*>=<*Value*>.

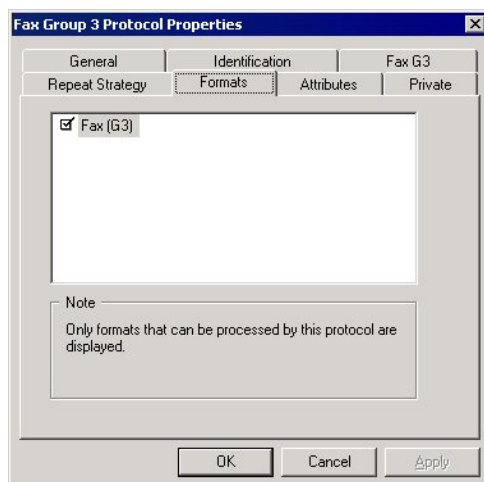
Example:

InsertMidH1=1

The possible entries are depicted in detail in the registry key [Private \[REG_MULTI_SZ\]](#).

10.4.6.6 Configuration Tab *Formats*

The configuration tab *Formats* is only displayed in the *Advanced Settings* of the telematics APL. In this dialog the various file formats are displayed which are supported by the respective protocol.



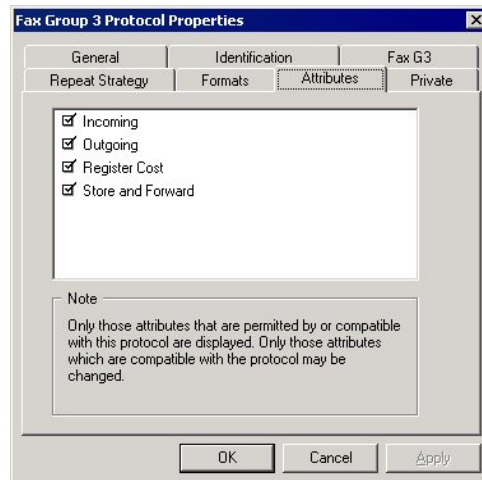
The XPR server automatically makes the necessary conversion (if possible) to one of the formats listed here for outgoing transmissions. If conversion is not possible, the XPR server generates an error message because the document cannot be sent with the selected protocol.

The Fax G3 protocol supports, for example, only the corresponding fax format.

These settings are automatically preset with appropriate parameters when a protocol of the XPR server is initially installed. Thus, they should not be modified.

10.4.6.7 Configuration Tab *Attributes*

The configuration tab *Attributes* is only displayed in the *Advanced Settings* of the telematics APL. In this dialog protocol attributes of the respective protocol are displayed and can be activated or deactivated by clicking the check box next to the entry.



If, for instance, outgoing traffic was deactivated and only incoming traffic was activated, this protocol would only accept incoming protocols but it would not send anything.

These settings are automatically preset with appropriate parameters when a protocol of the XPR server is initially installed. Thus, they should not be modified.

10.4.7 Fax G3 Post-Dialing

IMPORTANT:

The Fax G3 Post Dialing protocol works only in combination with the Fax G3 protocol. When the Fax G3 Post Dialing protocol is configured, the Fax G3 protocol must therefore always be active also.

At many companies, fax devices cannot be reached from outside via individual extensions. In such cases a central access via an automated attendant exists instead, via which the fax devices can be dialed as well.

When an external subscriber sends a fax to a company with such a solution, he/she needs to dial the central number of the automated attendant. After a connection has been established to the automated attendant, further digits must be dialed that set up the connection to the desired fax device. In this process it is important that these further digits are dialed delayed.

The Fax G3 Post-Dialing protocol provides a mechanism for dialing portions of a phone number with controlled delay. To this, the protocol defines the \$ sign within a phone number as dialing pause, which is one second by default.

Example:

The fax devices of a company can only be reached from outside via an automated attendant. This automated attendant has the phone number 02404901100. After the connection to the automated attendant has been set up, any fax device in the company can be dialed by post-dialing a three-digit number with delay. The delay between dialing the automated attendant and post-dialing the three-digit number must be at least 2 seconds. If the desired fax device can be reached, for example, via the post-dialed number 100, the entire phone number to be dialed reads: 02404901100\$\$100. Between the phone number of the automated attendant and the post-dialed number of the fax device you find two \$ signs in this case. For: $2 \times 1s = 2s$.

If required, a phone number may contain several pauses – for example:

02404901100\$\$1\$5\$8. Dialing such a phone number can be useful when menu entries are to be made in the automated attendant with the post-dialed digits.

The entry of the pause sign is supported by the following XPR clients:

- Web Assistant
- Communications
- Lotus Notes Fax Templates
- Outlook Extensions

After a connection to the desired phone number has been established, the Fax G3 Post-Dialing protocol waits for a fax tone for a specific period. If no fax tone can be recognized within this period, the protocol plays a greeting that prompts the recipient to push the start button of the fax device or to divert the connection manually to a fax device.

If the protocol does still not receive a fax tone after playing the greeting, it repeats the greeting up to four times by default. If no fax tone can be recognized in this period, the protocol interrupts the connection and repeats the fax transmission according to the repeat strategy configured for the protocol.

Adjusting the MTA routing rules

In the MTA a new routing rule must be configured for the pause sign '\$' to be correctly processed and the corresponding messages to be routed to the Fax G3 Post-Dialing protocol.

Add the following routing rule to the MTA routing rules in the indicated place:

IMPORTANT:

Do not replace the \$ sign in the routing rule with another special character. Most of the other special characters have already been allocated for other purposes and the XPR clients expect the \$ sign as dialing pause entry. If you enter another character instead of the \$ sign, the Fax G3 Post-Dialing protocol will not work correctly.

```
"NVS:FAXG3<(\..+)?>/<.+>" [%2 ? "[:digit:]+$+"]=NVS:FG3PD%1/%2
```

NCO variable EnablePostDialing

Set the **EnablePostDialing** NCO variable to **true** to ensure a smoothly operating Fax G3 Post-Dialing protocol.

```

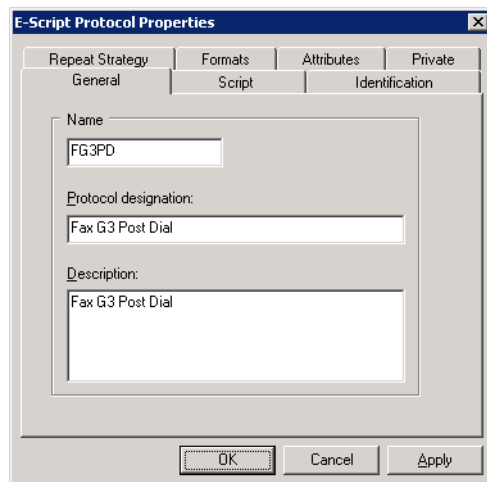
; Standard Routing Rules
NVS:STAND-IN/*=NVS:GUSTAV/*
NVS:VOICE.*/*[FLAG!=EXTERNCOPY & FLAG!=NOPREFERRED]=<NW>
NVS:*/*=<PREFERRED>
; Extended rules:
; an address representing a regular expression must be quoted
; subconditions may combined by '&' or '|', ';' is equivalent to '&'
; '?' denotes a regular expression match
; evaluation order of subexpressions can be grouped by '(' ')'
NVS:FAXG3<(\..+)?>/<.+>" [%2 ? "[:digit:]+$"] =NVS:FG3PD%1/%2
"NVS:FAXG[34](\..+)?/.*" [node(ORG)?="FAXG[34]" & FLAG!=VFSROUT]=NVS:GUSTAV/POSTMASTER
NVS:VOICE.*/*[node(ORG)=VOICE;FLAG!=VFSROUT;FLAG!=NOPREFERRED]=NVS:NIL/FAIL
; NVS:VOICE.*/*[node(ORG)=VOICE;FLAG!=VFSROUT;FLAG!=NOPREFERRED]=NVS:GUSTAV/POSTMASTER
NVS:EFT.*/*[node(ORG)=EFT]=NVS:GUSTAV/POSTMASTER
NVS:SMTP.*/*[node(ORG)=SMTP;FLAG=LOCALUSER;addr(ORG)!=MAIL-REPORT]=NVS:GUSTAV/POSTMASTER
NVS:LN.*/*[node(ORG)=LN]=NVS:GUSTAV/POSTMASTER
NVS:CC.*/*[node(ORG)=CC]=NVS:GUSTAV/POSTMASTER
NVS:*/*=<PRTVRIHES $REF rules>

```

If required, you find general information about editing the routing rules in [Chapter 7, "Message Transfer Agent \(MTA\)"](#).

Let's have a look at the configuration tabs of the associated protocol settings.

10.4.7.1 Configuration Tab *General*

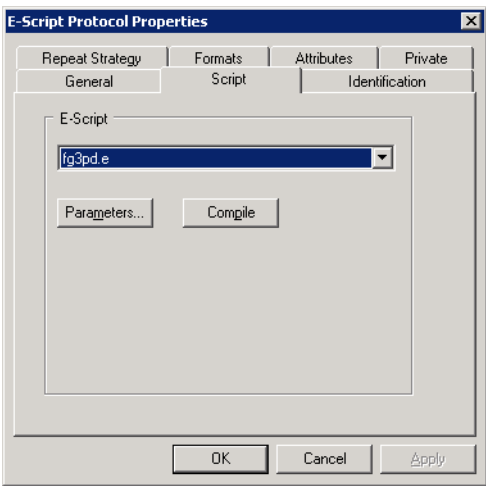


The elements displayed here comprise of the logical protocol name (**Name**), via which the protocol is addressed, a describing **Protocol designation:**, used for display in the XPR monitor, and a short **Description:** of the protocol, which appears in the configuration tab when the protocol is selected.

IMPORTANT:

So that the Fax G3 Post-Dialing protocol can operate trouble-free, it must be assigned the logical name *FG3PD*.

10.4.7.2 Configuration Tab *Script*



In the E-Script field select the *g3pd.e* entry to configure the Fax G3 Post-Dialing protocol.

Via the **Parameters** button you are taken to the **Script Parameters** dialog for the actual script configuration. Via **Compile** you can compile the actual script. This is only required when you have developed new scripts yourself which are thus present in the source. In most cases an already compiled object file is available which can be executed by the XPR server.

Parameters are entered in the **Script Parameters** dialog in the format *<Parameter>=<Value>*. Several parameter-value pairs are then separated from each other with a blank. The following parameters are available for the Fax G3 Post-Dialing protocol, with upper and lower case to be heeded.

Parameter	Description	Presetting
ftt	Specifies the time that the protocol waits for a fax tone after the connection setup and before the greeting for fax activation is played.	3 [Seconds]
mpr	Specifies how many times the greeting for fax activation is played before the protocol closes the connection to the subscriber. After each greeting repetition the protocol waits for a fax tone as long as is defined in the ftt parameter. If the protocol does not recognize a fax tone during this period, the greeting is either repeated or the connection closed.	5
psec	Specifies the length of the dialing pause, which is represented by the \$ sign in a phone number.	1 [Seconds]

Table 26 Parameters for the Fax G3 Post-Dialing Protocol

10.4.7.3 Configuration Tab *Identification*

The *Identification* tab for Fax G3 Post Dialing corresponds to the one of the Fax G3 protocol. Compare [Section 10.4.6.2, “Configuration Tab Identification”, on page 705](#).

10.4.7.4 Configuration Tab *Repeat Strategy*

The *Repeat Strategy* tab for Fax G3 Post Dialing corresponds to the one of the Fax G3 protocol. Compare [Section 10.4.6.4, “Configuration Tab Repeat Strategy”, on page 707](#).

10.4.7.5 Configuration Tab *Formats*

The *Formats* tab for Fax G3 Post Dialing corresponds to the one of the Fax G3 protocol. Compare [Section 10.4.6.6, “Configuration Tab Formats”, on page 709](#).

NOTE:

Only the **FaxG3** option may be activated for the Fax G3 Post-Dialing protocol.

10.4.7.6 Configuration Tab *Attributes*

The *Attributes* tab for Fax G3 Post Dialing corresponds to the one of the Fax G3 protocol. Compare [Section 10.4.6.7, “Configuration Tab Attributes”, on page 710](#).

10.4.7.7 Configuration Tab *Private*

The *Private* tab for Fax G3 Post Dialing corresponds to the one of the Fax G3 protocol. Compare [Section 10.4.6.5, “Configuration Tab Private”, on page 708](#).

10.4.8 Fax G3 Polling

NOTE:

The Fax G3 polling protocol sends fax messages up to a maximum length of 200 pages.

For the Fax G3 polling protocol the previously described configuration tabs *General*, *Repeat Strategy*, *Private* and furthermore *Formats* and *Attributes* of the Advanced Settings exist (cf. [Section 10.4.6, “Fax G3”, on page 702](#)).

10.4.9 Fax G4

NOTE:

The Fax G4 protocol sends fax messages up to a maximum length of 200 pages.

The Fax G4 protocol is the digital version of the Fax G3 protocol and is part of the ISDN services. It enables faster transmissions and higher resolutions of up to 200x200, 240x240, 300x300 and 400x400 dpi.

The **FAXG4#** field must be filled with the individually assigned extension in the XPR user database for each user. Use the international phone number format so that incoming fax messages can automatically be forwarded. This number is internally normalized and transcribed to the field **FAXG4** for use by the XPR server.

Example:

+49-1234-5678-90 would internally be converted into 491234567890.

You can select the same extension number range for the Fax G3 protocol as for Fax G4, as the XPR server can distinguish between these services with the help of the ISDN Service Indicator.

Fax polling is not possible with Fax G4.

In all XPR clients transmission is possible via entry of the destination number with simultaneous selection of the service Fax G4 in the send dialog. It is also possible to select the *E-Mail* service and enter the dial information FAXG4/
<destination number>.

Examples:

- 491234567890
- FAXG4/491234567890
- NVS:FAXG4/491234567890

The last example describes the complete address in the XPR format. This format is created, for example, by a mail gateway if it wants to send a Fax G4 document.

Let's have a look at the configuration tabs of the protocol settings.

For the Fax Group 4 protocol the previously described configuration tabs *General*, *Repeat Strategy* and furthermore *Formats and Attributes* of the Advanced Settings exist (cf. [Section 10.4.6, "Fax G3", on page 702](#)). The *Private* configuration tab does not provide any possibility for user settings at the moment.

Let's have a look only at the additional configuration tabs *Identification* and *Fax G4* in the protocol settings.

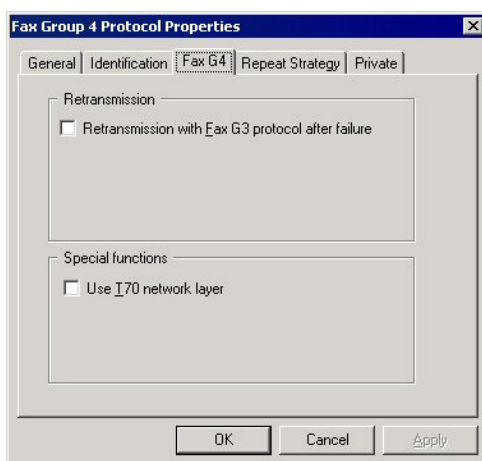
10.4.9.1 Configuration Tab *Identification*

In the *Identification* configuration tab the Fax G4 Identification is defined.

NOTE:

No header exists in the Fax G4 protocol. However, the identification may include characters according to standard F.200.

10.4.9.2 Configuration Tab *Fax G4*



The **Retransmission with Fax G3 protocol after failure** option can be set in the **Fax G4** configuration tab. Thus in case of an error it is assumed that the indicated phone number is that of an analog fax device and not a digital one. The fax can then perhaps be sent with the correspondingly lower resolution.

Via the **Use T70 network layer** option either the older T70NL or ISO8208 is defined as Layer -3. In case of doubt you should always use ISO8208.

10.4.9.3 Configuration Tab *Private*

The configuration tab *Private* includes individual configuration data regarding the respective protocol. The settings made here correspond to an INI configuration file known from the operating system Windows 3.1.

One protocol-specific entry is made per line in the format *Label*>=<*Value*>.

Example:

```
InsertMidHl=1
```

The possible entries are depicted in detail in the registry key ***Private*** ***[REG_MULTI_SZ]***.

10.4.10 Fax-on-Demand Server Script (Fax-on-Demand)

NOTE:

The fax-on-demand server script sends fax messages up to a maximum length of 200 pages.

The E-Script fax-on-demand server provides the user with the following three modes for fax-on-demand and the administration of fax-on-demand documents.

Normal Mode:

- Direct fax document polling with the telephone without DTMF entries.
- The extension number of the fax document is dialed via the keys of the telephone device and the fax document that is to be polled is diverted to a fax device or a fax number.
- Direct fax polling from a fax device in fax reverse polling mode.
- The extension of the fax document is dialed via the keys of the fax device. Subsequently, the start button of the fax device must be pressed to start fax polling.

DTMF Mode:

- Fax-on-demand with a telephone device by means of document selection via DTMF transmission.
Dial a DTMF access number on the telephone. When the connection has been established you are prompted per voice menu to enter the extension number(s) of one or several fax documents. Thereafter you are asked to push the start button at your telephone/fax combination or to divert the fax document to another fax calling number.

Supervisor Mode:

- Store, Rename and Delete fax-on-demand documents via DTMF transmission.
Via a specific access number and a Personal Identification Number (PIN) you will come to the administrator section. Here you can execute administrative functions via a voice menu.

The default settings of the fax-on-demand script offer users the possibility to use the **Normal Mode**.

Let's have a closer look at these three modes and how they work.

10.4.10.1 Direct Fax-on-Demand by Telephone (normal Mode)

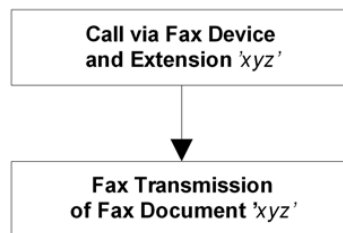
In this mode documents are selected according to the dialed extension number. The number of fax documents that can be stored is limited by the number of available extensions of the calling numbers. For each possible extension that has been assigned to a fax-on-demand script, one fax document can be stored.

The caller does not need a DTMF compatible telephone device. Just dial the extension of the desired fax-on-demand document with the telephone device. If the transmitted fax tone sounds, the telephone diverts manually to the calling number of a fax device or a fax phone number.

10.4.10.2 Direct Fax-on-Demand via the Fax Device (normal Mode)

Just like with direct fax polling via a telephone device, document selection with direct fax polling by a fax device in fax reverse polling mode occurs via the dialed extension number. Thus, the number of fax documents that can be stored is limited by the number of available extensions from the phone number pool.

For each possible extension that has been assigned to a fax-on-demand script, one fax document can be stored.



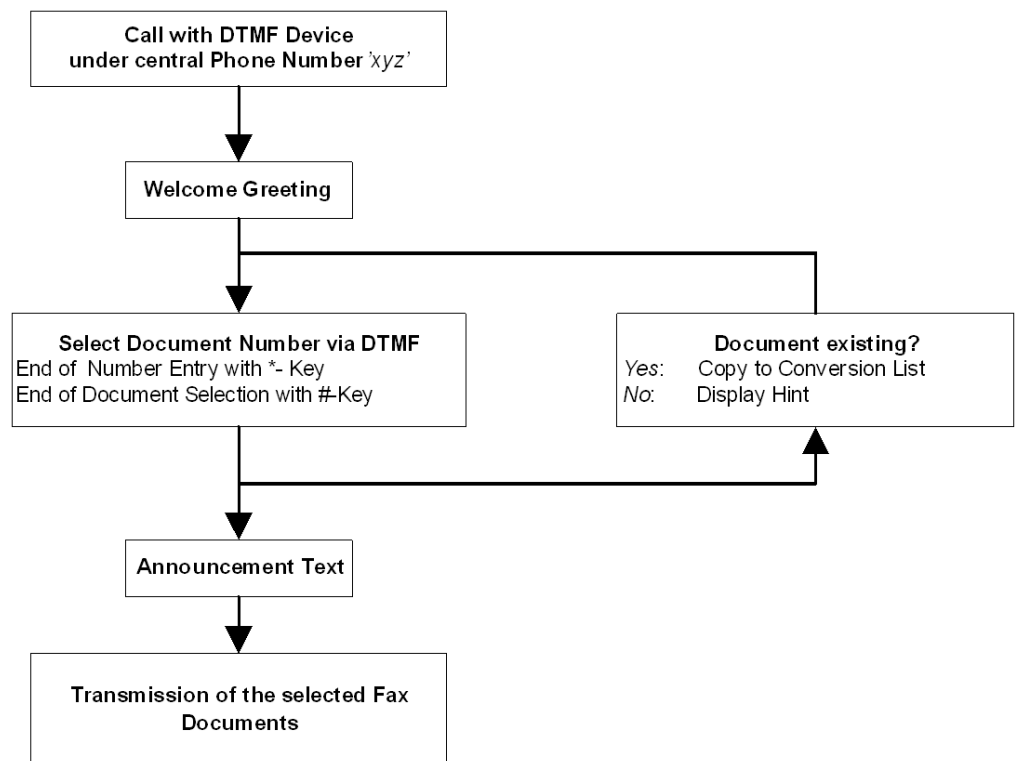
Just dial the extension of the desired fax-on-demand document with the fax device. If the connection has been established (fax tone), you need to press the start button of the fax device.

10.4.10.3 Fax-on-Demand by Telephone via DTMF (DTMF Mode)

Only one central phone number for the fax-on-demand server is required for the DTMF mode, that needs to be defined in the configuration dialog of the fax-on-demand script. Via this phone number a caller will come to a voice menu, where he/she can make his/her choice of documents via DTMF entries after a welcome greeting.

The advantage of this version is that an arbitrary number of documents can be stored and the document number may have an arbitrary length. Beyond that, the caller can poll any number of fax documents during a call since they can be selected one after another in an entry loop. As soon as all desired documents have been selected, fax transmission can be started via the # icon. Finally you only need to push the start button at the telephone/fax combination. If no fax device is available, the fax document can be diverted to a fax calling number.

Here as well the pollable documents are stored as `mrs<n>.fax` in the default setting of the script. The label `<n>` describes a document number naming each provided fax document uniquely.



After we have seen how available fax-on-demand documents can be polled by the XPR server, let us have a look at how the corresponding fax-on-demand documents can be stored on the server.

10.4.10.4 Storing Fax-on-Demand Documents

The pollable fax documents must be available in Fax G3 format⁴ in the directory `<XPR-Install>\userdata\fod`. The file names of the single documents need to be available in the format `mrs<n>.fax` (e.g. `mrs500.fax`) by default.

The fax-on-demand script enables additionally entering an alternative suffix instead of the expression “`fax`”. This requires the modification of the setting **Fax document names** in the *Documents* tab of the script configuration dialog.

There are two options to deposit Fax-on-Demand documents:

- Files are directly sent to the virtual file system of the XPR server. In case of this option fax documents are sent to the NVS address `NVS:<script name>/<document number>`. Here `<Script name>` describes the name that has been assigned to the fax-on-demand script in the corresponding configuration dialog. `<Document number>` is the unique number via which the respective fax can be polled. With this option, files are automatically converted into the desired Fax G3 format.

Example: `NVS:FOD/399`

- Reading in a fax-on-demand document using supervisor mode.

Let's have a closer look at the document administration via the Supervisor mode in the next section.

10.4.10.5 Supervisor Mode for Administration

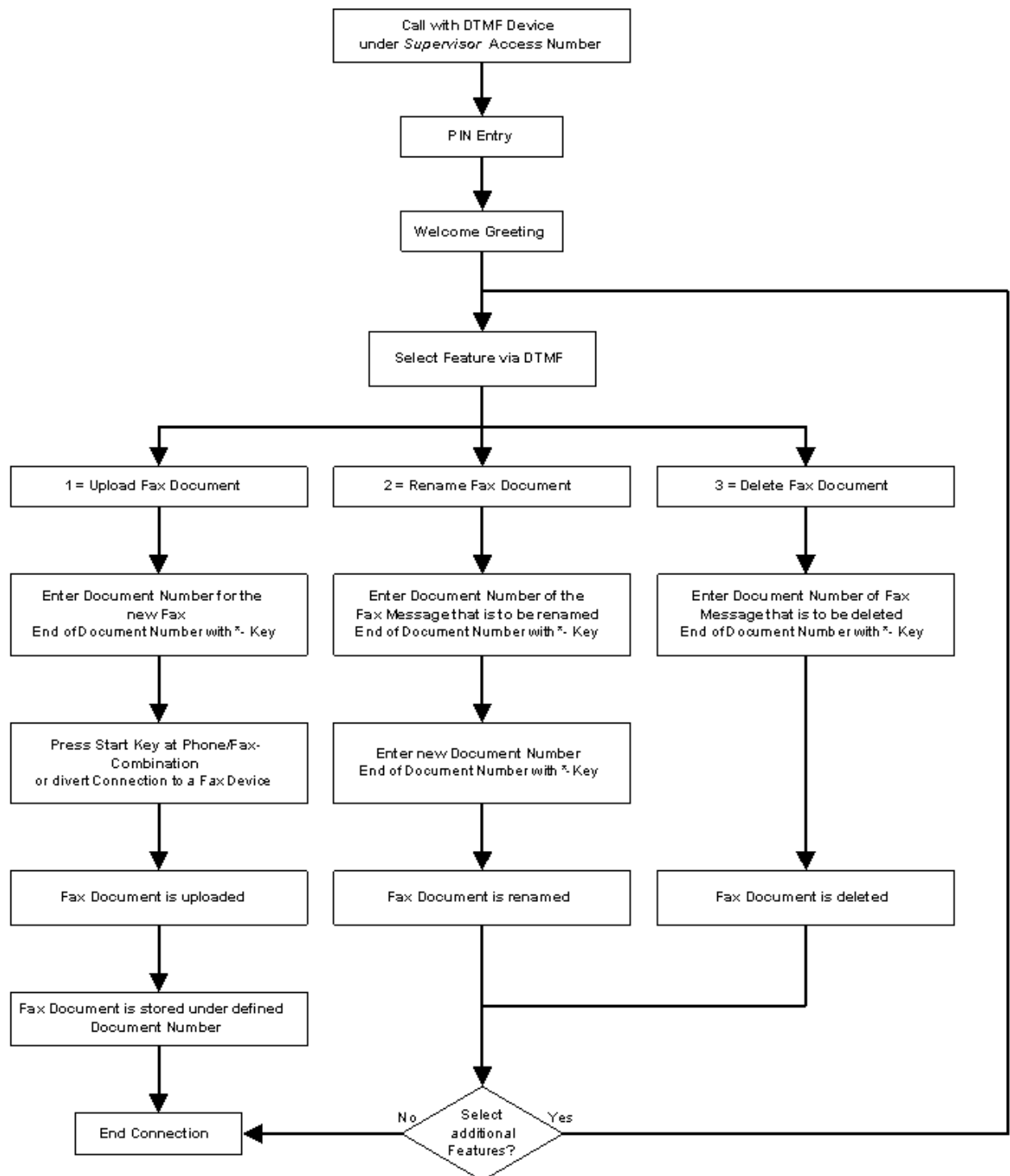
Supervisor mode is accessed via a phone number specified in the fax-on-demand script configuration. This calling number is taken from the numbering plan of the fax-on-demand script so that under this number no fax document can be polled.

To access the supervisor mode the caller needs to identify himself/herself by entering a PIN after dialing the access number.⁵ After the successful login you reach the supervisor menu in which you can edit fax-on-demand documents in the following way:

- Storing with key 1
- Renaming with key 2
- Deleting with key 3.

The following diagram shows the structure of a voice menu.

4. The Fax G3 format is generated, for example, by the fax printer driver of the XPR server or of the XPR clients.
 5. The maximum number of login attempts during a call can be determined in the configuration dialog of the fax-on-demand script.



Depositing a fax-on-demand document (Key 1):

Via key 1, fax-on-demand documents can be stored on the XPR server. The voice menu prompts you to enter the document number under which the fax-on-demand document is to be stored. Terminate the input of the phone number with

the * key. Subsequently, you need to push the start button at the telephone/fax combination via which the new document is sent to the XPR server.

The document is provided in the folder `<XPR-Install>\userdata\fod` in the syntax `mrs<document number>.fax` for fax polling.

Renaming a fax-on-demand document (key 2):

With key 2 you can rename a fax-on-demand document. The voice menu prompts you to enter the document number of the fax-on-demand document that is to be renamed. This entry has been finished with the * key. Then the user must enter the new document number and conclude this input with the * key. The fax-on-demand document is now stored in the folder `<XPR-Install>\userdata\fod` under the new document number.

Afterwards you will come to the feature selection again.

Deleting fax-on-demand document (key 3):

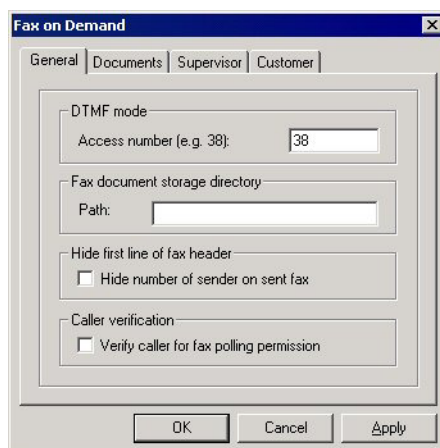
With key 3 you can delete a fax-on-demand document. The voice menu prompts you to enter the document number of the fax-on-demand document that is to be deleted. This entry has been finished with the * key. The selected fax-on-demand document is now deleted from the folder `<XPR-Install>\userdata\fod`.

Afterwards you will come to the feature selection again.

Let's have a look at the configuration tabs of the protocol settings.

For the Fax Group 4 protocol the above configuration tabs *Formats* and *Attributes* of the Advanced Settings exist (cf. [Section 10.4.6, "Fax G3", on page 702](#)). Therefore, we will only have a look at the differing configuration tabs *General*, *Documents*, *Supervisor* and *Customer*.

10.4.10.6 Configuration Tab *General*



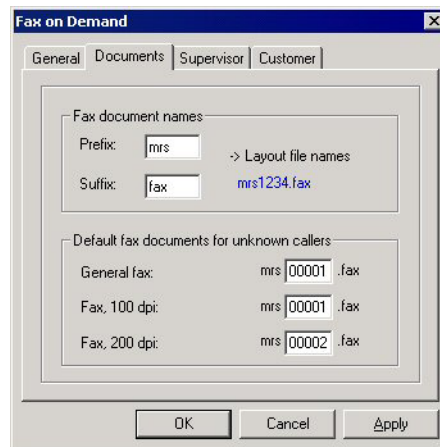
In the *DTMF mode* section the **access number** is entered via which a user can retrieve fax documents in the voice-menu navigated DTMF mode.

If the fax documents are not stored in the default folder `<XPR-Install>\userdata\fod`, you can specify the **path** to another storage directory in the *Fax document storage directory* section.

The **Hide number of sender on sent fax** option in the section *Hide first line of fax header* enables suppressing the originator information of the header in the retrieved fax message.

If only users entered in the XPR user database and for whom the fax-on-demand privilege **FAXG3REV** is set are to use the fax-on-demand service, this can be realized via the **Verify caller for fax polling permission** option. Users who are not entered in the XPR database will receive a default fax message in this case (cf. [Section 10.4.10.7, “Configuration Tab Documents”, on page 726](#)).

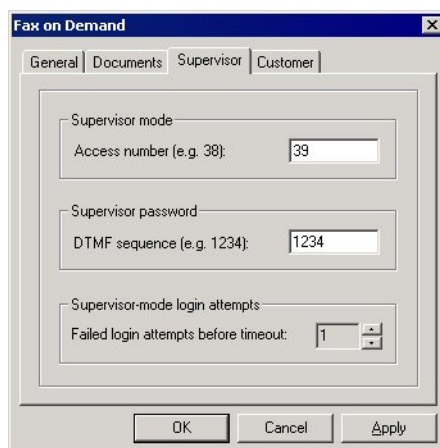
10.4.10.7 Configuration Tab *Documents*



In the *Fax document names* section the **Prefix** and **Suffix** of the saved fax-on-demand documents can be modified. Under *Layout file names* you can then see the modifications performed.

In the *Default fax documents for unknown callers* section you can define which fax documents the XPR server sends to users who are unknown to the system. These fax documents are only sent if the option **Verify caller for fax polling permission** is activated on the *General* configuration tab (cf. [Section 10.4.10.6, "Configuration Tab General", on page 725](#)).

10.4.10.8 Configuration Tab *Supervisor*



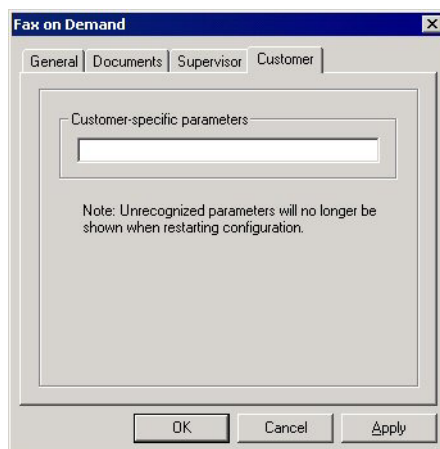
The image shows the 'Fax on Demand' configuration window with the 'Supervisor' tab selected. The window has four tabs: 'General', 'Documents', 'Supervisor', and 'Customer'. The 'Supervisor' tab contains three sections: 'Supervisor mode' with an 'Access number (e.g. 38):' field containing '39'; 'Supervisor password' with a 'DTMF sequence (e.g. 1234):' field containing '1234'; and 'Supervisor-mode login attempts' with a 'Failed login attempts before timeout:' field containing '1'. At the bottom are 'OK', 'Cancel', and 'Apply' buttons.

In the section *Supervisor mode* the **access number** is entered that leads to the voice menu operated Supervisor mode. In this mode you can store, rename and delete fax-on-demand documents.

The password (PIN) to enter the supervisor mode is specified in the **DTMF sequence** field.

The **Failed login attempts before timeout** field serves to define how many wrong login attempts are tolerated before the system cancels the login procedure.

10.4.10.9 Configuration Tab *Customer*



The image shows the 'Fax on Demand' configuration window with the 'Customer' tab selected. The window has four tabs: 'General', 'Documents', 'Supervisor', and 'Customer'. The 'Customer' tab contains a 'Customer-specific parameters' section with a large text input field. Below the field is a note: 'Note: Unrecognized parameters will no longer be shown when restarting configuration.' At the bottom are 'OK', 'Cancel', and 'Apply' buttons.

The **Customer-specific parameters** field enables the entry of future parameters in a command line that will be added customer-specific to the fax-on-demand server script and cannot be configured via the graphic configuration elements.

10.4.11 Fax-Fax Converter (Fax Forward)

NOTE:

The fax-fax conversion protocols send fax messages up to a maximum length of 200 pages.

To use the XPR server as fax concentrator, the fax-fax conversion protocol is applied. A possible scenario is the time-dependent transmission of all outgoing fax messages, e.g. for using the cheapest connection rates.

This has several technical and organizational consequences:

- How does the originator of a fax message receive information on successful time-dependent delivery of his/her message?
- Which fax ID should the external recipient receive? That of the XPR server or of the internal fax device?

Various possibilities provide a solution to these problems. The XPR server supports two different Fax Forward modes:

1. **Fax-fax Converter (transparent) mode**

In this mode the XPR server is invisible for the external recipient. Sending a fax message takes place as follows:

- The internal fax device sends a fax message to the XPR server. The server receives the final external recipient number together with the message.
- The XPR server receives the fax message, the destination number and the identification of the originator's fax device.
- Through the fax ID of the XPR server the internal device receives the XPR message ID as reference number.
- The cached fax message will be sent to the external recipient at the desired point of time (specified in the routing rules). In the process the received fax device is provided with the original fax ID of the internal sending fax device. Beyond that, no additional header line is inserted. The fax document remains unchanged and does not include a second header.
- After successful delivery the XPR server sends a return receipt to the internal fax device (you can deactivate this feature if you like). The return receipt contains several information such as the send date, send time, ID of the counterpart, the costs incurred etc.
- If no delivery is possible, the XPR server sends a return receipt with the reason of the error to the internal fax device. This feature can also be deactivated if desired.

2. Fax-fax converter (server) mode

In this mode the external recipient sees only the XPR server and not the originally sending internal fax device. The procedure is the same as the FFORWT mode with the exception of:

- The fax document header that has been inserted by the originating device is removed by the XPR server. Instead, the XPR server inserts the ID and header of the XPR server into the document during the transmission.

For the fax-fax converter feature a routing rule must be created that forwards the documents sent to the fax concentrator. Let us take a closer look at the structure of such a routing rule.

Example: `NVS:FFORWS.*/+4912345678947*[FLAG!=FLAG1=NVS:FAXG3/*[FLAG=FLAG1;DEFER=2:00]`

This rule would send all incoming fax messages with the phone number prefix **47** having **FLAG1** not set at **2:00 o'clock** and remove the prefix **47**. Simultaneously **FLAG1** is set, so that normal extensions that begin with the dialed prefix would not be continually processed.

Since the ISDN APL uses internationally normalized dialing numbers by default, the individual extension must precede the fax-fax converter prefix in international format in the above routing rule. The required extension is the OAD assigned to this protocol in the ISDN configuration.

In the example above the connection number is e.g. *49-2404-12345*.

Without the international dialing mode the routing rule would have the following appearance:

`NVS:FFORWS.*/+47*[FLAG!=FLAG1]= NVS:FAXG3/*[FLAG=FLAG1;DEFER=2:00]`

Essentially, through use of the prefix as selection criteria, an almost unlimited range of conversions is possible. In the above example the fax is internally sent to the example number *4701234567890*, which is then sent by the XPR server at **two o'clock** in the morning to the number *01234567890*. If the **DEFER=2:00** portion was omitted in the above routing rule, fax messages would directly be rerouted.

Let's have a look at the configuration tabs of the protocol settings.

For these protocols the above configuration tabs *General*, *Repeat Strategy*, and furthermore *Formats* and *Attributes* of the Advanced Settings exist (cf. [Section 10.4.6, "Fax G3", on page 702](#)). Therefore we will only have a look at the differing configuration tab *Private*.

10.4.11.1 Configuration Tab *Private*

The configuration tab *Private* includes individual configuration data regarding the respective protocol. The settings made here correspond to an INI configuration file known from the operating system Windows 3.1.

One protocol-specific entry is made per line in the format *Label*>=<*Value*>.

Example:

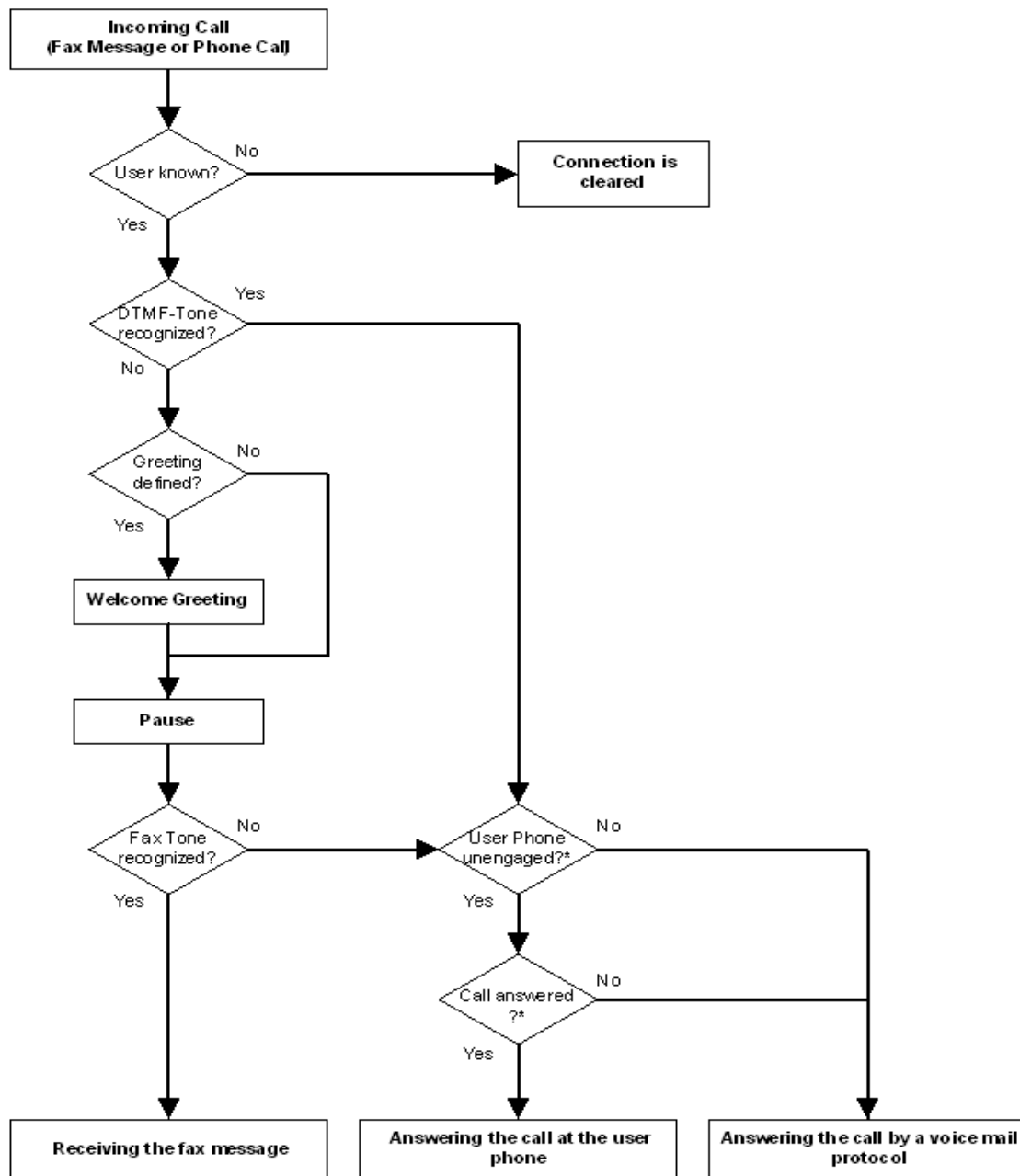
```
InsertMidHl=1
```

The possible entries are depicted in detail in the registry key *Private [REG_MULTI_SZ]*.

10.4.12 Single Number

The Single Number protocol enables access to the services telephone, voice mailbox and fax under one user extension. In this function it operates as call switch in the XPR server.

The following figure is a Single Number protocol function overview.



* If the *BlindTransfer* option has been activated, the telephone terminal device state is not checked. The call is then routed to the telephone terminal device at any rate.

If the Single Number protocol receives a call, it tries to find the addressed user. Therefore it compares the destination number with the contents of the Correlation Database field that is configured in the protocol parameter *Fax*. The default setting is the database field *FAXG3*.

If the addressed user could be found, Single Number might issue a welcome greeting that is to be defined. In the meantime, the incoming communication is searched for a possible fax tone. If this signal is contained in the transmission, the fax mailbox of the relevant user accepts the fax message.

If no fax tone was received until the end of the greeting and during an ensuing pause, the incoming call is handed over to the telephone of the relevant XPR users. During the pause a signal tone is played so that the caller still recognizes the existing connection. If the transfer to the telephone of the relevant XPR user fails, an alternative voicemail protocol is started. Which voicemail protocol starts results from the following prioritization:

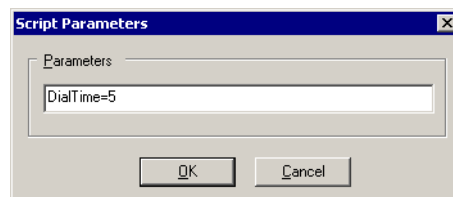
1. The voicemail protocol configured for the relevant XPR user.
2. The alternatively defined voicemail protocol for single number (see `SCRIPT` parameter below).
3. A voice mail protocol configured of a license.

The greeting does not start if a DTMF tone is determined with the call acceptance. The call is directly forwarded to the XPR user's telephone instead.

NOTE:

If the relevant services of all users are only to be reached via the Single Number protocol, an extension range is assigned to this protocol only. The fax and the alternate voice mail protocol do not require an extension range since accessing them is realized via the Single Number protocol.

The Single Number protocol is always active in the context of a telematics APL and must be established there as user-defined E-Script. The protocol is configured in the XPR monitor in the settings dialog of the Telematic APL used. You reach the associated parameter settings via the **Parameters** button in the *Scripts* configuration dialog.



Parameters are entered in the **Script Parameters** dialog in the format `<Parameter>=<Value>`. Several parameter-value pairs are then separated from each other with a blank. The following parameters are available for the Single Number protocol, with upper and lower case to be heeded.

Parameter	Description	Presetting
Play	Defines the file name of the welcome greeting played with an incoming call. The greeting does not start if a DTMF tone is determined with the call acceptance. The call is directly forwarded to the addressed XPR- user's telephone instead. The specified file must be stored in the <code><XPR-Install>\userdata\voice\SingleNumber</code> folder. All common file formats are supported.	"" (no welcome greeting is played)
Silence	Defines the length of the pause after the welcome greeting playback, before the call is forwarded to the addressed XPR user's telephone. If no welcome greeting has been defined, an incoming call is accepted with a pause of the length defined here. Default:	3 [Seconds]
Script	If the call transmission to the telephone device of the addressed XPR user fails, it is forwarded to the voice mail protocol by default that is individually defined for the addressed user. If such a binding does not exist, the parameter <code>Script</code> defines the name of the alternative voice mail protocol.	–
PHONE	Defines the database field in the correlation database from which Single Number takes the call number for the addressed XPR user's telephone. If this field is empty, a call to be forwarded is directly handed over to the alternative script. Default: PHONE	PHONE
Fax	Defines the database field in the correlation database from which Single Number takes the call number for the addressed XPR user's fax mailbox. Attention: For this parameter an entry is required, since Single Number also searches the called user on the basis of this information.	FAXG3
PbxSwitch	Defines the XPR switching mode. Possible values are: 0 – Calls are rerouted in the XPR server by a second parallel B-channel between XPR server and PBX. 1 – Calls are rerouted in the PBX (Path replacement (QSIG) or ECT (DSS1))	1
DialTime	Defines the time-out for the transfer to the relevant XPR user's telephone. If a call is not accepted after this period, it is handed over to the alternative voice mail protocol. Cf. parameter <code>Script</code> .	60 [Seconds]

Table 27 Parameters for the Single Number Protocol

Option	Description
BlindTransfer	Each transfer by the Single Number script is usually performed in the form of a supervised transfer. If this option is set, the transfer occurs as blind transfer. Attention: The blind transfer is not supported by every PBX.

Table 28 Options for the Single Number Protocol

10.4.13 SMI

The SMI protocol is used for internal communication between XPR servers. In this process, several servers are connected via the SMI transport protocol, thus a so-called Remote System Link. A Remote System Link must be configured in the MTA configuration dialog and the NVS address of the remote server must be entered.

Example: NVS:ISDNSMI/491234567890

Now determine the frequency (in seconds) that defines how often the respective connection is to be established and an automatic interconnection with all logical lines of the other system is performed.

Furthermore, an extension for the SMI transport protocol should be entered that can be used for all Remote System Links. In the remote system an entry should also be made to ensure the correct delivery of reports.

For the SMI protocol the above configuration tabs *General*, *Repeat Strategy*, and furthermore *Formats* and *Attributes* of the Advanced Settings exist (cf. [Section 10.4.6, "Fax G3", on page 702](#)). The additional *Private* configuration tab does not provide any possibility for user settings at the moment.

10.4.14 Voice

NOTE:

The Voice protocol has meanwhile been replaced with the PlayWave protocol. Thus, the Voice protocol should not be used anymore.

The Voice protocol is used for the playback of messages via telephone. In most cases this protocol is invoked directly by the XPR client.

CIT via the Voice protocol

A Message Waiting Indicator (mailbox LED) can be set via the Voice protocol for the Integral PBX from Bosch Telecom. For this purpose two numbers must be configured in the PBX for setting and resetting MWI signals. If this has been done, `VOICE/<ON-SEQ>` can be entered in the **CIT** field of the XPR user database to switch on MWI. `<ON-SEQ>` is the switching sequence followed by the number of the telephone device at which the MWI is to be set.

In order to reset the signal an additional field **XCIT** must be inserted into the XPR database. The entry `VOICE/<OFF-SEQ>` is the internal number used for the resetting sequence and is followed by the extension number.

Example:

Database field	Content
CIT	VOICE/9500543 The sequence 9500 has been coded as switching sequence at the <i>Integral</i> PBX. The Message Waiting Signal (MWI) is set with the extension 543 at the PBX, as soon as a new message has come in for a subscriber.
XCIT	VOICE/9501543 The sequence 9501 has been coded as resetting sequence at the Integral PBX and the Message Waiting Signal (MWI) is reset at the telephone device with the extension 543, as soon as the message has been retrieved.

The CIT must be enabled during the installation of the MTA so that it is active.

The Voice protocol provides among other things the above configuration tabs *General*, *Repeat Strategy*, *Formats* and *Attributes* of the Advanced Settings (cf. [Section 10.4.6, "Fax G3"](#), on page 702).

Via the additional configuration tab *Private*, script-specific settings can be made. Possible settings are described in detail in the registry key **Private [REG_MULTI_SZ]**.

10.4.15 PlayWave

With the PlayWave protocol you can create and play sound files for voice messages on a telephone. It is invoked by the XPR clients for this purpose. PlayWave is a further development and replacement of the Voice protocol.

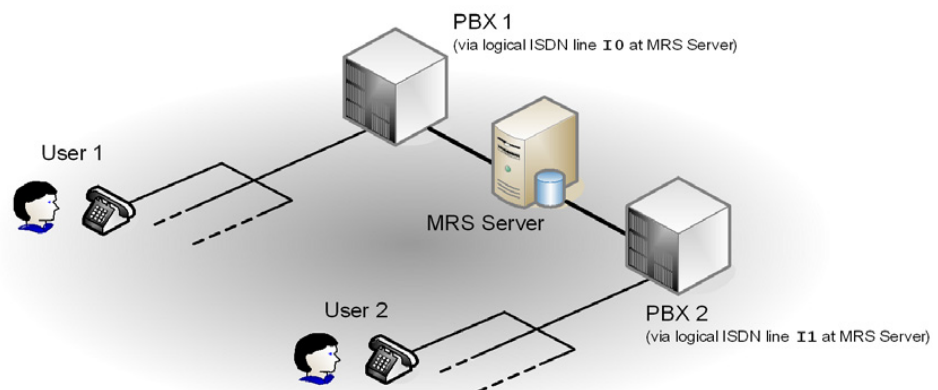
PlayWave is always active in the telematics APL context and is automatically added and configured during the installation of an ISDN or IP APL. The protocol is configured in the XPR monitor via the settings dialog of the telematics APL used.

The PlayWave protocol provides among other things the above configuration tabs *General*, *Formats* and *Attributes* of the Advanced Settings (cf. [Section 10.4.6, "Fax G3", on page 702](#)). You reach the associated parameter settings via the **Parameters** button on the *Script* configuration tab. Permitted PlayWave parameter settings are described in detail in the [Private \[REG_MULTI_SZ\]](#) registry value.

PlayWave transaction routing in case of multi-PBX-connections

If several PBXs are operated at one XPR server, addressing problems may occur when a user wants to play a voice message. The reason: PlayWave cannot automatically rout transactions to precisely the PBX at which the telephone of the user is found who wants to play the voice message.

To solve this addressing problem, you need to manually adjust the XPR server configuration. Let us take a closer look at such adjustments exemplified by two PBXs. Both PBXs are connected to the XPR server via the ISDN APL.



Adjust the XPR server configuration for this example as follows:

1. Create a new database field in the XPR server user database. We choose the field name **PBX** for our example. Compare [Section 34.2, "Adding a New User Data Field"](#) in this context.
2. In the **PBX** database field enter for each user which PBX his/her telephone is connected to.

For our example we use the following convention:

- Telephone at PBX 1: Enter *PBX1* in the **PBX** database field.
- Telephone at PBX 2: Enter *PBX2* in the **PBX** database field.

3. Add the following two rules to the MTA's routing rules:

```
NVS:TELELIB.*/*[ORGDB(PBX)=PBX1;FLAG!=FLAG1]=
NVS:TELELIB.I0/*[FLAG=FLAG1;FLAG=NOPREFERRED]
```

```
NVS:TELELIB.*/*[ORGDB(PBX)=PBX2;FLAG!=FLAG1]=
NVS:TELELIB.I1/*[FLAG=FLAG1;FLAG=NOPREFERRED]
```

These rules see to

- PlayWave transactions being sent to the ISDN card with the logical address *I0* for users with the database entry *PBX1*
- PlayWave transactions being sent to the ISDN card with the logical address *I1* for users with the database entry *PBX2*

NOTE:

If the IP APL is used instead of the ISDN APL to connect one or both PBXs, the relevant logical line in the routing rule is not called `TELELIB.I<line number>` but: `TELELIB.IP<line number>`.

10.4.16 Hicom Message Waiting Indication (MWI)

The Hicom MWI protocol transmits information via a D-channel required to address MWI LEDs and telephone displays of the Hicom system telephones. A Cornet-N layer is required for this functionality that can only be purchased via the producer Unify GmbH & Co. KG.

Depending on the PBX a callback number is required, which is dialed when the user presses the activated LED.

Let's have a look at the configuration tabs of the protocol settings.

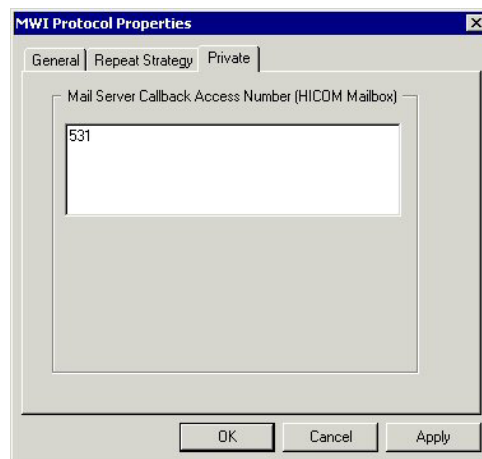
For this protocol the above configuration tabs *General*, *Formats* and *Attributes* of the advanced settings exist (cf. [Section 10.4.6, "Fax G3", on page 702](#)). Therefore we will only have a look at the differing configuration tab *Private*.

NOTE:

The settings on the *Repetitions* tab are not used for the Hicom Message Waiting Indication protocol.

10.4.16.1 Configuration Tab *Private*

On the configuration tab *Private* the callback number to the Hicom mailbox is indicated. This is normally the tie line number followed by a 1, so that the Hicom PBX connects through.



10.4.17 Message Waiting Indication (MWI)

The Message Waiting protocol is used by the ISDN and IP APL and enables MWI signaling via QSIG, Cornet N and Cornet NQ. It transmits the information required for setting the inbox LED and the telephone display via the D-channel. Depending on the PBX a callback number is required, which is dialed when the user presses the activated LED. In most cases this number corresponds to the callback access number configured with the TUI used, so that you are directly connected to the TUI by the telephone LED for playing back a new message.

The Message Waiting Indication protocol is now an integral component of the ISDN and IP APL. It is thus automatically active after the installation of those APLs. It is listed under the established protocols and can be configured there as usual.

NOTE:

The Message Waiting Indication protocol is now an integral component of the ISDN APL and thus automatically available after the installation of the ISDN APL. If you want to add it to one of these APLs once again, you need to use a user-defined E-script. Select the `mwivoice.e` E-script in this case.

You must not assign the name `MWI` to the newly added script. Use, for example, the name `MWIVOICE` instead.

While the MWI protocol integrated in the APL only supports the MWI information transmission in the D-channel, the `mwivoice.e` script can also transfer MWI information via a phone number to be dialed. The latter is, for example, required for the MWI connection of a Bosch Tenovis PBX.

In general, the MWI notifications of the different communication protocols are not able to transmit the precise number of waiting messages. An MWI notification can accordingly only signify that a new message is waiting or that no waiting message exists any more. Therefore, the XPR server only sends a corresponding MWI notification if

- the number of waiting messages increases
- the last waiting message was played by the user.

Some communication protocols can also transmit the precise number of waiting messages in their MWI notifications – for example the SIP protocol. Hence the XPR server IP APL can also send an MWI notification whenever the number of waiting messages arbitrarily changes – for example, if a user plays only two of five waiting messages. The user can thus always see the respectively current number of waiting messages on the telephone display.

NOTE:

So that the XPR server IP APL sends an MWI notification each time the number of waiting messages changes, the Notification APL must be configured accord-

ingly.

You find details on this in [Section 16.4.2, “Internal Settings”, on page 1038](#).

Let's have a look at the configuration tabs of the protocol settings.

For this protocol the above configuration tabs *General*, *Formats* and *Attributes* of the advanced settings exist among other things (cf. [Section 10.4.6, “Fax G3”, on page 702](#)). Therefore we will only have a look at the differing configuration tab *Private*.

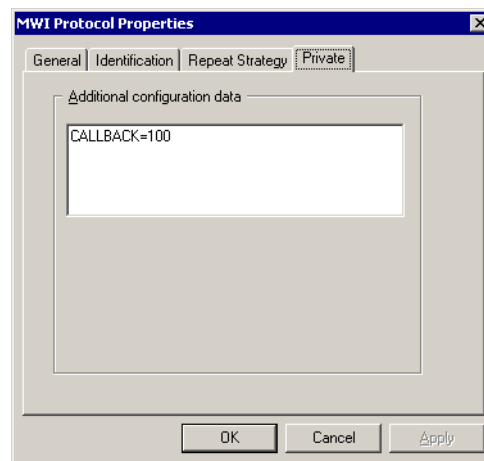
NOTE:

The settings on the *Repetitions* tab are not used for the MWI protocol.

NOTE: In case of a HiPath 4000 the MWIInterrogate feature must be disabled.

10.4.17.1 Configuration Tab *Private*

You can perform settings for the MWI Message Waiting Protocol via individual parameters on the *Private* configuration tab.



The following parameters are available:

Parameter	Description
CALLBACK	Defines the phone number that is dialed by pushing the mailbox key on the telephone device. As a rule, this phone number corresponds to the callback access number of the TUI used. Thus a user is directly connected with the TUI by pushing the mailbox key and can listen to their newly arrived message. Attention: Further settings need to be performed for most of the PBXs to make callback via the mailbox key work. The number e.g. set in the script as callback access and used as callback number in the MWI protocol must also be administered in the Hicom 300. This is done in the <code>AMO RICHT</code> with the parameter <code>PM</code>. Depending on the Hicom PBX a maximum of 20 servers can be administered here that may set LEDs to telephone devices via the MWI protocol.
-DSE	This button activates a hard defined timer. The APL will be idle for 1000 msec after the transmission of an MWI message. During this time no new actions can be performed via the APL. Attention: Activating this button may lead to performance restrictions of the respective APL.
ON	Defines the phone number that is used to set the MWI of a telephone device. Attention: This setting is only analyzed if the <code>-VOICE</code> button is also activated. The indicated phone number must have the format <code><Phone number>p</code>.
OFF	Defines the phone number that is used to deactivate the MWI of a telephone device. Attention: This setting is only analyzed if the <code>-VOICE</code> button is also activated. The indicated phone number must have the format <code><Phone number>p</code>.
-VOICE	This button activates the MWI information transmission via a call at the defined phone number of the respective PBX. See also the parameters <code>ON</code> and <code>OFF</code>.

Table 29

Parameters for the Message Waiting Indication Protocol

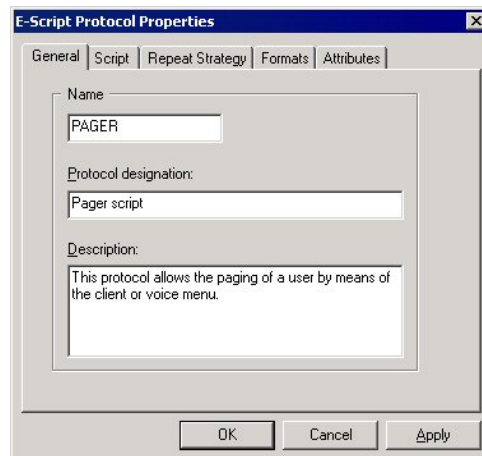
10.4.18 Pager

Pagers are devices able to receive messages. These messages include a simple signal tone in the simplest case, or a short text message (e.g. a callback number). Furthermore, it is possible to receive voice mails. The types of messages that can be received depend on the respective pager equipment (speakers, display, etc.).

Pager services are provided by service providers. The service access is always realized via a so-called paging terminal. This can be addressed from other communication networks. The way the pager recipient is addressed in this context may vary for different paging terminals. This requires an individual configuration of the terminal communication.

To transmit messages to a pager recipient, the pager protocol is available in an XPR environment. This protocol must be selected during the server installation or during a server update to allow the configuration of the protocol on the XPR server.

Let's have a look at how the pager protocol is added after its installation and configured.



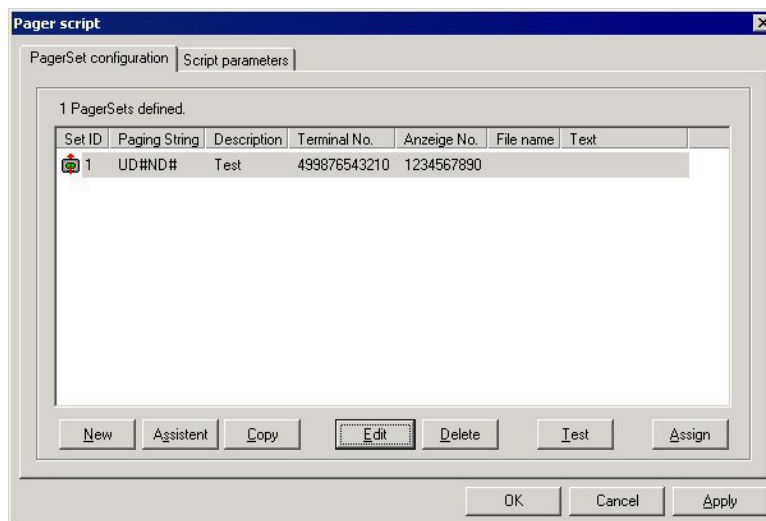
At first, the pager protocol is added to the XPR configuration as E-script. For this, select **PAGER** as the **Name**.

IMPORTANT:

The Notification APL addresses the pager protocol via this logical name. If a name different from **PAGER** is assigned to the pager protocol, the protocol will not function correctly.

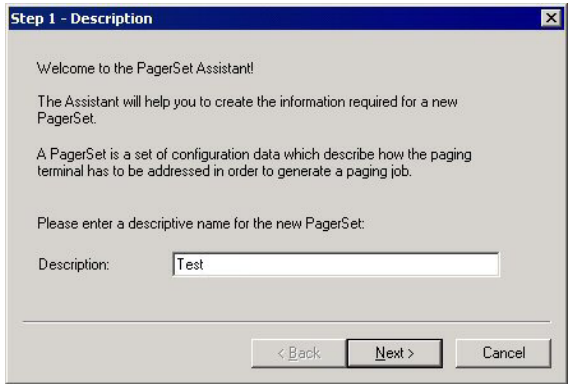
You can also bind the protocol to an extension number so that you can trigger a call to a configured pager via a Telephone User Interface (TUI).

As with other protocols, the configuration dialogs can be reached via the **Parameters** button on the *Script* configuration tab.



Since there are many types of paging terminals and the access mechanism is not standardized, you need to first configure the DTMF sequence for the desired service provider and its paging terminals. This pager configuration is called pager set. The XPR server provides a wizard for the configuration of such a pager set.

Wizard



The configuration steps of the wizard lead to a paging string that determines the type of access and the type of data transmitted to the paging terminal.

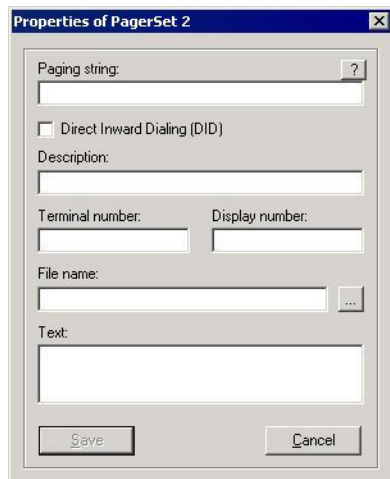
First a **Description** or a name is required for the pager set.

The paging string determined by the wizard comprises the following elements:

Element	Meaning
M	Terminal number
U	Pager number of the user
N	Display number
A	Phone number of a caller
P	Sound file
D	Delay/short pause
0-9#*	DTMF tone

Table 30 Elements for the Pager Sequence of the Pager Protocol

Without the wizard you can create a new pager set via the **New** button or use an existing pager set as template for a new one via the **Copy** button. **Edit** serves for modifying an already created pager set. Pressing any of these buttons takes you to the following dialog.



The dialog box is titled "Properties of PagerSet 2". It contains the following fields and controls:

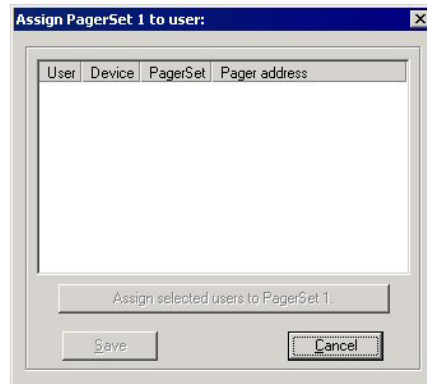
- Paging string:** A text input field with a help icon (?) to its right.
- Direct Inward Dialing (DID):** A checkbox.
- Description:** A text input field.
- Terminal number:** A text input field.
- Display number:** A text input field.
- File name:** A text input field with a browse button (...) to its right.
- Text:** A large text area.
- Buttons:** "Save" and "Cancel" buttons at the bottom.

Here you can directly enter the **Paging string** using the elements described in the table. The **File name** refers to a voice file to be transmitted to the pager recipient. You can optionally enter a text as well. This text is then, via the Text-to-Speech feature of the XPR server, converted into a voice message.

The entry in the **Display number** field describes the callback number to be displayed on the addressed pager recipient's display after the message transmission.

Via the **Direct Inward Dialing** option the phone number of the pager recipient is directly attached to the end of the paging terminal access number. In this special case it is not part of the paging string.

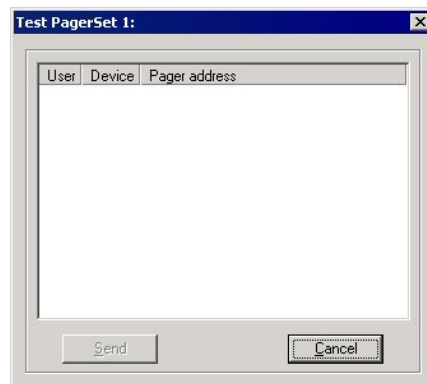
Assigning pager sets to users



After the pager sets have been installed, the single pager users are assigned via the **Assign** button. Therefore the dialog lists all users with a pager address. Via the **Assign selected users to...** button the selected entries can be assigned to the respective pager set.

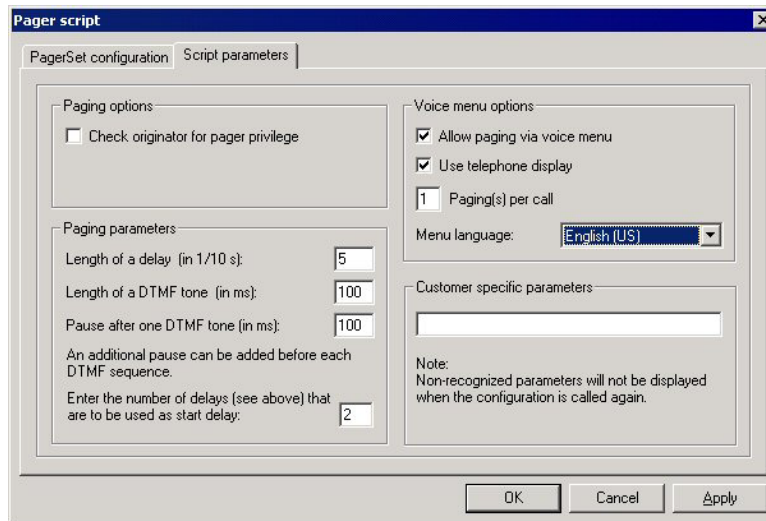
This procedure will be finished by **Save**.

Testing pager sets



Click the **Test** button to display a list of the users assigned to this PagerSet. Now you can select these and perform a notification test via the **Send** button.

Script parameters



- Paging options**
 By means of **Check originator for pager privilege** the originator of a pager notification is checked for having the *Paging Privilege*. If this privilege has not been assigned, the respective user is not allowed to send pager messages.

IMPORTANT:

Sending a signal tone to a page recipient is not restricted by this privilege.

- Voice menu options**
 When you activate the **Allow paging via voice menu** option and an extension number has been assigned to the pager protocol, this number can be dialed and a notification sent via TUI. The **Use telephone display** option simplifies TUI usage for internal users. This requires telephones supporting this option.
Paging(s) per call limits the number of paging messages that may take place with a call.
 The last option in this section enables setting the TUI **Menu language**.
- Paging parameters**
 These are special parameters for setting the length of the delays used in the PagerSet and of DTMF tones. Normally, a modification of these default settings is not necessary.

10.4.19 SMS (TAP or UCP Protocol)

The XPR server offers various options to send SMS messages (cf. [Chapter 14](#), “[Short Message Service \(SMS\)](#)”). The most simple of these options is the SMS protocol, which is supported by the ISDN APL but not by the IP APL.

In this solution SMS messages to be sent are transmitted to Short Message Service Centers (SMSC). These centers handle the further routing of the messages depending on the mobile phone network concerned.

For SMS message transmission to the SMCSs, the SMS protocol supports the TAP (Telecator Alphanumeric Protocol) and the UCP (Universal Computer Protocol) as transport protocols.

The digest algorithm

The XPR server offers among other things the option to forward incoming messages as SMS message. This is particularly considered useful for MWI notifications⁶ or forwarding of e-mails. In this process it happens ever so often that rerouted e-mails reach a length that does not fit in the cellphone display. In this case the SMS protocol can intelligently shorten the message. The mechanism used for this purpose is the digest algorithm. It filters superfluous information (e.g. blank lines or greeting phrases) from messages to be sent as SMS message.

The manner in which the digest algorithm is to shorten messages is defined via various variables. You find detailed information on this in [Section E.20.2.6](#), “[Private \[REG_MULTI_SZ\]](#)”, on page 1929.

Example:

The XPR server receives the following e-mail to be forwarded as SMS message to the relevant user.

Originator: john@far.com "John Smith"

Subject: We got the contract

Body:

Sunday evening, 06:45pm

Hi Mae,

At last we got the contract regarding your offer to the ABC inc.

Regards,

John

6. MWI notifications are generated by the Notification APL.

Since it would not be very useful to have this message displayed on a cellphone unchanged, we use the digest algorithm. We configure it in the following format:

```
{ORNAME}: {SUBJECT,80} - {DIGEST,40}
```

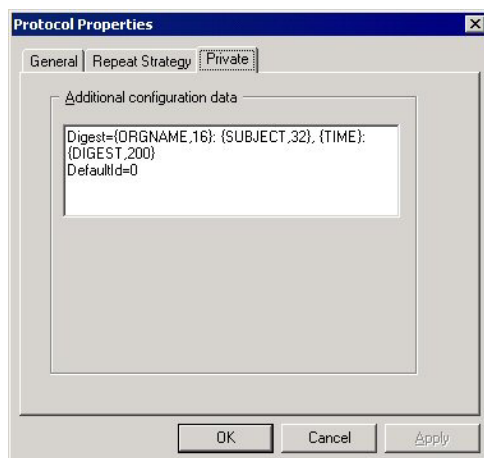
In this definition, {ORNAME} forms the originator name, {SUBJECT,80} is the message subject limited to 80 characters and {DIGEST,40} represents the message contents reduced to 40 characters. The result of our example thus reads:

```
John Smith: We got the contract - At last we got the contract
regarding...
```

Let's have a look at the configuration tabs of the protocol settings.

The SMS protocol has among other things the above *General* and *Repeat Strategy* configuration tabs (c.f. [Section 10.4.6, "Fax G3", on page 702](#)). Therefore we will only have a look at the differing *Private* configuration tab.

10.4.19.1 Configuration Tab *Private*



The configuration tab *Private* includes individual configuration data regarding the respective protocol. The settings made here correspond to an INI configuration file known from the operating system Windows 3.1.

One protocol-specific entry is made per line in the format *Label*>=<*Value*>.

Example: Digest={{DATE}}, {DIGEST}}

The possible entries are described in detail in [Section E.20.2.6, "Private \[REG_MULTI_SZ\]", on page 1929](#).

10.4.20 AMIS

The Audio Messaging Interchange Specification (AMIS) is a protocol developed by the Electronic Messaging Association (EMA) for the exchange of voice mails between two dissimilar voice messaging systems. Thus it is part of the voicemail networking protocols (see also [Section 10.1.4, “Voice Mail Networking”, on page 539](#)). AMIS has been defined for both analog and digital communication.

The E-Script AMIS.e of the XPR server implements the analog version of the AMIS protocol. Protocol data is transmitted by means of DTMF tones via regular telephone lines. The actual voice mail is simply played by the transmitting server and rerecorded by the receiving server.

If you wish to add AMIS to an XPR configuration via the **Add** button on the *Protocols* tab like other automatically installed default protocols (Fax G3, Fax G4, etc.), you need to select **Voicemail (AMIS)** during the setup.

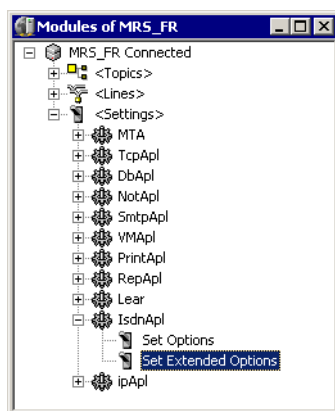
Let's have a closer look at the AMIS configuration in the next sections.

10.4.20.1 Configuration

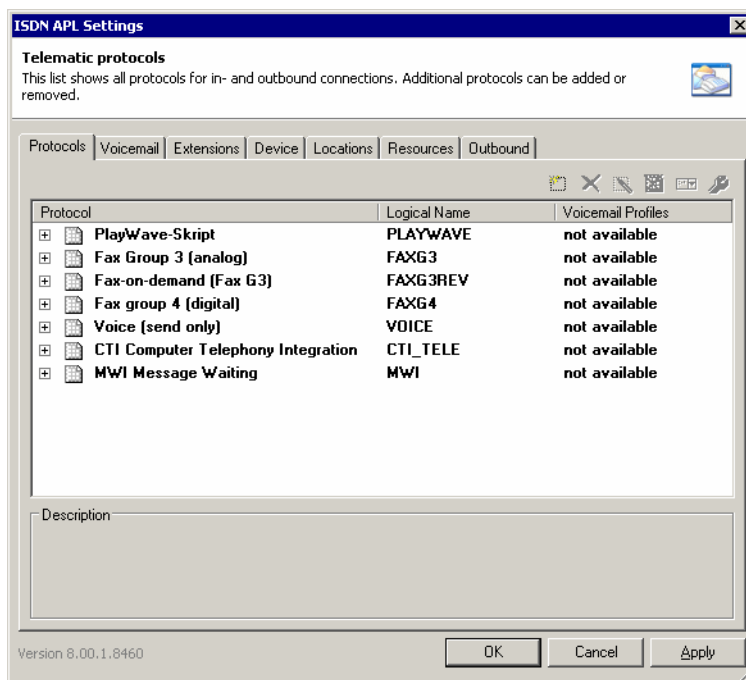
The AMIS protocol can be configured for the ISDN APL used after it has been installed on the XPR server.

Proceed as follows:

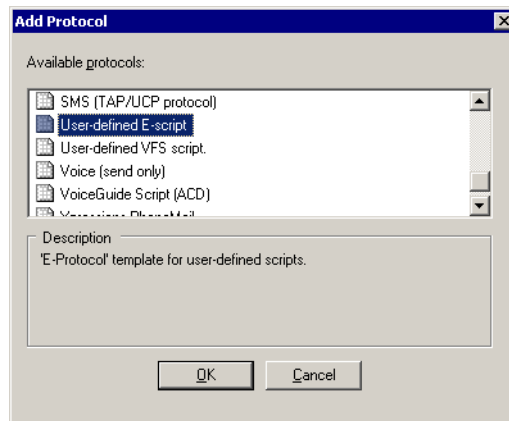
1. Start the XPR server and the XPR monitor.
2. In the *Components* window of the XPR monitor select **IsdnApi > Advanced Settings**.



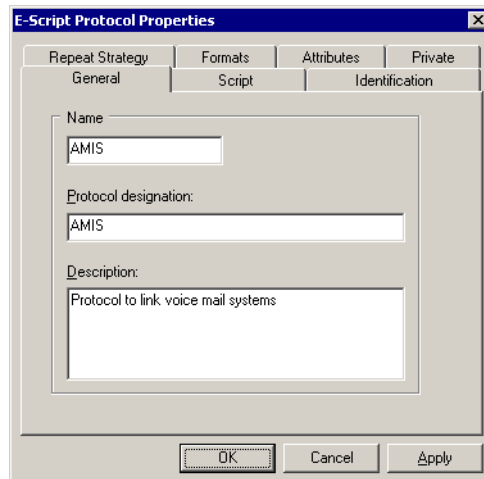
3. Select the **Add** icon in the toolbar of the *Protocols* configuration tab.



4. Select the **User-defined E-script** entry from the displayed protocol list and confirm your choice with **OK**.

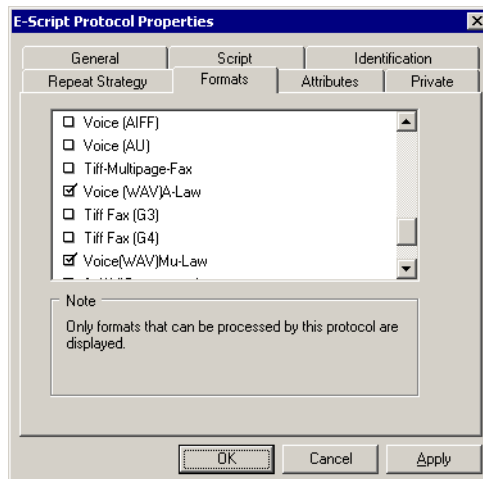


5. Enter *AMIS* in the **Name** field of the configuration tab *General*.



6. Enter a short protocol name in the field **Protocol designation** and a meaningful **Description** in the corresponding field. These entries serve for a better overview later on.

7. Switch to the *Formats* configuration tab.



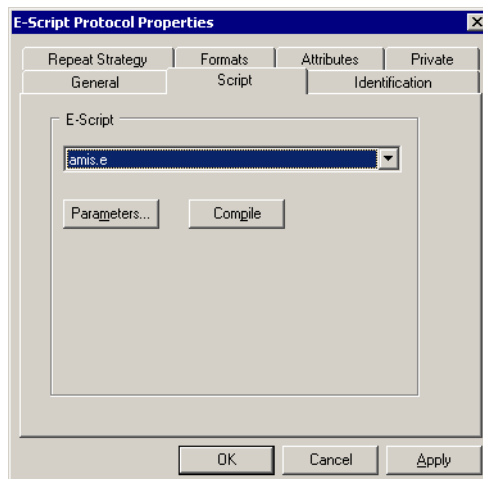
8. In the list of formats select the three entries

- **Voice (WAV),**
- **Voice (WAV) A-Law** and
- **Voice (WAV) μ -Law.**

IMPORTANT:

Since the AMIS protocol only supports these three formats, no other entry may be selected additionally.

9. Switch to the *Script* configuration tab.



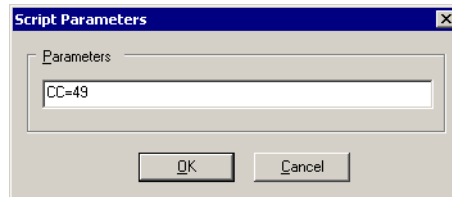
10. In the **E-Script** field select the list entry *amis.e*.

11. Then click the **Parameters** button.

12. Enter all required script parameters in the format
<Parameter name>=<Parameter value> and confirm the entry with **OK**.

IMPORTANT:

If several parameters are to be entered at once, you can enter them one after another. Separate them by a blank.



The following three parameters must necessarily be entered in the script:

- CC=<International country code of the XPR server> (e.g. 49)
- NDC=<Area code of the XPR server> (e.g. 2404)
- SN=<Subscriber code of the XPR server inclusive extension> (e.g. 901100)

The following parameters are available:

Parameter	Description	Presetting
CC	International country code of the local XPR server at which the AMIS protocol can be reached by external callers.	empty
NDC	National Destination Code of the local XPR server at which the AMIS protocol can be reached by external callers.	empty
SN	Subscriber Number of the local XPR server at which the AMIS protocol can be reached by external callers.	empty
COUNTRY	TUI language code of the local XPR server. (0=German, 1=English-UK, 2=French, 4=Spanish)	0
LANGUAGE	Language code for reports of the local XPR server. (German, English-UK).	English
DBA_FIELD	The XPR database field AMIS searches for the AMIS mailbox number of a user. If the value VOICE# is indicated for this field, incoming AMIS messages are sent to the regular voice mailbox of the respective recipient.	AMIS
RECORDING_CUT	Part of a voice mail (in ms), that is cut off at the end of each received file. This cutting is used to avoid DTMF tones at the end of transmitted messages.	200

Table 31 Parameters for the AMIS Protocol

13. Assign also the following parameter to AMIS:

- DBA_FIELD=VOICE#

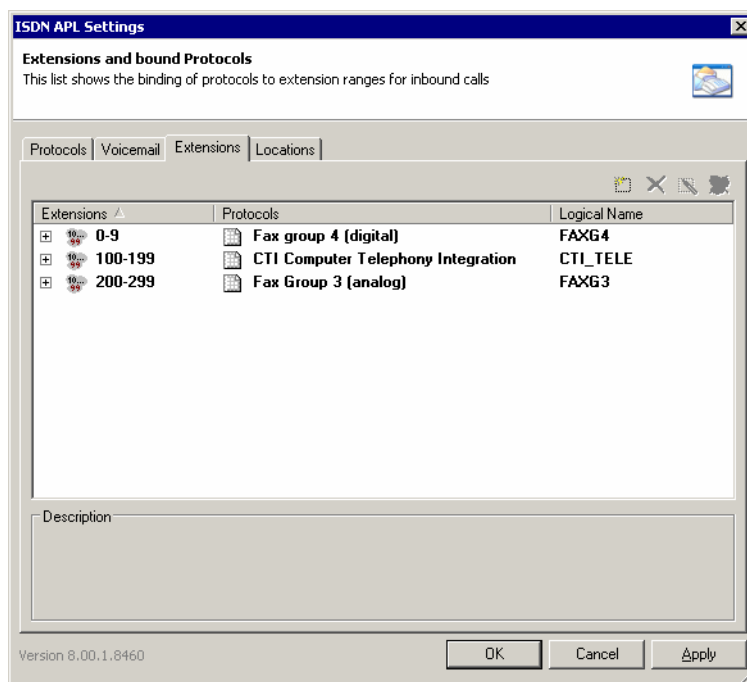
This assignment specifies that the original voice mailboxes of the users are used for AMIS messages.

Now we have installed the AMIS protocol on the XPR server. A corresponding extension number range needs to be assigned to AMIS as for all other protocols. This range must match the entries in the following parameters:

- CC
- NDC
- SN

Proceed as follows:

1. Switch to the *Extensions* configuration tab.



2. Select the **Add** icon in the toolbar to add a new extension number range for the AMIS protocol.

NOTE:

In each telematics APL you can configure a maximum of 1024 extension ranges.

3. Define the phone number range in the **Start** and **End** fields the AMIS protocol is to use in the XPR server.

IMPORTANT:

If several extension ranges are specified in the IP APL, the number of digits of the different extensions must be the same for all extension ranges – for example 3 digits.

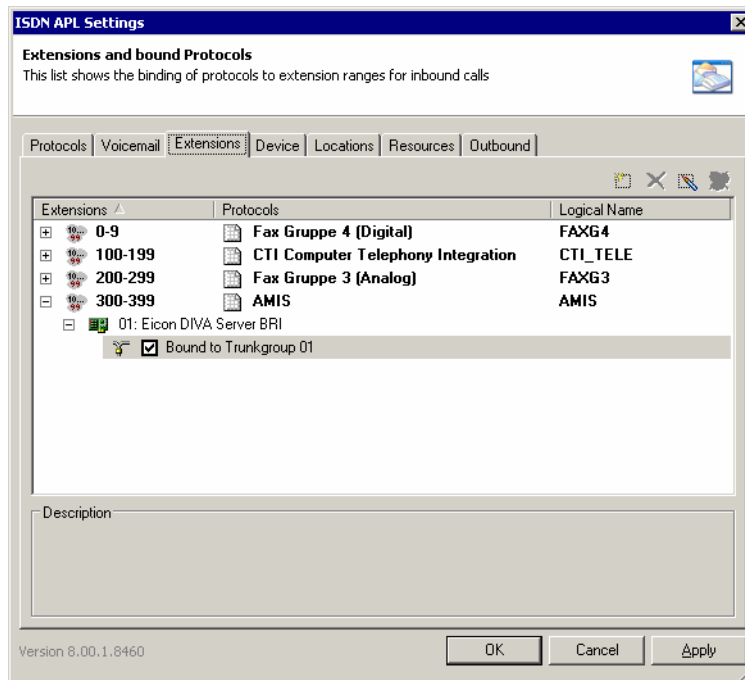
The screenshot shows the 'Extension Properties' dialog box with the following settings:

- Extension:**
 - ☒ Range (Start to End)
 - ☐ Discrete MSN
 - Begin: 300
 - End: 399
 - ☐ Allow missing digits (Number too short)
 - ☐ Allow superfluous digits (Number too long)
- Bindings:**
 - Protocol: AMIS [AMIS] (dropdown menu)
 - ☐ Create also for all other suitable Protocols
- Description:**
 - Extension range for AMIS

Buttons: OK, Cancel

4. In the **Protocol** field select *AMIS*.
5. Enter a short, meaningful entry in the **Description** field. This entry serves for a better overview later on.
6. Save your settings by clicking on the **OK** button.

7. Expand the display for the newly created extension number range.



8. Select the trunk group and the associated location information to be used for the AMIS protocol.

IMPORTANT:

The trunk group to be selected here must have been previously configured.

Now you have configured the AMIS protocol in the telematics APL of the XPR system.

You need to perform the following settings in the Web Assistant for the AMIS protocol to work correctly.

- Configuring location profiles for the networked voice mail systems
- Assigning the user privilege **AMIS Privilege** for all users who are to send voice mails via AMIS.

See [Section 10.1.4.1, “AMIS”, on page 540](#) and the descriptions in the *Web Assistant* manual.

10.4.21 CTI Computer Telephony Integration

The *CTI Computer Telephony Integration* protocol is a component of the ISDN APL and automatically started with the APL by default. This automatic start can only be disabled by the *CtiLayerActive [REG_DWORD]* registry value.

CTI Computer Telephony Integration provides basic CTI features, which can be used via the following signaling protocols.

- CorNet N,
- CorNet NQ and
- QSIG

These CTI basic functions comprise the CTI transactions:

- PHONECALL
- DIVERSION
- QUERY
- DISCONNECT

You find continuative information about these transactions in [Section 17.3.3, “CTI Transactions”, on page 1054](#).

To establish a communication connection between two subscribers, *CTI Computer Telephony Integration* opens two parallel B-channels to the connected PBX. After the establishment of the two connections to the conversational partners, the XPR server directly connects them in the PBX via ECT (*Explicit Call Transfer*). The previously occupied B-channels are then available again to execute other communication requests.

Default settings for the PHONECALL transaction

The complete invocation of the PHONECALL transaction contains the following parameters:

- Caller
- Callee
- Switch mode
- Switch type
- Time-out

Example:

```
PHONECALL CALLER=100 CALLEE=200
SWITCH_MODE_CALLSWITCH_SUPERVISED SWITCH_TYPE=PBX_SWITCH
TIMEOUT=120
```

If PHONECALL is not invoked with all parameters, default values are used for the missing information. These default values are defined in corresponding registry values and can be modified if required.

Under the `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\PP-COM\MRS\IsdnApl` registry key the following registry values define the default settings for the PHONECALL transaction:

- `CtiSwitchMode` [REG_DWORD]: defines the switch mode default value
- `CtiSwitchType` [REG_DWORD]: defines the switch type default value
- `CtiTimeout` [REG_DWORD]: defines the timeout default value

You find further information on these registry values in [Section E.20.2.1, “General Entries”](#), on page 1889.

10.4.22 CTI Light

The CTI Light script is used for basic telephone connection management. SimpleDialer for Notes uses it to set up telephone connections and to close them.

CTI Light is installed and configured via the `CtiLight.e` script.

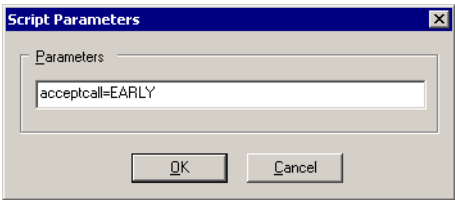
IMPORTANT:

So that the CTI Light protocol can operate trouble-free, it must be assigned the logical name `CTILIGHT`.

10.4.23 Vogue

The Vogue protocol can realize functions of an automated attendant. These are configured by the XPR application *Application Builder*.

Vogue is always active in the context of a telematics APL and configured there as protocol. The associated configuration is accordingly accessible in the XPR monitor via the settings dialog of the telematics APL used. In the associated protocol settings you find the configuration of the Vogue settings via the **Parameters** button in the *Script* configuration tab.



Parameters are entered in the **Script Parameters** dialog in the format *<Parameter>=<Value>*. Several parameter-value pairs are then separated from each other with a blank. The following parameters are available for the Vogue protocol, with upper and lower case to be heeded.

Parameter	Description
Debug	Activates the emission of additional debug outputs. The following parameter values can be set: APP Information on the current Vogue application. BOX Information on the current Vogue box. CORREL Information on the correlation database. DBA Information on the general database access. EVENT Information on event handler, timer etc. FUNC Information on all function calls. ODBC Information on external databases. RES Information on storage allocation and addresses. TIME Information on time profiles. UTIL Information on internal additional functions.

Table 32 Parameters for the Vogue Protocol

Parameter	Description
	VAR Information on variable processing. VOGUE Information on the VOGUE protocol. ALL Activates all additional information described. This additional information is displayed depending on the following display options of a XPR log monitor: <i>Level 3:</i> <i>VOGUE, APP BOX, DBA, VAR, TIME, UTIL, CORREL, ODBC, EVENT, ALL</i> <i>Level 4:</i> FUNC, RES
language	Defines the language in which the Vogue announcements are put out. The following languages are currently generally supported. Which of these can be eventually used is determined by the purchased XPR licenses. – GERMAN – BRITISH – FRENCH – ITALIAN – SPANISH – DUTCH – AMERICAN – PORTUGUESE – BRAZILIAN – AMERICANSpanish – CANADIAN – FRENCH – RUSSIAN – TURKISH
maxcalls	Defines the maximum number of simultaneous Vogue entities (calls). When this value is reached, no further calls are accepted.
switchmode	Defines in which manner a call is forwarded. The following parameter values can be set: BCH Transfer via another B-channel between PBX and XPR server. PBX Transfer to the PBX (Path Replacement).
tenant	<i><Tenant ID></i> Defines a default-tenant-ID used for name dialing in a multi-tenant solution. Only those users who belong to the tenant with this tenant ID are then announced to the caller. This setting applies for an SIP connection only. The tenant function disables the filter function via \$AAFILTER of the Name Dialing control. See the <i>Application Builder</i> manual on this.

Table 32 Parameters for the Vogue Protocol

Behavior in case of activated offline mode

With the **Accept call at application start** option of the Vogue applications you can deactivate or activate the offline mode individually for each application. If the offline mode is active for an application, a call is not immediately accepted upon the application start, but specific conditions need to be fulfilled first (cf. *Application Builder* manual).

If a call is accepted delayed in this way, the Vogue protocol reboots the relevant Vogue application in the online mode. This leads to offline-capable application boxes being run through twice for a call at the start of a Vogue application.

Vogue language settings

If the Vogue protocol routes a caller to another telematics script, this telematics script uses for all greetings the language that the Vogue protocol has already defined for the caller – for example via a national language box.

10.4.24 Caller Guide

IMPORTANT:

The Caller Guide script requires installation and licensing of the ASR server. You find this server on the XPR setup medium.

The Caller Guide is a routing assistant. It is possible to search contacts in the XPR database and create a direct connection to the thus found entry.

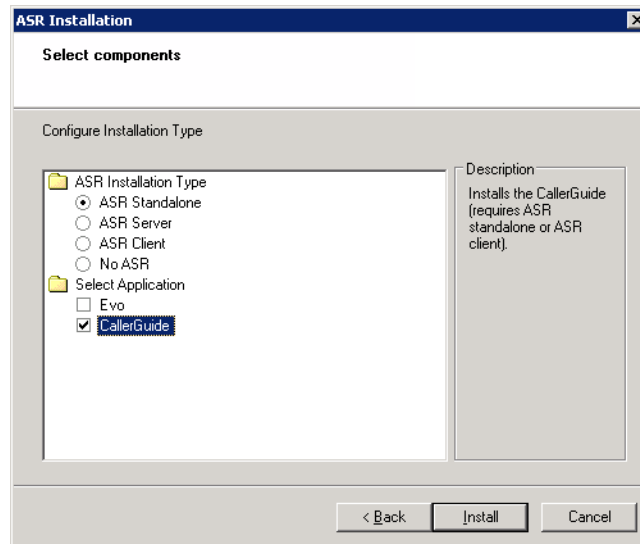
A couple of standardized commands and an efficient speech recognition system allow to use the Caller Guide easily via voice. Search entries and administration of the Caller Guide are also easily possible via the telephone keys. Prompts or the telephone display including the search hit list simplify the usage.

The Caller Guide is not automatically installed during the XPR server setup like other default protocols (Fax G3, Fax G4, etc.). For this reason, it cannot simply be added via the **Add** button in the configuration tab *Protocols* in a XPR configuration. So that you can use the Caller Guide in the XPR server, it must have been previously installed from the XPR setup medium.

The following paragraphs include information on the installation, setup and configuration of the Caller Guide script. The menu structure is described in the *Client Applications* manual.

10.4.24.1 Installation

The CallerGuide script can be installed via the XPR server default setup. You can pick the Caller Guide script for installation in the component selection. Please note that the Caller Guide script setup also requires the installation of an ASR stand-alone or ASR client. Click on the **Install** button to install the selected components.



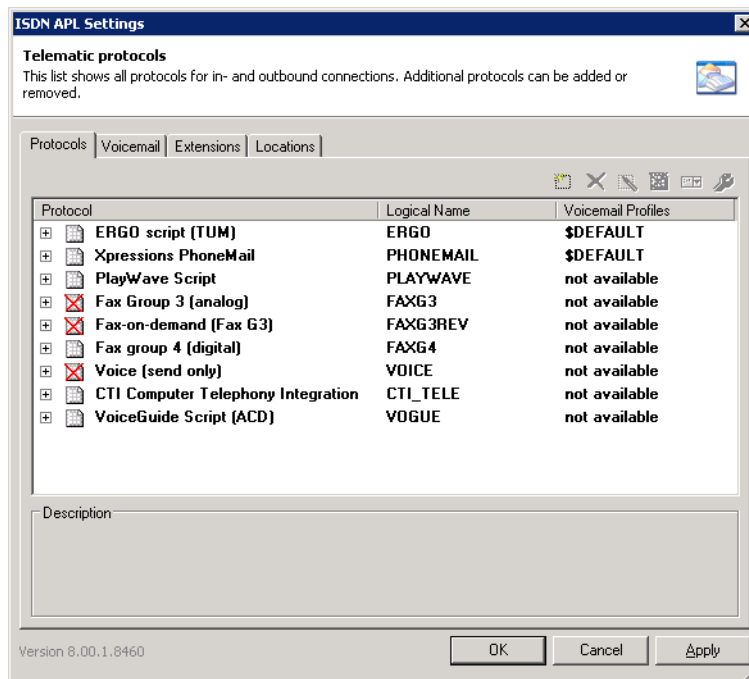
You can also open the Caller Guide script setup menu separately from the XPR server default setup. Start therefore the `setup.exe` file in the `XpressionsInstall\AddOn\Misc\ASR` directory of the OpenScape Xpressions V7 setup medium.

After the successful installation of the Caller Guide you need to configure the script in the telematics APL as follows.

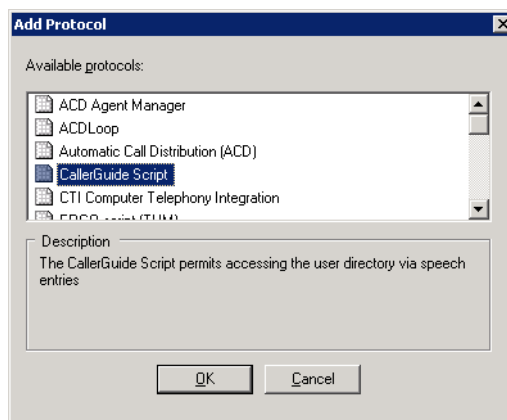
10.4.24.2 Installation

The Caller Guide is installed with the help of the settings pages of the applied telematics APL.

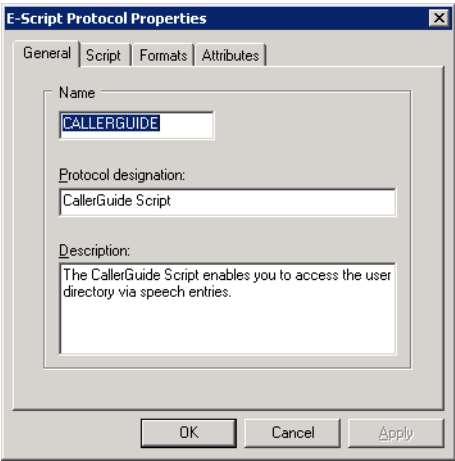
1. First start the XPR monitor and open the settings pages of the applied telematics APL in the modules window.



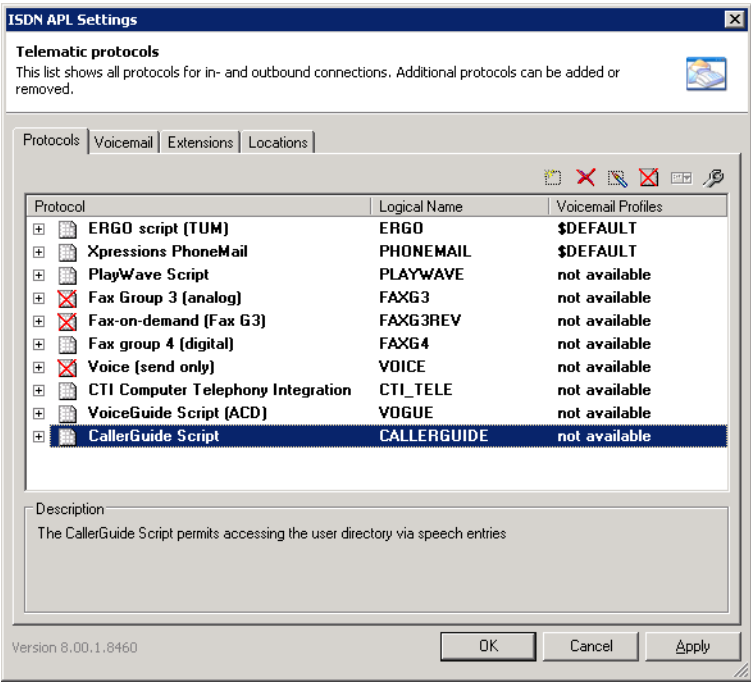
2. Click the **Add** button in the toolbar to install a new protocol.
3. A new dialog is displayed. In this dialog, select the protocol named **CallerGuide Script** and confirm your selection with **OK**.



4. In the next step, assign a **name** to the selected protocol. Use the name *CallerGuide* to make the identification easier. Confirm your settings by clicking on the **OK** button.



5. Now the newly installed script for the Caller Guide applied is displayed on the **Protocols** tab of the settings pages of the applied telematics APL.



In the next paragraph you will learn how to configure the Caller Guide script.

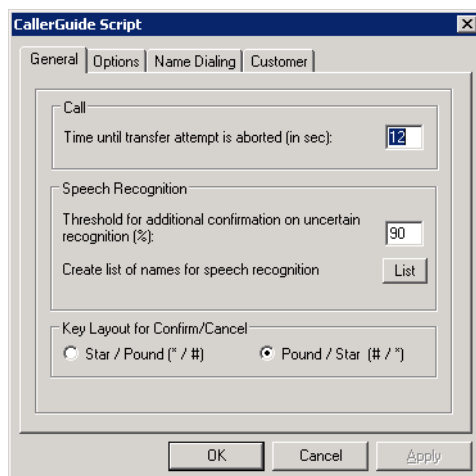
10.4.24.3 Configuration

The setup of the Caller Guide script and its configuration are performed in the configuration pages of the applied telematics APL.

Select the Caller Guide script and click the **Script Parameters** button in the toolbar to open the Caller Guide script configuration pages. The Caller Guide script configuration is divided into the tabs *General*, *Options*, *Name Dialing* and *Customer*.

The General tab

On this tab general settings for the Caller Guide script operations are performed.



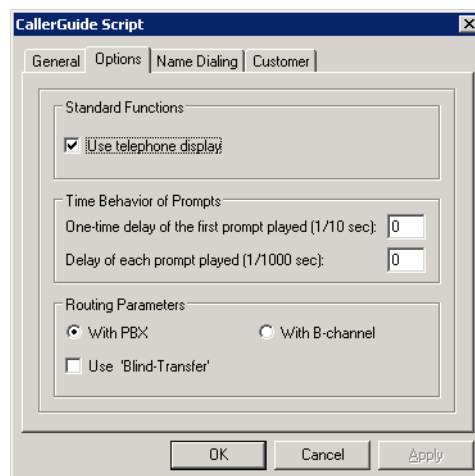
In the following table the possible settings are explained:

Field	Description
Time until transfer attempt is aborted (in sec)	In this field you determine how long the system tries to establish a connection to the desired contact. A connection attempt refers to the connection setup to a configured tracking phone number of the contact. If the time for a connection attempt to a configured tracking phone number is up, the next configured tracking phone number is dialed. If the connection attempts to all configured tracking phone numbers fail, you will be diverted to the mailbox and you can leave a message. The entry is made in seconds. Maximum is 99 seconds. The default value is 12 seconds.
Threshold for additional confirmation on uncertain recognition (%)	The percentage stands for the degree of the accordance the speech recognition program must recognize between search entry and the entries in the database in order to display search hits. If only a percentage of the threshold entered in this field is reached, the recognized result must be confirmed. The default value for the limitation threshold is 90%.

Field	Description
Create list of names for speech recognition	By clicking the List button, user entries are read from the XPR database and saved to a file. This file is a grammar for the speech recognition system and serves as the basis for the search via voice. This file must be updated before the start of the Caller Guide and for each database modification. This process is automatically performed once a day by the Maintenance Script. Attention: User information containing digits will not be recognized by the Caller Guide speech recognition. Besides the names, further fields can be implemented for each user. These fields will then be used by the Caller Guide for recognition. You find further information on relevant database fields in Section 10.4.1.8, "Enable addressing via names", on page 610.
Key Layout for Confirm/Cancel	In this section the keys to be used for the features <i>Confirm</i> and <i>Cancel</i> are determined. Either the * key or the # key is assigned to the respective function. By default, the * key is used for confirmation and the # key for canceling.

The Options Tab

In the *Options* tab optional settings are performed.



The following table depicts the individual setting options

Field	Description
Use telephone display	In this field it is determined whether the telephone display is used for the additional display of search hits. Search hits or queries are displayed and not only announced via greeting if the option is activated. This function is activated by default.
One-time delay of the first prompt played (1/10 sec)	Via the option One-time delay of the first prompt played, a delay for the first prompt played after a new connection has been established can be defined. The background of this option is that different PBX in a voice mail system signalize by establishing the D-channel that the first system announcement can be started. The B-channel required for the transmission is only established with delay, so that the first announcement is played back respectively truncated for the caller if no delay takes place. The entry is made in tenths of a second and can be between 0 and 99. By default the value is set to 0. Thus the delay is disabled.

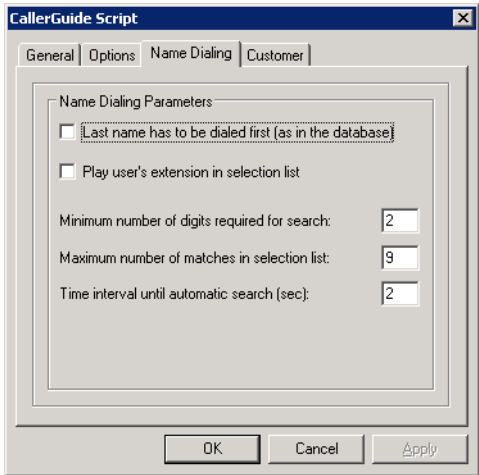
Field	Description
Delay of each prompt played (1/1000 s)	The option Delay of every Prompt played defines a minimum delay for each announcement. In certain PBX system types, prompts which directly follow a keypad entry may be slightly truncated at the beginning when replayed. If this behavior occurs with your PBX it can be leveled out by defaulting a suitable delay period. The entry is made in thousands of seconds. The delay can be set from 0 to 9999 milliseconds. Default set is 0 milliseconds, thus no delay.
Routing with PBX or B-channel.	The options With PBX and With B-channel define how a call is forwarded. The option PBX refers to the transfer within the PBX (path replacement). The B-channel option includes the transfer via an additional B-channel between PBX and XPR server.
Use 'Blind-Transfer'	For a blind transfer the availability of the destination is not checked at the time of the transfer. Thus a caller might receive a busy signal or even be rerouted to the original voice mailbox. Attention: Users may configure different individual phone numbers in the Web Assistant, to which a caller is routed if required (see the <i>Web Assistant</i> manual). If forwarding via blind transfer is configured with the Use Blind Transfer option, a caller may always only be forwarded to the first of such configured phone numbers. All other configured phone numbers will not be considered.

NOTE:

The Blind Transfer feature is only available with the PBX protocols Cornet N and Cornet NQ by default. To use Blind Transfer also for other PBX protocols, it must be configured manually (cf. [Section E.20.2.3, "Private \[REG_MULTI_SZ\]", on page 1920](#)).

The Name Dialing Tab

The *Name Dialing* tab defines the possible settings for the search of contacts via the telephone keys.



To optimize searching in the database on the basis of name dialing, the XPR server uses the `VM_VANITY` database field. In this database field the XPR server deposits a user-individual vanity number created from another database field of the respective user. You find more details on this in [Section 11.11, “Vanity Number Support”, on page 895](#).

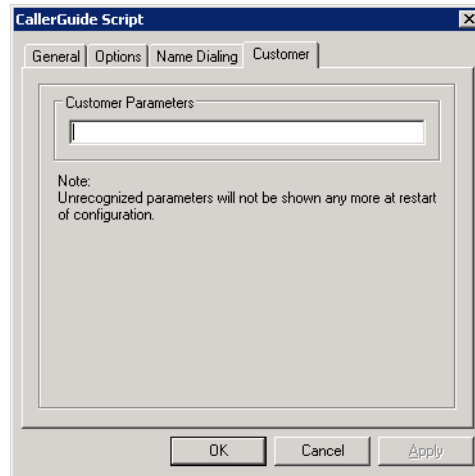
The following table defines the possible settings of this configuration page: You find further information on relevant database fields in [Section 10.4.1.8, “Enable addressing via names”, on page 610](#).

Field	Description
Last name has to be dialed first (as in the database)	The Caller Guide script compares the search information entered for name dialing with the entries of the NAME fields of the XPR database. Depending on the users being stored with leading first name or last name, the operating note Last name has to be dialed first must be activated or not. This option only defines which user note is played to the caller via the Caller Guide script. The selected option does not influence the search algorithm of the XPR server. Note: Please note that mixing the order of first and last name in the NAME fields of the XPRdatabase can lead to serious problems in the search algorithm of the Caller Guide script.
Play user's extension in selection list	Via this option you can determine whether the respective extension of the contact is also issued. Thus the user can note this number for later usage.
Minimum number of digits required for search	It is not necessary to enter the complete name of the desired contact for a search. This field determines how many digits are necessary for the entry so that a search can be started. By default two digits are necessary. A maximum of 9 digits are possible for a minimum entry.

Field	Description
Maximum number of matches in selection list	Here you determine the maximum number of search hits in a selection list. This field refers to the name search by telephone keypad only. The list that may be announced during the search is restricted to a maximum of five hits and cannot be modified. The maximum number of hits in a selection list after a search by telephone keypad is 9. You can invoke each hit by pushing the keys 1-9. By default 9 matches are possible in the list.
Time interval until automatic search (sec)	The time interval until the automatic search defines how long the system waits after the user's search entry via the telephone keys until an automatic search is run. On the basis of the digits entered before the automatic search run issues a search hit list. Via the automatic search run the entry is not canceled, so that it is possible to enter further digits via the user and the user can be rendered more precisely. This represents a simplified search for the user, since a hit list can be issued after the entry of each digit and the user can select a search hit. Thus it is not necessary to enter unnecessarily many digits. By default 2 seconds is set as time interval. Maximum is 99 seconds.

The *Customer Tab*

On this tab you can perform further special settings via a command line.



The following parameters are supported:

- **tenant=<tenant ID>**
Defines a default tenant ID, which is used for name dialing in a multi-tenant solution. Only those users who belong to the tenant with this tenant ID are then announced to the caller.

10.4.24.4 Defining the maximum Number of Search Hits

A maximum number of 10 search hits is defined by default. This default value may be too low considering a sometimes large number of search hits or names that occur very often. So if a limit of 10 was set, only the first 10 search hits of the alphabet would be considered and the search stopped. For example, if 12 search hits were scored, two would be dismissed.

Therefore you can change the maximum number of search hits. But you should only perform this modification if you can be sure that the names you look for are indeed found more often than ten times as search result. An unnecessary adaptation is a waste of system resources.

Up to now, the maximum number of search hits cannot be adjusted via the dialogs of the CallerGuide configuration. To change this value you need to supplement either the Caller Guide configuration file (1) or the configuration file of the speech recognition system (2) using an editor.

1. Caller Guide Configuration File:

You find the configuration file `Common.cfg` in the directory:

`<XPR-Install>\res\e\CallerGuide\ASR.`

Enter the following line in this file:

`swirec_max_parses_per_literal=<value between 1 and 99>`

2. Configuration File of the Speech Recognition System:

If you use the speech recognition system by SpeechWorks, you find the file `Baseline.xml` in the directory:

`<XPR Install>\SpeechWorks\OpenSpeech Recognizer\config.`

Add the following lines to this file:

```
<!-- Max parses evaluated for each literal and grammar Valid
values are 1-99 -->
```

```
<param name="swirec_max_pares_per_literal">
```

```
<value> <number> </value>
```

```
</param>
```

`<number>` specifies an integer value between 1 and 99. If you use another speech recognition system you need to revert to its corresponding configuration file or perform option 1.

Either way a value between 1 and 99 can be specified. Save the files after the modification but without changing the file storage location.

You may use only one option to change the value for the maximum number of possible search hits. The system first checks the entries in the configuration file of the Caller Guide and if no appropriate entry can be found there, the file of the speech recognition system is used. If you have added entries in both files, only the entry in the configuration file of the Caller Guide is considered.

10.4.24.5 Tracking Phone Numbers and Personal Announcements

Tracking phone numbers are phone numbers defined by the user which the Caller Guide script dials for the connection setup to the respective XPR user. A total of five phone numbers or deputies can thus be defined in a list. The individual list entries are addressed one after another until a connection can be established or until the complete list has been addressed.

The tracking phone number configuration and the recording of personal greetings is effected via the Web Assistant. You configure the phone numbers via the menu option **Voice Mail System** of the **Personal settings** menu.

Instead of using the name prompts for the individual XPR users that have been created automatically by the TTS system, each XPR user can create their own prompt. The names of the XPR users are played as result after each search.

The announcements are recorded via the menu option **Announcements** in the **Personal settings** menu and add these to the **user data**.

NOTE:

For detailed information on the configuration of numbers and the recording of personal announcements please refer to the *Web Assistant* manual.

10.4.24.6 Defining Name Pronunciation

If the user does not record a private greeting, the voice recognition automatically creates a greeting using the name fields in the database. The user name voice recognition also orients by this automatically generated user name pronunciation.

For names that are not properly recognized and incorrectly pronounced by the voice recognition, further fields can be specified in the database for the respective user. In these fields you can enter the user names in a way that they correspond to the correct pronunciation. In other words, you specify the user name the way it is pronounced.

When a name announcement is created for the user, the voice recognition will access this field then. User names will now be announced according to their pronunciation and will also be recognized by the voice recognition according to this pronunciation.

To enable this more precise name greeting, open the **DB-Tool** (`<XPR Install>\SDKTools\DBTool.exe`). Find the entries of the respective user and add a database field of type **VM_ASR_NAME** for this user. If this field does not exist yet, create a database field with the key **VM_ASR_NAME_01**. Assign the user name to this entry for the voice recognition. Write the name the way it is pronounced.

NOTE:

VM_ASR_NAME describes as topic all database fields of this type and is no database field in its own right. The actual database fields are numbered and read **VM_ASR_NAME_01** to **VM_ASR_NAME_99**.

Domain	Classname	Class	Keyname	Key
DOC	USER	PETROV	S_LOGIN_WEB	2005.08.04-11:11:56
DOC	USER	PETROV	VM_NAME	PETROV_NAME_1.pcm
DOC	USER	PETROV	VM_PROTOCOL	ERGO
DOC	USER	PETROV	VM_TIMEPROFILE	WEEK_PROFILE_BASIC
DOC	USER	PETROV	VM_VANITY	738768
DOC	USER	PETROV	WEB_FIRST_LOGIN	2005.06.27-16:10:56
DOC	USER	POSTMASTER	ALIAS	A335FDA9
DOC	USER	POSTMASTER	GROUP	USER
DOC	USER	POSTMASTER	LNREPLICATION	
DOC	USER	POSTMASTER	MAILBOX	POSTMASTER
DOC	USER	POSTMASTER	NAME	Commutazione
DOC	USER	POSTMASTER	PASSWORD	3702854253
DOC	USER	POSTMASTER	PREFERRED	MAILBOX
DOC	USER	POSTMASTER	SMTP	postmaster@company.com
DOC	USER	POSTMASTER	VM_ASR_NAME	switchboard
DOC	USER	POSTMASTER	VM_VANITY	266688294663
DOC	USER	SARTRE	ALIAS	20031611
DOC	USER	SARTRE	CTIJOURNAL	X
DOC	USER	SARTRE	GROUP	USER
DOC	USER	SARTRE	LNREPLICATION	
DOC	USER	SARTRE	LOGIN_STAT	42, 14:24:53 29.06.2005, WEB
DOC	USER	SARTRE	MAILBOX	SARTRE
DOC	USER	SARTRE	NAME	SARTRE
DOC	USER	SARTRE	NOT_ACTIVE	0
DOC	USER	SARTRE	NOT_LAG	0
DOC	USER	SARTRE	NOT_SHORT	0

Ready Loaded in 0.972 s 3104 Correl-Records

Several names for a specific user or contact can also be assigned by database fields of the type VM_ASR_NAME. For each name a database field is created and a consecutive numbering attached to the key name: VM_ASR_NAME_01, VM_ASR_NAME_02, VM_ASR_NAME_03 ... The highest possible numbering is VM_ASR_NAME_99.

For names that are to contain additional notations for the voice announcement, you can indicate the same database field for specification. For example, another name may be used for the post master. Proceed as described above: Change respectively define in the database the values for the fields of type VM_ASR_NAME (VM_ASR_NAME_01 to VM_ASR_NAME_99) of the corresponding user.

NOTE:

If the post master is used as operator, it is mandatory to specify a value for the Name database field (may also be a field of type VM_ASR_NAME).

There is the greeting *ConfirmHelp.pcm*

(*<XPR Install>\res\e\CallerGuide\<language>*) that prompts the user in the course of the call to confirm his/her entry or to connect to the operator. This voice prompt is only correctly executed, if a specification is contained in the Name database field or in one of the VM_ASR_NAME postmaster fields (for example the value "operator"). For the name of the switching center is copied to the name grammar used and can only be recognized by the system, if an entry is in the name field. Otherwise the Caller Guide script cannot recognize the name for the switching center and establish a connection to the central switching center. Open the DB-Tool and check the post master entries. An entry must be in the

Name key respectively in a key of the VM_ASR_NAME_01 to VM_ASR_NAME_99 database fields of the postmaster. And this entry must exactly match the name used in the *ConfirmHelp.pcm* greeting for the central switching center.

10.4.24.7 Excluding Users from the Caller Guide Search

With database fields of type VM_ASR_NAME you cannot only define the pronunciation of a name (see [Section 10.4.24.6, “Defining Name Pronunciation”](#)), but also exclude users from being searched for with the Caller Guide. I.e. such users cannot be found and thus not be contacted via the Caller Guide.

To assign this property to users, open the DB-Tool and look for the entries of the corresponding users. In the VM_ASR_NAME_01 key, value **x** must be entered. You can enter the **x** lower or upper key. Then save your modifications and the user will not be integrated in the speech grammar used by the Caller Guide. The entries of the keys NAME or further ASR keys such as VM_ASR_NAME_02 will not be considered for the respective user in the Caller Guide speech grammar either.

NOTE:

By means of name dialing these users are still available.

10.4.25 Conversation Recorder

With the Conversation Recorder protocol, XPR users may record telephone conversation.

When a participant in a telephone conference starts the Conversation Recorder protocol, the conference then consists of the original participants plus the protocol itself. As soon as the Conversation Recorder protocol starts recording, the connected conversational partners are informed accordingly by announcement.

After the conversation has come to an end, the recording is sent as voice mail to the user who has initiated it via the Conversation Recorder protocol.

You find further information about how to operate the Conversation Recorder in the *Client Applications* manual.

IMPORTANT:

Recording conversation without explicit consent by all conversational partners may violate the penal and data protection regulations of the country in which conversation is recorded.

IMPORTANT:

Before you use the Conversation Recorder protocol please obtain qualified legal advice as regards the regulations that apply for conversation recording in the country in which you want to record conversation and the effects such regulations may have on using the Conversation Recorder protocol.

IMPORTANT:

Please document at any rate the consent given by the participating parties before each start of a conversation recording.

10.4.25.1 Technical Requirements

So that you can use the Conversation Recorder protocol, the following must be installed in the XPR server:

- a telematics APL, since the protocol only works in the context of a telematics APL.
- the CTI APL, since the protocol is controlled via CTI transactions. Furthermore, a CTI link must have been configured and activated for the PBX used.

10.4.25.2 Permitting Conversation Recorder Protocol Usage

Before an XPR user may apply the Conversation Recorder protocol, letter **R** must be entered for him/her in the Correlation Database field **VM_AUTH_CODES**. You can change this user data via the Web Assistant, for example.

10.4.25.3 Installation

The Conversation Recorder protocol is not installed during the XPR server setup on the server system. Instead, the protocol is installed belatedly with a started XPR server and the installation file `ConversationRecorder.exe`. You find this installation file on the XPR product data carrier in the directory:

```
XpressionsInstall\AddOn\ex\ConversationRecorder
```

The installation file creates in the directory

```
<XPR-Install>\res\E\ConversationRecorder the log file
```

`ConversationRecorder.vo`. Beyond that, it defines in the same directory the resource directories for three announcements:

- for the announcement that the conversation is being recorded
- for the announcement that recording has been finished by pressing a DTMF key and
- for the announcement that recording has been finished due to reaching the maximum recording time.

10.4.25.4 Configuration

The Conversation Recorder protocol is configured via the settings of the telematics APL used. Proceed as follows:

1. Open the advanced settings of the telematics APL used in the XPR monitor.
2. Switch to the **Protocols** tab.

3. Select the **Add** icon. The **Add Protocol** dialog opens.
4. From the available protocols select the entry **User-defined E-script**.
5. Select **OK**. The **E-Script Protocol Properties** dialog opens.
6. Switch to the **General** tab.
7. In the **Name** field enter a name for the protocol – example: *CONVREC*.
This name
 - identifies the protocol in the telematics protocols list at a later date
 - defines the topic on which the protocol's reports may be issued in the XPR monitor logging
8. In the **Description** field adjust the text to explain the function of this protocol – example: *Conversation Recorder*.
This description is displayed on the **Protocols** tab in the **Description** section when you select the protocol defined here.
9. Select **Apply**.
10. Switch to the **Script** tab.
11. Select the **ConversationRecorder.e** entry in the selection field.
12. Select **Parameters** to perform further settings for the Conversation Recorder protocol.

You can specify the following parameters in the entry line:

Parameter	Function
-rmtopic (Remove XPR Monitor Topic)	The XPR server enables the representation of 64 topic entries per XPR component in the XPR monitor. This enables you to control the server components logging. The topic entry for the Conversation Recorder protocol is available under the telematics APL used and the name defined for the protocol. If no topic entry is generated for the Conversation Recorder protocol because the maximum number of 64 has been reached, the XPR monitor can be configured via this parameter string in a way that a less important topic is removed from the telematics APL branch used and the Conversation Recorder protocol is inserted as topic instead.
rec= <value> Value in seconds Default value = 300	Normally the value "Max. duration of messages (in seconds)" is read out for user groups and considered for the recording duration. If this entry is not defined for the relevant group, the value of the rec. parameter applies. After this period the Conversation Recorder protocol plays an appropriate greeting, closes the connection and sends the recording.
delay= <value> value in 1/10 seconds Default value = 10	Depending on the connected PBX it may happen that the beginning of the recording announcement is cut off. Via this parameter you can define a delay for the recording announcement.
timeout= <value> Value in seconds Default value = 5	The Conversation Recorder protocol terminates when it does not receive all transactions required for setting up the necessary connections from the CTI APL within the time specified.

Parameter	Function
-RecordOnly	In case of an Alcatel OXE R8/R9 with SIP support there is a special button for recording telephone conversation. When you push this button, a second connection as conference with Ergo is usually set up. You cannot configure this number, which always addresses the external voicemail system. If, however, this key is pushed, a special parameter is transferred. At the parameter's transfer the IP APL checks whether a protocol is entered in the registry value ConvRecProtocol [REG_SZ]. If so, this protocol is addressed instead of the voicemail number. Just for this case you can configure the Conversation Recorder as protocol with Recordonly. Then activate this protocol via the above registry value and the record button at the Alcatel OXE R8/R9 is operable.

13. Select **OK** to save your modifications and to leave your settings.
14. Select **OK** in the **E-Script Protocol Properties** dialog. You return to the **advanced settings** dialog.
15. Switch to the **Extensions** tab.
16. Click **Add** to define an extension for the protocol. The **Extension Properties** dialog opens.
17. In the **Extension** section enter the desired extension from the available extension range – example **Begin:** 500, **End:** 500.
18. In the **Protocol** drop-down menu select the previously defined Conversation Recorder protocol – for our example *CONVREC*.
19. Complete the extension definition with **OK** in the **Extension Properties** dialog.
20. Complete the telematics APL configuration with **OK** in the **APL Settings** dialog.

You have thus completely configured the Conversation Recorder protocol.

NOTE:

When using a CorNet protocol, the registry value [NeedConference \[REG_DWORD\]](#) must be additionally set to 1. In the Registry Editor, look under `HKLM\SOFTWARE\Wow6432Node\PP-COM\MRS\ISDNAPL\PROTOCOLS\ (XX)` for the value `ScriptName` with the content `ConversationRecorder.e`.

10.4.25.5 Tips and Tricks

Despite an existing usage permission the Conversation Recorder protocol may disallow recording. In this case the protocol is not authorized to set up a conference switch.

NOTE:

The CTIAPL must grant the Conversation Recorder protocol this right, otherwise the CTI transaction for establishing the conference switch will be rejected with *ACL_AccessDenied*.

You solve this problem by adding the **ACL_AccessListCheck [REG_DWORD]** registry value for the XPR server. Proceed as follows:

1. Start the registry editor on the XPR server computer system.
2. Switch to the directory:

HKLM\SOFTWARE\Wow6432Node\PP-COM\MRS\CTIAPL

3. Create the **ACL_AccessListCheck [REG_DWORD]** value and assign it the entry **0**.

After the CTIAPL reboot the Conversation Recorder protocol should now be able to set up a conference switch.

10.5 General Configuration of Telematics Services

The configuration of telematics services via the ISDN APL or IP APL is marked by the terms *Protocol*, *Extension*, *Location*, *Device* and *Trunk Groups*. Let's have a closer look at the meaning of these expressions.

10.5.1 Telematics Service Elements

10.5.1.1 Protocols

A protocol is the actual telematics service that is realized by the respective telematics APL. Which protocols can be used in an XPR environment depends mainly on the applied system hardware and the applied APL. Further information on this will follow in the later chapters about the configuration of the single telematics APLs.

Protocols can be divided into two groups depending on their implementation. Into those that are realized directly in the code of the respective APL, and those that have been implemented in a script language of the XPR server. The latter are also called scripts in the XPR context and are added to the APL as protocol if necessary. The most efficient script language at the moment that has been developed for the XPR server is simply called *E*. Accordingly, scripts that have been realized in this language are called E-scripts. One of these scripts is e.g. PhoneMail, which implements a voice mail system.

If we install an executable telematics service on the XPR server, the protocol is its actual kernel. From this we can conclude that further elements are required in addition to the protocol. One of these elements is the so-called location. We will have a look at it in the following paragraph.

10.5.1.2 Location

The location is another element in the context of configuring telematics services. The term location describes all necessary calling number information required to determine its exact 'position' in the international hierarchical communication network. This information is the basis for a correct phone number localization or normalization (cf. [Section 9.2, "Calling Number Handling in the XPR Server", on page 333](#)).

Part of the location information is e.g. the area code.

IMPORTANT:

The phone number information for XPR users is stored in the Correlation Database of the XPR server in normalized format. The respective normalization always takes place on the basis of the corresponding location information. If location settings are modified in an existing XPR environment, the phone number information of existing users is **not** automatically updated in the Correlation Database.

As a consequence, corresponding modifications of the user information must be performed manually. The XPR tool *NumberConversionPrepare* can be used for this purpose.

Please note:

Number Conversion Prepare does not adjust the CIT database field.

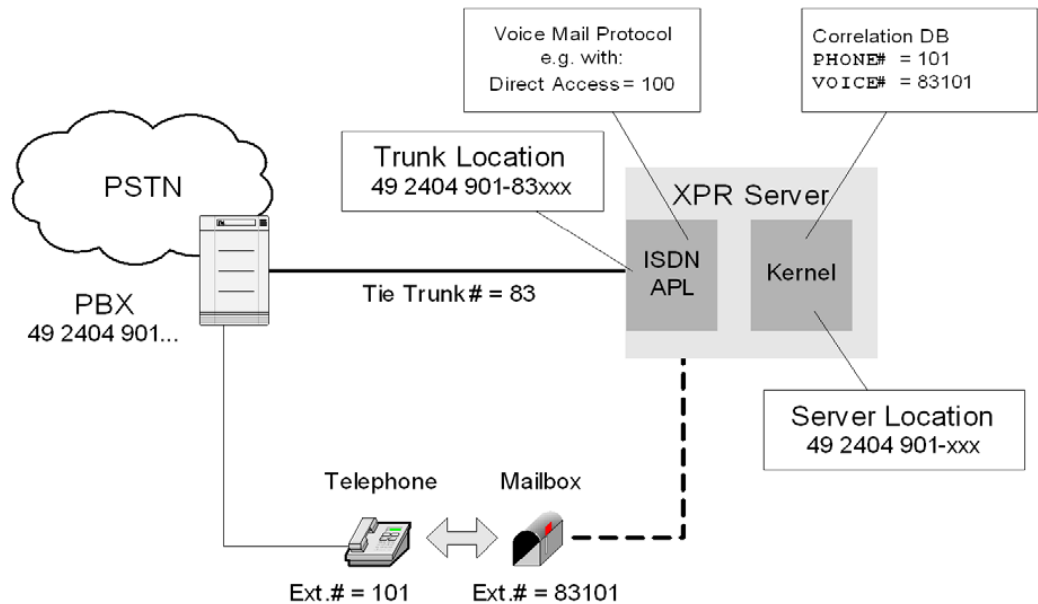
Server and trunk locations

Principally, there is a distinction between the server location and the line locations in the telematics context. Whereas the server location exists just once for a XPR server, several trunk locations can exist depending on the configuration. Especially for the connection of several external communication systems to the XPR server, diverse individual trunk locations must be configured. These represent specific features regarding the addressing that differ from the server location settings.

Let's have a look at the following example:

An XPR server is connected to the PSTN via a PBX. The connection between the PBX and the XPR server is realized via a trunk that is addressed via the trunk ID 83.

A voice mail protocol is attached to the ISDN APL. The Correlation Database of the server contains the extension information for the voice boxes of the voice mail users.



The server location contains the same settings as the connected PBX. This is the normal case. Additionally, a trunk location has been configured. It serves e.g. for correctly handling the phone number information that reaches the XPR server via the tie line. The trunk location only differs from the server location by the additional trunk ID.

Let's have a look at the resulting particularities:

- If the Direct Access of the voicemail protocol is to be addressed, this is done via the extension *100*. In this case the *83100* *must not* be dialed. The reason is that the voice mail protocol is bound to the ISDN APL and the ISDN APL uses the trunk location for the treatment of phone numbers. In this location the *83* is already indicated as trunk ID. Therefore it must not be dialed a second time when the Direct Access is addressed.
- If a user reaches his/her voice box via Direct Access, he/she must log on with his/her mailbox number. This information is synchronized with the Correlation Database. For this procedure the entry is normalized with the XPR server using the server location. In this location the trunk ID has not been configured. For a correct normalization the *83* must be entered when the mailbox number is entered.

10.5.1.3 Extensions

The term extension is well known in the world of telecommunication. The extension is one option to address several devices at one public telephone connection. This function is in the XPR server area the same. The only difference in our case is that via extensions no telephone or fax devices are addressed, but the various XPR server protocols.

We have already learned that a protocol is the actual kernel of an XPR service. Thus we can say here that different extensions provide access to the diverse telematics services that are installed on an XPR server.

IMPORTANT:

The extension ranges for FAXG3, VFS and E-scripts may not clash, since they cannot be distinguished by the service information transmitted by the D channel.

NOTE:

In each telematics APL you can configure a maximum of 1024 extension ranges.

10.5.1.4 Devices

The term device describes an interface that enables outward communication and thus external systems in the XPR server system. These include e.g. ISDN boards that provide the physical interfaces for the ISDN APL. In case of the IP APL, the TAPI interfaces configured on the XPR server system represent the devices.

The communication of the devices takes place via so-called channels that are e.g. realized by the single B-channels in an ISDN board.

10.5.1.5 Trunk Groups

A trunk group describes the logical summary of an arbitrary number of channels. The channels provided by a device can be divided into several trunk groups. Still, it is not possible to sum up channels of different devices in one trunk group.

Now we have an overview of the most important components we need to consider for the telematics service configuration. The next section describes the principal configuration procedure.

10.5.2 General Procedure for the Configuration of a Telematics Service

IMPORTANT:

For the Telematic APL configuration the NCO configuration files of the XPR server are accessed via the *NCOAdmin*. Please make sure that the NCOAdmin used and the NCO configuration files are on hand in the same version. If this is not the case, a warning points to this incompatibility at the beginning of the telematics configuration.

For configuring the protocols, extensions, locations and devices there is one settings tab of the same name each in the telematics APL configuration dialogs. The trunk groups configuration occurs in the *Devices* tab as well.

For the implementation of a new telematics service we recommend the following configuration sequence as regards the single elements:

1. Configuration of the Protocol
2. Location configuration
3. Configuration of the device with its trunk groups
4. Configuration of the associated extensions

IMPORTANT:

The extension ranges for FAXG3, VFS and E-scripts may not clash, since they cannot be distinguished by the service information transmitted by the D channel.

IMPORTANT:

If several extension ranges are specified in the IP APL, the number of digits of the different extensions must be the same for all extension ranges – for example 3 digits.

NOTE:

In each telematics APL you can configure a maximum of 1024 extension ranges.

10.6 Telematics Service Configuration Example Scenarios

In this chapter we will have a look at the principal scenarios using the XPR server with its telematics services. The scenarios cover a great part of the XPR installations.

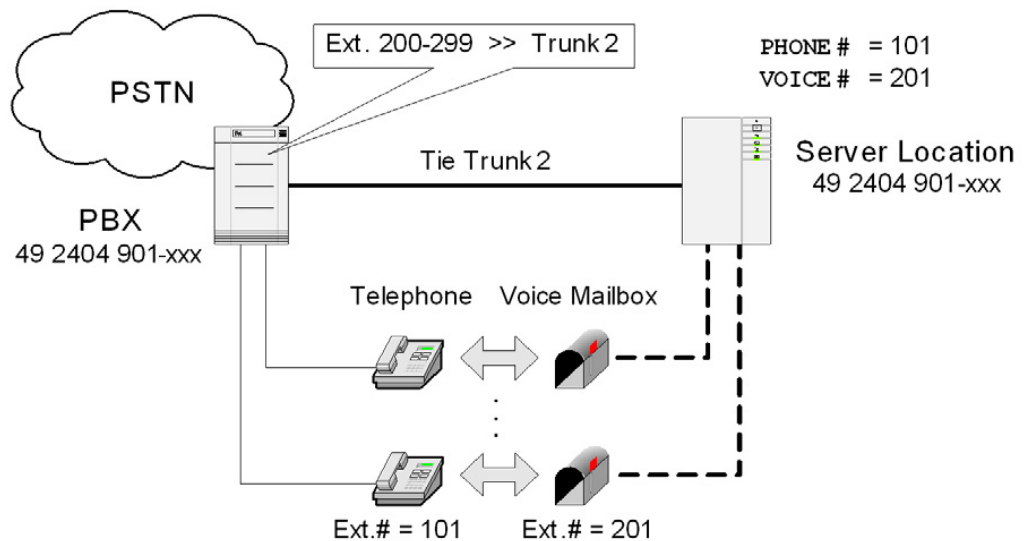
We have a look at the following scenarios:

1. XPR server via tie trunk *without* trunk ID at a PBX
2. XPR server via tie trunk *with* trunk ID at a PBX
 - Trunk ID is part of the XPR user extension
 - Trunk ID is no part of the XPR user extension
3. XPR Server via internal S0-Bus at small PBX with MSNs
 - PBX with point-to-point connection to the PSTN
 - PBX with point-to-multipoint connection to the PSTN
4. XPR Server without PBX at the PSTN
 - XPR server with point-to-point connection to the PSTN
 - XPR server with point-to-multipoint connection to the PSTN

For each listed scenario we consider:

- A short description of the solution
- An enumeration of the most important particularities
- The special advantages/disadvantages of the solution (if existing)
- Individual configuration aspects

10.6.1 XPR Server via Tie Trunk without Trunk ID at a PBX



Description:

- The XPR server is connected to the PSTN via a PBX.
- The connection between XPR server and PBX occurs via a tie line and a telematics APL.
- An individual extension range is assigned to the trunk on the PBX side. Its phone number is automatically routed to the XPR server. These extensions are available for assigning telematics services.

Specials:

- The phone number of a telephone (PHONE) and the phone number of the assigned telematics service (e.g. VOICE) are not identical.
- The phone number of a telematics service (e.g. VOICE) can be dialed and thus be addressed internally or externally.

Advantages:

- The existence of the tie trunk between PBX and XPR server is hidden from the user.
- The users do not have to dial a tie line number.
- The telematics service can be addressed internally or externally with the phone number being correctly normalized.

Disadvantages:

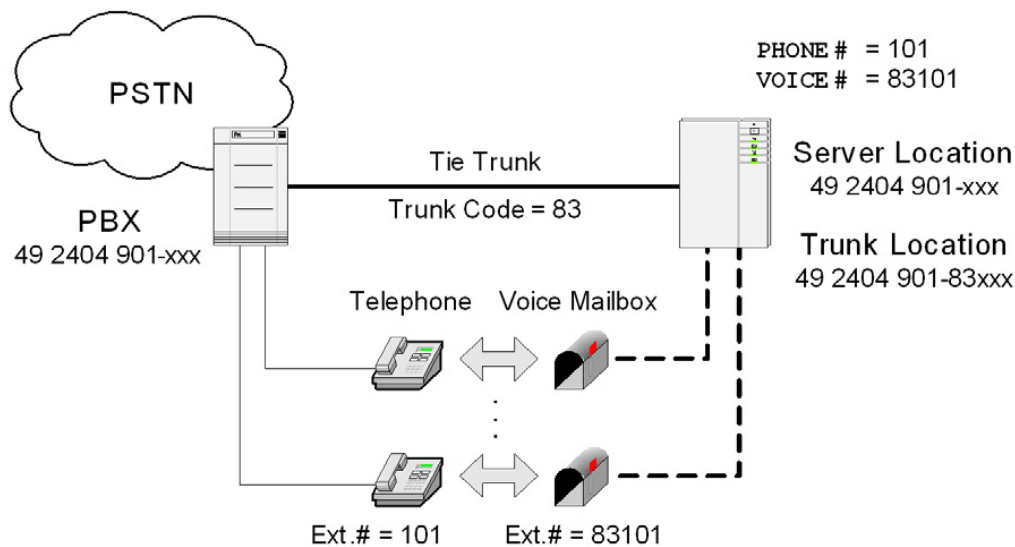
- Additional extensions must be allocated in the PBX for the telematics service.

Configuration:

- The telematics service is configured as usual under the extensions that are configured for the XPR server.
- The telephone extension is assigned to the PHONE# database field, the extension of the XPR extension number range is assigned to the database field of the assigned telematics service (e.g. VOICE#).
- The server location is used as trunk location.

10.6.2 XPR Server via Tie Trunk *with* Trunk ID at a PBX

10.6.2.1 Trunk ID is Part of the XPR User Extension



Description:

- The XPR server is connected to the PSTN via a PBX.
- The connection between XPR server and PBX occurs via a tie line and a telematics APL.
- The routing from the PBX to the XPR server is performed by dialing the tie line ID.

Specials:

- The phone number of a telephone (PHONE) and the phone number of the assigned telematics service (e.g. VOICE) are not identical. The extension of a telematics service starts with the number of the tie line. The telephone extension does not.
- The phone number of a telematics service can be dialed and thus be addressed internally or externally.

Advantages:

- The phone number of a telematics service reflects the structure of the telephone network with its preceding tie line ID.
- The telematics service can be addressed internally or externally with the phone number being correctly normalized.

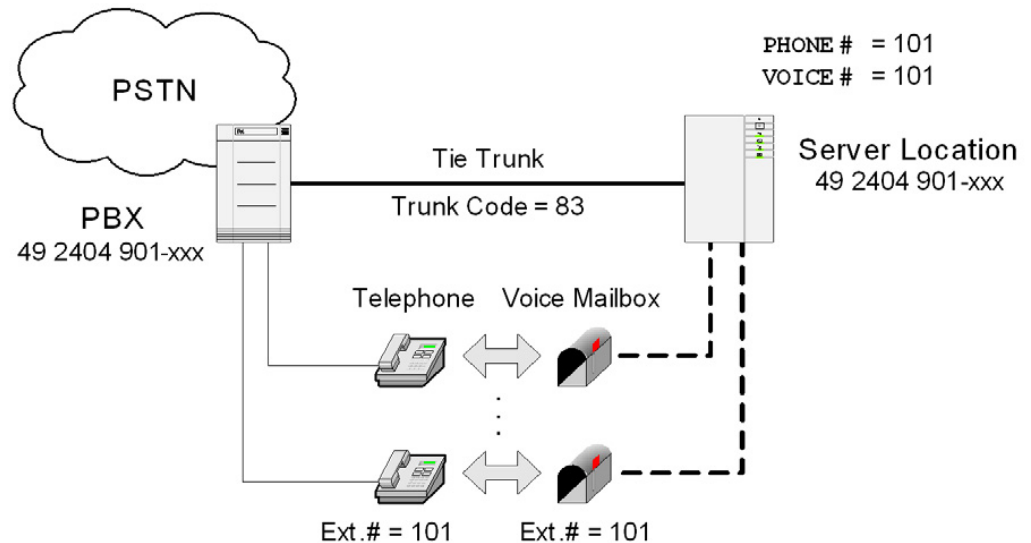
Disadvantages:

- The extension of the telematics service contains the trunk ID. This extension must also be specified for the authentication at the voice mail system.

Configuration:

- A new trunk location must be created on the basis of the server location (see [Section 9.5.2, “Defining a new Location”, on page 396](#)). Within this, the new tie line ID must be supplemented.
- This new location must be assigned to all trunk groups of the respective tie line.
- If the PBX sends phone numbers with the tie line ID to the XPR server, the option **PBX sends Called Numbers with Trunk Code** must be activated.
- The telephone extension is assigned to the PHONE# database field, an extension with preceding tie line ID is assigned to the database field of the assigned telematics service (e.g. VOICE#).
- During the configuration of a voice mail protocol the tie line ID must not precede the respective access numbers.

10.6.2.2 Trunk ID is no Part of the XPR User Extension



Description:

- The XPR server is connected to the PSTN via a PBX.
- The connection between XPR server and PBX occurs via a tie line and a telematics APL.
- The routing from the PBX to the XPR server is performed by dialing the tie line ID.
- The XPR server removes the tie line ID from all phone numbers of this tie line.

Specials:

- The tie line ID is ignored during the configuration of a telephone number (PHONE) and of the phone number of the assigned telematics service (e.g. VOICE). Thus they may be identical.
- The phone number of a telematics service (e.g. VOICE) cannot be dialed directly, as the preceding tie line ID is missing in the (VOICE-) configuration.
- Typically, a user telephone is diverted to a central access number of the telematics service. Here the correct user is then found via the redirecting number (cf. [Section 10.1.5, "Redirecting Numbers", on page 551](#)).

Advantages:

- Users do not have to consider the tie line ID.
- The phone number of a telematics service can correspond to the phone number of the assigned phone device.

Disadvantages:

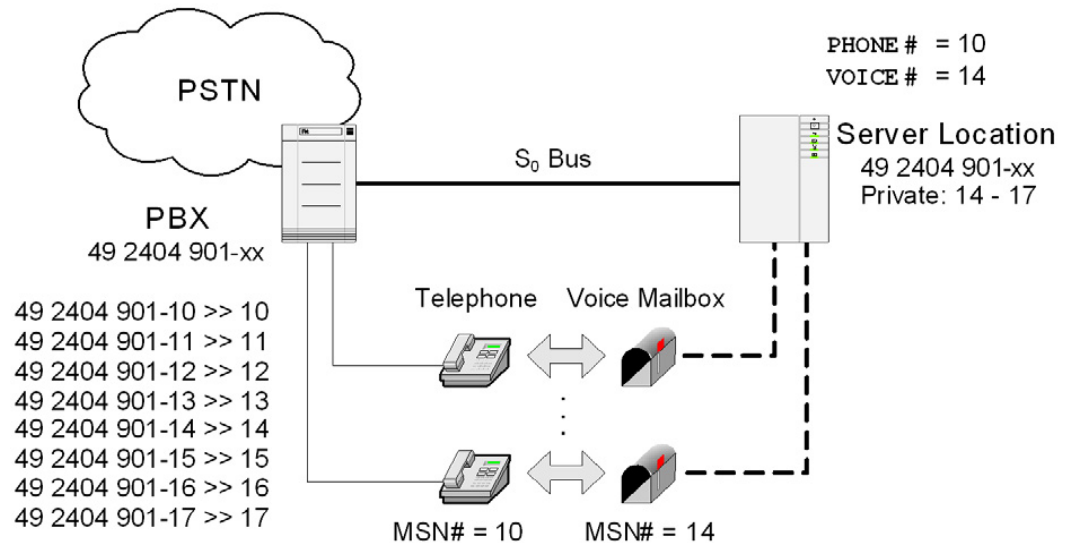
- All phone numbers of the respective trunk ID are incorrectly normalized because of the missing tie line ID. **Since this may cause problems, we advise against the configuration of this scenario!**
- The telematics services cannot be addressed directly via the extensions configured in the XPR server (e.g. in VOICE). This does not matter for installations in which the voice mail system is only addressed in Forward or Direct Access (cf. [Section 10.1.5, "Redirecting Numbers", on page 551](#)).
- It is not possible to configure e.g. the voice mail number without tie line ID, but to indicate the tie line ID for fax numbers in the same trunk groups. If the tie line ID is to be ignored, this is always applicable to all protocols bound to the respective trunk group.

Configuration:

- The server location is used as trunk location.
- The tie line ID must not precede the telematics service extensions (VOICE#, FAX# etc.).
- If the tie line ID is not transferred from the PBX to the XPR server, no further configuration is necessary.
- If the tie line ID is transferred from the PBX to the XPR server, it must be removed from the XPR server. Therefore the variable **SkipCalledNumberDigits** must be added to the respective connect point (see [Section 9.5.3, "Defining a new Variable", on page 398](#)). Its content defines the tie line ID length.

10.6.3 XPR Server via internal S0-Bus at small PBX with MSNs

10.6.3.1 PBX with Point-to-Point Connection to the PSTN



Description:

- The XPR server is connected to the PSTN via a small PBX.
- The PBX possesses a point-to-point connection to the PSTN.
- The connection between the XPR server and the PBX occurs via a S0-Bus and an ISDN APL.
- The PBX automatically converts the point-to-point connection extensions to single internal MSNs.

Specials:

- The phone number of a telephone (PHONE) and the phone number of the assigned telematics service (e.g. VOICE) correspond to internal MSNs and are not identical.

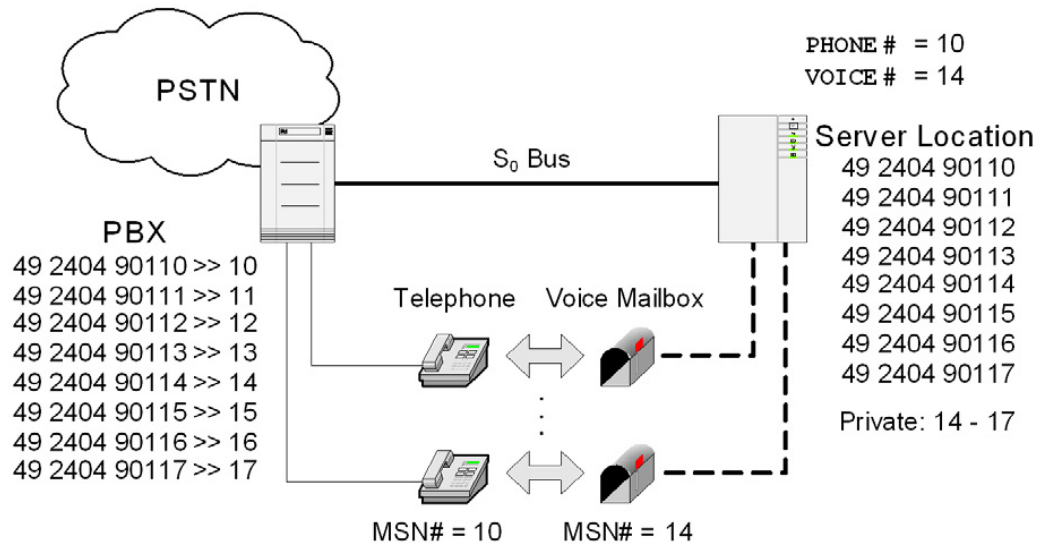
Disadvantages:

- A telematics service cannot be addressed internally and externally via the same phone number. Internally the MSN of the telematics service, externally the extension assigned to the MSN must be dialed.

Configuration:

- The telematics service is configured as usual under the MSNs that are configured for the XPR server.
- The telephone MSN is assigned to the PHONE# database field, an MSN of the XPR extension number range is assigned to the database field of the assigned telematics service (e.g. VOICE#).
- The server location is used as location.
- The point-to-point connection is defined in the location as usual.
- The variable **PrivateNumbers** must be added to the location as number range list (see [Section 9.5.4.2, "Defining a Number Range List as Variable", on page 402](#)). In it you need to define the internal MSNs that are assigned to the XPR server.
- The length of the internal MSNs must be assigned to the variable **MaxExtensionLength**.

10.6.3.2 PBX with Point-to-Multipoint Connection to the PSTN



Description:

- The XPR server is connected to the PSTN via a small PBX.
- The PBX possesses a point-to-multipoint connection to the PSTN.
- The connection between the XPR server and the PBX occurs via a S0-Bus and an ISDN APL.
- The PBX automatically converts the point-to-multipoint connection MSNs to single internal MSNs.

Specials:

- The phone number of a telephone (PHONE) and the phone number of the assigned telematics service (e.g. VOICE) correspond to internal MSNs and are not identical.

Disadvantages:

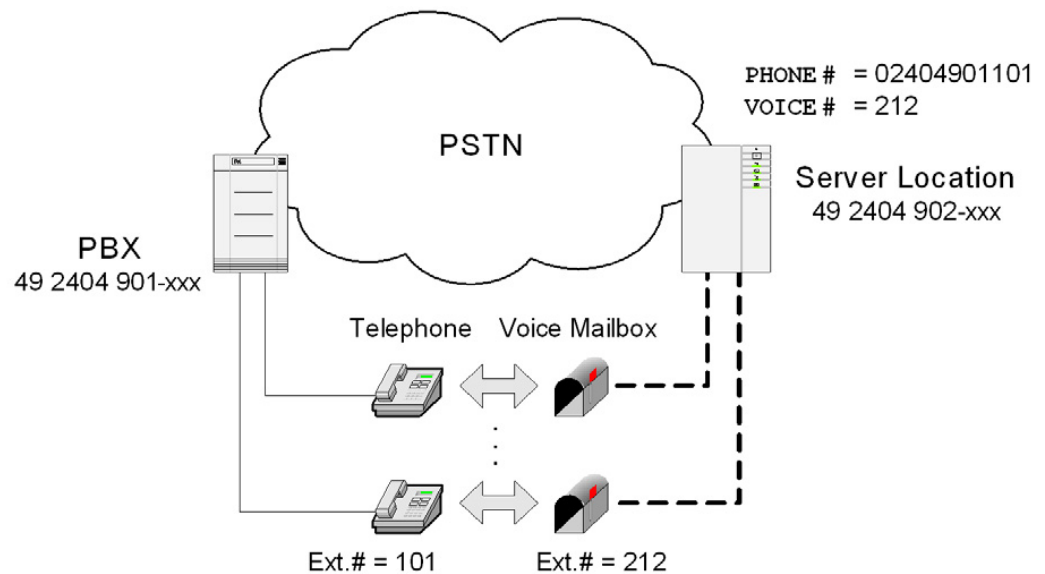
- A telematics service cannot be addressed internally and externally via the same phone number. Internally the MSN of the telematics service, externally the MSN of the point-to-multipoint connection assigned to the internal MSN must be dialed.

Configuration:

- The telematics service is configured as usual under the MSNs that are configured for the XPR server.
- The telephone MSN is assigned to the PHONE# database field, an MSN of the XPR extension number range is assigned to the database field of the assigned telematics service (e.g. VOICE#).
- The server location is used as location.
- The point-to-multipoint connection MSNs are defined as phone number range in the location.
- The variable **PrivateNumbers** must be added to the location as number range list (see [Section 9.5.4.2, "Defining a Number Range List as Variable", on page 402](#)). In it you need to define the internal MSNs that are assigned to the XPR server.
- The length of the internal MSNs must be assigned to the variable **MaxExtensionLength**.

10.6.4 XPR Server without PBX at the PSTN

10.6.4.1 XPR Server with Point-to-Point Connection to the PSTN



Description:

- The XPR server is connected to the PSTN via a point-to-point connection. No external prefix is required.

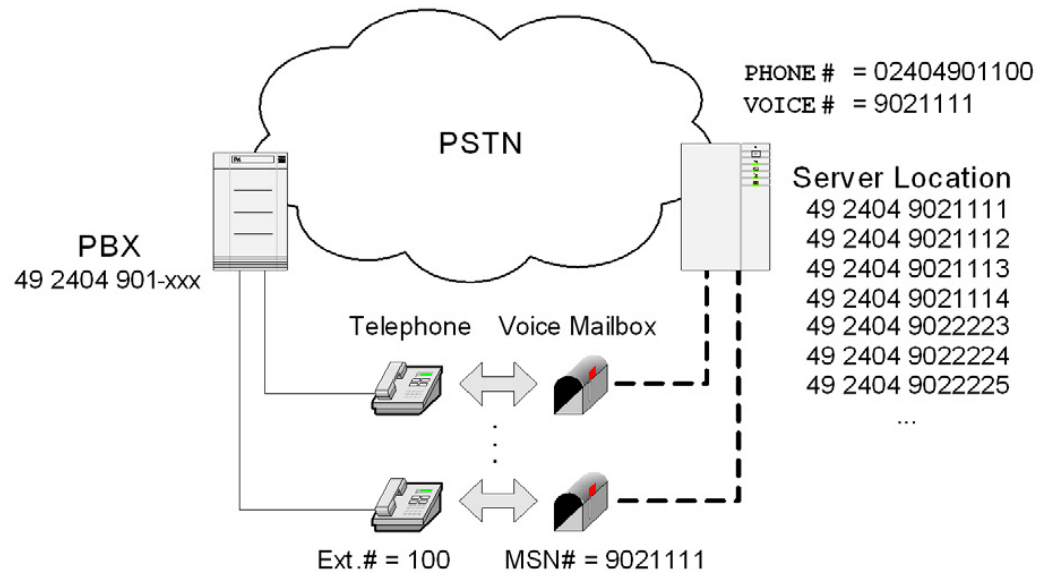
Specials:

- The extension of a telematics service corresponds to a phone number that can be dialed after the phone number of the individual point-to-point connection.

Configuration:

- The server location is used as location.
- The extension length must be assigned to the variable **MaxExtensionLength**.
- The variable **DirectLine** must be added to the respective connect point (see [Section 9.5.3, "Defining a new Variable", on page 398](#)). The value **true** must also be assigned.

10.6.4.2 XPR Server with Point-to-Multipoint Connection to the PSTN



Description:

- The XPR server is connected to the PSTN via a point-to-multipoint connection. No external prefix is required.

Specials:

- The phone number of a telematics service corresponds to an MSN of the point-to-multipoint connection.

Configuration:

- The server location is used as location.
- No **originator address** must be assigned to the location.
- The **number range** must be added to the location. All MSNs of the point-to-multipoint connection must be assigned to it.
- The value **0** must be assigned to the variable **MaxExtensionLength**.

10.6.5 Remarks concerning the internal Phone Number Length

The internal phone number length (**MaxExtensionLength**) can be defined individually for each location. It should correspond to the maximum length of *all* internal phone numbers. In addition to the actual phone numbers you must also consider the tie trunk numbers.

If the internal phone number length is greater or equal to the phone number length of the local area network, problems might come up. Localized local telephone network numbers are wrongly treated as internal phone numbers in such a case and consequently incorrectly normalized.

A workaround could be as follows:

- The global variable **UIDialAlwaysArea** is set to **true**. Thus also local telephone network numbers are always localized with area code. For the normalization of numbers that are entered via GUI or TUI, the user always needs to enter the local prefix. Setting the variable **DialAlwaysArea** has the same effect, but here all NCO rules are changed and not only the user interface rules.
- Optionally, it is possible to dial the external prefix for all external calls. In this case the option **GUIUserDialsExtPrefix** or **TUIUserDialsExtPrefix** must be set to **true**.
- If only a few local telephone network numbers are affected by the problem (e.g. the headquarters of a big company in a large city), they can be excluded on purpose from the normalization of internal numbers.

For this

- a number range list with the corresponding numbers can be defined in a global NCO variable and excluded from normalization by means of a phone number range condition

or

- a batch condition can be used to selectively exclude such numbers.

10.6.6 Remarks on Number Ranges

The default configuration assumes that all extensions following the originator address are assigned to the location as numbers that can externally be reached.

If not all extensions of an originator address are available and the rest of the numbers is used by a third party, a number range must be configured. This defines the extensions that can actually be used.

Therefore another entry of the type 'Range Code' is added to the location. The numbers that can externally be reached are entered there. All numbers that have not been configured in the range are now considered as internal, private numbers that cannot be externally reached.

10.7 Specific Solutions with the Telematics APL

10.7.1 IP APL and the HiPath 3000

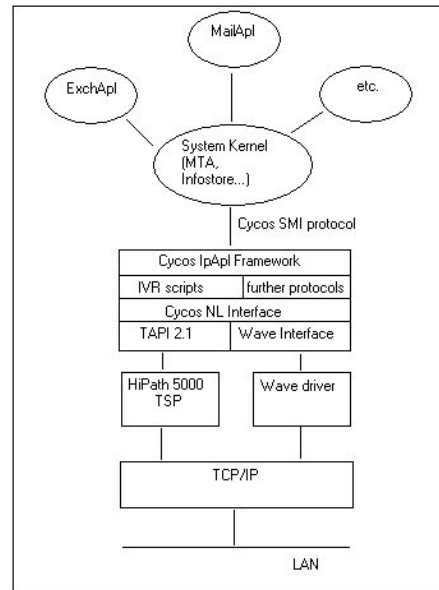
Prerequisite for integrating a HiPath 3000 is the installation and configuration of the HG 1500 module, also known under the name *Hicom Lan Bridge*.

It can be used after the configuration, being able to replace the conventional boards for the services *Voicemail* and *Fax*.

Bind the extensions configured in the HiPath 3000 to the corresponding protocols. As protocols, *PhoneMail* or another voicemail protocol and *Vogue* are supported.

10.7.2 IP APL and the HiPath 5000

In connection with the HiPath 5000 communication platform the IP APL works like a voice mail server. The IP APL is compatible to the TSP and Wave driver by Unify GmbH & Co. KG. The IP APL functionalities depend on the features that Unify GmbH & Co. KG have integrated in the respective TSP and Wave driver.



MTA - Message Transfer Agent
 SMI - Standard Message Interface
 IVR - Interactive Voice Response
 NL Interface - Network Layer Interface
 TAPI - Telephony Application Programming Interface
 TSP - Telephony Service Provider

The IP APL calls the TAPI of the HiPath 5000 TSP. The TAPI recognizes the addressing mechanism of the IP APL. Thus the IP APL can communicate with the TSP via the TAPI. All HiPath-H.323 lines are opened. Wave applications are linked to these lines. The IP APL sends and receives data via these applications.

The NL interface of the XPR server is the link between the line layer of the interface and the protocol layer. The line layer is in charge of hardware and network functions, in this case TAPI. On the protocol layer e.g. IVR scripts are implemented. SMS protocols are currently not supported.

10.8 Creating a new SIP Certificate for the XPR Server

You need to employ TLS to encode the SIP-based communication between XPR server and the connected PBX. To this the IP APL needs a corresponding client certificate that identifies it as authorized communication partner against the PBX.

NOTE:

In the following steps we will create the new certificate with the Open Source program OpenSSL. You find this tool under *<XPR Install>\SDKTools*.

NOTE:

The steps 2 and 3 of the following description can usually only be performed by the OpenScape Voice system administrator.

How to create a new client certificate.

1. Execute the following lines as an OpenSSL command to create a new certificate request:

```
openssl req
-newkey rsa:1024
-sha1
-keyout srvkey.pem
-out srvreq.pem
-nodes
-config openssl.cnf
```

NOTE:

for parameter config you can specify the full path of the openssl.cnf file, e.g. `-config \my_confssl\openssl.cnf`

Also instead of specifying the `-config` option you can define the environment variable `OPENSSL_CONF` which contains the full path of openssl.cnf file.

an easy example for openssl.cnf looks like:

```
[ req ]
```

```
distinguished_name = req_distinguished_name
```

```
[ req_distinguished_name ]
```

```
countryName = Country Name (2 letter code)
```

```
countryName_default = US
```

countryName_min	= 2
countryName_max	= 2
localityName	= Locality Name (eg, city)
organizationalUnitName	= Organizational Unit Name (eg, section)
commonName	= Common Name (eg, YOUR name)
commonName_max	= 64
emailAddress	= Email Address
emailAddress_max	= 40

for more information about openssl.cnf files, please refer to the openssl documentation.

The following files have been newly created in the folder of the OpenSSL program:

- Pair of keys `srvkey.pem`
- Certificate request `srvreq.pem`.

2. From the root certificate `root.pem` of OpenScape Voice copy the portion of the certificate and save it in a new text file with the name `rootcert.pem`.

You find the root certificate `root.pem` on the OpenScape Voice computer system in the directory `/usr/local/ssl/certs`.

IMPORTANT:

You need to store the certificate without the private key in an individual certificate file for the following reason:

When signing the new pair of keys at a later date you export the certificate file from OpenScape Voice. The private OpenScape Voice key, however, must never be exported from the system for security reasons.

3. Execute the following lines as an OpenSSL command to create a new certificate from the certificate request and the pair of keys:

```
openssl x509
  -req
  -in srvreq.pem
  -sha1
  -extensions certificate_extensions
  -CA rootcert.pem
  -CAkey root.pem
  -CAcreateserial
  -out srvcert.pem
  -days 3650
```

4. Execute the following OpenSSL command to sign the newly created certificate with the root certificate of OpenScape Voice:

```
cat srvcert.pem root.pem > srv.pem
```

The new client certificate `xpr.pem` has now been created in the folder of the OpenSSL program.

You have now created a new client certificate for the XPR server, which has been signed by the root certificate authority of OpenScape Voice.

So that the XPR server uses the new client certificate, you need to configure the SIP device of the IP APL as follows:

- Activate the **TLS** option on the **SIP** tab
- Configure the certificate settings on the **Security** tab.

10.9 Configuration Reference for ISDN Connections (ISDN APL)

The configuration of the ISDN APL is performed from the XPR monitor. The basis is the TeleCfg library of the XPR server providing unified operation of all telematics APLs and services (cf. [Section 10.1.1.2, “The Modules TeleCfg and TeleCfg API”](#), on page 526).

NOTE:

For the Telematic APL configuration the NCO configuration files of the XPR server are accessed via the *NCOAdmin*. Please make sure that the *NCOAdmin* used and the NCO configuration files are on hand in the same version. If this is not the case, a warning points to this incompatibility at the beginning of the telematics configuration.

To start the ISDN APL configuration, select the **IsdnApi > Set options** menu option in the modules window of the XPR monitor. Via the alternative menu item **Set extended options** additional settings can be made via further tabs. Sections describing this extended functionality are labeled with the addition (Extended options).

In most cases the regular setting options for the APL configuration are sufficient.

Since all modifications are dynamically effected, a restart of the ISDN APL is not necessary after changes have been made.

The information contained in this chapter is divided into the following sections:

- [Protocols](#)
- [General Voicemail Settings \(Voicemail\)](#)
- [Extensions](#)
- [Devices \(Advanced Settings\)](#)
- [Locations](#)
- [Resources \(Advanced Settings \)](#)
- [Outbound \(Advanced Settings\)](#)

10.9.1 Protocols

Protocols

Protocols are services supported by the various APLs. The ISDN APL supports the following protocols:

- Sending/receiving Fax G3
(see [Section 10.4.6, “Fax G3”, on page 702](#))
- Fax G3 polling for a Fax-on-Demand (FOD) server
(see [Section 10.4.8, “Fax G3 Polling”, on page 715](#))
- Sending/receiving Fax G4
(see [Section 10.4.9, “Fax G4”, on page 716](#))
- SMI protocol
(see [Section 10.4.13, “SMI”, on page 734](#))
- Message Waiting Indication (MWI)
for MWI information transmission via QSIG, CorNet N and CorNet NQ
(see [Section 10.4.17, “Message Waiting Indication \(MWI\)”, on page 739](#))

NOTE:

The *Message Waiting Indication* protocol is now an integral component of the ISDN APL and thus automatically available after the installation of the ISDN APL.

While the MWI protocol integrated in the APL only supports the MWI information transmission in the D-channel, the *mwivoice.e* script can also transfer MWI information via a phone number to be dialed. The latter is, for example, required for the MWI connection of a Bosch Tenovis PBX.

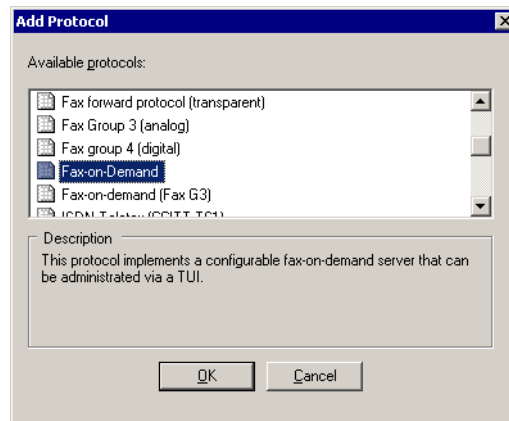
- SMS protocol
(see [Section 10.4.19, “SMS \(TAP or UCP Protocol\)”, on page 748](#))
- CTI Computer Telephony Integration
(see [Section 10.4.21, “CTI Computer Telephony Integration”, on page 757](#))

Scripts

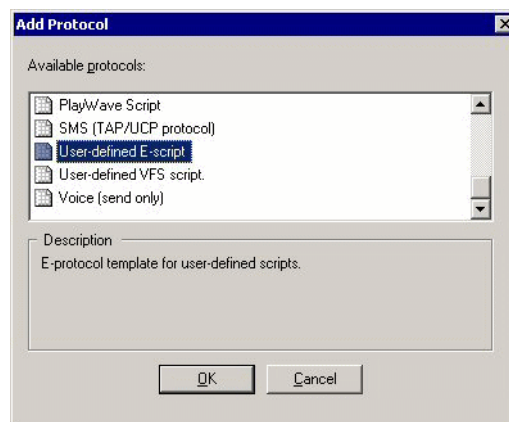
With the help of the script language E of the Unify Software and Solutions GmbH & Co. KG, further individual protocols for the XPR server can be implemented. As with its predecessor VFS, user-specific voice and fax mailboxes, fax-on-demand servers etc. can be realized. In contrast to VFS, E is a more powerful language with a larger API, implementing nearly all XPR-specific features.

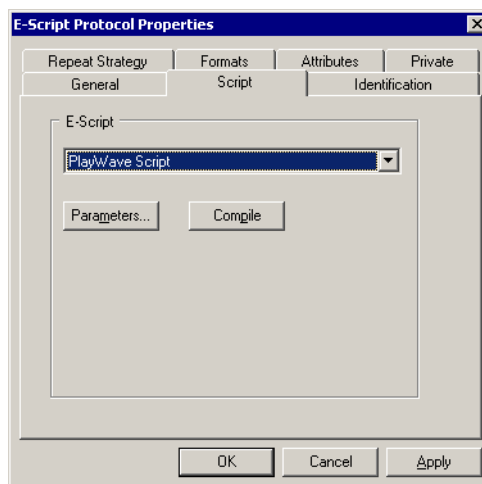
Via the **Add** button in the toolbar of the *Protocols* settings tab scripts can be configured in two ways:

- Adding the desired script by name in the *Add Protocol* dialog.



- Adding a user-defined script in the *Add Protocol* dialog and subsequent specification of the desired script in the configuration tab *Script* below protocol properties.





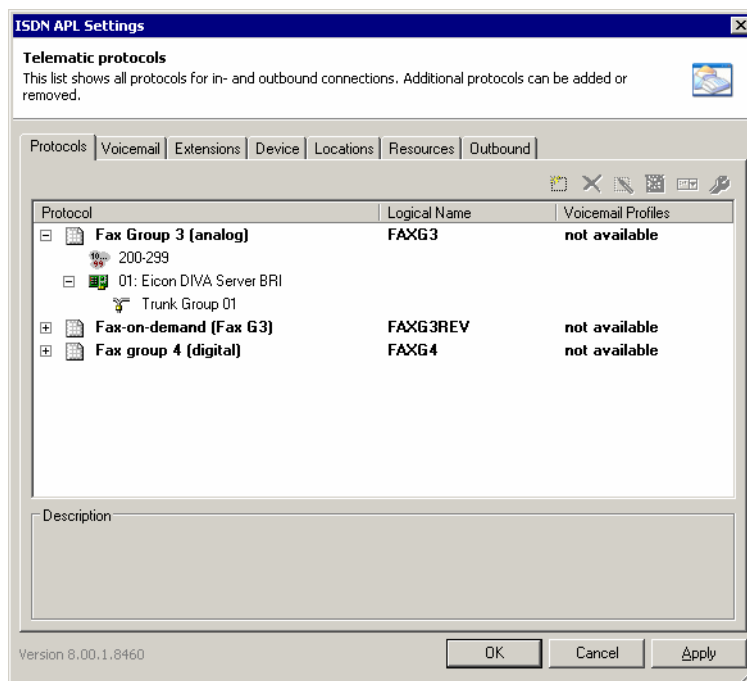
Via the **Parameters...** button in the configuration tab *Script* you will then come to the actual script configuration. Via **Compile** you can compile the script. This is only required when you have developed new scripts yourself which are thus present in the source. In most cases an already compiled object file is available which can simply be executed by the server.

The XPR server standard scope of delivery already includes scripts the configuration of which is described in [Section 10.4, "Protocols of the XPR Server", on page 593](#).

The ISDN APL supports the following scripts:

- Evo as the latest voice mail script with integrated speech recognition
(see [Section 10.4.1, “Evo”, on page 594](#))
- Ergo as modern voice mail script
(see [Section 10.4.2, “Ergo”, on page 617](#) for the configuration and the user manual *Ergo* for the Ergo operation)
- PhoneMail
(see [Section 10.4.3, “PhoneMail”, on page 638](#) for the configuration, and the *PhoneMail* user manual for the operation of PhoneMail)
- Voicemail VMS
(see [Section 10.4.4, “Voicemail VMS”, on page 678](#) for the configuration and the *VMS* user manual for the operation of Voicemail VMS)
- Fax G3 Post-Dialing
(see [Section 10.4.7, “Fax G3 Post-Dialing”, on page 711](#))
- Standard Fax Polling Server
(see [Section 10.4.10, “Fax-on-Demand Server Script \(Fax-on-Demand\)”, on page 719](#))
- Single number
(see [Section 10.4.12, “Single Number”, on page 730](#))
- Voice for playback via telephone
(see [Section 10.4.14, “Voice”, on page 735](#))
- Playwave
(see [Section 10.4.15, “PlayWave”, on page 736](#))
- CTI Light
(see [Section 10.4.22, “CTI Light”, on page 759](#))

The XPR server does not distinguish functionally between protocol and scripts. Accordingly, in the following the collective term protocol is used for both.



The protocols list shows all currently configured telematics protocols. If the protocol display is expanded by the plus sign before the respective list entry, the associated device and trunk group is displayed as well.

Protocols already installed on the XPR server are added via the **Add** icon. Protocols already added can be **Removed**, **Deactivated** and **Activated**. The **Deactivate** icon adapts to the status of the selected entry and changes to **Activate** when the selected protocol has been deactivated before.

If the protocol desired for configuration is not displayed in the selection list after you have clicked **Add**, it has not yet been installed on the XPR server. The subsequent installation is performed in two ways depending on the protocol:

- Protocols integrated in the setup – such as the *PhoneMail* script – are installed belatedly by executing the XPR setup anew. In the setup dialog *Select components* under the menu item **Services** select the desired protocol.
- Project - specific protocols – such as the AMIS script – are either contained in the `XpressionsInstallAdd-On\` directory of the XPR product data carrier or can be obtained from your system integrator on request. Via the corresponding installation file the required protocol is individually installed belatedly.

After the respective reinstallation the protocol is available in the selection list of the dialog *Add Protocol*.

Parameters of the selected protocols can be displayed and modified through selection of the **Edit** icon. These properties are described in detail in [Section 10.4, “Protocols of the XPR Server”, on page 593](#).

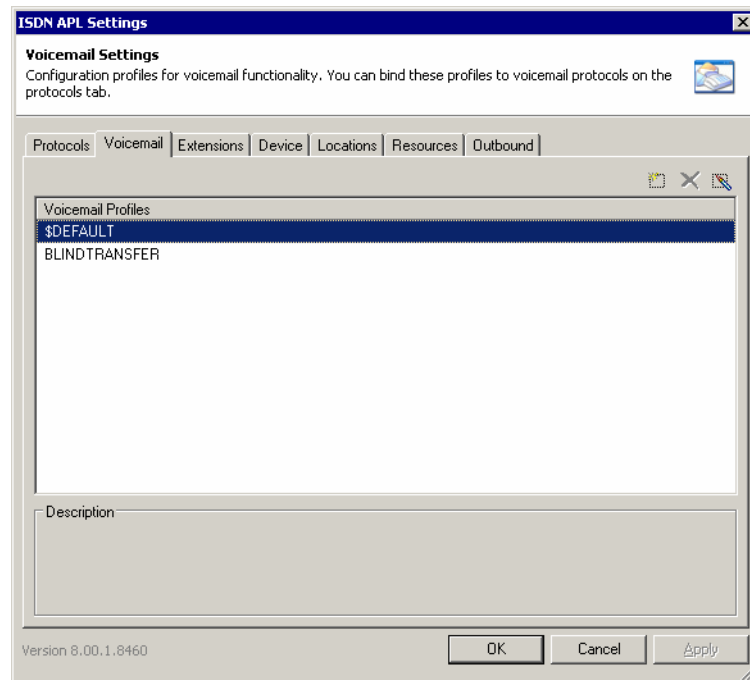
The **Select Profile** icon sets the entry in the **Voice mail profiles** column in an editable state for the selected protocol.

The **Script Parameters** icon opens the configuration dialog for the selected protocol. In this dialog the associating script parameters can then be edited.

Parameters of the selected protocols can be displayed and modified through selection of the **Properties** button. These properties are described in detail in [Section 10.4, “Protocols of the XPR Server”, on page 593](#).

10.9.2 General Voicemail Settings (Voicemail)

Newer voicemail systems, such as PhoneMail, support a shared database layout for globally used features, which means that this configuration data can be globally configured for all these systems. **Configuration profiles** can be configured with these global settings for simplification. Such a profile can then be assigned to a protocol in the *Protocols* tab in the **Voice mail profiles** list column.



During the installation of the XPR server the default profile `$DEFAULT` is configured. The default settings in the `DEFAULT` profile cannot be modified so that you can always return to them.

Another profile can be generated via the **Add** button. At the beginning this profile has the settings of the `$DEFAULT` profile. Existing profiles can be modified with **Edit** or removed with **Delete** with the exception of `$DEFAULT`.

IMPORTANT:

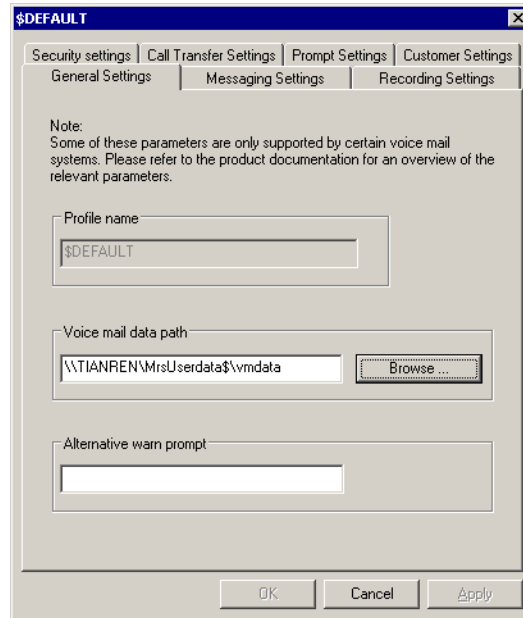
Not all voice mail systems support all provided setting options. If a corresponding feature is intended in the respective voice mail system, it is set according to the configuration. Settings for features that are not supported are ignored by the respective voice mail system.

The configuration dialog for profiles consists of the parameter tabs *General Settings*, *Messaging Settings*, *Recording Options*, *Security Settings*, *Call Transfer Settings* and *Prompt Settings*.

Let's have a closer look at them.

10.9.2.1 General Settings

The **Profile name** field defines the name with the help of which this configuration profile can be assigned to a protocol later. The name of the default profile `$DEFAULT` cannot be changed.



All greetings recorded by the user or system greetings recorded by the administrator are stored in the sub-directory `vmdata` of the invisible directory `<XPR Install>\MrsUserdata$`. Via the **Voicemail data path** field a profile-specific directory can be defined if required.

You can replace the audio warning that sounds a few seconds before the end of a recording by entering an announcement in the **Alternative warn prompt** field.

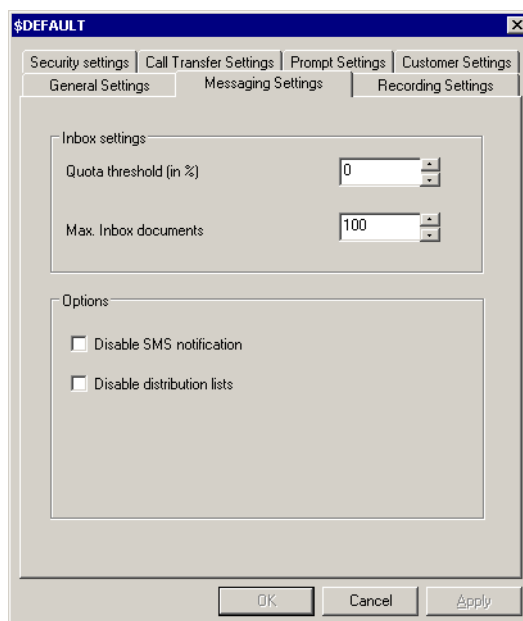
IMPORTANT:

Ergo does not support the **Alternative warn prompt** feature.

IMPORTANT:

EVO does not support the **Alternative warn prompt** feature.

10.9.2.2 Messaging Settings



In the XPR server database, maximum permissible quotas can be defined for users' inboxes. In the **Quota threshold** field a percent-based quota threshold can be defined for a fill level warning in this context. If the inbox of a user reaches this relative fill level, the TUI informs him/her that his/her maximum permissible data amount will soon be reached.

IMPORTANT:

The quota threshold is only active when the MTA for quotas is configured.

NOTE:

Configuring this option in True Unified Messaging solutions does not make sense. In this type of environments the Microsoft Exchange or Lotus Notes message store is used, which is not monitored by the MTA quota feature.

In **Max. Inbox documents** the number of messages offered by the TUI is restricted. Consequently, you will only receive the first n messages of the sorting set in the Web Assistant. The number n corresponds to the value set here. This restriction is valid independently for each configured user folder.

IMPORTANT:

First, filtering occurs according to the number of inbox documents set here. Then, sorting occurs exclusively via these messages.

In the *Options* section the indicated features **SMS Notification** and **Distribution Lists** are enabled or disabled.

IMPORTANT:

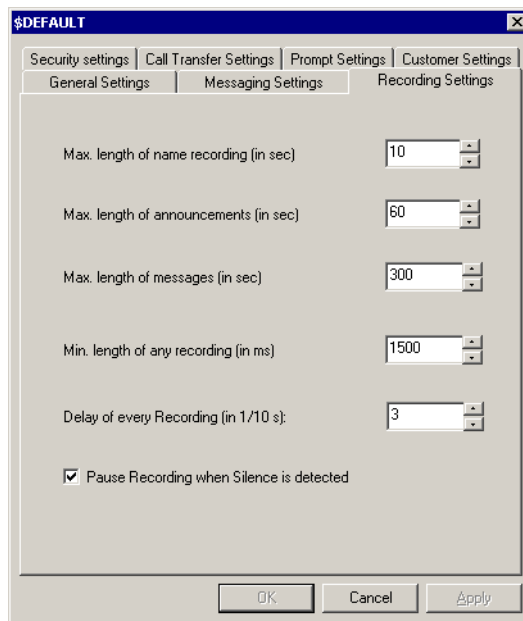
Setting the option **Disable distribution lists** is not possible for VMS. For this script the distribution lists cannot be disabled.

IMPORTANT:

Setting the option **SMS notification** is not possible for PhoneMail. For this script the SMS notifications cannot be disabled.

10.9.2.3 Recording Settings

In this tab settings for the maximum length of recordings are made. Left voice mails can thus not unintentionally cause large files.



The **Max. length of name recording** option limits the length of name recordings. Such a name recording can be recorded by mailbox owners in order to inform the caller about the name of the mailbox owner. This helps the caller to make sure that he/she has dialed the correct number. The entry is made in seconds.

Via the option **Max. length of announcements** the length of user-defined announcements and greetings that can be played via the TUI is limited. The entry is made in seconds.

The **Max. length of messages** limits the length of a message a caller can leave. Shortly before the recording time is up, the caller receives a warning. The entry is made in seconds.

The option **Min. length of any recording** defines the recording time a recorded message, name recording or announcement must have at least to be saved. Thus, e.g. no new message is stored if the caller hangs up immediately. The entry is made in milliseconds.

Via the option **Delay of every Recording** the start of recordings is delayed. This avoids e.g. recording of parts of the announcement that was played last at the beginning of a new recording. The entry is made in 1/10 seconds. Its default value is 3.

Via **Pause Recording when Silence is detected** you can make the system automatically stop a recording after detecting a speaking pause. The user is then automatically taken to the menu where he/she can play the recording or, after pressing a button, continue it.

IMPORTANT:

The **Pause Recording when Silence is detected** option is permanently activated in PhoneMail and VMS and cannot be disabled.

10.9.2.4 Security Settings

The **Min. telephone password (PIN) length** option specifies the minimum number of digits in a new PIN. The longer the PIN, the greater the security it provides. On the other hand, users can often remember passwords that are much too long only with the help of undesired notes. An entry in this field is thus always a compromise of security requirements and usability.

Via the **Number of stored telephone passwords (PIN)** option the encrypted storage of a defined number of the PINs used last is activated. If a user modifies his/her PIN, this information is always referred to for a check. If the new PIN is

found in the stored entries, the system rejects it as invalid and prompts the user to reenter the PIN. So users really need to enter a new PIN and cannot toggle between two old PINs. Entering **0** deactivates this function.

IMPORTANT:

The option **Number of stored telephone passwords (PIN)** is not supported by Ergo.

IMPORTANT:

The option **Number of stored telephone passwords (PIN)** is not supported by EVO.

The option **Telephone password (PIN) expiration** defines a number of days after which a PIN is considered invalid and the user is prompted to enter a new one. Entering **0** deactivates this function.

NOTE: PhoneMail supports a maximum of 180 days that can be specified for the **Telephone password (PIN) expiration** option.

IMPORTANT:

The option **Telephone password (PIN) expiration** is not supported by Ergo.

IMPORTANT:

The option **Telephone password (PIN) expiration** is not supported by EVO.

The **Max. tolerated login failures** option defines which number of failed login attempts activates the measures selected in the section *Sanctions on too many invalid logins*. Furthermore, the system ends the respective conversation when this value has been reached, so that it could be necessary to set up a new connection to the voice mail system. If the option **Lock voicebox** is activated, a new attempt to log in is not possible. In this case the administrator needs to re-enable the voice mailbox first. This can be done by resetting the XPR database field **VM_LOGIN_FAILED** of the user concerned and at the same time setting a new value for the PIN if the subscriber has forgotten it.

IMPORTANT:

In EVO the option **Lock voicebox** is always active and *cannot* be disabled.

The **Default PIN** field defines a default PIN each user may use for his/her first login at the system.

IMPORTANT:

To avoid unauthorized access, users are forced to change the default PIN to a user-individual PIN when logging on to their voice box for the first time.

NOTE:

When creating a new user the administrator can change the default PIN to another, individual PIN. In this case the relevant user will not be forced to change the default PIN to a user-individual PIN during the initial logon to his/her voice box.

We expressly recommend this procedure.

Each user can define up to three trusted numbers in the Web Assistant (cf. also the *Web Assistant* manual). If the voicebox of the relevant user is then queried by one of those numbers, identification by specifying the configured PIN is omitted. This feature must be released in the voicemail settings with the **Allow usage of Trusted Numbers** option.

IMPORTANT:

In VMS the option **Allow usage of Trusted Numbers** is not supported.

When using trusted numbers please note:

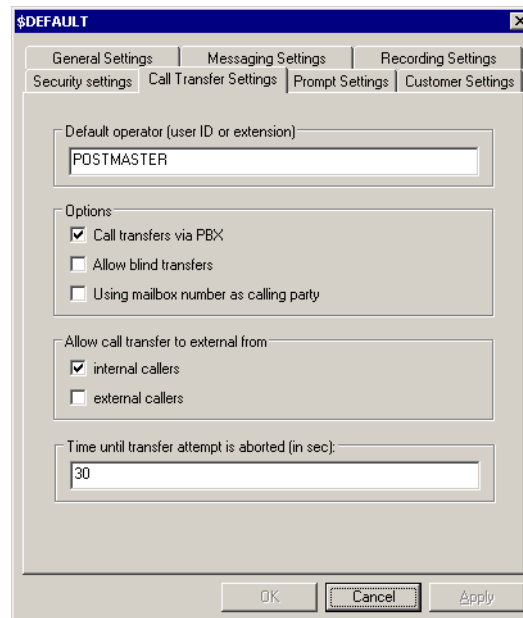
- For security reasons, different XPR users cannot define identical trusted numbers.
- If the voice mail system is called from a connection that has been defined as trusted number, the mailbox access is no longer secured with a PIN. Please keep this fact in mind for the release of this feature and the selection of trusted numbers.
- To identify a trusted number via the voice mail system the phone number of the caller's device must be transmitted. This is only possible for digital PBX systems and must possibly be released.
- With some gateway operators that route VoIP calls to the fixed or mobile network you find a security hole. They allow their users to specify an arbitrary phone number as individual phone number. These users can

consequently query each mailbox that is accessible via trusted numbers. As long as this security hole exists we recommend not to use trusted numbers.

NOTE:

If the PhoneMail protocol callback access is dialed from a trusted number, continuous messages output is active by default. This setting can be modified with the **-noctn** PhoneMail parameter.

10.9.2.5 Call Transfer Settings



A caller can be forwarded from his/her voice box to a postmaster account if required. Therefore in the **Default operator** field the respective extension of user ID of this account must be entered. In the latter case the XPR server searches for the corresponding phone number via the XPR user database.

The **Call transfers via PBX** option defines whether forwarding a call is performed within the PBX (*Path Replacement*). However, this is not always possible and depends of the scope of services of the applied PBX. If this option has not been

activated, a caller that is to be routed externally by the XPR server is routed via a second parallel channel back to the PBX and from here to the public telephone network.

IMPORTANT:

If the applied PBX does not support the *Path Replacement* feature, the option **Call transfers via PBX** must not be activated.

Via the **Allow blind transfers** option this transfer type is activated. Blind transfer means that the availability of the destination is not checked at the time of the transfer. Thus a caller might receive a busy signal or even be rerouted to the original voice mailbox.

NOTE:

The Blind Transfer feature is only available with the PBX protocols Cornet N and Cornet NQ by default. To use Blind Transfer also for other protocols, it must be configured manually (cf. [Section E.20.2.3, "Private \[REG_MULTI_SZ\]", on page 1920](#)).

NOTE:

Settings of the PBX used may prevent calls from being forwarded via blind transfer; even if the **Allow blind transfers** option is active.

In the HiPath 3000, the decision whether calls are forwarded via supervised transfer or by blind transfer is made via system settings. The **Allow blind transfers** option does not take any effect then.

With call rerouting to a voice mailbox the call number of the original caller is passed on to the PBX as originator ID by default. In this case the voice mailbox owner as the actual causer cannot be charged for the reroutings.

If the **Using mailbox number as calling party** option is activated, the mailbox number of the called voice mailbox is passed on to the PBX as originator ID.

IMPORTANT:

The **Using mailbox number as calling party** option is not supported by VMS.

The options **Allow call transfer to external from ...internal callers** or **...external callers** define whether a caller can be routed externally. In this way, a mailbox owner can offer the caller alternatives to leaving a message. For example, the caller can be connected to an external telephone, a deputy or the operator.

IMPORTANT:

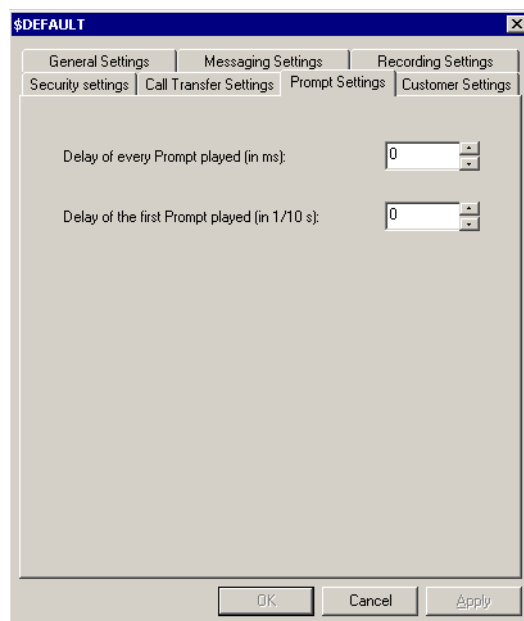
The option **Allow call transfer to external from ...internal callers** or **...external callers** is not supported by VMS.

The **Time until transfer attempt is aborted** defines a period after which the attempt to establish a transfer is abandoned. The entry is made in seconds.

IMPORTANT:

The option **Time until transfer attempt is aborted** is not supported by VMS.

10.9.2.6 Prompt Settings



The option **Delay of every Prompt played** defines a minimum delay for each announcement.

In certain PBX system types, prompts which directly follow a keypad entry may be slightly truncated at the beginning when replayed. If this behavior occurs with your PBX it can be leveled out by defaulting a suitable delay period. The delay can be set from 0 to 9999 milliseconds. Default set is 0 milliseconds, thus no delay.

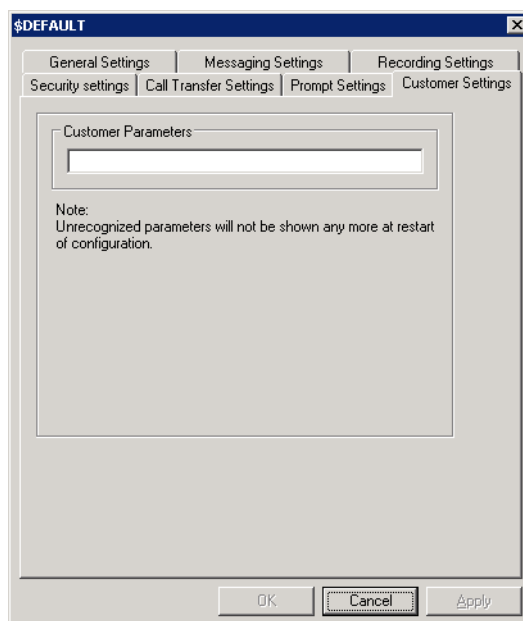
Via the option **Delay of the first Prompt played** a further delay can be defined for the first voice mail system announcement after each connection setup. The entry is made in 1/10 seconds.

NOTE:

In case of PhoneMail, the customer parameter *wlcsst* has precedence over the settings performed here.

The background of this option is that different PBX in a voice mail system signalize by establishing the D-channel that the first system announcement can be started. The B-channel required for the transmission is only established with delay, so that the first greeting is played back respectively truncated for the caller.

10.9.2.7 Customer Settings



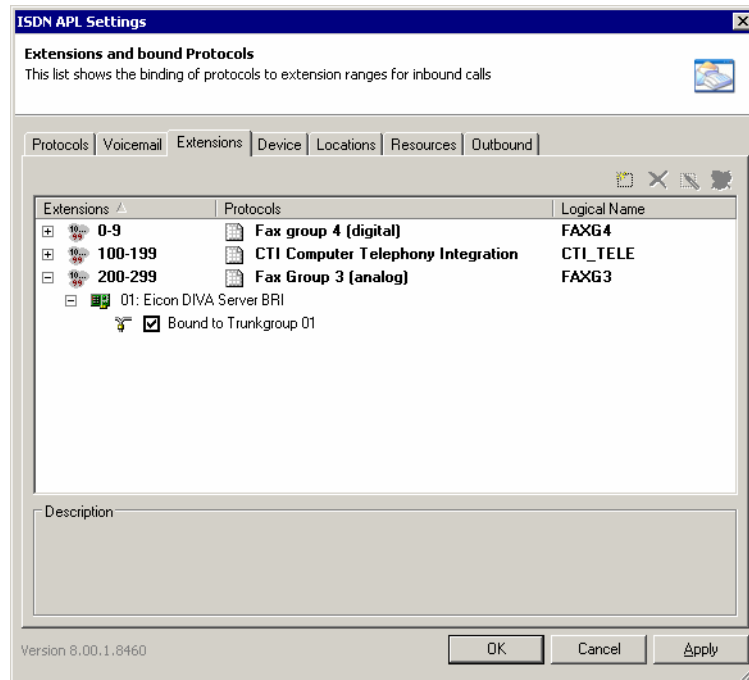
Here you can perform system-wide voice mail settings. This requires a customer-specific adjustment of the PhoneMail script to which the relevant voice mail profile is assigned.

Features can also be enabled on a project-specific basis by entering the relevant parameters. Please refer to the descriptions of the customer-specific parameters for the respective protocols to learn which features are available in this way (cf. [Section 10.4, “Protocols of the XPR Server”, on page 593](#)).

10.9.3 Extensions

In the configuration tab *Extensions* the extension number ranges for the installed protocols are assigned. Incoming calls are bound to the various protocols through the use of extension number ranges.

No assignment to an extension number range is necessary for outbound communication.



The extensions list shows all extension ranges currently configured with their assigned protocol. If the extension display is expanded by the plus sign before the respective list entry, the associated device and trunk group is displayed as well. Each trunk group displayed can be activated/deactivated for the corresponding extension via a check box preceding the entry.

Extension number ranges are newly created via the **Add** icon or deleted via the **Remove** icon.

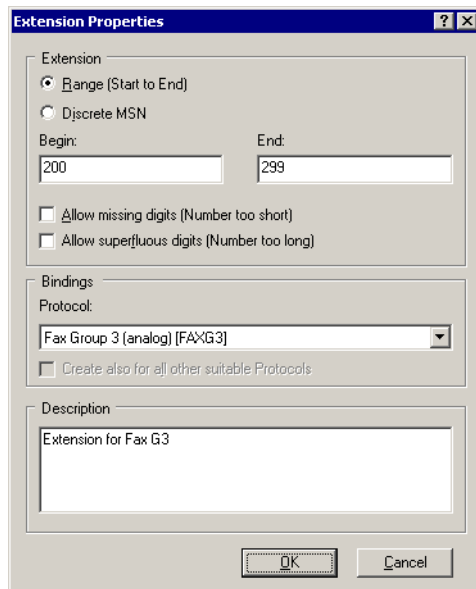
NOTE:

In each telematics APL you can configure a maximum of 1024 extension ranges.

Deactivate disables the selected extension number range. Its current configuration is kept. If a deactivated extension number range is selected, the button changes to **Activate**, and the extension number range may be reactivated.

Via selection of the **Edit** button you are taken to the configuration of the selected extension range, device or trunk group.

Let's have a closer look at the possible extension range settings.



If the XPR server can be reached via a point-to-point connection, the start or the end of an extension range can be defined via the **Begin** and **End** fields. In doing so make sure that both values consist of the same number of digits. The **Begin** and **End** values can only be set if the **Range** option has been previously selected.

If no point to point connection but a point to multipoint connection is available, a **Discrete MSN** (Multiple Subscriber Number) can be assigned to the extension range.

The **Allow missing digits** and **Allow superfluous digits** options define the behavior with the assignment of incoming call number and extension range or of the assigned protocol.

The **Allow missing digits** option defines whether the externally dialed call numbers may be of variable length. The extension number range entered in the **Begin** and **End** fields then determines the maximum length of the incoming number.

IMPORTANT:

The effects of this option together with **Allow superfluous digits** are not defined, since these options use different search algorithms. Therefore, always only one of these options should be active.

Example:

For an extension number range from 700000 to 999999 (**Start**=700000; **End**=999999) the varying extensions 7-9, 70-99, 700-999,..., 700000-999999 are allowed with activated **Allow variable length** option.

The **Allow superfluous digits** option defines whether additional digits after the actual call number are ignored.

IMPORTANT:

The effects of this option together with **Allow variable length** are not defined, since these options use different search algorithms.

Example:

A user has the entered extension 50. If the **Allow superfluous digits** option is active, the extensions 500 and 50123 also apply for this user. If the option is deactivated, the ISDN APL no longer assigns these extensions the user with the extension 50 because of the additional digits or does not accept respective calls at all.

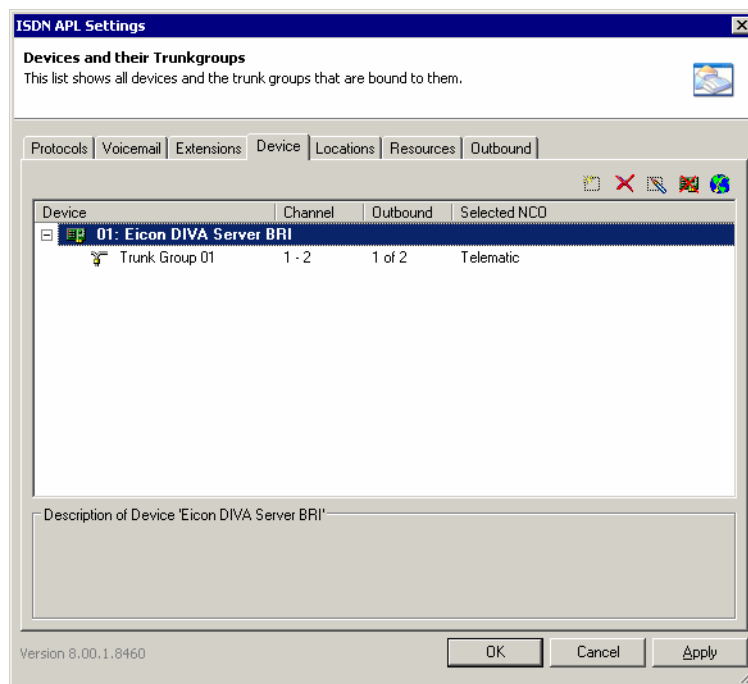
In the *Bindings* section you can indicate for which installed **Protocol** the respective extension number range is to be used. When the service type can be determined from the D-channel service information, it is possible to assign a single extension number range to several services (protocols). This possibility is realized during the creation of a new extension number range via the option **Create also for all other suitable Protocols**. It automatically defines corresponding extension ranges for the installed protocols for which it is possible. These are usually Fax G4 and one protocol that can receive Fax G3 – for example PhoneMail.

IMPORTANT:

The extension ranges for the Fax G3 protocol and the VFS and E-scripts must not overlap, since they cannot be told apart by the service information transmitted by D-channel.

You can enter a short text description for a better overview in the **Description** text field to indicate the purpose of the respective extension range.

10.9.4 Devices (Advanced Settings)



The configuration tab *Devices* displays all ISDN boards installed in the XPR server and supported by the ISDN APL. Since an automatic hardware detection is performed for this, no further ISDN devices can be manually added.

Existing devices are deactivated (**Disable**) or activated (**Enable**) via the corresponding button. A card that has been configured but is not found during the start is independently deactivated by the ISDN APL. This occurs on grounds of the assumption that a hardware failure may have happened and thus the comprehensive configuration files are to be saved. If the card has been removed indeed, the corresponding configuration data can be finally removed via the **Remove** button.

Remove is only possible for deactivated cards, since physically existing cards are automatically added during the next restart by the automatic hardware recognition. Removing would thus not make sense.

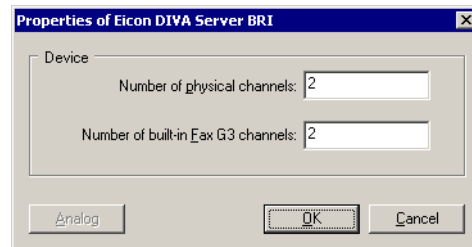
If the device display is expanded by the plus sign before the respective list entry, the associated trunk groups are displayed as well. Via the **Add** button new trunk groups can be added to a device. With **Delete** existing trunk groups are removed.

If a device or trunk group is selected in the list, the **Edit** button can be pushed to open a configuration dialog. In this dialog the settings of the selected element can be edited.

The **Number Conversion Administration** button opens a limited NCOAdmin version. With this version NCO settings for locations, NCO clients and variables can be performed. Furthermore, it is possible to adjust general configuration

settings for NCO on the *Configuration* tab of the NCOAdmin (cf. [Chapter 9](#), “[Number Conversion Object \(NCO\)](#)”).

10.9.4.1 Device Properties



In the device properties the settings are defined that describe the resources of the relevant ISDN board. In most cases this information is automatically evaluated by the ISDN APL.

The **Number of physical channels** field defines how many channels of the respective ISDN board are used for communicating with the PBX. With an S0 board it is a maximum of 2 channels and with an S2M board a maximum of 30 channels. If the maximum number of channels is not to be used, you can enter a number smaller than 2 or 30 here.

Number of built-in Fax G3 channels describes the number of channels for which hardware-based fax resources are available on the relevant ISDN board.

The **Analog** button is currently not used by the IP APL.

10.9.4.2 Trunk Group Properties

Trunkgroup Properties

Trunkgroup Parameters

From Channel: 1 To: 2 Max. outbound channels: 1

Number Conversion Object: Telematic Location: Location with Trunk# (49-2404-901-83)

☐ PBX sends Called Numbers with Trunk Code

☐ PBX sends Calling Numbers of unknown type without external line prefix

PBX sends Calling Numbers of unknown type without external line prefix

Extensions (inbound)

Extensions	Protocols	Description
☒ 0-9	Fax group 4 (digital)	
☒ 100-199	CTI Computer Telephony Integration	
☒ 200-299	Fax Group 3 (analog)	Extension for Fax G3

Protocols (outbound)

Protocols	Description
☒ CTI_TELE	CTI Computer Telephony Integration
☒ FAXG3	Fax Group 3 (analog)
☒ FAXG3REV	Fax-on-demand (Fax G3)
☒ FAXG4	Fax group 4 (digital)

OK Cancel

The physical channels of a device can be divided into different trunk groups, to which individual extension ranges with the associated protocols can be bound at a later date.

Via the **From Channel:** and **To:** fields it is defined which channels of the selected device belong to the respective logical trunk group. This enables e.g. dividing a S_{2m} board with 30 channels into several logical units.

The **Max. outbound channels** field defines the maximum number of outgoing connections. Thus channels can be reserved for incoming communication, so that even with a high volume of outgoing connections resources for incoming traffic are available.

The **Number Conversion Object** defines the NCO used by the ISDN APL for call number conversion for the corresponding trunk group. In most cases *Telematic* is to be set here. If location information is to be used for call number conversion that deviates from the location configured in the NCO, this information can be selected in the **Location** field. The information is then preferred to the setting in the NCO.

The **PBX sends Called Numbers with Trunk Code** option defines whether the connected PBX transfers the trunk group to the XPR server with a call number.

Furthermore, the **Calling numbers of unknown type without external line prefix** setting defines whether the PBX transfers originator call numbers of type *Unknown* without external prefix to the XPR server.

In the *Extensions (inbound)* portion, extension ranges can be activated/deactivated for the relevant trunk group. Via the **add**, **delete** and **edit** icons a new extension can be generated or the selected extension be deleted or edited.

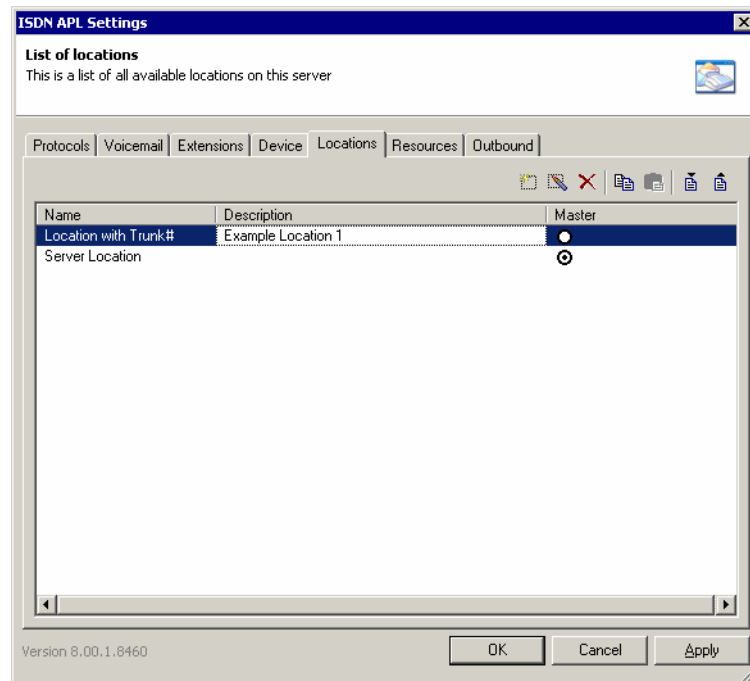
In the *Protocols (outbound)* section, outgoing protocols can be activated/deactivated for the relevant trunk group by the assigned checkbox.

IMPORTANT:

If you deactivate a trunk group for outgoing traffic, you need to disable the following option in the MTA for the associated logical line, too: **Line enabled for outbound transactions**.

10.9.5 Locations

In the *Locations* tab XPR server locations are defined and edited.



A detailed description of this dialog and all settings that can be reached from here is found in [Section 9.9.5, “NCO Locations”, on page 447](#).

Let's have a look at the extended options of the ISDN APL.

10.9.6 Resources (Advanced Settings)

NOTE:

To see the *Resources* configuraton tab you need to log on to the XPR monitor with a user account that has the supervisor privilege.
This tab is not displayed to users with the service privilege.

ISDN APL Settings

Resources
Enter the total number of resources to be reserved. The information provided here will be compared with the license key information.

Protocols | Voicemail | Extensions | Device | Locations | **Resources** | Outbound

Hardware

Total no. of resources reserved:		Detected hardware:	
2	Line resources	2	
2	Voice resources	2	
2	Fax resources	2	

Restart of the APL

☐ Release all existing connections immediately

☐ Restart used services/drivers, too

Restart

Version 8.00.1.8460

OK Cancel Apply

In the *Hardware* section, the number of **Line resources** (B-channels), **Voice resources** and **Fax resources** to be used is defined. With ISDN the latter ones normally correspond to the number of lines.

IMPORTANT:

All existing devices of the applied ISDN cards must be activated, so that the number of the automatically found lines and voice resources is displayed correctly. This takes place in the *Device* tab.

If an ISDN board supports the fax service, the maximum number of lines is always displayed among the found fax resources for technical reasons. This also applies if the actual number of installed fax resources is smaller.

The column on the right hand side displays how many resources the ISDN APL hardware detection has determined each. The left column defines, how many of these determined resources are actually to be used by the ISDN APL. Please note: the number in the left column must not exceed the number of the respectively purchased licenses. But it may surely fall short. In this way resources (licenses) can be distributed among the ISDN APLs of the different XPR systems

in a distributed XPR system.

With the **Restart** button the ISDN APL can be manually rebooted. If the **Release all existing connections immediately** option was previously activated, all communication relations established at this time are closed. The regular end of the existing connections is not temporized. A fax message just being transmitted must in this case be sent anew after the restart.

IMPORTANT:

A restart via the option **Release all existing connections immediately** interrupts immediately all existing communication connections that are performed via the respective ISDN APL during the time of the restart.

If the restart is performed with the **Restart used services/drivers, too** option, the ISDN APL reboots all its associated services and drivers as well. This is only possible for ITK ISDN cards.

10.9.7 Outbound (Advanced Settings)

Normally, call charges are billed by the applied PBX in an XPR environment. Therefore the XPR server needs to provide information that enables assigning the arising charges to the individual originators or specific cost centers. To guarantee this, the ISDN APL transmits respective information via the D-channel of a connection. This information is adapted to the respective requirements via a calling line identification (CLI) configuration.

The screenshot shows the 'ISDN APL Settings' dialog box with the 'Outbound Connections' tab selected. The title bar reads 'ISDN APL Settings'. Below the title bar, the tab is labeled 'Outbound Connections'. The main text area says: 'Evaluation of charging units and configuration of phone number formats for outbound connections (to influence charging evaluation on the PBX)'. There is a small icon of a telephone handset on the right. Below the text, there are several tabs: 'Protocols', 'Voicemail', 'Extensions', 'Device', 'Locations', 'Resources', and 'Outbound'. The 'Outbound' tab is active. The settings are organized into three sections:

- Charge pulse evaluation:** Contains a checked checkbox for 'Enabled' and a text box with the value '6' followed by the label 'Currency units per pulse'.
- Calling Line Identification for outbound calls:** Contains three radio button options:
 - ☒ CQSTINFO field from user database, or local extension if empty
 - ☐ Local Extension (Voicemail- or Fax Field from user database)
 - ☐ Use the following CLI: (followed by an empty text box)
- Number Normalization for outbound calls:** Contains two unchecked checkboxes:
 - ☐ International format for Called Number
 - ☐ International Format for Calling Number

 At the bottom left, it says 'Version 8.00.1.8460'. At the bottom right, there are three buttons: 'OK', 'Cancel', and 'Apply'.

Via the **Enabled** option in the *Charge pulse evaluation* section, call charging by the XPR server is activated. The server evaluates the charge pulse of the respective service provider for this purpose.

In most cases charges are already evaluated in the PBX so that this option can be deactivated then.

The **Currency units per pulse** field contains the price per pulse in the local currency. In Germany the specification *6* would mean six Eurocent per pulse. Some PBXs do not deliver the call charges per call charge pulse but in currency units. In this case, the charge rate should be set to *1*.

IMPORTANT:

The call charges information the service provider delivers are not always correct. For example, some service providers offer discount rates that depend on call duration or daytime. This discount is only applied to the final bill and not when transferring the charge pulse.

The PBX can use the calling line identification (CLI) the XPR server transmits in the D-channel for bookings of the arising call charges. Furthermore, the CLI is also required by some PBXs to enable an outgoing connection.

Which information the XPR server transmits as CLI to the PBX can be set via the following options in the *Calling Line Identification for outbound calls* section:

- **COSTINFO field from user database, or local extension is empty**
Transmits the entry of the COSTINFO field in the XPR user database to the PBX. So billing users can be summarized in groups.
- **Local Extension**
Transfers for each connection establishment the user-individual extension for the relevant service from the XPR user database to the PBX.
- **Use the following CLI**
Transfers an originator ID to be defined here and used for all subscribers of the relevant XPR server to the PBX.

IMPORTANT:

If CAD is to be used for connections via the ISDN APL, this field must remain empty.

If an originator ID is entered in the text field without activating the actual option with the associated option field, the entered originator ID is used as fallback setting (see the following ranking).

For these three options the following ranking applies:

- If the **COSTINFO field ...** option is active and the COSTINFO database field is not filled in for a relevant user, the XPR server transmits the local extension of the user as CLI.
If the XPR server cannot determine the local extension of the caller either, the originator ID is transmitted as CLI that is specified in the text field under **Use the following CLI**.
- If the **Local Extension** option is active and the XPR server cannot determine the local extension of the caller, the originator ID is transmitted as CLI that is specified in the text field under **Use the following CLI**.
- If the **Use the following CLI** option is active, the originator ID is transmitted as CLI that is specified in the associated text field.

The **International format for Called Number** or **Calling Number** options define whether destination or originator call numbers are always transferred in the international format (e.g. 492404901100) by the XPR server to a connected PBX.

10.10 Configuration Reference for Voice-over-IP Connections (IP APL)

The IP APL configuration is performed in the XPR monitor. The basis is the TeleCfg library providing a unified operation of all telematics APLs and services (cf. [Section 10.1.1.2, “The Modules TeleCfg and TeleCfg API”, on page 526](#)).

NOTE:

For the Telematic APL configuration the NCO configuration files of the XPR server are accessed via the *NCOAdmin*. Please make sure that the *NCOAdmin* used and the NCO configuration files are available in the same version. If this is not the case, an alarm message at the beginning of the telematics configuration indicates this incompatibility.

To start the IP APL configuration, select the **IpApI > Set options** menu option in the modules window of the XPR monitor. Via the alternative menu item **Set extended options** additional settings can be made via further tabs. Sections describing this extended functionality are labeled with the addition (Extended options).

In most cases the regular setting options for the APL configuration are sufficient.

Since all modifications are dynamically effected, a restart of the IP APL is not necessary after changes have been made.

The information contained in this chapter is divided into the following sections:

- [Protocols](#)
- [General Voicemail Settings \(Voicemail\)](#)
- [Extensions](#)
- [Devices \(Advanced Settings\)](#)
- [Locations](#)

10.10.1 Protocols

NOTE: Up to 128 protocols can be configured in the IP APL.

Protocols

Protocols are a service supported by the IP APL. The IP APL supports the following protocols for H.323 devices:

- Sending/receiving Fax G3
(see [Section 10.4.6, “Fax G3”, on page 702](#))

IMPORTANT:

If you connect a HiPath 3000 or HiPath 4000 via the IP APL and want to use the fax service, the method of fax error rectifying must be identically configured in the HiPath and IP APL. If the settings differ, the number of fax transmission errors increases.

IMPORTANT:

If you connect a HiPath system with HG module via the IP APL and want to use the fax service, logging must not be activated in the HG module. If logging is active, the number of fax transmission errors increases.

IMPORTANT:

Sending and receiving of fax messages may cause disturbances in the IP APL if heavy fax traffic and the execution of maintenance script jobs coincide.

Therefore, perform maintenance script jobs at times when you do not expect heavy fax traffic – e.g. at night. If the described problem arises just the same, reduce the priority for the automatic XPR server maintenance.

IMPORTANT:

The IP APL currently supports T.38 fax services for connections via H.323 and SIP.

IMPORTANT:

The IP APL supports fax transmissions up to a maximum transmission rate of 14400 bit/s.

NOTE:

The IP APL always resends the entire fax message when the connection collapses during the message transmission. The continuation of an interrupted message transmission with the Fax G3 option **Retransmission enabled** is not supported by the IP APL.

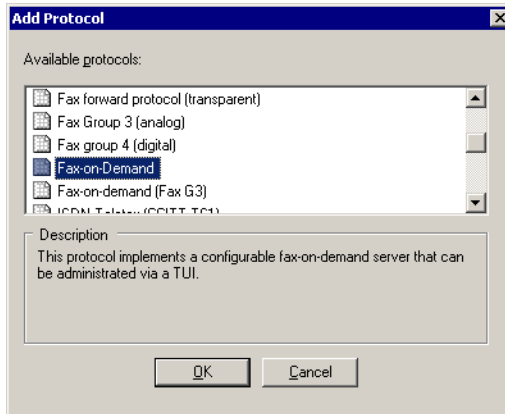
- Message Waiting Indication (MWI)
for MWI information transmission via QSIG, CorNet N and CorNet NQ
(see [Section 10.4.17, “Message Waiting Indication \(MWI\)”, on page 739](#))

Scripts

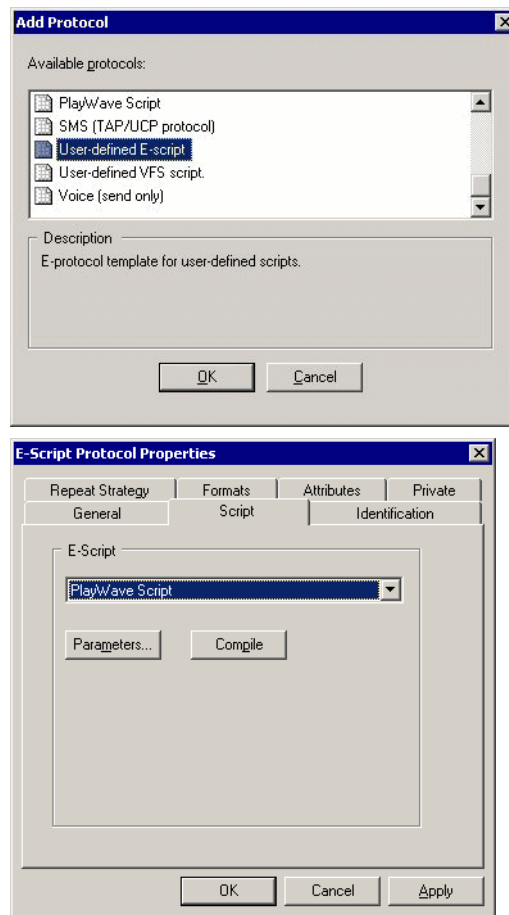
With the help of the script language E, further individual protocols for the XPR server can be implemented. As with its predecessor VFS, user-specific voice and fax mailboxes, fax-on-demand servers etc. can be realized. In contrast to VFS, E is a more powerful language with a larger API, implementing nearly all XPR-specific features.

Scripts can be installed via the **Add** button in the *Protocols* tab in two alternative ways:

- Adding the desired script by name in the *Add Protocol* dialog.



- Adding a user-defined script in the *Add Protocol* dialog and subsequent specification of the desired script in the configuration tab *Script* below protocol properties.



Via the **Parameters...** button in the configuration tab *Script* you will then come to the actual script configuration. Via **Compile** you can compile the script. This is only required when you have developed new scripts yourself which are thus present in the source. In most cases an already compiled object file is available which can simply be executed by the server.

The XPR server standard scope of delivery already includes scripts the configuration of which is described in [Section 10.4, “Protocols of the XPR Server”, on page 593](#).

The IP APL supports the following scripts:

- Evo as the latest voice mail script with integrated speech recognition (see [Section 10.4.1, “Evo”, on page 594](#) for the configuration, and the *Evo* user manual for the operation of Evo)
- Ergo as modern voice mail script (see [Section 10.4.2, “Ergo”, on page 617](#) for the configuration and the user manual *Ergo* for the Ergo operation)

- PhoneMail
(see [Section 10.4.3, “PhoneMail”, on page 638](#) for the configuration, and the *PhoneMail* user manual for the operation of PhoneMail)
- Voicemail VMS
(see [Section 10.4.4, “Voicemail VMS”, on page 678](#) for the configuration and the *VMS* user manual for the operation of VMS)
- Playwave
(see [Section 10.4.15, “PlayWave”, on page 736](#))
- CTI Light
(see [Section 10.4.22, “CTI Light”, on page 759](#))

The protocol settings correspond to those that have been already described for the *ISDN APL* (see [Section 10.9.1, “Protocols”, on page 805](#)).

10.10.2 General Voicemail Settings (Voicemail)

The general voice mail settings correspond to those that have been already described for the ISDN APL (see [Section 10.9.2, “General Voicemail Settings \(Voicemail\)”, on page 811](#)).

10.10.3 Extensions

NOTE:

In each telematics APL you can configure a maximum of 1024 extension ranges.

The extension settings of the IP APL correspond to those described for the ISDN APL (cf. [Section 10.9.3, “Extensions”, on page 824](#)).

10.10.4 Devices (Advanced Settings)

IMPORTANT:

In the IP APL, only **one** device may be activated at a time.

IMPORTANT:

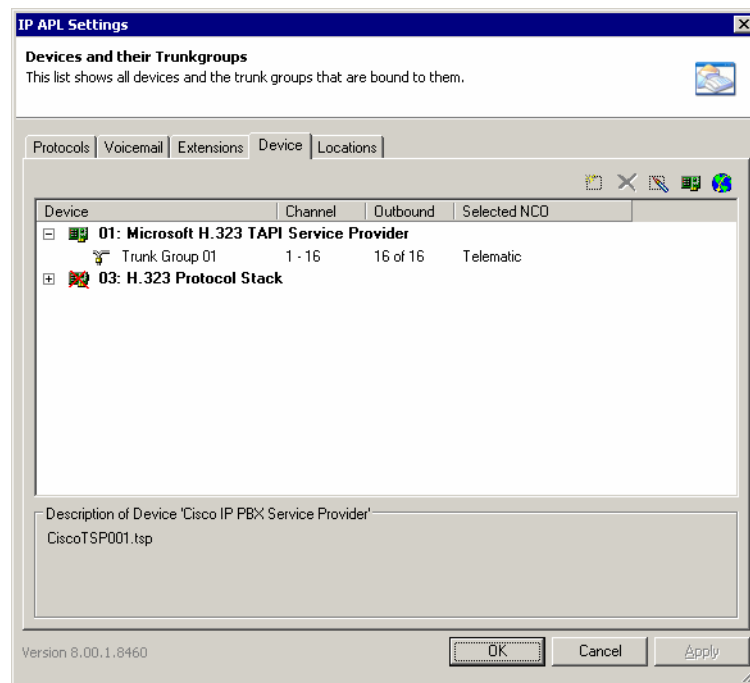
The IP APL currently supports T.38 fax services for connections via H.323, CorNet IP and SIP.

IMPORTANT:

The IP APL supports fax transmissions up to a maximum transmission rate of 14400 bit/s.

The configuration tab *Devices* displays all available interfaces installed in the XPR server and supported by the IP APL. To recognize the available interfaces, the XPR server searches the individual computer system. For this reason, no new devices can be manually added in the IP APL with the **Add** button.

The IP APL communicates with external systems via a network interface card (NIC), which must be installed in the XPR server system.



You can disable or enable single available devices via the **deactivate/activate** icon. If you expand a device entry via the preceding plus sign, the trunk groups assigned to the relevant device are displayed. Via the **add** icon you can add new trunk groups to a device. With the **delete** icon you remove a selected trunk group.

If you select a device or trunk group in the list, you can open a configuration dialog via the **edit** button. Via this configuration dialog you can edit the properties of the selected element.

These are:

- [Properties of H.323-based Devices](#)
- [Properties of SIP-based Devices](#)
- [Trunk Group Properties](#)

10.10.4.1 Properties of H.323-based Devices

NOTE:

The IP APL can be instantiated in an XPR server several times. This requires each IP APL to use an individual IP address. The IP address of an IP APL is stored under the respectively associated registry value **Private** in the **LISTEN** parameter.

The properties for H.323-based devices are divided into the following areas:

- [Device](#)
- [Streaming](#)
- [Fax](#)
- [QoS](#)
- [QDC](#)

The following sections describe the respectively associated settings in detail.

Device

H.323 Protocol Stack / HiPath CorNet-IP

Device Settings
Configuration related to Channels

Device | Streaming | Fax | QoS | QDC

Device

Number of physical channels: 16

Number of built-in Fax G3 channels: 0

Gateway address: 10 . 1 . 35 . 15

Gatekeeper

IP address: . . .

Registration E.164 address:

Registration H323 name:

☒ Default ☐ Intel PIMG

☐ HiPath 3000 >= V5.0 ☐ HiPath 4000 >= V2.0

☐ H323 Trace

Fake IDs

Fake caller ID:

Fake called ID:

Intel PIMG access numbers:

Type Of Number for outgoing calls: Unknown

Numbering plan for outgoing calls: Unknown

OK Cancel Apply

The **Number of physical channels** field defines how many parallel channels are to be used for the communication with the connected PBX.

In the **Number of built-in Fax G3 channels** field you specify how many of the physical channels are to be usable for sending fax messages.

IMPORTANT:

If you connect a HiPath 3000 or HiPath 4000 via the IP APL and want to use the fax service, the method of fax error rectifying must be identically configured in the HiPath and IP APL. If the settings differ, the number of fax transmission errors increases.

IMPORTANT:

If you connect a HiPath system with HG module via the IP APL and want to use the fax service, logging must not be activated in the HG module. If logging is active, the number of fax transmission errors increases.

IMPORTANT:

Sending and receiving of fax messages may cause disturbances in the IP APL if heavy fax traffic and the execution of maintenance script jobs coincide. Therefore, perform maintenance script jobs at times when you do not expect heavy fax traffic – e.g. at night. If the described problem arises just the same, reduce the priority for the automatic XPR server maintenance.

If the IP APL is to communicate with a H.323 gateway, the **Gateway address** defines under which IP address this gateway can be reached. We assume here that an operable network connection exists between the XPR server and the relevant gateway.

If the IP APL is to communicate with a HiPath system via CorNet-IP, enter the IP address of the relevant HG module in the **Gateway address** field.

NOTE:

To use the IP APL with CorNet-IP you need a corresponding CorNet-IP license in the XPR server. Your sales partner will provide further information.

If you want to connect the IP APL with a H.323 gatekeeper, the **Gatekeeper – IP address** field defines the IP address of the relevant gatekeeper. We assume here that an operable network connection exists between the XPR server and the relevant gatekeeper.

If the IP APL is to use E.164 addresses (ISDN phone numbers) at an H.323 gatekeeper, the **Gatekeeper – Registration E.164 address** field defines the E.164 address under which the XPR server registers with the gatekeeper. When the gatekeeper then receives communication requests for the respective phone number, these are transmitted to the XPR server.

If the IP APL is to use H.323 names at an H.323 gatekeeper, define in the **Gatekeeper – Registration H.323 name** field the H.323 name with which the XPR server registers with the gatekeeper. When the gatekeeper then receives communication requests for the respective H.323 name, these are transmitted to the XPR server.

The IP APL H.323 protocol was customized for connecting the following PBXs:

- PBXs with native H.323
- PBX IP media gateway (Intel PIMG)
- HiPath 3000 /5000 from software version 5.0
- HiPath 4000 from software version 2.0

If required, activate one of these adaptations via the associated option: **Intel PIMG**, **Hipath 3000 >= V5.0** and **Hipath 4000 >= V2.0**. The **Standard** option activates the H.323 protocol in its standard version.

The **H323 Trace** check box activates the H.323 logging of the IP APL. This requires the name of the logging file to be specified in the associated text field. If this file name merely consists of a name without directory path, the IP APL saves this file in the `SYSTEM32` Windows directory. If you specify a directory path along with the file name, the IP APL stores the log file in the associated directory at a later date.

IMPORTANT:

Logging claims a considerable portion of the XPR server system computing power. This may deteriorate the system performance of the XPR server from the user view.

Therefore, activate logging only for the period in which you actually need it for the error search.

IMPORTANT:

The specified directory must already exist, since the IP APL does not create any new directory structures.

Some PBXs do not always transfer the target and / or originator number of the connection to the XPR server during the connection setup. This applies e.g. for the Intel PBX IP Media Gateway, when it diverts a call. In such a case you can define phone numbers in the **Fake caller ID** or **Fake called ID** fields, which the IP APL then uses as target or originator number.

If you use the IP APL at an Intel PBX IP Media Gateway, you can enter in the **Intel PIMG access numbers** field a list of all access numbers that the XPR server uses. The single phone numbers must be separated by a comma.

These access numbers must be specified when the XPR server uses several access modes but the PBX does not transfer any target phone numbers to the server.

NOTE:

The **Intel PIMG access numbers** field is only active if the **Intel PIMG** option has been selected for the H.323 protocol.

Example:

ACCESSNUMBERS=901,902,903

The entry in the **Type Of Number for outgoing calls** field specifies which number type (Type-of-Number) the IP APL transfers to the PBX in case of outgoing communication. This value is used by the IP APL in the following cases:

- When an outgoing call is set up
- When a supervised transfer is set up
- When an MWI message is sent.

The entry in the **Numbering plan for outgoing calls** field specifies which numbering plan the IP APL transfers to the PBX in case of outgoing communication. This value is used by the IP APL in the following cases:

- When an outgoing call is set up
- When a supervised transfer is set up
- When an MWI message is sent.

Streaming

The screenshot shows a Windows-style dialog box titled "H.323 Protocol Stack / HiPath CorNet-IP". Below the title bar is a section labeled "Streaming Settings" with the subtitle "Configuration related to Streaming, Codec and DTMF". There are four tabs: "Device", "Streaming", "Fax", "QoS", and "QDC", with "Streaming" currently selected. The "Streaming" tab contains three sections: "Streaming" with "Packet size (msec):" set to 20 and "First RTP Port:" set to 29100; "Codec" with checkboxes for G.711a (checked), G.711μ (checked), and G.729AB (unchecked); and "DTMF Settings" with checkboxes for "DTMF via RFC 2833" (checked), "DTMF via signalling messages" (checked), and "In-Band DTMF Detection for G.711" (checked). At the bottom are "OK", "Cancel", and "Apply" buttons.

For voice information sent by the IP APL via the H.323 device you can specify the associated packet size in the **Packet size** field. You state it in milliseconds. If you use the default of 30ms, the IP APL sends e.g. every 30ms a packet with 30ms voice information.

IMPORTANT:

The entry in the **Packet size** field must be in line with the terminal devices used. Specifying a packet size not supported by the terminal device used will significantly deteriorate the voice transmission quality.

NOTE:

The G.729 codec of the IP APL does not support any packet sizes exceeding 30ms. If a higher value has been configured for the packet size, the IP APL automatically uses a packet size of 30ms for G.729 transmissions.

The size of the RTP packets that the IP APL receives is determined by the remote terminal device.

Setting larger packet sizes holds the following advantages and disadvantages:

- + Smaller transmission delays need not significantly deteriorate the voice quality of a connection.
- Losing packets during transmission leads relatively quickly to a worse voice quality.
- The voice information playback is strongly delayed. Reason: with each voice connection, some voice packets are always buffered before the playback of the received voice information starts.

Setting smaller packet sizes holds the following advantages and disadvantages:

- + Losing packets during transmission need not significantly deteriorate the voice quality of a connection.
- + The voice information playback is delayed less strongly. Reason: with each voice connection, some voice packets are always buffered before the playback of the received voice information starts.
- Even smaller transmission delays may audibly deteriorate the voice quality of a connection. Such delays occur when e.g. the computer system of the XPR server works mostly under high processor load.

In the **First RTP Port** field you specify from which port number the IP APL allocates TCP/UDP ports for the RTP communication. Beginning with this port the IP APL periodically allocates the next 400 ports.

IMPORTANT:

If a firewall exists between the IP APL and the terminal devices, you need to activate the following TCP/UDP ports in the firewall:

<first RTP port> to <first RTP port>+400

In the **Codec** range you select the codecs that can be used for RTP communication. Available are **G.711a**, **G.711μ** and **G.729AB**. The IP APL dynamically negotiates with the respective communication partner which codec to later use for a connection.

Since the G.711 codec does not compress data to be transmitted, the following applies:

- + It requires a relatively low computing performance to encode or decode the signal
- With 64 kb/s per connection, it requires a relatively high transmission bandwidth

Since the G.729AB codec compresses data to be transmitted, the following applies:

- + It requires a lower transmission bandwidth
- It requires a higher computing performance to encode or decode the signal

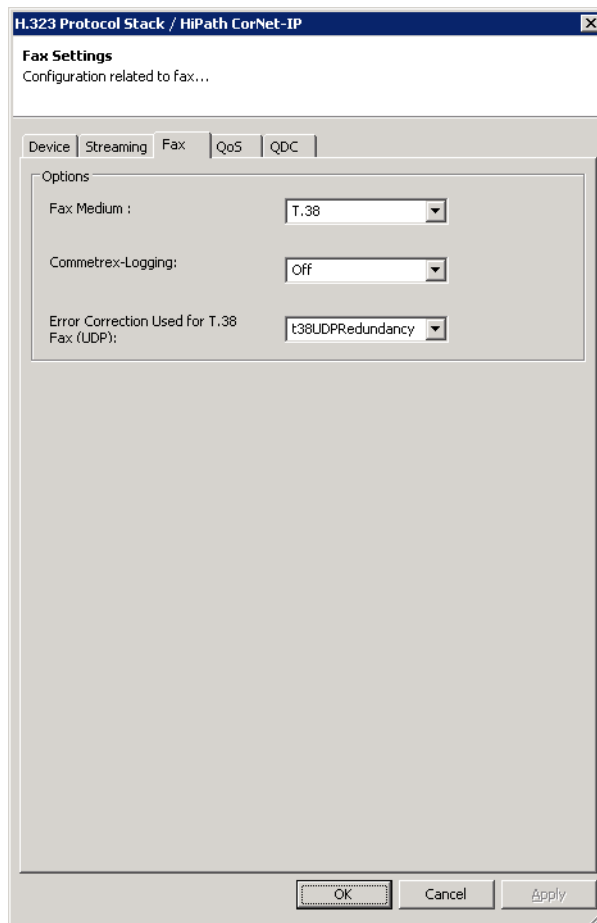
In the *DTMF Settings* section you specify how the IP APL processes DTMF signals. The following options are available:

- Out-of-band recognition via RFC 2833
- Out-of-band recognition via signaling messages
- In-band DTMF recognition for G.711

All three options are active by default, with **In-Band DTMF Detection for G.711** being the only option that can be disabled.

In-band DTMF recognition for G.729AB is not possible. The G.729AB codec is optimized for voice transmission. In-band DTMF information might therefore not be uniquely regained any more.

Fax



In the **Preferred Outgoing Fax Medium** field you specify whether fax messages are sent via G.711 or T.38. This setting is valid for all fax messages received or sent via the H.323 device of the IP APL. If the IP APL supports G.711 as well as T.38 fax we recommend to use T.38 fax. The T.38 fax technology uses various technical mechanisms that see to a reliable fax transmission and an improved transmission quality.

IMPORTANT:

The setting in the **Preferred Outgoing Fax Medium** field must match the corresponding setting in the gateway.

The SIP stack supports a logging that you can activate in the **Commetrex-Logging** field. If you activate the logging, the log information subsequently generated is put out in log files. These log files are stored in the directory `\system32\` under the name `trm*.log`.

IMPORTANT:

Logging claims a considerable portion of the XPR server system computing power. This may deteriorate the system performance of the XPR server from the user view.

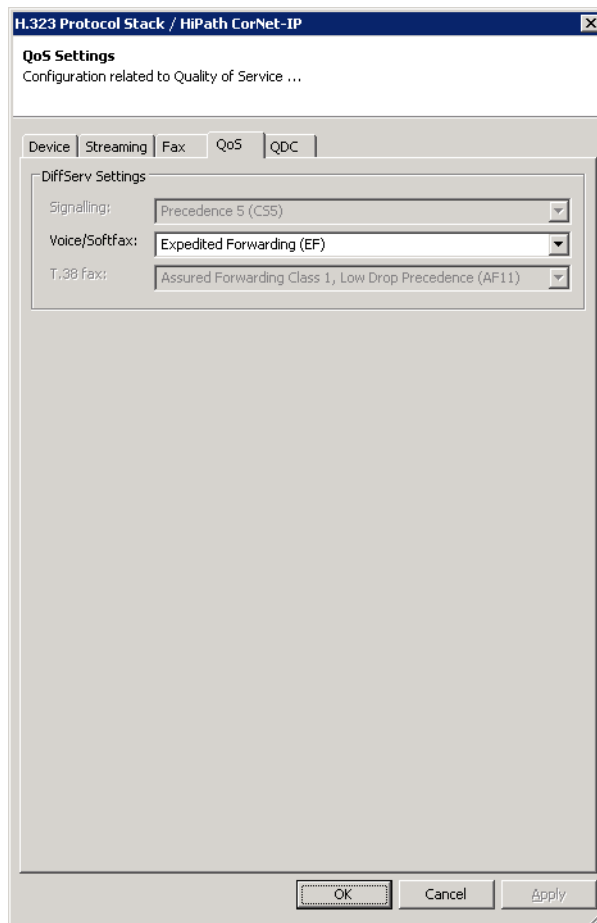
Therefore, activate logging only for the period in which you actually need it for the error search.

IMPORTANT:

Each of the log files can reach a size of several 10MB.

Under **Error Correction Used for T.38 Fax (UDP)** the fax-error correction method is set that the IP APL uses for communication via T.38.

QoS



On the **QoS** tab you specify which QoS setting the IP APL uses for RTP-**Voice/Softfax**. The QoS settings for **Signaling** and **T.38 fax** are grayed out and do not affect the IP APL behavior.

IMPORTANT:

The registry value `DisableUserTOSSetting` under `HKLM\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters` must be set to 0 for the QoS settings of the IP APL to be used for communication.

In most Windows versions this registry value is not configured by default. In this case you need to manually add it as `REG_DWORD` as described in the respective passage. Furthermore, the computer system needs to be rebooted for the registry modification to take effect.

If the IP APL cannot find this registry value with the entry 0, a corresponding error message is issued in the XPR monitor during the IP APL start.

QDC

H.323 Protocol Stack / HiPath CorNet-IP

QDC Settings
Configuration related to Quality of Service Monitoring

Device | Streaming | Fax | QoS | **QDC**

QoS protocol version: 0

General Settings

QCU hostname: 127.0.0.1

QCU UDP port: 12010

Threshold - Codec Independent

Maximum Jitter Threshold: 20

Average Round Trip Delay threshold: 100

Threshold - Noncompressing Codecs

Lost Packets Threshold: 10

Consecutive lost packets threshold: 2

Consecutive good packets threshold: 8

Threshold - Compressing Codecs

Lost Packets Threshold: 10

Consecutive lost packets threshold: 2

Consecutive good packets threshold: 8

Report Mode: OFF

Report Interval (sec): 60

Observation Interval (sec): 10

Minimal Session Length (100 ms): 20

OK Cancel Apply

Using the QoS Data Collection you can capture data in a HiPath system environment to analyze the voice and network quality of the systems. By means of various thresholds QDC defines a minimum quality for the codec's working method and for different network parameters and monitors its compliance.

The QDC monitoring is based on cyclic surveillance intervals. If a threshold is violated within such a surveillance interval, a corresponding message is generated. Such messages are collected and sent to the QoS Monitoring Control Unit (QCU) in the form of a report. This transmission occurs at the end of a so-called report interval or after the respective session has closed.

Under **General Settings** you define the address under which the IP APL reaches QoS Monitoring Control Unit (QCU). Under **QCU Hostname** you specify the IP address or host name under which the QCU can be reached; under **QCU UDP port** you specify the port number used. The default value for the UDP port is 12010.

In the **Threshold – Codec Independent** section you specify the following thresholds that concern network parameters:

- **Maximum Jitter Threshold**

The jitter value is measured on the basis of the packet propagation time of two consecutive RTP packets and checked against this threshold.

The value is indicated in milliseconds. Its default value is 20 milliseconds and may range from 0 to 255.

This threshold is monitored for transgression.

- **Average Round Trip Delay Threshold**

The round trip delay is measured in send and receive direction as sum of the packet propagation times and checked against this threshold.

The value is indicated in milliseconds. Its default value is 100 milliseconds and may range from 0 to 65535.

This threshold is monitored for transgression.

In the **Threshold – Noncompressing Codecs** and **Threshold – Compressing Codecs** sections you specify the following thresholds that depend on the codec used:

- **Lost Packets Threshold**

Defines the threshold for voice packets that are lost during the voice decoding. This value describes the number of lost packets in relation to the total number of packets.

The value is indicated in per milles. Its default value is 10‰ and may range from 0 to 255.

This threshold is monitored for transgression.

- **Consecutive lost packets threshold**

Defines the threshold for voice packets that are consecutively lost during the voice decoding.

Its default value is 2 and may range from 0 to 255.

This threshold is monitored for transgression.

- **Consecutive good packets threshold**

Defines the threshold for voice packets that are consecutively and faultlessly processed during the voice decoding.

Its default value is 8 and may range from 0 to 255.

This threshold is monitored for falling short.

Under **Report Mode** you define the occasion at which reports are sent to the QCU. The following options are available:

- **OFF**

Deactivates the report transmission.

- **EOS Threshold exceeded**

Reports are always sent after the end of a session and only in the case of at least one threshold violation.

- **EOR Threshold exceeded**

Reports are always sent after the end of a report interval and only in the case of at least one threshold violation.

- **EOS (End of Session)**
Reports are always sent after the end of a session even if no threshold was violated.
- **EOR (End of Report Interval)**
Reports are always sent at the end of a report interval even if no threshold was violated.

Next to **Report Interval** you define the duration of the report interval in seconds. The default setting is 60 seconds and may range from 0 to 65535.

Observation Interval defines the value for the observation interval in seconds. This value cannot be changed and is set to 10 seconds.

In the **Minimal Session Length** field you define how long a session must at least last for the creation or reports. This value is specified in multiples of 100 milliseconds.

Its default value is 20 (2 seconds) and may range from 0 to 255.

10.10.4.2 Properties of SIP-based Devices

The properties for SIP-based devices are divided into the following areas:

- [Device](#)
- [SIP](#)
- [Streaming](#)
- [Fax](#)
- [Security](#)
- [QoS](#)
- [QDC](#)

The following sections describe the respectively associated settings in detail.

Device

The following fields correspond to those for the H.323-based device (cf. [Section 10.10.4.1, “Properties of H.323-based Devices”, on page 844](#)).

- **Number of physical channels**
- **Number of built-in Fax G3 channels**

IMPORTANT:

Sending and receiving of fax messages may cause disturbances in the IP APL if heavy fax traffic and the execution of maintenance script jobs coincide.

Therefore, perform maintenance script jobs at times when you do not expect heavy fax traffic – e.g. at night. If the described problem arises just the same, reduce the priority for the automatic XPR server maintenance.

In the **Number of G.729AB channels** field you define how many channels are to be used exclusively for the communication with the G.729AB codec. If the **G.729 AB** option under **Codec** is not selected, this field is not evaluated.

SIP

In the **SIP Proxy IP Address** field you specify under which IP address and which TCP/UDP port the SIP proxy can be reached. We assume here that an operable network connection exists between the XPR server and the relevant SIP proxy. As alternative to the IP address you can also specify the complete name of the SIP proxy in the **SIP Proxy DNS Name** field.

NOTE:

If the XPR server is used at an OpenScape Voice cluster, the SIP proxy must be defined via its complete cluster name – example: *OSV.Alsdorf.com*.

Cf. [Section 10.3.14, “IP APL at a Layer 3 Cluster of OpenScape Voice”, on page 590](#).

In the **Own IP Address** field you define the IP address and the TCP/UDP/TLS port under which the IP APL is to be accessible for the SIP proxy. If SIP is also used for conferences on the default port 5060 via the Media Server, two IP addresses are required. Specify in this case explicitly the IP address to be used by the IP APL.

The TCP/ UDP/TLS ports under **SIP Proxy IP Address** and **Own IP Address** are allocated as follows:

- for the options **UDP** and **TCP** (see below) with value 5060
- for the options **TLS** (see below) with value 5061.

With the **Act as SIP Trunk** and **Act as SIP User** options you set whether the SIP connection to the SIP proxy is configured trunk-based (SIP trunk) or user-based. If the **Act as SIP User** option is selected, you need to specify in the **Own SIP user name** field the SIP user name to be used by the IP APL as originator name for the SIP communication.

IMPORTANT:

In the **Own SIP user name** field an extension must be entered that the PBX knows from the extension range for the XPR server – for example, the call-back extension of the possibly implemented voice mail protocol.

With the **UDP**, **TCP** and **TLS** options you define which protocol the IP APL is to use for the SIP communication with the gateway. If TLS is selected here, the settings on the **Security** tab will be evaluated as well (cf. [Section 10.10.4.2, “Security”, on page 868](#)).

IMPORTANT:

TLS is store-and-forward-based protocol. With the **TLS** option you merely activate the TLS-based encryption between the XPR server and the PBX used. To ensure encryption of the SIP management information on the entire transmission network XPR server – SIP terminal device, TLS must also be implemented between PBX and telephone.

IMPORTANT:

Activating TLS may claim a considerable portion of the XPR server system's computing performance. This may deteriorate the system performance of the XPR server from the user view.

NOTE:

OpenScope Voice respectively HiPath 8000 endpoints do not use TLS by default. For using TLS you need to set the **MTLS** transport protocol or the **Use Server Virtual Address** option for the relevant endpoints.

Streaming

SIP Protocol Stack

Streaming Settings

Configuration related to Streaming, Codec and DTMF

Device

SIP

Streaming

Fax

Security

QoS

QDC

Streaming

Packet size (msec): 30

First RTP Port: 29100

First T.38 Port: 12500

Codec

1. ☒ G.711a

2. ☒ G.711μ

3. ☐ G.729AB

DTMF Settings

☒ DTMF via RFC 2833

☒ DTMF via signalling messages

☒ In-Band DTMF Detection for G.711

OK

Cancel

Apply

For voice information sent by the IP APL via SIP you can specify the associated packet size in the **Packet size** field. You state it in milliseconds. If you use the default of 30ms, the IP APL sends e.g. every 30ms a packet with 30ms voice information.

IMPORTANT:

The entry in the **Packet size** field must be in line with the terminal devices used. Specifying a packet size not supported by the terminal device used will significantly deteriorate the voice transmission quality.

IMPORTANT:

For HiPath PBXs the packet size setting should not exceed 30ms. Higher values will significantly deteriorate the voice transmission quality.

NOTE:

The G.729 codec of the IP APL does not support any packet sizes exceeding 30ms. If a higher value has been configured for the packet size, the IP APL automatically uses a packet size of 30ms for G.729 transmissions.

The size of the RTP packets that the IP APL receives is determined by the remote terminal device.

In the **First RTP Port** field you specify from which port number the IP APL allocates TCP/UDP ports for the RTP communication. Beginning with this port the IP APL periodically allocates the next 400 ports.

IMPORTANT:

If a firewall exists between the IP APL and the terminal devices, you need to activate the following TCP/UDP ports in the firewall:
<**first RTP port**> to <**first RTP port**>+400

IMPORTANT:

The port ranges for RTP and T.38 (see below) must not clash.

In the **First T38 Port** field you specify from which port number the IP APL allocates TCP/UDP ports for the T.38 communication. Beginning with this port the IP APL periodically allocates the next 200 ports.

IMPORTANT:

If a firewall exists between the IP APL and the terminal devices, you must activate the following TCP/UDP ports in the firewall:

<<**First T.38 Port**> to <**First T.38 Port**> + 199

IMPORTANT:

The port ranges for RTP and T.38 (see above) must not clash.

Setting larger packet sizes holds the following advantages and disadvantages:

- + Smaller transmission delays need not significantly deteriorate the voice quality of a connection.
- Losing packets during transmission leads relatively quickly to a worse voice quality.
- The voice information playback is strongly delayed. Reason: with each voice connection, some voice packets are always buffered before the playback of the received voice information starts.

Setting smaller packet sizes holds the following advantages and disadvantages:

- + Losing packets during transmission need not significantly deteriorate the voice quality of a connection.
- + The voice information playback is delayed less strongly. Reason: with each voice connection, some voice packets are always buffered before the playback of the received voice information starts.
- Even smaller transmission delays may audibly deteriorate the voice quality of a connection. Such delays occur when e.g. the computer system of the XPR server works mostly under high processor load.

In the **Codec** range you select the codecs that can be used for the communication. Available are **G.711A**, **G.711μ** and **G.729AB**. The IP APL dynamically negotiates with the respective communication partner which codec to later use for a connection.

You use the arrow keys between the codec options to configure how the IP APL prioritizes the selected codecs during the codec negotiation. The further to the left a codec option is positioned, the higher the IP APL prioritizes the associated codec. Example: You want the G.729AB codec to have the highest priority. Consequently, you move it to the extreme left with the relevant arrow keys.

Since the G.711 codec does not compress data to be transmitted, the following applies:

- + It requires a relatively low computing performance to encode or decode the signal.
- With 64 kb/s per connection, it requires a relatively high transmission bandwidth.

Since the G.729AB codec compresses data to be transmitted, the following applies:

- + It requires a lower transmission bandwidth.
- It requires a higher computing performance to encode or decode the signal.

In the *DTMF Settings* section you specify how the IP APL processes DTMF signals. The following options are available:

- Out-of-band recognition via RFC 2833
- Out-of-band recognition via SIP
- In-band DTMF recognition for G.711

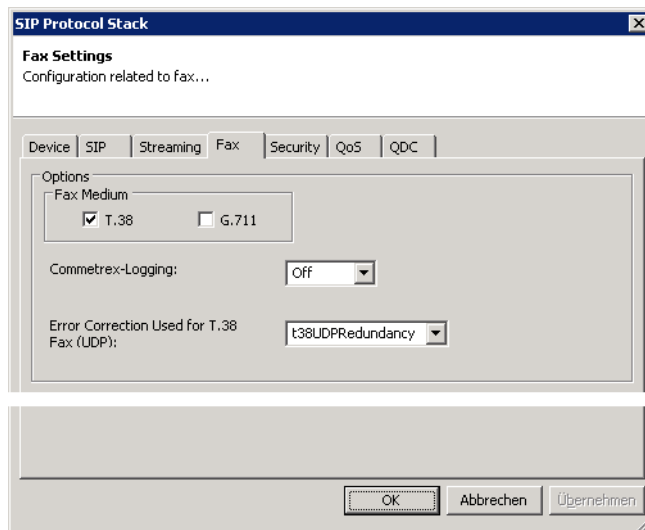
All three options are activated by default.

IMPORTANT:

Some SIP gateways convert DTMF-in-band information into out-of-band information without filtering out the in-band information then. In this case the gateway transfers a DTMF tone out-of-band and in-band simultaneously to the IP APL. This leads to problems, when all three options for DTMF recognition are active. In this case only activate the in-band recognition or only the two out-band recognitions. In doing so you should prefer the out-band options, since the DTMF transmission to RFC 2833 is state-of-the-art.

In-band DTMF recognition for G.729AB is not possible. The G.729AB codec is optimized for voice transmission. In-band DTMF information might therefore not be uniquely regained any more.

Fax



IMPORTANT:

If you connect a HiPath 3000 or HiPath 4000 via the IP APL and want to use the fax service, the method of fax error rectifying must be identically configured in the HiPath and IP APL. If the settings differ, the number of fax transmission errors increases.

IMPORTANT:

If you connect a HiPath system with HG module via the IP APL and want to use the fax service, logging must not be activated in the HG module. If logging is active, the number of fax transmission errors increases.

IMPORTANT:

Sending and receiving of fax messages may cause disturbances in the IP APL if heavy fax traffic and the execution of maintenance script jobs coincide. Therefore, perform maintenance script jobs at times when you do not expect heavy fax traffic – e.g. at night. If the described problem arises just the same, reduce the priority for the automatic XPR server maintenance.

Under **Preferred Outgoing Fax Medium** you set whether the IP APL sends and receives fax messages via G.711 or T.38. If you activate only one of the possible options, the IP APL uses just this medium. If you activate both options, the IP APL prefers medium T.38. If the communication partner does not support medium T.38, the IP APL uses medium G.711.

If the IP APL environment supports G.711 as well as T.38, we recommend to use T.38. The T.38 technology uses various technical mechanisms that see to a reliable fax transmission and an improved transmission quality.

The SIP stack supports a logging that you can activate in the **Commetrex-Logging** field. If you activate the logging, the log information subsequently generated is put out in log files. These log files are stored in the directory `\system32\` under the name `trm*.log`.

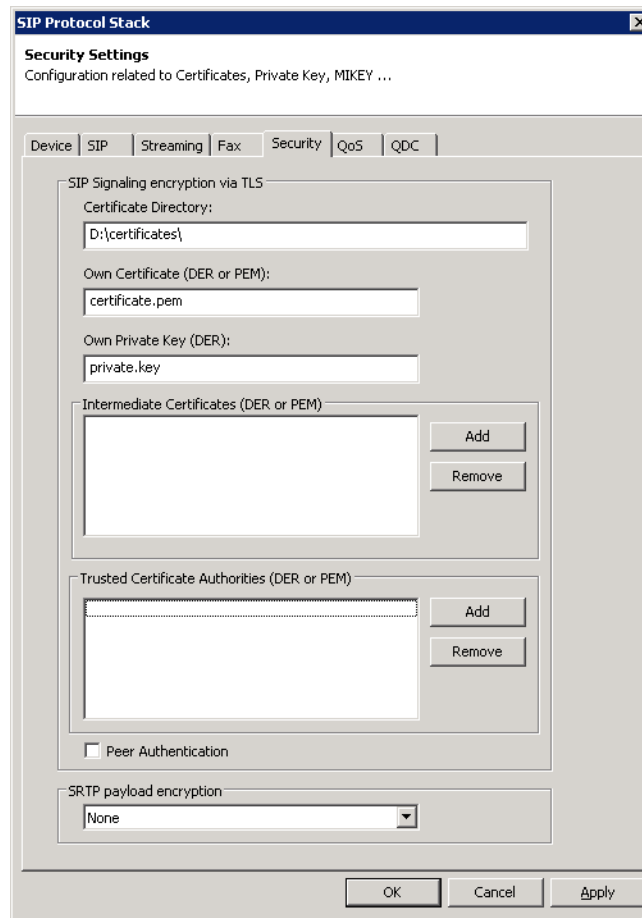
IMPORTANT:

Logging claims a considerable portion of the XPR server system computing power. This may deteriorate the system performance of the XPR server from the user view.

Therefore, activate logging only for the period in which you actually need it for the error search.

Under **Error Correction Used for T.38 Fax (UDP)** the fax-error correction method is set that the IP APL uses for communication via T.38.

Security



You need to employ TLS to encode the SIP-based communication between XPR server and the connected PBX. To this the IP APL needs a corresponding client certificate that identifies it as authorized communication partner against the PBX.

How to proceed is described in [Section 10.8, “Creating a new SIP Certificate for the XPR Server”, on page 801](#). Subsequently, you need to configure the described settings.

In the **Certificate Directory** field enter the path under which these certificates are stored.

For certificates to be used by the IP APL please note:

- The certificates must be stored on the drive on which the IP APL is also installed.
- The IP APL does not support certificates that are read-protected by password.
- The privileges for accessing the certificates must be so configured that the IP APL has read-access to the certificates.

In the **Own Certificate** field enter the name of the file that contains the certificate for the IP APL. With this certificate the IP APL authenticates itself against other communication partners. The file defined in this way must be stored in the directory defined in the **Certificate Directory** field. The IP APL accepts certificates of the formats DER and PEM.

In the **Own Private Key** field you define the name of the file that contains the private key for the IP APL. The file must be stored in the directory defined in the **Certificate Directory** field. The IP APL accepts private keys of the formats DER and PEM. PEM-based private keys must not be password protected then.

If required, you may add or remove files that contain proxy certificates for the IP APL under **Intermediate Certificates**. The specified files must be stored in the directory defined in the **Certificate Directory** field. The IP APL accepts intermediate certificates of the formats DER and PEM.

Under **Trusted Certificate Authorities** you can add or remove files that contain certificates from trustworthy certificate authorities whose certificates are to be accepted by the IP APL. The specified files must be stored in the directory defined in the **Certificate Directory** field. The IP APL accepts certificates of the formats DER and PEM.

When a TLS connection is set up, only the subscriber who accepts a connection needs to authenticate with his/her certificate by default. If you activate the **Peer Authentication** option, the subscriber who sets up the connection must also authenticate himself/herself.

If the RTP-based communication between XPR server and a terminal device is to be encrypted, an individual key must be exchanged for each RTP connection by means of MIKEY or SDES. This exchange occurs via the SIP communication. Thus, from the XPR server to the PBX and from there to the RTP terminal device, respectively reversely.

Your selection in the **SRTP payload encryption via MIKEY** field defines whether MIKEY or SDES and thus also SRTP is used between XPR server and terminal device. If you select the **MIKEY** or **SDES** option here, MIKEY or SDES and thus simultaneously also SRTP is active. The option **None** deactivates SRTP.

The XPR server uses for SDES a best-effort implementation. This allows setting up a connection even if the communications partner does not support encryption. 32- and 80-bit authentication tags can be negotiated.

IMPORTANT:

The MIKEY implementation of the XPR server currently only supports profile 0 of the MIKEY recommendation RFC3830. With this, MIKEY key data are merely sent uncoded. Therefore, TLS must definitely be activated to encode the MIKEY communication.

If TLS is not configured, the key data will be transmitted decrypted and thus in a legible format. This would be a security hole, which may lead to a violation of the system integrity.

IMPORTANT:

MIKEY may currently only be used after an individual project release.

IMPORTANT:

Activating TLS may claim a considerable portion of the XPR server system's computing performance. This may deteriorate the system performance of the XPR server from the user view.

QoS

NOTE:

The settings described here are displayed only for operating systems up to and inclusive Windows Vista. In more recent operating system versions you need to configure QoS settings policy-based and directly in the Windows operating system.

You need to configure two policies: one for SIP and one for RTP data. To each of these policies you need to assign the application IpApl.exe and the ports via which the relevant data is transferred.

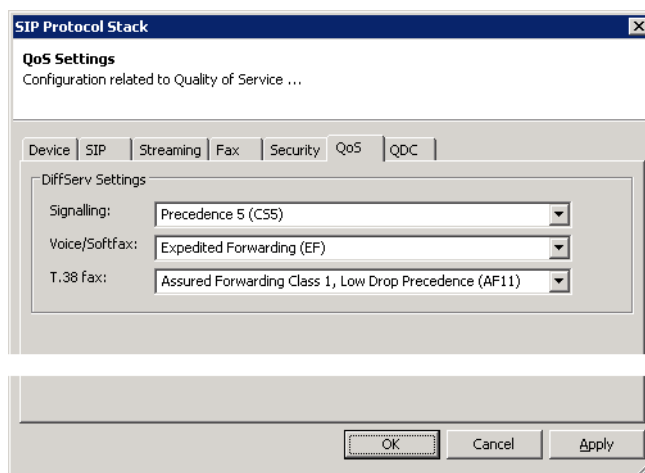
You find details on this in the producer documentation for the Windows operating system used.

IMPORTANT:

The registry value `DisableUserTOSSetting` under `HKLM/SYSTEM/CurrentControlSet/Services/Tcpip/Parameters` must be set to 0 for the QoS settings of the IP APL to be used for communication.

In most Windows versions this registry value is not configured by default. In this case you need to manually add it as `REG_DWORD` as described in the respective passage. Furthermore, the computer system needs to be rebooted for the registry modification to take effect.

If the IP APL cannot find this registry value with the entry 0, a corresponding error message is issued in the XPR monitor during the IP APL start.



On the **QoS** tab you specify the QoS settings that the IP APL uses for the SIP communication.

In doing so you can define an individual QoS class for SIP signaling, SIP voice and SIP fax transmissions.

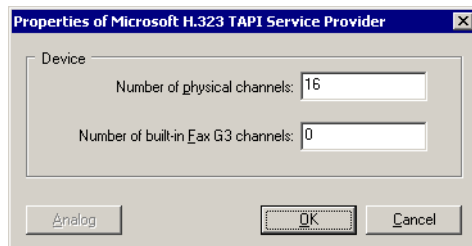
QDC

The settings on the QDC tab correspond to those for the H.323-based device (cf. [Section 10.10.4.1, “QDC”, on page 856](#)).

Properties of all other device types

NOTE:

The IP APL currently supports T.38 fax services for connections via H.323 and SIP.



The following fields correspond to the settings for the H.323-based device (cf. [Section 10.10.4.1, “Properties of H.323-based Devices”, on page 844](#)).

- **Number of physical channels**
- **Number of built-in Fax G3 channels**

IMPORTANT:

Sending and receiving of fax messages may cause disturbances in the IP APL if heavy fax traffic and the execution of maintenance script jobs coincide.

Therefore, perform maintenance script jobs at times when you do not expect heavy fax traffic – e.g. at night. If the described problem arises just the same, reduce the priority for the automatic XPR server maintenance.

The **Analog** button is currently not used by the IP APL.

10.10.4.3 Trunk Group Properties

The trunk group properties correspond in their function to those in the ISDN APL (cf. [Section 10.9.4.2, “Trunk Group Properties”, on page 829](#)).

10.10.5 Locations

The *Locations* settings correspond in their function to those in the ISDN APL (cf. [Section 10.9.5, “Locations”, on page 831](#)).

10.10.6 Several IP APLs on one Server

Only one VoIP device can be active for an IP APL. If you wish to connect several PBXs you need to either install one IP APL on a dedicated satellite for each of these systems or configure several IP APLs on one server (kernel or satellite).

The central idea is to assign several IP addresses to the XPR server. This is done either by alias or via several network boards. Each IP APL is thus connected to a unique IP address.

The protocols SIP and CorNet-IP can be used both, so that hybrid environments are possible, too.

The number of IP APLs simultaneously operating on a computer is restricted by

- the number of Voice/Fax channels per computer. See the *Release Notice* on this.
- the codecs used.
- the number of possible IP address aliases⁷ of the operating system.
- the hardware of the XPR computer (RAM, number of network boards⁸,...)

10.10.6.1 Installation

We describe the installation based on an example with one network board, one alias and four IP APLs. You can configure other combinations analog to the example described here.

- Real IP address: 192.168.10.204
- Alias IP address: 192.168.10.205

Description	Name	Protocol	IP Address	Port
First IP APL	IPAPL	SIP	192.168.10.204	5060
Second IP APL	IpApl20	SIP	192.168.10.205	5060
Third IP APL	IpApl204	CorNet IP	192.168.10.204	1720
Fourth IP APL	IpApl205	CorNet IP	192.168.10.205	1720

NOTE:

The combinations of IP address and port must be unique on an XPR server.

7. An alias is another IP address assigned to the TCP/IP protocol. To this, add further IP addresses in the **Properties** of the TCP/IP protocol under **Advanced > IP Settings > IP addresses**.

8. A combination of aliases and network boards is possible.

You install the first IP APL via the normal setup routine. You start and configure the routine just normally. In our example by SIP at an OpenScope Voice.

You need to install the second, third and fourth IP APL via command line. In the command line, execute the following commands:

```
IpApl Install -name=IpApl20 -branding=XPR
IpApl Install -name=IpApl204 -branding=XPR
IpApl Install -name=IpApl205 -branding=XPR
```

After each setup command another key is created in the registry, for the second IP APL e.g. HKLM\SOFTWARE\Wow6432Node\PP-COM\MRS\IpApl20.

You can start the other IP APLs from the command line via the following commands:

```
IpApl Start -name=IpApl20
IpApl Start -name=IpApl204
IpApl Start -name=IpApl205
```

The logical lines from each ipapl should have different indexes in order to be handled separately.

The index is taken from the first match of the sequence below:

1. AplIndex
2. Index of apl registered name (in case of ipapl2 it would be 2, in case of ipapl3 it would be 3, or in case ipapl name has no number this will not be a match)
3. System index

another example with names:

IpApl uses VOGUE_1 (Range 100 - 109)

IpApl_B uses VOGUE_2 (Range 200 - 209)

If you save IpApl settings, correl contains

```
<server>/$SYSTEM E-SCRIPTS VOGUE|VOGUE_1 IP0 Automatically
generated by TeleLib
```

```
<server>/$SYSTEM ESCRIPT VOGUE|VOGUE_1 IP 0 100-109
```

If you save the IpApl_B settings, afterwards the correl record is replaced by

```
<server>/$SYSTEM E-SCRIPTS VOGUE|VOGUE_2 IP0 Automatically
generated by TeleLib
```

```
<server>/$SYSTEM ESCRIPT VOGUE|VOGUE_2 IP0 200-209
```

Here you see that both use Index 0 (IP0)

Here the IpApl_B should be modified to use index 1. This configured via registry entry AplIndex [REG_DWORD].

```
<server>/$SYSTEM E-SCRIPTS VOGUE|VOGUE_1 IP0 Automatically
generated by TeleLib
<server>/$SYSTEM ESCRIPT VOGUE|VOGUE_1 IP 0 100-109

<server>/$SYSTEM E-SCRIPTS VOGUE|VOGUE_2 IP1 Automatically
generated by TeleLib
<server>/$SYSTEM ESCRIPT VOGUE|VOGUE_2 IP1 200-209
```

After the start, you can configure each of these IP APLs in the XPR server via their names. You can thus add protocols, extension ranges etc. as you please.

Besides configuring CorNet IP via XPR monitor, the **Private** registry entry must also be changed for it. To do this you need to open the registry key with the correct name. For the third IP APL thus HKLM\SOFTWARE\Wow6432Node\PP-COM\MRS\IpApl204\Devices\02. Supplement the entry LISTEN=192.168.10.204 in value **Private**. So that this change affects the third IP APL, stop and reboot it. Proceed analog for the fourth IP APL and add LISTEN=192.168.10.205.

Subsequently, add the new IP APLs in HKLM\SOFTWARE\Wow6432Node\PP-COM\MRS\Service\Access Protocol Layers for them to be automatically started and stopped. To do this, look for the entry "IpApl,". Paste the following three lines under this entry:

```
IpApl20,
IpApl204,
IpApl205
```

Displaying new lines in the XPR monitor

The final step is to introduce the physical lines of the newly added IP APLs to the XPR monitor. Open the **Properties** of the **Physical Lines** window and add a **New Filter** for each new IP APL.

10.11 Ending Telematics APLs “softly”

The three telematics APLs support softly ending the APL services via the command line entry `net pause <APL-Name>apl`.

Example: `net pause ipapl`

After this command the respective APL does not accept any further calls while all existing connections are handled without interference until they are closed normally. As soon as all connections are closed, the APL can be ended completely with the command `net stop <APL-Name>apl`.

Example: `net stop ipapl`

Alternatively, you can restart the respective service with the command `net continue <APL-Name>`.

Example: `net continue ipapl`

10.12 Supported Standards

IMPORTANT:

Protocol standards may contain optional features. Such optional features need not be implemented in a standard-conformable system. Depending on the optional features a producer enables, the range of features of different protocol implementations may vary.

The following table lists standards supported by the telematics APLs.

Default (– Not supported; x supported)	ISDN	IP
AMIS-ANALOG (version 1, edition 2, February 1992)	X	X
CorNet IP	–	X
CorNet N	X	–
CorNet NQ	X	–
EDSS1	X	–
H.323	–	X
QSIG	X	–
RFC 2198 (RTP payload for redundant audio data)	–	X
RFC 2543 (SIP)	–	X
RFC 5746 (TLS renegotiation)	–	X

Table 33 Standards supported by the Telematics APLs

11 Mail APL

NOTE:

An administrator with *service privilege* only sees the **Printer Embedded Codes** and **Advanced** tab.

11.1 Standard User Mailbox

All non-active document delivery is administered by the Mail APL. All users that are not connected with the XPR server through an SMI transport (TCP/IP, V.24, ISDN etc.) receive their messages through the Mail APL.

The following shows the minimum required user database entries (e.g.: TESTUSER).

Field	Content
USER	TESTUSER
Password	#####
Group	USER
Preferred	MAILBOX
Mailbox	TESTUSER

The Preferred field always points to the database field which contains the preferred delivery address. Via reference to the Mailbox field instead of a delivery address in the field of an SMI transporter no active delivery takes place. The documents are then only stored in the mailbox of the specified user. In case of active delivery the attempt is made to immediately send the incoming message to the user's computer. To this, a client that can accept the message must be operated there.

11.2 Timed Copies

Mailbox administrator functions can be used to check whether documents have met specified age limitations, and if met, measures taken (e.g. alarm copies) to ensure delivery to another user. Such measures are realized as alarm copy.

Alarm copies are defined through the Awake rules and are similarly defined as those of Carbon Copies. In addition to a delivery condition each awake rule always contains a time-dependent condition. The time period can range from 10 seconds to 30 days before the appearance of a condition, that requires an action to be initiated. Typical actions are: automatic copying of unread mail, copying of received faxes after a certain time limit, etc.

The awake rules are administered by the Mail APL, but the actual rules are configured by the MTA. See [Section 7.1.3, "Routing Rules", on page 200](#).

11.3 Broadcasts

Broadcasts are a special form of automated distribution lists in which the recipients are determined on the basis of specific criteria from the user database. Sending a broadcast requires the *Send Broadcast Privilege*. This privilege applies comprehensively to all recipients so that, for example, you can transmit messages to automatically determined fax recipients without the *Fax G3 Privilege*. Thus a broadcast reaches all potential recipients.

Syntax of possible target addresses:

NVS : <Server>/BCU : <Keyname> or
NVS : <Server>/BCU : <Expression>

<Server> is here the XPR server name. <Keyname> is a corresponding field from the user database. <Expression> is an optional expression that must be valid for a user for receiving the message. BCU means *BroadCast User* since broadcasts can only be sent to users. For <Keyname> and <Expression> only capital letters may be used. If you refer to a database field in an <Expression>, you should furnish the database field with the `UPPER` attribute. In this way the content will be reasonably processed via the <Expression>.

To send a message to all users of the XPR server, address to NVS : <Server>/BCU : . The `PREFERRED` database field is default set and can be omitted.

Examples

Given are two users with the following database entries on the XPR server:

John Doe:

CLASSNAME	CLASS	KEYNAME	KEY
USER	JOHNDOE	PREFERRED	VOICE
USER	JOHNDOE	VOICE	+4924041234567
USER	JOHNDOE	SMTP	johndoe@some.where
USER	JOHNDOE	BUILDING	RED

Jane Doe:

CLASSNAME	CLASS	KEYNAME	KEY
USER	JANEDOE	PREFERRED	EXCH
USER	JANEDOE	VOICE	+4924047654321
USER	JANEDOE	EXCH	JaneDoe@XPR
USER	JANEDOE	BUILDING	BLUE

NVS:XPR/BCU:

Two messages are sent, one to NVS:VOICE/+4924041234567 and the other one to NVS:EXCH/JaneDoe@XPR.

NVS:XPR/BCU:EXCH

One message is sent to NVS:EXCH/JaneDoe@XPR because John Doe has no Exchange address.

NVS:XPR/BCU:VOICE

Both users receive a message because both have an entry in the VOICE database field. Target addresses: NVS:VOICE/+4924041234567 and NVS:VOICE/+4924047654321

NVS:XPR/BCU:BUILDING=RED

Example of an address with *<Expression>*. Only if the BUILDING=RED expression is true, the message is delivered to the relevant user's preferred address. In this case the outcome of this is a send job to NVS:VOICE/+4924041234567.

11.4 Mailing Lists

Thirdly, the Mail APL administers simple mailing lists as are used in the Internet. For this purpose there are three commands that can be used in a text message to the user `LISTPROC`.

`SUBSCRIBE Listname Name Surname`

Subscribe to a mailing list. The mailing list is used for sending messages to the various subscribers (e-mail address).

Example: `SUBSCRIBE LP-DEVELOPMENT Joe User`

`UNSUBSCRIBE Listname`

Remove the individual e-mail address from the `Listname` list. Messages will no longer be sent to these e-mail addresses by the mailing list processor.

Example: `UNSUBSCRIBE LP-DEVELOPMENT`

`HELP`

With this command a message is returned with operational help and a list of all mailing lists existing on the server.

Internally mailing lists are treated as distribution lists that begin with the abbreviation “LP”. The definition of new lists is no longer supported since the XPR Client 2.5 required for this purpose is no longer supported. You still may, however, maintain existing lists via Communications.

To transmit a message to a mailing list, it must simply be sent to the following address:

`LST:Listname.`

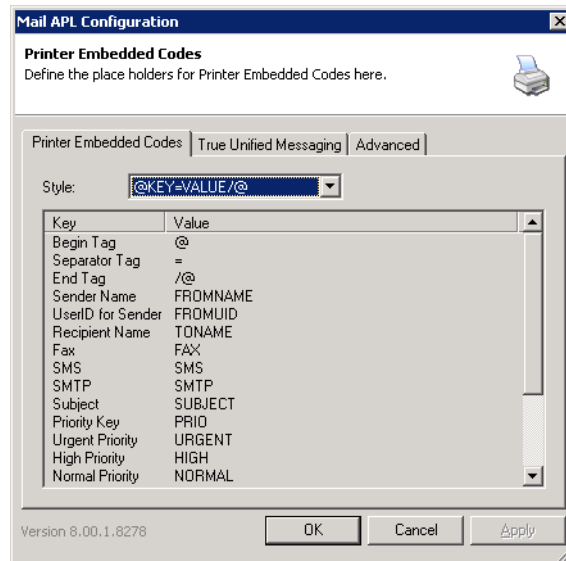
The following routing rule must be used so that the user `LISTPROC` can also be accessed from the Internet:

`NVS:SMTP/listproc*=NVS:$(NODE)/LISTPROC`

With this rule all incoming SMTP queries destined for a listproc user are routed to the mailbox `LISTPROC` user who maintains the XPR mailing lists. Without the rule all external queries addressed to `LISTPROC` would be routed to the Postmaster account.

11.5 Printer Embedded Codes

By means of printer embedded codes you can place information in a document to be evaluated by the XPR server without any special installations on the client computers. Only a corresponding PostScript printer on the XPR server is used as network printer by the clients.



Perform the following configuration steps:

1. Install a printer depending on your system:
 - a) In case of Windows Server 2008 R2 the printer included in the scope of delivery "HP LaserJet 2300 Series PS" should be used.
 - b) In case of Windows Server 2012 and Windows Server 2016 the *HP's Universal Printer Driver*, you can download under <https://support.hp.com/us-en/drivers/selfservice/UPD/4157320/model/4157320>.
2. Connect this printer to the "MRS Server Fax Monitor" port.
3. Select a name that ends in "EC" for "Embedded Codes". Thus, for example "XPR EC". "EC" must be preceded by a blank.
4. Share the printer in the network.
5. Switch the printer to the compatibility mode:

IMPORTANT:

On the client computers the printer must also be adapted to the compatibility mode though it is a network printer!

- a) Open the **Properties** of the printer.
 - b) On the **General** tab click on **Printing Preferences....**
 - c) Click on **Advanced**.
 - d) Under **Document Options > PostScript Options > PostScript Output Option** select **Optimize for Portability**.
 - e) Select **OK** three times.
6. Activate the functionality via the registry value [SupportEC \[REG_DWORD\]](#).

The Mail APL evaluates the embedded codes contained in the PostScript code of the print output and replaces these with blanks in the hardcopy.

IMPORTANT:

A Courier font must be used for making the Embedded Codes legible to the Mail APL. The printer drivers write texts binary coded in the created PostScript file for other fonts, so that the Mail APL cannot recognize the Embedded Codes anymore.

The following embedded codes are supported with the precise syntax being configurable in each case. Normally available default:

Embedded Code Example	Meaning
@FAX=263/@	Recipient fax number.
@SMTP=xy@unknown.de/@	Recipient Internet e-mail address.
@FROMUID=MAM/@	Individual XPR user ID.
@FROMNAME=Mark Maier/@	Individual name or originator name.
@SENDTIME=13:30:00/@	Send time for delayed transmission.
@SENDDATE=17.06.2001/@	Send date for delayed transmission.
@PRIO=normal/@	Message priority
@SUBJECT=Testing PEC/@	Message subject. With fax this can be displayed on the optional cover page.
@TONAME=Thomas Crown/@	Recipient name.

You can define an arbitrary number of different fax and Internet e-mail recipients per embedded code in a document. Each specified recipient receives a copy of the message then.

NOTE:

The document generated by the printer driver is a postscript file. The original file cannot be recovered from this file anymore. This is why a Word document cannot

be sent as original Word document via this function.
Depending on the SMTP APL settings this created document will be sent to Internet e-mail recipients in one of the formats configured for the SMTP APL.

The syntax of an embedded code thus reads:

<BeginTag><Token><Separator><Content><EndTag>

<BeginTag>

Example: "@"

<Token>

There are the following tokens: FAX, SMTP, FROMUID, FROMNAME, SENDTIME¹, SENDDATE, PRIO, SUBJECT, TONAME.

<Separator>

Default: "="

<Content>

Depending on the *<Token>* used, the corresponding content is here entered by the user. See above table.

<EndTag>

Example: "/@"

1. SENDTIME only works in combination with SENDDATE.

11.5.1 End-of-Job-Code

With the special End-of-Job-Code `@@END` you can have a new document created in a print job. This document will then be parsed as individual job by the Mail APL. In this new document the recipient etc. must be specified via individual embedded codes. It is thus possible to use the serial letter feature of a word processing program via this code.

NOTE:

This code may only be positioned at the end of a page or immediately before a pagebreak. In Microsoft Word, for example, you create a pagebreak via the key combination **[Ctrl] + [Enter]**.

IMPORTANT:

The compatibility mode of the PostScript printer used must be active!

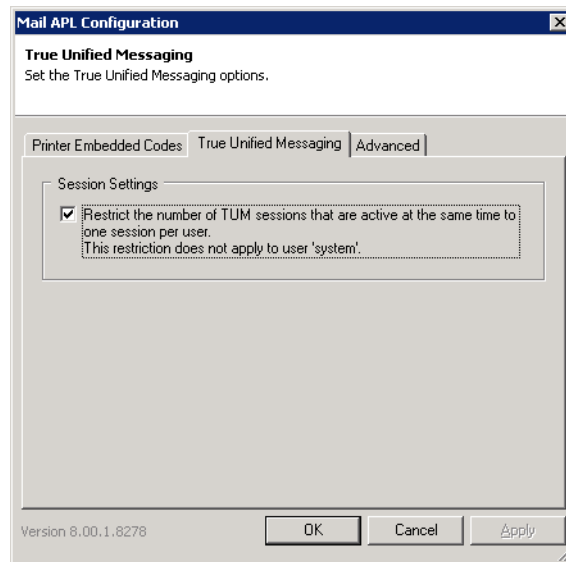
Example:

```
@SMTP=mk@company.com/@
@FAX=+49123456789/@
This is message 1
@@END
<Page Break>
@SMTP=John.Doe@somewhere.com/@
@FAX=+1987654321/@
This is message 2
@@END
```


11.6 True Unified Messaging (TUM)

The Mail APL also serves as TUM provider. Thus, all applications via the TUM protocol can access messages of the XPR server with the help of the Mail APL. These are e.g. the TUIs, but also the Notification APL.

The option **Restrict the number of TUM sessions that are active at the same time to one session per user** prevents a mailbox from being simultaneously accessed via several sessions by TUM interface. Thus, the option is basically a locking mechanism.



The TUIs as well as the Web Assistant access the user mailboxes via the TUM interface. So if you are logged in at the system by the Web Assistant, you cannot log on via the TUI until you have logged off from the Web Assistant. The period until you are automatically logged off from the Web Assistant is set to 10 minutes by default. After this period you can thus access the voicemail system again, even if you have forgotten to log off beforehand.

Other TUM providers e.g. for Lotus Notes or Microsoft Exchange have default set this restriction to a TUM session.

The user `SYSTEM` is a user automatically created by the XPR server. This user is furnished with minimum rights and required e.g. for access via TUM. With TUM a new message must always be generated by a user. Therefore, a voicemail system accessing messages by TUM always specifies this user when a caller leaves a message.

11.7 Distrib Protocol

Files can be sent directly to the virtual file system of the XPR server through use of the Distrib Protocol. Files to be used in the fax-on-demand system are automatically converted to the desired fax format.

Thereby, addresses with corresponding directories are defined. Allowable formats can additionally be assigned in which text files are automatically converted.

In the standard configuration the XPR server recognizes the addresses `NVS:DIS/<File>` (any file), `NVS:SFOD/<File>` (fax-on-demand file in the Cynos Fax G3 format) and `NVS:STOD/<File>` (fax-on-demand file in the TIFF format).

Further address types can be defined in the Registry.

11.8 The NIL Protocol

The Mail APL provides the logical line `NVS:NIL` for data transmissions. All documents sent over this line are immediately deleted by the XPR server. Documents are replaced with a notice which contains information about the administrative deletion. Researching such a transaction in the global journal can only be done by an administrator.

The purpose of this protocol are rules that automatically filter out unwanted messages and thus save XPR server resources. An example of such messages is the so-called spam, thus unsolicited advertisements by e-mail.

This can be carried a step further by sending all messages to the address `NVS:NIL/ATOMIZE`. In this case the message is deleted completely, and no journal entries are made. Consequently, this transaction does not leave any trace! An error in the rules that forward messages to this address will therefore hardly be detected.

Lastly, there is the `NVS:NIL/FAIL` address. All messages redirected to this address will be answered with an error report. This way the sender can be informed of the reject reason.

Examples

- If so-called spam mails (unsolicited advertisement e-mails) continue to be sent from the same address, these can be eliminated through use of a routing rule. The following rule deletes, for example, messages from the `spam.org` domain automatically:

```
NVS: *.*/*[org=NVS:SMTP.*/*@spam.org]=NVS:NIL/ATOMIZE
```

- Another application of the NIL protocol could be for restricting the size of outgoing transmissions. A routing rule for this purpose would have the following appearance:

```
NVS: *.*/*[org=NVS:$NODE/*;LEN>1000000]=  
NVS:NIL/TRASH[SUBJ=Mail too long - denied]
```

Through use of this rule, all messages larger than 1000000 bytes and originating from the own system would not be sent. At the same time, the document would be deleted and the subject line modified by a note to the originator. Since the mail has been marked as deleted, the following possibility is recommended. Here, a report is sent to the originator.

If a database query is implemented in this routing rule, specific users can be excluded from this rule.

- Sending a report to every originator is another solution for the above example:

```
NVS:SMTP.*/*[org=NVS:$NODE/*;LEN>1000000]=
NVS:NIL/FAIL[SUBJ=Mail too large - discarded]
```

Consequently, all Internet e-mails larger than 1000000 bytes would not be sent. At the same time, the document would be deleted and the subject line modified by a note to the originator. In this case the originator receives a failure report.

- A type of Robinson list via which transmission to specific recipients is prevented. For this purpose define a group (for example `ROBINSON`) and subsequently a rule such as:

```
NVS:FAXG3/*[GROUP(REC)=ROBINSON]=NVS:NIL/FAIL
```

All fax G3 send jobs concerning recipients who are members of the `ROBINSON` group would consequently be reported to the originator as failed. Via the corresponding report forms this could be done in a more ingenious way to adapt the error report accordingly.

11.9 Address Book Consistency

The Mail APL registers itself with the kernel for address book replication so that consistency checks can be performed. Each address book modification that does not consider the attributes of the address book fields is automatically corrected by the Mail APL.

11.10 Server CTI Journal

The Mail APL administers a central CTI journal, in which information from all available CTI transaction providers is stored. For the query the Mail APL creates by means of the CTI transaction `MONITOR` a monitor point at all CTI transaction providers. The providers then deliver regularly status information to the Mail APL using the `MONITORSTATUS` transaction.

Therefore, since all required status information is always in the server CTI journal, a CTI application need not query all CTI transaction providers itself. This provides the advantage that this information is continually collected and not just when CTI applications are running. Furthermore, information in the central CTI journal can be synchronized between numerous heterogeneous clients.

A particularity is here the support of the Alcatel Twin Device. This pair consists of a normal and a mobile phone key. A call is always signaled on both phones and can be answered at will. The PBX delivers for each of the phones the corresponding entries. A call answered on one device will be reported as not accepted on the other device. In the server CTI journal such information can be combined to a single entry, so that only one entry per call is available in the journal. This requires the activation of this feature by means of [UseAlcatelTwinDevice \[REG_DWORD\]](#).

To activate the CTI journal the following fields must be entered in the user database.

PHONE	DNO, UNIQUE
PHONE#	DNOREAD, UNIQUE
CTIJOURNAL	CHAR, UPPER

`CTIJOURNAL` has a length of 1 and is therefore a switch. An uppercase `X` activates the CTI journal for this user. The `PHONE#` database field contains the user's local phone number, which is also automatically entered in `PHONE` by normalization.

Next, an APL is required that functions as a CTI transaction provider. A line must also be provided with the form `NVS:CTI.*` so that a monitor point can be configured.

`MONITORSTATUS` reports will now be written to the correlation database, whereby one portion is the journal information and the other the current status of the telephone device. The domain `<Server Name>/$CTIJOURNAL` is always included for entries in the CTI journal. `<Server Name>` is the XPR server name.

Journal entries

CLASSNAME	CLASS	KEYNAME	KEY
USER	<Username>	<UniqueID>	<Type> <OtherPartyNumber>

<Username>

XPR user name (User ID).

<UniqueID>

Unique identification number with the format YYMMDDhhmmssnnn.

YY := Current year - 1990.

MM := Current month whereby 01 is used for January.

DD := Day of the month.

hhmmss := Time in a 24-hour format.

nnn := unique sequential number. 000 with the first call in a given second, one more with each further call in the same second. Maximum are 1000 calls in a second.

<Type>

UI := Unsuccessful Incoming call

UO := Unsuccessful Outgoing call

SI := Successful Incoming call

SO := Successful Outgoing call

<OtherPartyNumber>

Caller telephone number or that of number called.

Example

```
USER      MK      090507120155000  UI|1234567890
```

User MK was called on 7 May 1999 at 12:01:55 by 1234567890 and did not accept the call for no obvious reason. Consequently, the device may have been occupied already, or nobody answered the phone.

Status entry

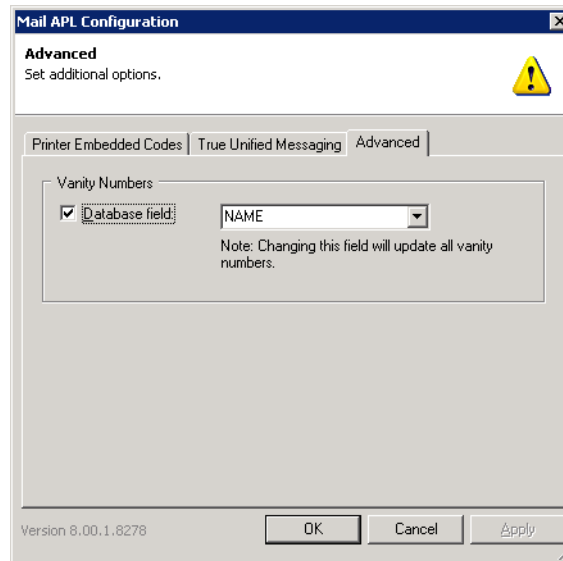
CLASSNAME	CLASS	KEYNAME	KEY
USER	<Username>	STATE	<Info>
<Info> := <State> <Direction> <OtherPartyNumber>			
<State>			
IDLE, CONNECTING, CONNECTED or BUSY.			
<Direction>			
I for incoming calls, O for outgoing or undefined calls types.			
<OtherPartyNumber>			
Caller telephone number or that of number called.			

Example

USER	MK	STATE	CONNECTED I 1234567890
User MK was called by 1234567890 and is currently connected.			

11.11 Vanity Number Support

In addition to numerals you also find letters printed on telephone dial buttons these days. Instead of cryptic telephone numbers such as 0700-2926724 you are thus enabled to keep in mind numbers of the format 0700-CYCOSAG. Such letter representations of telephone numbers are called vanity numbers.



The XPR server can use these letter combinations for dialing. To this, the digit/letter sequence is transferred from a database field to be specified to the VM_VANITY database field as number. The **database field** for this conversion can be selected here from the fields NAME and VM_HI_DSP_NAM. VM_HI_DSP_NAM contains an alternative name for representation on the display of a Hicom telephone and is used, for example, by VMS. The result in the VM_VANITY field can now be used by client applications such as a voicemail system.

The assignment of letters to numerals on the dial buttons has been standardized by the ITU. However, there are two recommendations for this assignment, option A and B. Practically, mostly option A is used, thus it is applied as default by the XPR server.

Option A

1	2 ABC	3 DEF
4 GHI	5 JKL	6 MNO
7 PQRS	8 TUV	9 WXYZ
	0	

The XPR server additionally contains a conversion table that places some special characters on specific letters, thus converting them into the numerals assigned to these letters.

Since the correlation database includes the entries in the OEM character set (code page 437), the assignment occurs for characters with a value greater than or equal to 128 to the ASCII characters A to Z.

The following table shows the assignment:

Decimal	OEM	Assigned	Decimal	OEM	Assigned
128	Ç	C	146	Æ	AE
129	ü	UE	147	ô	O
130	é	E	148	ö	OE
131	â	A	149	ò	O
132	ä	AE	150	û	U
133	à	A	151	ù	U
134	â	A	152	ÿ	Y
135	ç	C	153	Ö	OE
136	ê	E	154	Ü	UE
137	ë	E	159	f	F
138	è	E	160	á	A
139	ï	I	161	í	I
140	î	I	162	ó	O
141	ì	I	163	ú	U
142	Ä	AE	164	ñ	N
143	Å	A	165	Ñ	N
144	É	E	225	ß	SS
145	æ	AE			

Please note that all characters not listed here except A to Z are not adopted. The names “Doe, John”, “DoeJohn” or “DOEJOHN” thus result in the same numbers.

Since the assignment of vanity numbers to users, for example, via the user name cannot be unique, a corresponding dialing mechanism in a client application must consider this. In case of dialing via the number composed from the name as vanity number, the possible users are offered for selection.

12 Internet Mail (SMTP APL)

In addition to the SMTP service (Simple Mail Transfer Protocol), the SMTP APL provides several internet services concerning sending and receiving e-mails via the internet. Therefore the SMTP APL supports the protocols SMTP (client and server), POP3 (client and server), IMAP4 (server) and VPIM. The latter serves for networking voice mail servers and is configured via the Web Assistant. See also [Section 10.1.4, “Voice Mail Networking”, on page 539](#). In the SMTP APL the protocol is provided automatically.

NOTE:

If a TTS system is installed, the subject is in case of VPIM automatically sent as additional voice file. You can disable this via [NoVpimSubject \[REG_DWORD\]](#). Users to use the VPIM must have the *AMIS/VPIM Privilege*.

Furthermore, fax and SMS transmission from SAP R/3 is possible via the SMTP APL. For more information refer to the *SAP R/3 Gateway* manual.

12.1 Configuration

The configuration is performed from the XPR monitor as usual. The configuration dialog is started by double clicking the **Set Options** entry in the modules window under **<SmtpApl/Settings>**.

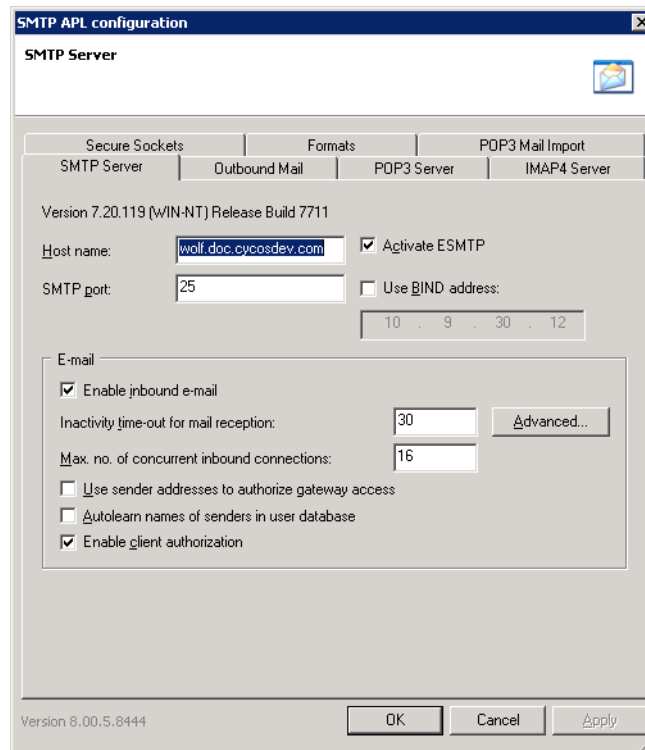
NOTE:

An administrator with *service privilege* only sees the **SMTP Server**, **Outbound Mail**, **POP3 Server**, **IMAP4 Server** and **Secure Sockets** tabs. On the **SMTP Server** tab he/she can only use the **Advanced** option.

12.1.1 SMTP server

The SMTP server enables receiving and sending e-mails via the Internet protocol Simple Mail Transfer Protocol (SMTP). For send operations some additional configurations can be performed in the **Outbound Mail** configuration tab.

12.1.1.1 General Settings



The TCP/IP Host name of the XPR Server (including the domain), is used as the default entry in the field **Host name** by the XPR Server. This entry is used for creating the originator address.

If you enter only the domain but not the host name, the XPR server creates originator addresses of the type `user@domain`. When the computer name is entered, the originator addresses are of the type `user@host.domain`.

The originator address can be individually configured for the user within the user database. Enter the complete SMTP address of the respective user in the SMTP field of the user database. This address is also used for inbound routing to the users.

The **SMTP port**: entry determines which port is used by the SMTP APL for in and outbound e-mail traffic. The default setting is 25, but when used behind a firewall, another setting may be more appropriate.

The **Use ESMTP delivery reports** option activates some advanced features, as e.g. delivery status notifications which represent an extension of the SMTP protocol (extended SMTP). Senders using ESMTP are then notified when an e-mail is received at the XPR server. Conversely, an XPR user only receives

confirmation of receipt if the relevant partner system supports this extended SMTP protocol. In addition to the ESMTP feature `DSN`, `8BITMIME`, `SIZE` and `STARTTLS` are activated via this option.

IMPORTANT:

This switch should remain activated. If you would like to deactivate single ESMTP features, you have to use the registry value [Receive_ESMTP_Capabilities \[REG_MULTI_SZ\]](#).

In the **Use BIND address:** field you can enter the IP address the SMTP server then binds itself to. In most cases this is the default IP address of the computer. In a multi-host system with numerous IP addresses, the desired IP address should be stated here, since assignment was otherwise not unique. Via the registry you can enter different IP addresses for the services SMTP server, POP3 server and IMAP4 server.

12.1.1.2 E-Mail

Via **Enable inbound mail** the gateway for incoming SMTP messages is activated. Receiving mails then occurs simultaneously through the maximum number of channels specified in **Max. no. of concurrent inbound connections**. If a value of 16 is entered, then 16 SMTP messages could be simultaneously received.

In the dialog field **Inactivity timeout for mail receipt:**, the time is given in seconds after which a transmission is terminated if no data come up any more.

By means of the **Use sender addresses to authorize gateway access** option the originator's send privileges can be checked, if the recipient address of a transmission job was e.g. `NVS:FAXG3/1234567890@domain.com`. Here the XPR server would be ordered to forward the incoming e-mail as fax message. In this case the originator must be entered in the user database and able to send Fax G3 documents.

Upon activating this option a pseudo user with the user ID `SMTP` and the privileges *Internet Mail Privilege*, *Trusted Domain Privilege*, *E-Mail Privilege*, and *USER-Privilege* is automatically defined. Without this pseudo user the SMTP APL would not be allowed to forward external messages to internal users, since the external user does not have the respective rights. In the event that a user with this identifier already exists when this option is activated, a malfunction might be the result since this user is not automatically assigned the above privileges then.

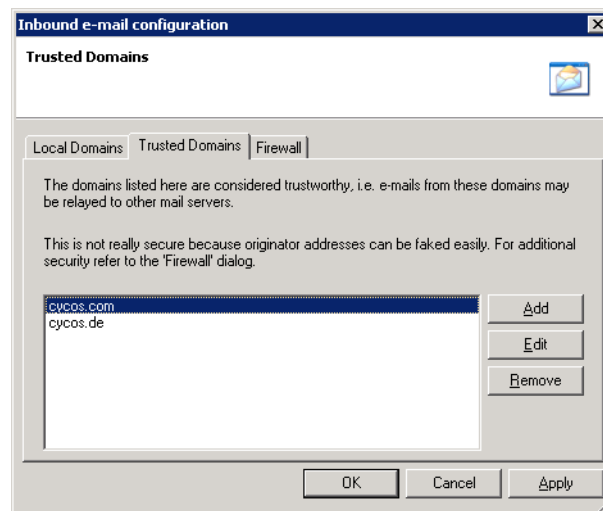
When the option **Autolearn names of senders in user database** is enabled, a contact entry is automatically created in the user database using the originator address of incoming messages. Thus, if a local user receives a message, an entry is made in the correlation database on the basis of the sender's real name.

Attention should be given to the fact that these automatically generated entries lead to a relatively fast expansion of the correlation database. Also the following conceivable scenario may cause problems: Someone has sent himself a message from his private Internet account to the company he works for. Two entries with the same name exist in the correlation database. If a person does not know the user name of the recipient and runs a search using the recipient's full name, this person will receive both addresses and could then send the message incorrectly to the private address instead of the company account.

Enable client authorization activates another ESMTP feature. In this case, the `AUTH` token, which is used for authorizing the SMTP originator using a password, is sent to the client. Via this `AUTH` token the connected client is informed that the SMTP server has this feature and the client can thus use it. Several processes are supported then. You can find more on this in [Section 12.2.1.2, “Authentication according to RFC 2554”](#), on page 916.

Advanced Button

Selecting the **Advanced** button enables the entry of local and trusted domains.



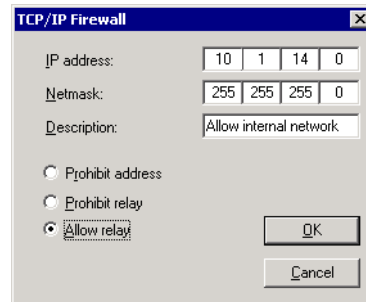
Messages are never forwarded to other Internet Hosts from within a **Local Domain**. Messages are only transmitted internally within these domains.

If the local domain has an MX-Record which points to the XPR Server, it will automatically be considered to be a local domain and must not be entered as such.

An entry for **Trusted Domains** permits SMTP messages to be sent to non-local users via the XPR server. Messages from non-authorized originators will be disregarded, without any notification to the sender.

Since recipient addresses in the Internet are easily feigned, further security measures should be set in the configuration dialog of the **Firewall** tab so that the server is not used as a relay station. Hereby access to the SMTP APL can

explicitly be permitted or refused for certain IP networks. Without an entry each address is considered “non-local”. Handling here corresponds to the description of the TCP/IP APL.



Blocked addresses do not allow a connection establishment at all any more. Blocking relay corresponds to the default if no entry is made in the firewall. Only messages to local users are accepted.

If for example the local forms for SMTP are used, relaying must be allowed for the IP addresses that use these forms. Here the incoming message is forwarded e.g. to the ISDN APL (relayed) to convert it into a fax.

Some mail servers do not allow receiving messages from a mail server that is classified as so-called Open Relay via which messages can thus be sent by everyone. Such an Open Relay is at any rate a security problem enabling so-called spammers to send their mails via the individual mail server. In this way companies can incur considerable costs as the spammer simply sends one mail with the complete recipient list to the Open Relay which subsequently routes the message to all recipients at the company's expense! For this reason we recommend to globally block relaying here and to give explicit permission only for networks where it is desired. Blocking receipt of mails from an Open Relay is normally done via lists available in the Internet. Whether the individual mail server is an Open Relay can be checked e.g. under <http://www.abuse.net/relay.html>.

Relay Authentication Strategy

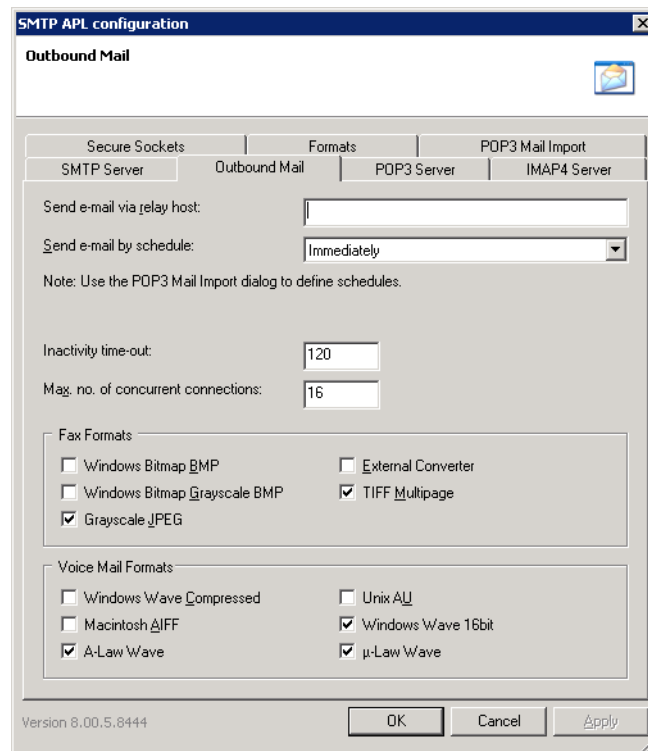
Relaying refers to the act of sending a message via an additional SMTP server. Direct delivery to the target SMTP server would be normal, but the originators may be behind a firewall or on-line only for a short while. Therefore they possibly transfer their e-mails to an SMTP server that is on-line permanent so that this server then sends the messages to the target SMTP server. In this case the XPR SMTP server would act as so-called Relay Host, defining via the following strategy when it can be used by an originator for message transmission.

- Without firewall or trusted domain entries each originator is considered “non-local”, thus must not use the SMTP server as relay.
- Firewall entries are compared with the physical IP address of the originator; trusted domains with the “Mail From” entries in the header of the e-mail. If at least one firewall entry was defined, then all unauthorized originators and

those who satisfy a relevant exclusion entry in the firewall entries are considered to be non-local, unless they have an entry as a trusted domain. Only local originators are allowed to use the SMTP server as relay.

- Through a successful verification by means of `AUTH` command or “SMTP after POP/IMAP”, the originator is also considered local except he or she would be excluded via a firewall entry.

12.1.2 Outgoing E-mail



You can optionally enter the IP address or the host name of a mail relay server to which messages are routed first using **Send mail via relay host**. This is common practice e.g. when the XPR Server cannot fully access the Internet but can reach another SMTP server that takes over this function. This could be for example a firewall which is used to protect the company's network from Internet intrusion.

NOTE:

The SMTP APL is used for message routing within an SN network (system networking network). If system networking is used in combination with the **Send e-mail via relay host** option, routing information must be configured in the relay host, so that all XPR and connect server addresses can be reached from there. For further information please refer to [Section 8.11, "SMTP Routing via Relay Host"](#), on page 328.

The option **Send mail by schedule**: allows the selection of a direct network connection or of one defined in the user database. For user-defined connections, schedules can be assigned to users in the configuration tab **POP3 Mail Import**. In this constellation, a PPP-Connection is established through the Windows RAS service. Outbound Internet e-mail messages are then sent over this connection. Outgoing Internet e-mail messages are sent immediately when a direct network

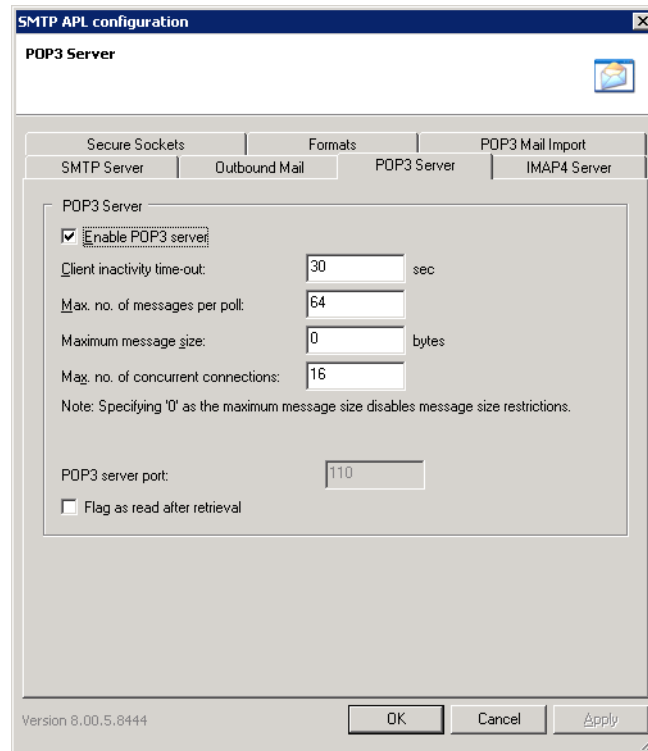
connection (dedicated line, etc.) or equivalent Internet connection is used. This happens either directly or indirectly through the Relay Host which was entered in this dialog.

After the time selected under **Inactivity timeout**, the server clears down an inactive outgoing connection.

Max. no. of concurrent connections: is the number of send jobs that can be carried out parallel. This value should not be measured too high if the available band width is relatively small. Otherwise the send processes are increasingly canceled owing to timeouts as the receiving party had to wait too long.

If required, outbound fax and voice messages can be converted into one or more formats to be selected under **Fax Formats** or **Voice Mail Formats**. It goes without saying that this only applies to rerouted or directly sent documents and not to attachments of normal e-mails. Precisely one conversion is performed each, even if several possible target formats are specified. Here, an internal evaluation comes to bear that performs the “cheapest” conversion from the converters point of view. An overview of the formats can be found in [Appendix A, “Document Formats”](#).

12.1.3 POP3 Server



The **Enable POP3 server** option activates the POP3 server at the **POP3 server port** displayed.

In the **Client inactivity timeout:** field you can enter the time in seconds after which the POP3 server terminates transmission in case of irregularities in the form of connection inactivities. This value can be adapted individually via a respective database entry of the user. Therefore create a field named `POP3_TIMEOUT` in the user database and enter a higher value for users with a very slow connection.

In case of a connection, the messages set in **Max. no. of messages per poll:** are transmitted to the POP3 client with the **Maximum messages size:** in bytes. An entry of zero in **Maximum messages size** denotes that the set amount of messages can, regardless their size, be transferred in one go.

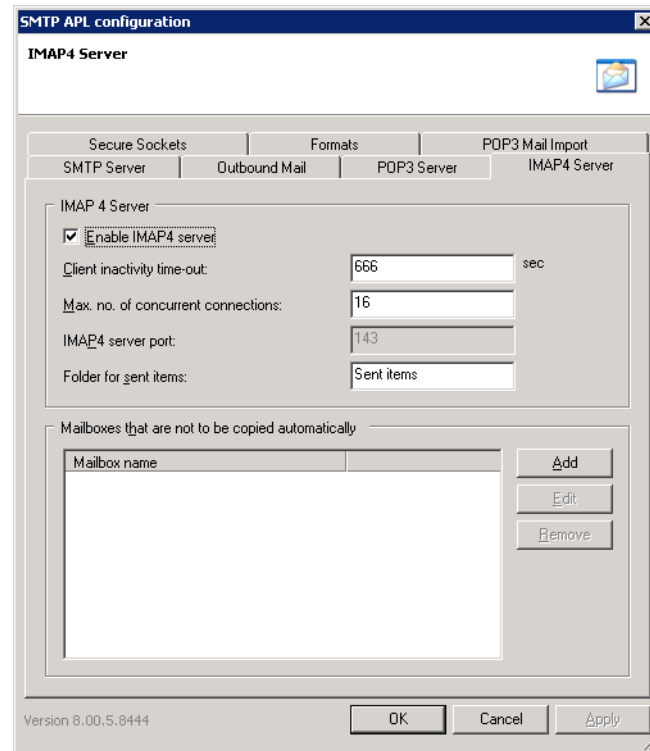
IMPORTANT:

If **Max. no. of messages per poll** were set to zero, *no* messages would be transmitted any more!

Max. no. of concurrent connections: limits the number of POP3 clients that can simultaneously access the server.

Via **Flag as read after retrieval** you can inform the XPR Server that polled messages are flagged as read on the server as soon as they have been polled via a POP3 client. Since there is no further interaction between the POP3 client and the POP3 server after message polling, this is the only way to indicate these messages accordingly. Otherwise polled messages would be considered unread and thus new with a later access to the individual XPR mailbox via another client (TUI, Lotus Notes, etc.).

12.1.4 IMAP4 Server



Selecting the option **Enable IMAP4 server** activates the IMAP4 server on the port indicated in the field **IMAP4 server port**. The port can be set via the registry if required.

With the IMAP4 protocol, documents remain on the server and only header information is fetched at login. Since only a small amount of data is being transferred, restrictions required by POP3 servers becomes unnecessary.

In the option **Client inactivity timeout:**, the time is entered in seconds after which the IMAP4 server terminates a connection if no data are transferred to and from the client any more. The presetting is 666 seconds which is a bit more than the Microsoft Outlook standard poll rate, querying new messages every 600 seconds.

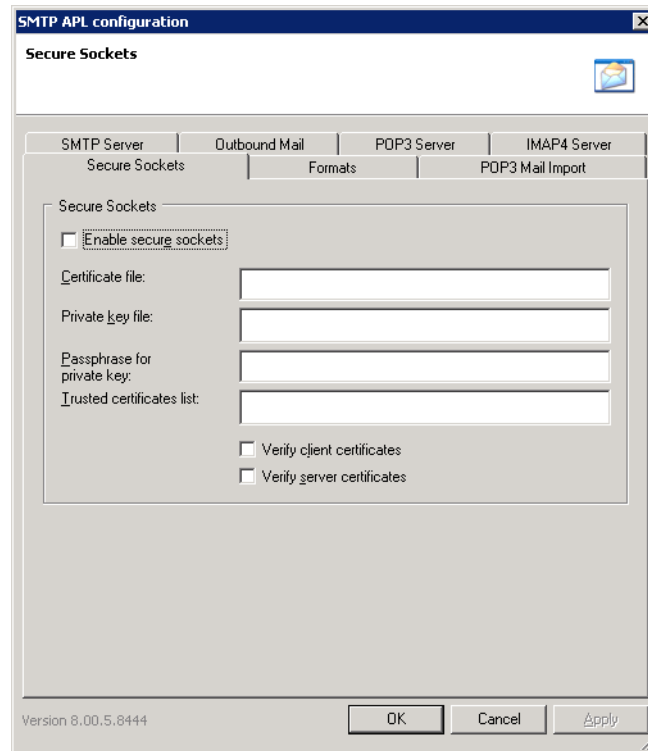
Max. no. of concurrent connections: restricts the number of IMAP clients that may simultaneously access the server.

Individual folders can be configured as a repository for transmitted and deleted messages. The names of these folders should be entered in the **Folder for sent items:** field.

In the **Mailboxes that should not be copied automatically** field you can specify the XPR Server folder name for which XPR is to ignore a copy command. Note that for example Outlook provides a setting called 'Save copies of messages in "Sent Items" folder', via which copies of the sent documents are automatically

generated. But since the XPR Server has a corresponding folder for all outgoing documents, these copies are pointless. In particular when access is made via older IMAP clients that can handle folders only restrictedly or not at all, documents are displayed twice since these clients display all documents from all folders in a flat view. The user can thus specify that the XPR server ignore the copy instruction for specific folders if the above setting is selected.

12.1.5 Secure Sockets



Via the **Enable Secure Sockets** you can activate an SSL ciphering (Secure Sockets [SSL/TLS]) for IMAP, POP, SMTP sending and receiving.

NOTE:

Using SSL V2 and V3 is always disabled in the XPR server. TLS V1, V1.1 or V1.2 is always used.

The used ports are preset to the ports used by Outlook 2000, that is for the port 995 for POP3 and the port 993 for IMAP4. These ports can be adapted via the registry if required.

For SMTP sending and receiving the STARTTLS command is supported. The option **verify server certificates** enables you to check the certificates of receiving stations for the case that the SMTPApI acts as client, thus sends messages and the option **verify client certificates** enables you to check the certificates of the station for the case that it is acting as server and receives messages.

If the verify client option is used, the certificates will be used whenever smtpapi receives a connection (when it receives a message).

If the verify server option is used, the certificates will be used whenever smtpapi connects to another server (when it sends a message).

Both options "Verify client certificates" or "Verify server certificates" will never be used at the same time, but they can be used by the same smtpapl as it sometimes can send messages and in other times it will receive messages.

With secure sockets activation the entries **Certificate file**, **Private key file**, **Passphrase for private key** and **Trusted CA file** must contain reasonable values. The procedure for requesting the necessary files is as follows:

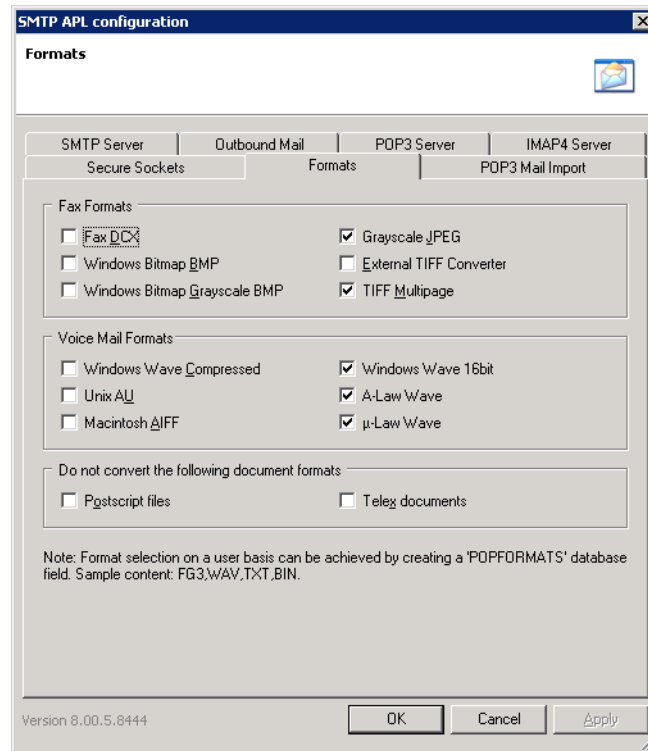
You need a certificate of an internationally accepted CA (Certificate Authorities). Such a CA is e.g. Verisign (www.verisign.com), however, also one of the most expensive. In order to obtain a certificate you should follow the procedure issued by the individual CAs.

The **Certificate file**, the **Private key file** and the **Passphrase for private key** received from the CA are entered. The files must be stored in the directory `<XPR Install>\res\certs`. The password must at any rate be entered via the configuration tab here since it is stored in the registry enciphered. The term "Passphrase" is to point out that a whole sentence rather than a simple password should be used to enhance security. If you create an individual certificate, please definitely make sure that the resulting files are coded with the Base64 method. All certificates coded in another way lead to an error message in the XPR monitor.

The **OpenSSL** program is required to request the certificate or for generating a simple test certificate to view the general functionality. You find this tool under `<XPR Install>\SDKTools\opensslcy.exe`.

NOTE: Even with self-signed certificates, the CA root certificate is needed. You can't use the end entity certificate as the CA file. You can create the CA root certificate as well as the self-signed certificate.

12.1.6 Formats



File formats, into which documents and attachments for POP3 and IMAP4 clients are converted. This field can be overwritten by a database entry `POPFORMATS` of the user. For an individual assignment via the user database the format `BIN` should *always* be entered.

If a fax or voice mail is already in one of the selected formats, it is simply forwarded to the recipient. Otherwise the fax or voice mail is converted to one of the formats the clients support. Precisely one conversion is performed each, even if several possible target formats are specified. Here, an internal evaluation comes to bear that performs the “cheapest” conversion from the converters point of view.

If Postscript or telex files can be displayed by the client a conversion to either a graphic or text format should be included. Otherwise, postscript and telex files are delivered in one of the selected fax formats.

An overview of the formats can be found in [Appendix A, “Document Formats”](#).

12.1.7 POP3 Mail Import

The Windows remote data transmission service (RAS) must be installed for the POP3 mail import. With the POP3 mail import, you can download Internet mail for your XPR users from another POP3 server to the XPR server using either a PPP or a RAS connection.

Either an Alias account is used under which all internet mail from the provider is pooled for the user, or each user is assigned a time frame in which a connection is to be made. If the account for which messages are being fetched has no entry in the user database field `GROUP`, it will be treated as an Alias account for a complete Internet User/Domain group.

12.1.7.1 New Database Fields

Four new database fields must be installed in the user database for use with the POP3 Mail-Import service. These are described in the following table:

Database field	Meaning
<code>PMI-SCHEDULE</code>	Includes the name of a time schedule. This schedule determines the time at which a connection to the POP3 server is established. See Section 12.1.7.3, "Active Schedules", on page 913 . (Attributes: <code>CHAR</code>)
<code>PMI-USERNAME</code>	User name for which e-mail is retrieved from the POP3 server. If no entry is given, the XPR user ID will be used. (Attributes: <code>CHAR</code>)
<code>PMI-PASSWORD</code>	User login password for the POP3 server. (Attributes: <code>CHAR</code> , <code>CIPH</code>)
<code>PMI-HOSTNAME</code>	Hostname of the POP3 server at which the e-mail is to be retrieved. (Attributes: <code>CHAR</code> , <code>LOWER</code>)

These fields may contain either a pseudo account (Default: `MAILIMPORTER`), which is used for retrieving e-mail for all users in a company or else only for those users for whom an Internet e-mail address was set up at the POP3 server. A combination of both these possibilities is also possible. The XPR Server recognizes pseudo accounts with `PMI` fields through the empty user database field `GROUP`.

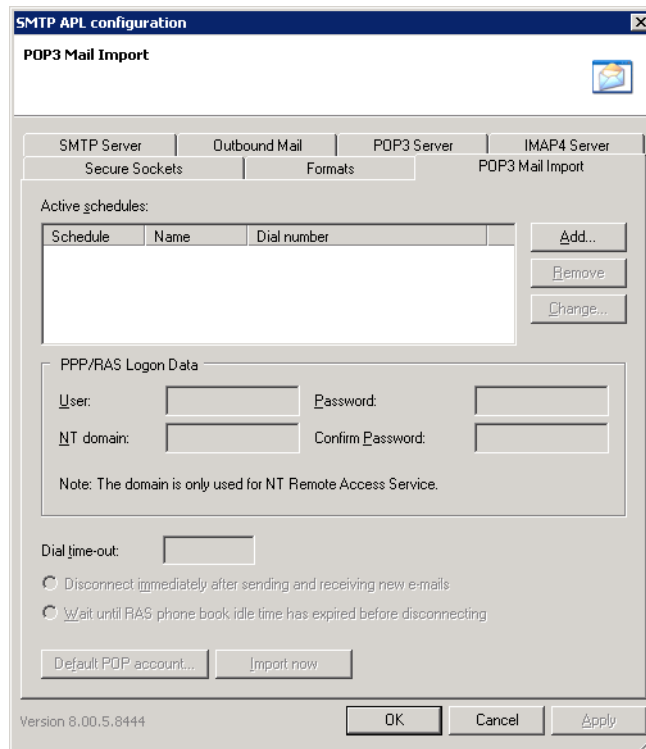
The SMTP APL searches the user database for users with the field `PMI-SCHEDULE` and imports their Internet e-mail in accordance with the scheduling data.

12.1.7.2 Authentication for sending

Messages are imported and any existing messages are also sent in parallel at this time. If the SMTP server of the Internet mail provider is being used here as a relay, the following authentication mechanisms are possible:

- SMTP after POP
Because authentication has already taken place through the POP3 mail import, the relay server accepts the incoming messages for a certain time. See also [RelayAllowedSecs \[REG_DWORD\]](#).
- Authentication according to RFC 2554
If the relay server offers one of the PLAIN, LOGIN or CRAM-MD5 procedures, this is used. CRAM-MD5 is the preferred choice, as it is the most secure of the three. In this case, authentication is performed via the database fields PMI-USERNAME and PMI-PASSWORD.

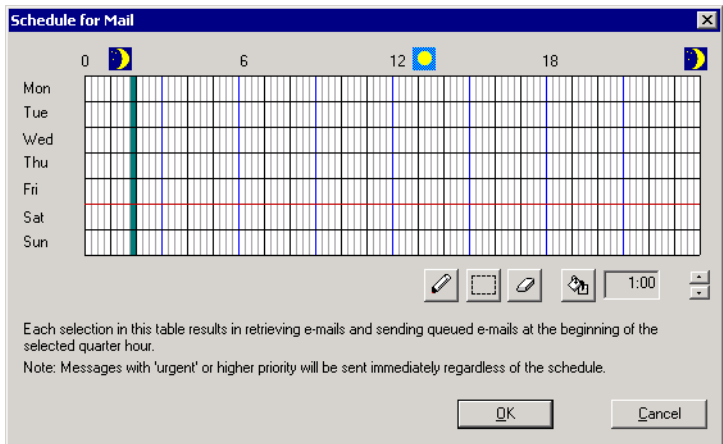
12.1.7.3 Active Schedules



New schedules can be inserted with the **Add** button. The new schedule must be assigned a name and a dialing number from the RAS telephone book. The new schedule must then be assigned to a minimum of one user before it can be executed.

To delete an existing schedule simply select the schedule and subsequently the **Remove** button.

After the creation of a new schedule, the times at which it is executed must be entered. This is done through selection of the **Edit** button. In each of the selected ranges a connection is established by means of RAS. Via this connection the e-mail for the different users is exchanged with the POP3 servers set in the user database.



The function of the individual buttons is explained in the following table:

Button	Meaning
	Assigns "pen" characteristics to the mouse pointer with which you can select/delete the individual fields of the scheduling table.
	This button enables the selection of a range within the scheduling table. The functions of the following two buttons can be applied to the area within marked range or to that outside the range.
	Deletes either the complete schedule, or that within or outside the marked range.
	After a time interval assigned, the left-hand icon (fill icon) is selected. The complete schedule or that within or outside the marked range can then be filled using the fill tool. The complete schedule or the area within or outside the marked range would be filled, beginning at 0:00 (12 o'clock midnight) with the selected time interval. Using this method, an hourly POP3 Mail Import can be easily configured.

PPP/RAS Logon Data for <Schedule>

Users and their **password** can be assigned to every schedule. The password is entered for the user and subsequently confirmed through a second entry of the password. This account data is used for establishing a PPP connection. The optional **NT Domain** is only required when a connection to another Windows NT computer is to be set up to exchange Internet e-mail messages with a POP3 server within that Windows network.

The **Dial timeout:** option defines the time in seconds after which dialing is stopped due to the non-establishment of a connection. A redial attempt will not be executed.

An existing RAS connection can either be immediately terminated through use of the option **Disconnect immediately after sending and receiving new email**, or after expiration of the configured RAS inactivity time-out when the option **Wait until RAS phone book idle time has expired before disconnecting** is selected. It should be noted that even though the first option is somewhat more cost effective, it does not take into consideration that other data transfer activities may be occurring during the connection time. An immediate termination of the RAS connection does exactly what it implies regardless of any other background activities. In the case of the inactivity time-out, a reasonable amount of time should be given for Windows NT RAS services.

Through selection of the button **Default POP account** POP3 servers and POP user names with their corresponding password can be entered. Internet mail for this account (MAILIMPORTER) would be fetched according to the times stipulated in the schedule entered in the field **Import by schedule**.

Default Mail Import POP Account

Internet address of the POP3 server: PMI-HOSTNAME

POP user name: PMI-USERNAME

Password: PMI-PASSWORD

Confirm password:

Import by schedule: PMI-SCHEDULE

Note: These entries correspond to the database fields of the MAILIMPORTER user account. You may create additional mail import accounts by filling in all of these fields for other user accounts in the client's user editor.

OK Cancel

When the button **Import now** is selected a connection attempt is immediately executed. Internet e-mail for those users whose database contains an entry for the selected schedule in the field `PMI-SCHEDULE` will be fetched once the connection has been established.

12.2 SMTP (Simple Mail Transfer Protocol)

SMTP (Simple Mail Transfer Protocol) defines an international standard for e-mail transmissions within the Internet. Messages are exchanged worldwide in a 7-Bit ASCII code.

An extension of SMTP is MIME (Multipurpose Internet Mail Extensions) in which arbitrary data (images, voice mails, binary files, etc.) is transmitted through SMTP. Since there are numerous extensions to the SMTP protocol, the term ESMTP (Extended Simple Mail Transfer Protocol) is generally used in association with Internet mail. Among these extended services, Delivery Status Notification (RFC 1891) is supported by the SMTP APL so that, depending on the server, delivery reports are sent to the message recipient.

12.2.1 Authentication

12.2.1.1 SMTP after POP/IMAP

SMTP after POP/IMAP accepts messages from an SMTP client for a configurable time after a POP/IMAP connection to this client. You can set the time in seconds in the registry value `RelayAllowedSecs`. However, this is a somewhat makeshift procedure and you should, where possible, use one of the following procedures according to RFC 2554.

12.2.1.2 Authentication according to RFC 2554

Another ESMTP feature is the `AUTH`-Token which serves to authorize the SMTP originator by means of a password. Via this `AUTH` token the connected client is informed that the SMTP server has this feature. The client may thus use it. There are various procedures by which the password can be transferred. For incoming messages, the XPR server offers the procedures:

- PLAIN (Plain login mechanism (single step) according to RFC 2595)

The user password is transmitted here base64-coded. This is a well known simple coding, so that one might also speak of plain text. It is only secure if a mechanism such as SSL is used for the actual SMTP connection.

- CRAM-MD5 (Challenge-Response Authentication Mechanism according to RFC 2195)

With this process the password transmitted by the user is already relatively safe owing to the MD5 procedure (RFC 1321). Although a decoding approach theoretically exists, it would in practice take an exorbitant amount of calculation. If you were to compare the life cycle of MD5 with that of

passwords, you can regard MD5 as being secure even in the coming decades. We recommend using this procedure if you can configure it in the client.

- LOGIN (Plain login mechanism (two step))

This is a non-standard process, where the password is transmitted in the clear text. For example, Microsoft Outlook uses this procedure. It is only secure if a mechanism such as SSL is used for the actual SMTP connection.

For the CRAM-MD5 process the SMTP APL needs to know the password in the clear text. This, however, is not possible with the default database entry `PASSWORD`. Therefore, the database field `POP-PASSWORD` is used here, which should be added to the user database with type `CIPH,CHAR` and a reasonable password length (approx. 40 characters) when the above feature is employed. If the field `POP-PASSWORD` is not available, there is another fallback for this procedure to the alternative database field `SMTPAUTH-PWD`, which must also be equipped with the attributes `CIPH` and `CHAR`. With the `PLAIN` and `LOGIN` processes, the entry `PASSWORD` is used alternatively to a not existing or empty `POP-PASSWORD` database field. In addition, the password transferred by the client is encoded internally with the one-way algorithm used for `PASSWORD` and subsequently checked against this.

Please note that authentication for the SMTP server may be required and cannot be explicitly configured in the Netscape Messenger. Netscape Messenger automatically uses the `PLAIN` procedure if it is offered.

If you do not want to have explicit authentication with a password, you must deactivate the `AUTH` feature with the registry key `Receive_EnableAuth`.

12.2.2 Relay Authentication Strategy

Relaying refers to the act of sending a message via an additional SMTP server. Normal refers to messages directly sent to the destination SMTP server. However, in the case of relaying, originators may be behind a firewall or only briefly online and may choose to forward their e-mails to an SMTP server that is permanently online so that it sends the messages to the destination SMTP server. In these cases, the XPR SMTP server acts as a relay host and uses the following strategies to define when it can be used by an originator for sending messages.

- If neither firewall nor Trusted Domain entries have been defined, each originator is considered local and may thus use the SMTP server as relay.
- Firewall entries are compared with the physical IP address of the originator; trusted domains with the "Mail From" entries in the header of the e-mail. If at least one firewall entry was defined, then all unauthorized originators and those who satisfy a relevant exclusion entry in the firewall entries are considered to be non-local, unless they have an entry as a trusted domain. Originators not local must not use the SMTP server as relay.

- Through a successful verification by means of `AUTH` command or “SMTP after POP/IMAP”, the originator is also considered local except he or she would be excluded via a firewall entry.

12.2.3 Sending Mail via an SMTP Relay

When sending mail via a relay host, it is of course also possible to use the authentication mechanisms according to RFC 2554 as discussed above (see registry value `RelayHost`). However, because some SMTP servers differentiate between upper and lower case lettering for the user account and password, whilst the database field `USER` only allows upper case, it is possible to assign an alternative user name and a plain-text password via the database fields `SMTPAUTH-USR` (Attribute: `CHAR`) and `SMTPAUTH-PWD` (Attributes: `CHAR`, `CIPH`). If `SMTPAUTH-PWD` is not available, the database field `POP-PASSWORD` (Attributes: `CHAR`, `CIPH`) is taken.

12.2.4 Setting Reply-To Field

If you send SMTP messages from a foreign system such as Lotus notes via the XPR server, you might receive originator addresses of this type:

```
"LN/<First name> <Last name>/<Notes>"@domain.com
```

Now you can add the field `SMTPREPLYTO` to the user database and insert one alternative originator address for each user. This address is written to the Reply To header field, so that answers are forwarded to this address.

12.3 POP3 and IMAP4 Servers

SMTP always attempts to deliver the messages directly to the recipient. These messages are often delivered to the POP3 (Post Office Protocol Version 3) server because very few users keep their PCs running permanently and rarely have a direct connection to the Internet. The POP3 server receives the e-mails and saves them until they are retrieved by the user with a POP3 client. With POP3 messages are flagged as deleted on the server after they have been retrieved and are only available on the client computer.

The IMAP4 (Internet Message Access Protocol Version 4) serves the same purpose as POP3 but is more modern. Messages remain on the server and therefore, the deletion of messages are dependent on the servers configuration. IMAP4 offers several advantages since messages can be presorted to various mailboxes. This allows for a clear concise overview with large amounts of incoming mail. In most cases, the IMAP4 client retrieves only the header file when querying for new mail. The complete message is only retrieved when explicitly requested. As opposed to the POP3 client which retrieves all new messages, this method of retrieval allows users with lower transfer rates select only those messages immediately needed.

Computers where a WWW browser such as Netscape or Microsoft Internet Explorer is installed contain a POP3 or IMAP4 client which provides these features to the XPR user.

12.3.1 Authentication

Clients usually transfer their user ID and password through POP/IMAP in plain text, and these are checked against the database fields `USER/PASSWORD`. If the database field `POP-PASSWORD` exists for a user, this is taken instead of `PASSWORD`. This procedure should only be carried out by an SSL secure connection as it is otherwise too insecure.

As a POP3 server, the XPR server also supports the APOP procedure according to RFC 1939, where no plain text password is transferred. Instead a string is transferred which identifies the desired mailbox and an MD5 Digest. To do this, however, the XPR server must know the plain text password, so the database field `POP-PASSWORD` for the users must be maintained.

As an IMAP4 server, the XPR server also supports the CRAM-MD5 procedure according to RFC 2095. This procedure functions in a similar way to the APOP procedure, so the database field `POP-PASSWORD` for the users must be maintained.

Besides this procedure, it is also possible to transfer the Windows user account via the intranet in the form `Domain\Account` and thus make use of the Windows authentication. This requires that the `LMAccount` database field be accordingly maintained on the XPR server. See [Section 5.4, "Client log-in via Windows User](#)

[Account](#)", on page 162.

12.4 Standards

The SMTP APL supports the following standards:

RFC	Degree of support
821	SMTP (a restriction results from the maximum length of 64 characters in case of an e-mail address).
822	SMTP (fully supported)
1651	ESMTP (fully supported)
1870	SIZE (fully supported)
1891	DSN (fully supported)
1939	POP3 (fully supported)
2045	MIME (fully supported)
2046	MIME (fully supported)
2060	IMAP4rev1 (fully supported)
2421	VPIM (MUST and SHOULD only)
2554	AUTH (fully supported)
2595	SSL/TLS (so far supported by OpenSSL)
2683	IMAP4rev1 (fully supported)

Table 34 Supported RFCs the SMTP APL

13 The XPR Webserver (Web APL)

IMPORTANT:

A possibly installed IIS (Internet Information Server) **must not** be uninstalled; the server is automatically deactivated by installing the Web APL!

13.1 Overview

Via the WEB APL a complete HTTP 1.0 web server is available. Within the XPR system the web server serves e.g. as interface for the administration of the user data via the Web Assistant as well as for complete access to the individual mailbox via any HTML browser such as the Microsoft Internet Explorer.

Another available script performed by the Web APL is the IP-Phone Assistant, which enables access to text messages, voicemails and greetings via an optiPoint application module or an OpenStage 60 respectively 80 telephone. You find additional information on this in the *IP-Phone Assistant* manual.

The complete integration of the E-Script language on the server enables the realization of almost any scenario over a HTTP connection. The HTML pages sent to the Web Assistant contain XPR-specific information which is delivered by the E-script. This could be, for example, the fax document the user desires or his/her inbox.

Besides the Web Server functionality the WEB APL can also operate as HTTP Client and be controlled by other XPR components via transactions to automatically poll HTML pages from any Web Server. The information contained in these pages can be processed per script to e.g. readout certain stock exchange quotations. If required, desired functionalities can be requested from the sales department.

Configuring the Web APL

The WEB APL is configured via the XPR monitor.

1. Open the entry **WebApl** in the component window under **Settings**.
2. Double-click on the option **Edit Settings** and enter your administrator password.

The WEB APL configuration dialog is displayed.

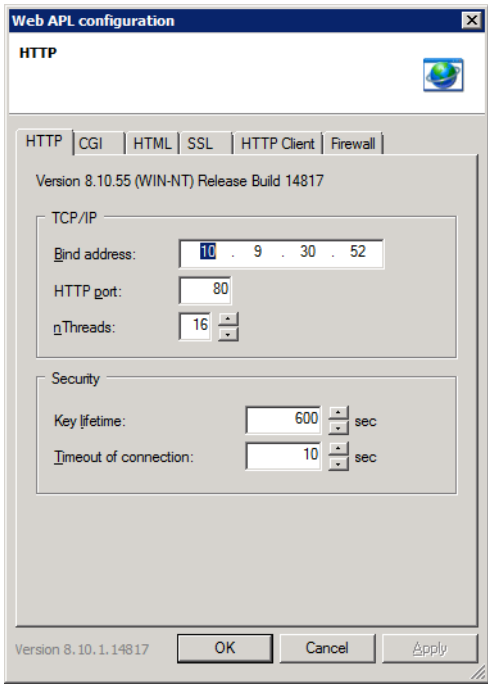
13.2 Configuring the Web APL

NOTE:

An administrator with the *service privilege* only sees the **CGI**, **SSL** and **Firewall** tabs.

13.2.1 HTTP Tab

IMPORTANT: The HTTP – not HTTPS – protocol is disabled by default for security reasons. You must switch it on via the registry value [HTTP_Enable \[REG_DWORD\]](#) to activate it.



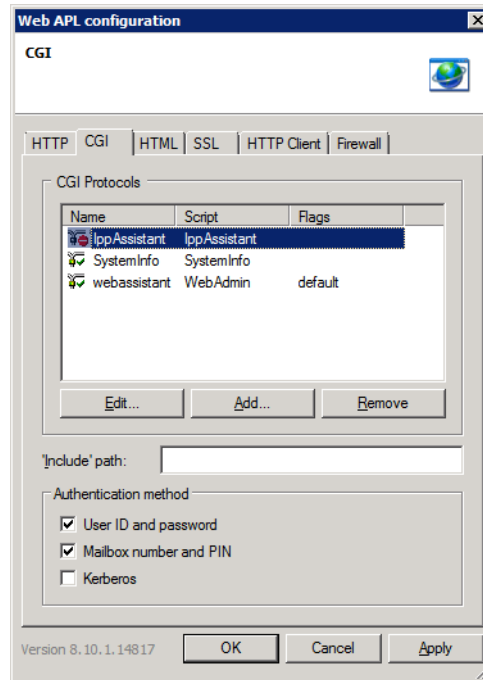
Option	Description
TCP/IP	
Bind Address	In this section the bind address is entered the web server is to use. This is of interest to the administrator when more than one IP address is available for the server.
HTTP Port	The HTTP port entry determines which port is used by the web server for queries and replies.
nThreads	The number of nThreads defines the number of web browsers which may be used simultaneously.

Option	Description
Security	
Key lifetime	Users log in to the XPR server by entering their account name and associated password. After the check-up has been completed, a key is issued by the web server which is valid for subsequent queries by the user. After the key lifetime in seconds has expired, the key loses its validity and the user must login again to receive a new key. The maximum value is 32767 seconds, which corresponds to somewhat more than 9 hours. This procedure increases security, so that likelihood of manipulation on the URL containing the key is reduced. This security feature may be inadvertently deactivated by the client. In the Web Assistant you can have your inbox automatically updated. If this period is smaller than the time-out set here, the Web Assistant will continuously request data and thus reset this time-out.
Time-out of connection	If no data is currently being transferred, the connection to the client will be released after the expiration of the connection time-out in seconds.

13.2.2 CGI Tab

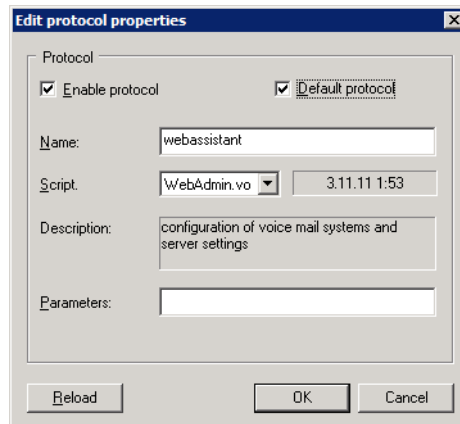
In this configuration tab the protocols provided by the Web APL are entered. For each additional protocol an **E-Script** must be given which executes the dynamic replacement in the sent HTML pages. This could be for example, the current inbound journal of the logged-in user.

If one of these scripts is uncompiled, the **Include path**: to the E-Header Files needs to be specified as well. This is only necessary with locally written E-Scripts.



In the **Authentication method** section you can set whether a login should only be possible via **User ID and password**, **Mailbox number and PIN**, or via **Kerberos**. Kerberos enables single sign-on (SSO) for the Web Assistant. You find details about the SSO configuration and requirements in [Section 13.2.2.1, “Configuring Single Sign-on \(SSO\)”](#), on page 927.

Via **Edit**, **Add** and **Remove** the configuration of existing protocols can be altered, new protocols be added or existing ones be removed again. In the first two cases the following settings dialog opens:



Option	Description
Script	Via the Script pull-down menu one of the installed scripts is specified. In the case of a file with the extension *.vo, this is a previously compiled file, and the date and time of its creation is displayed in the opposite field.
Name, Parameter	Above the script the name of the protocol is given. Thus various protocols can be installed based on one E-Script. Depending on the parameters entered, these protocols show a different behavior. Attention: Dependencies may occur in the HTML pages and partly also in the script itself that directly reference the protocol name. Therefore the file name should always be the first choice as protocol name and not before this name works, others should be tried.
Reload	If the script is an E-Script not previously compiled, it can be Reloaded after an alteration.
Default protocol	Precisely one of these protocols is the default protocol, which is automatically invoked when the web server is addressed, i.e. a page like www.cycos.com is called in a web server. The other protocols can be addressed by attaching the protocol name in the following manner: www.domain.com/cgi_bin/<Protocol>

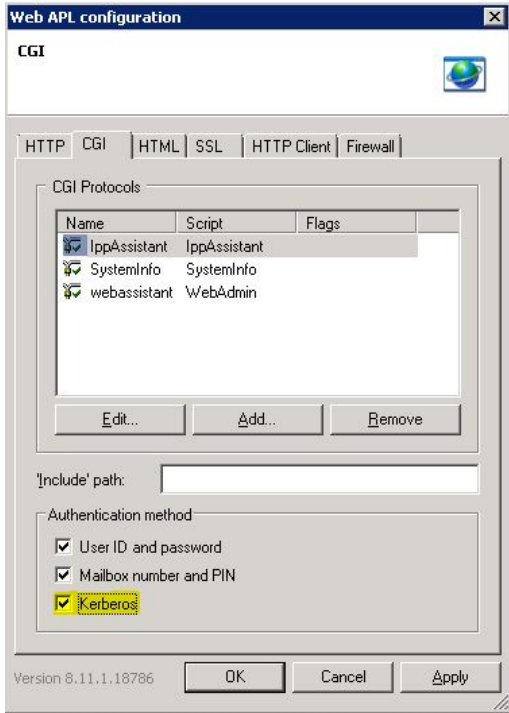
13.2.2.1 Configuring Single Sign-on (SSO)

Single sign-on enables a Windows user to deploy further network services after he/she has authenticated at his/her workstation without having to authenticate against such services again. This is possible in the scope of XPR for the Web Assistant.

NOTE: If you usually login in Web Assistant using the domain as an alias and not the hostname, you need to add the domain on the following registry key:
HKLM\Software\Wow6432Node\PP-COM\MRS\WebApl\SsoDomains

The following requirements need to be complied with:

- The **Kerberos** option is active in the Web APL as **authentication method**.



- The user's `LMACCOUNT` field contains the Windows domain and the Windows user account.

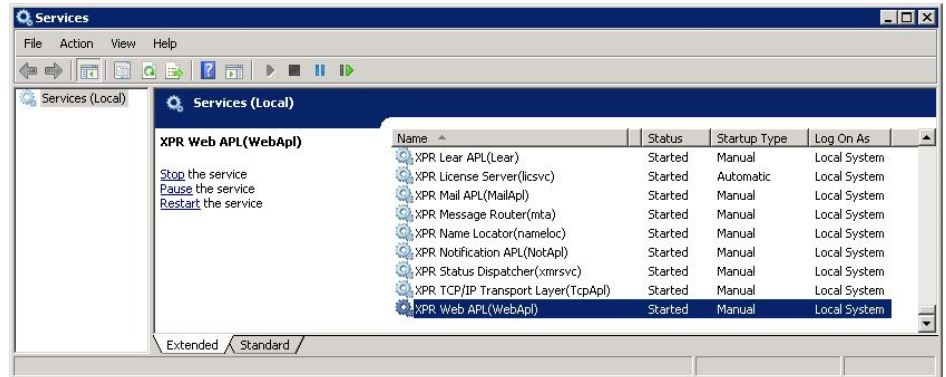
The screenshot shows the 'DbTool - XPRCLUSTERCOPIA on XPRCLUSTERCOPIA (local machine)' window. It contains a table with the following data:

Domain	Class name	Class	Key name	Key
XPRCLUSTERCOPIA	USER	ZZ1000	GROUP	USER
XPRCLUSTERCOPIA	USER	ZZ1000	LMACCOUNT	COPA\ZZ1000

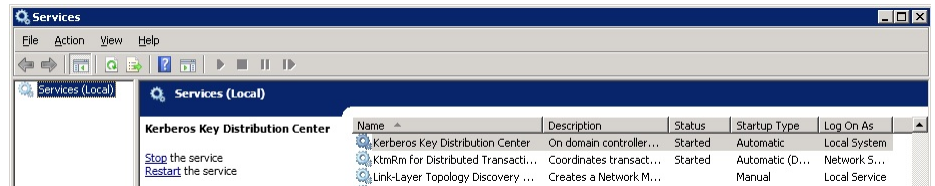
- The Web APL must run with a local system account. Assigning a domain account is not possible.

NOTE: This requirement implicitly prevents setting up the Web APL on a satellite if you wish to use the *single sign-on* feature.





- Kerberos expects a running service *Key Distribution Center* (KDC). In case of Windows Server 2008, this service is a component of the *Active Directory Domain Services*. In case of Windows Server 2003 it is the *kdc* service. The *Key Distribution Center* is active on a domain controller if you do not explicitly deactivate it.



- Kerberos uses time stamps. The time must therefore be synchronized between all involved computers (domain controller, XPR server with Web APL, client PC). You can achieve this via the Network Time Protocol (NTP), for example.
- The browser must be configured on the client, so that it sends the Windows login data. This is possible as of Internet Explorer 6 and Firefox 4.

Configuring Internet Explorer

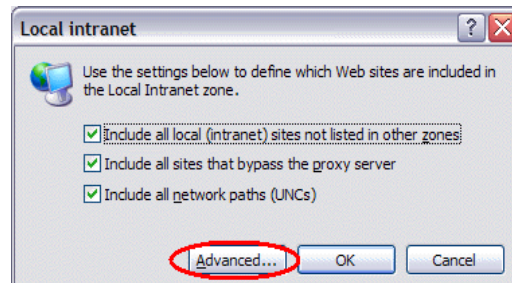
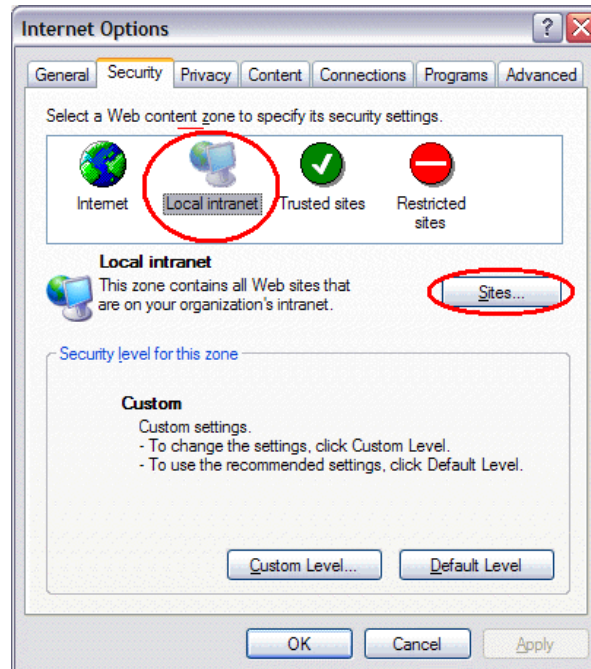
Microsoft delivers the appropriate settings in the <http://technet.microsoft.com/en-us/library/ms995329.aspx> article for the Internet Explorer. In there, follow the instructions given under *Client Side–Internet Explorer*. For your convenience, you may find them below as well.

Configure local intranet sites

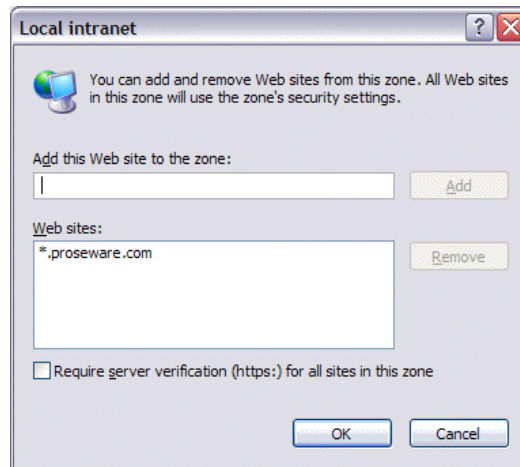
First, configure the “Local intranet” properties in Internet Explorer.

1. In Internet Explorer, click **Tools**, and then click **Internet Options**.
2. Click the **Security** tab.
3. Click **Local intranet**.

4. Click **Sites**.



5. Ensure that **Include all sites that bypass the proxy server** is checked, then click **Advanced**.
6. In the **Local intranet (Advanced)** dialog box, enter all relative domain names that will be used on the intranet (for example, *.proseware.com).

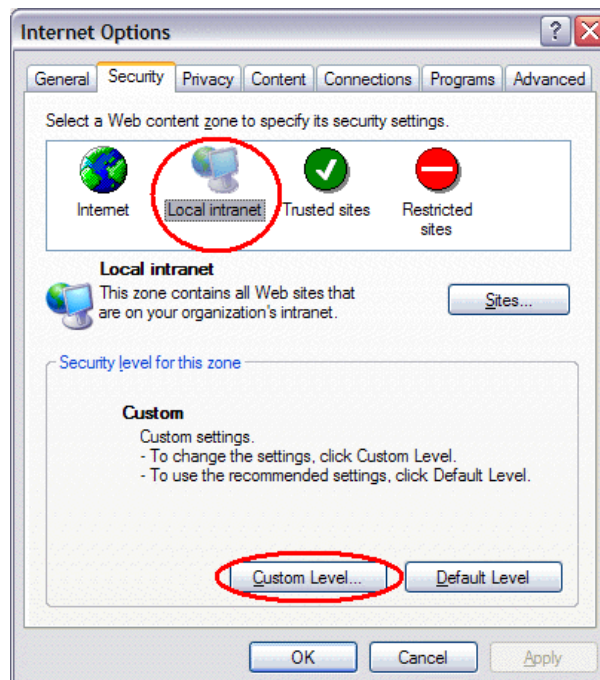


Copy/Paste the URL address the client use to login in Web Assistant (e.g., `https://xprservername.domain.net/cgi_bin/webassistant/start`). Only the FQDN name of the XPR server is used.

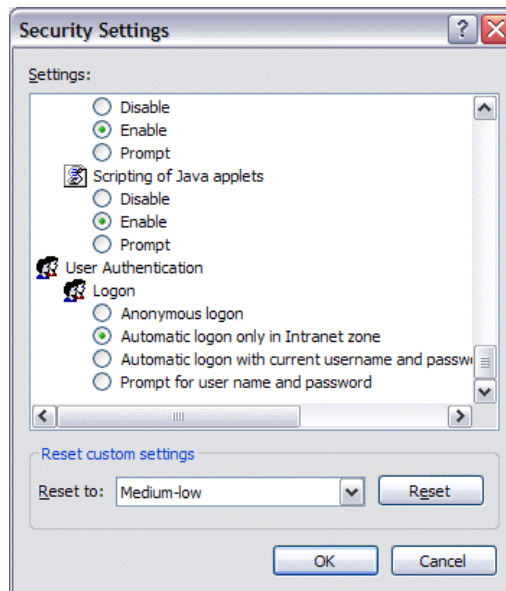
7. Click **OK** to close the dialog boxes.

Configure intranet authentication

1. Next, click the **Security** tab, click **Local intranet**, and then click **Custom Level**.



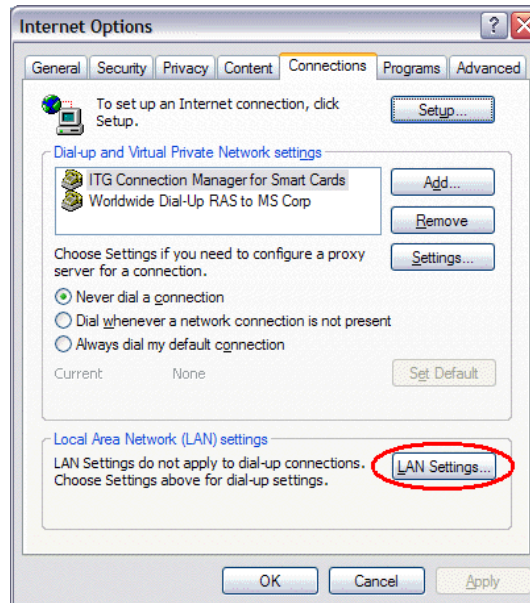
2. In the **Security Settings** dialog box, scroll down to the User Authentication section of the list.



3. Select **Automatic logon only in Intranet zone**. This setting will prevent users from having to re-enter logon credentials; a key piece of the solution.
4. Click **OK** to close the **Security Settings** dialog box.

Verify proxy settings

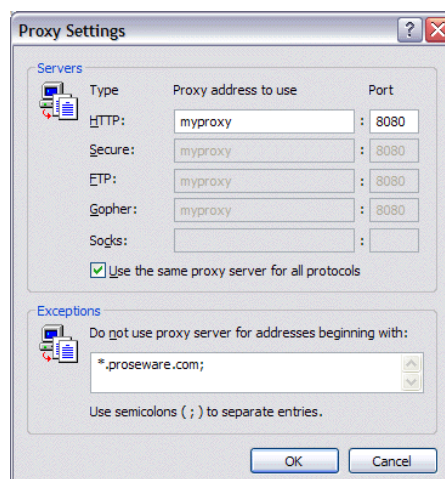
1. In Internet Explorer, click **Tools**, and then click **Internet Options**.
2. Click the **Connections** tab.



3. Click **LAN Settings**.

NOTE: An automatic configuration script can be used to create these settings. We are making the settings manually for ease of explanation. For information about using automatic configuration scripts, see Microsoft's TechNet site.

4. Verify that the proxy server address and port number are correct.
5. Click **Advanced**.
6. In the **Proxy Settings** dialog box, ensure that all desired domain names are entered in the **Exceptions** field (for example, *.proseware.com):

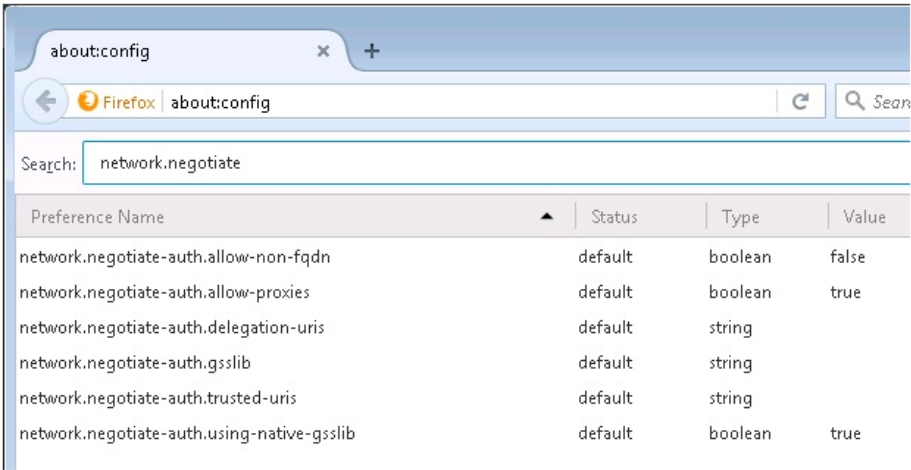


- 7. Click **OK** to close the **Proxy Settings** dialog box.

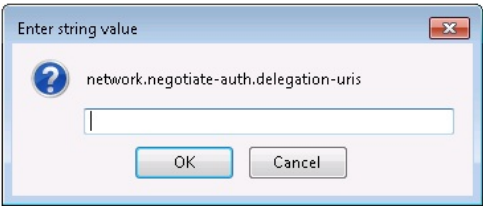
Configuring Firefox

The following steps are required for Firefox 4:

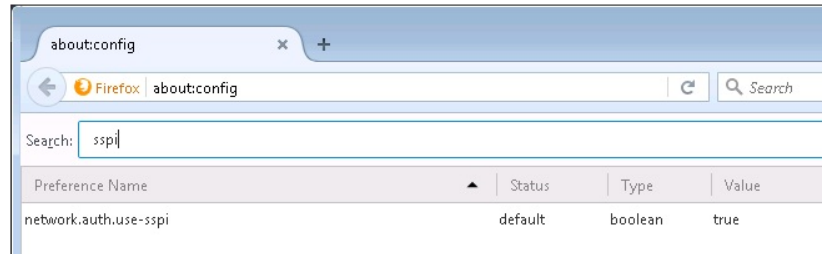
- 1. Enter `about:config` in the *address bar*.
- 2. Enter `network.negotiate` under **Filter** (or under **Search**, in newer versions of Firefox).



- 3. Add the individual domain or the Web Assistant address under **network.negotiate-auth.delegation-uris**, for example `xprservername.domain.net`. If a value has already been entered, add the individual entry separated by a comma.



- 4. Enter `sspi` under **Filter** (or under **Search**, in newer versions of Firefox).
- 5. Set **network.auth.use-sspi** to `true`.



- You need to invoke the Web Assistant with its FQDN address. Thus for example
<https://xprserver.xpressions.net/>, not
<https://xprserver/>

13.2.2.2 Creating an HTML Forwarding Page

Here you can manually generate a corresponding HTML forwarding page for each protocol to enable users to invoke the protocols via the following invocation:
www.domain.com/<Protocol>

The contents of these files would then include a meta tag of the following type as it is also used in the index.htm for the default HTML page:

```
<meta http-equiv="Refresh" content="0; URL=/cgi_bin/WebAdmin/start">
```

Please note that the specification of the protocol in the URL must precisely correspond to the name of the protocol as it has been configured in the Web APL, thus upper and lower case must be correct as well. If you made a mistake here, the referenced page would not be found and the Web APL would call the default set protocol.

The adaptations depicted in the following paragraph are required on the client computers for the Meta-Tag is executed on a Windows server.

13.2.2.3 Using Web Protocols under Windows Server

As a result of the new restricted security settings of the Internet Explorer under Windows Server, web protocols can only be used after easing or customizing several security settings.

IMPORTANT:

Please note that your system becomes vulnerable to potential assaults from other web sites you might visit when security settings are eased. If you are not sure whether you are allowed to modify the security settings, it is necessary that you contact your system administrator.

You can customize the security settings globally (for the whole "Internet" zone) or for single web sites (trusted sites). Both settings are performed in the browser menu under **Tools > Internet Options...** in the **Security** tab.

If you want to add, for example, the Web Assistant to the list of trusted web sites, select the **Trusted sites** zone on the **Security** tab before you click on the **Sites...** button. Enter the HTTP address of the Web Assistant in the following dialog and **add** it to the address list. If you have a SSL certificate and want to use it, check mark the option **Require server verification (https:) for all sites in this zone**.

For global modifications select the **Internet** zone on the **Security** tab before you click on the button **Custom Level....** In the following window the functions **Active Scripting** and **META REFRESH** must be adjusted to **Enable**. Save your settings by clicking on the **OK** button.

13.2.2.4 Replication Trigger for LDAP

The LDAP APL supports a replication that is executed at configurable times. So that a replication can also be executed immediately, you can add the LdapSync.vo protocol here in interaction with the LDAP APL.

To have a replication immediately executed, you can then simply address the following link:

```
http(s)://<Hostname>/cgi_bin/<Protocol name>/<LDAP Server>
```

Example:

```
https://cycos.com/cgi_bin/LdapSync/Ex2003
```

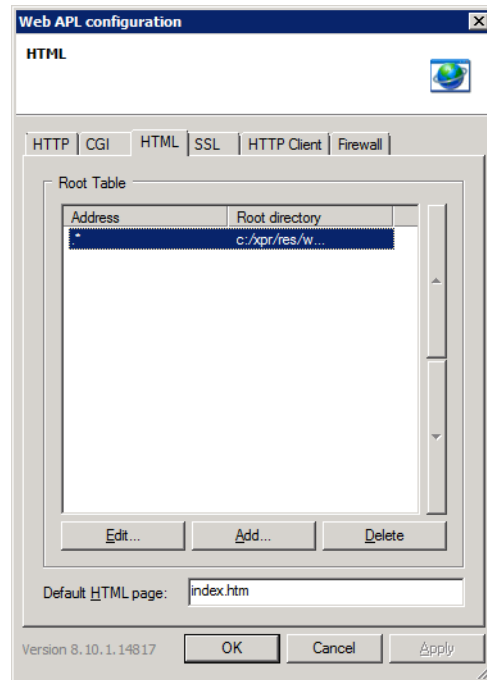
If you want to configure an *<LDAP Server>* as default, you can make the corresponding setting in the **Parameters** field. You need to specify the `ldapservers=<LDAP Server>` parameter for this purpose. In this case an invocation of the following link is sufficient:

```
http(s)://<Hostname>/cgi_bin/<Protocol name>/
```

Example: LdapSync with parameter `ldapservers=Ex2003`

```
https://cycos.com/cgi_bin/LdapSync/
```

13.2.3 HTML Tab



Through use of the **Root Table**, various directories can be given, to which individual addresses are assigned. In this way numerous www sites under various addresses may be hosted (Web Hosting).

The buttons **Edit**, **Add** and **Delete** can be used for the configuration of addresses and start directory.

Addresses are given in regular expressions. Further information on regular expressions can be found in [Section 7.4.4.1, “Regular Expressions”, on page 248](#).

Additionally, addresses are processed from the top of the table until a match is found for the requested address. Therefore, the order in which addresses appear in the table is important. The order can be rearranged with the arrow on the right hand-side of the menu.

The default HTML page is sent to the Web Client when no other one is explicitly requested. This is normal during the first request since in most cases only the web address for example `www.domain.com` is given.

The HTML file referenced here normally contains a special HTML tag that forwards to one of the installed protocols, thus for example:

```
<meta http-equiv="Refresh" content="0; URL=/cgi_bin/WebAdmin/start">
```

The XPR Webserver (Web APL)

Please note that the specification of the protocol in the URL must precisely correspond to the name of the protocol as it has been configured in the Web APL, thus upper and lower case must be correct as well. If you made a mistake here, the referenced page would not be found and the Web APL would call the default protocol if it has been defined.

13.2.4 SSL Tab

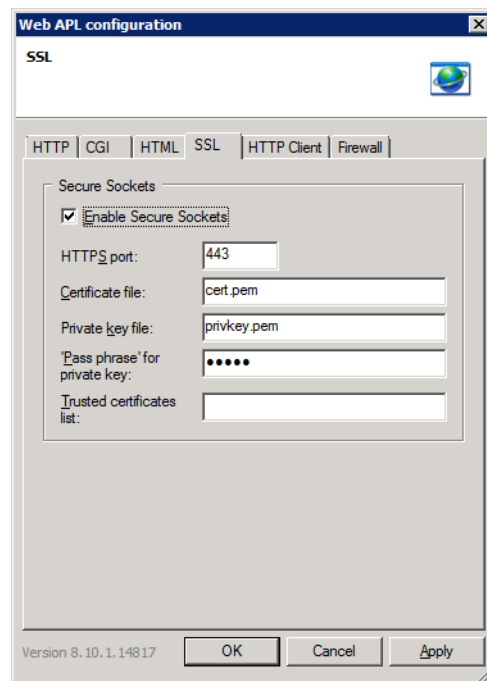
In this dialog you can configure the Secure Socket Layer protocol (SSL). The protocol's primary purpose is to enable a safe and particularly private communication between two applications. In this case the two applications are the web server realized by the Web APL and the web browser employed by the user.

Consequently, with an active SSL connection, e.g. the password transmission for polling individual messages can no longer be read by the administrator in charge of the systems used for the message transfer.

The Web APL as well as the SMTP APL are attached to a unique configuration with a certificate for SSL. The information on activating SSL in [Section 12.1.5, "Secure Sockets", on page 909](#) are thus also valid for the Web APL.

NOTE:

Using SSL V2 and V3 is always disabled in the XPR server. TLS V1, V1.1 or V1.2 is always used.



13.2.4.1 SSL Connection Problems

If the server has no Internet connection, it cannot load any updated certificates from the Microsoft Update server. In this case, four messages of the following content are written in the event display for each SSL connection:

Failed auto update retrieval of third-party root list sequence number from: <<http://www.download.windowsupdate.com/msdownload/update/v3/static/trustedr/en/authrootseq.txt>> with error: This network connection does not exist.

You find further information and solution options concerning this problem under <http://support.microsoft.com/kb/317541/en-us>.

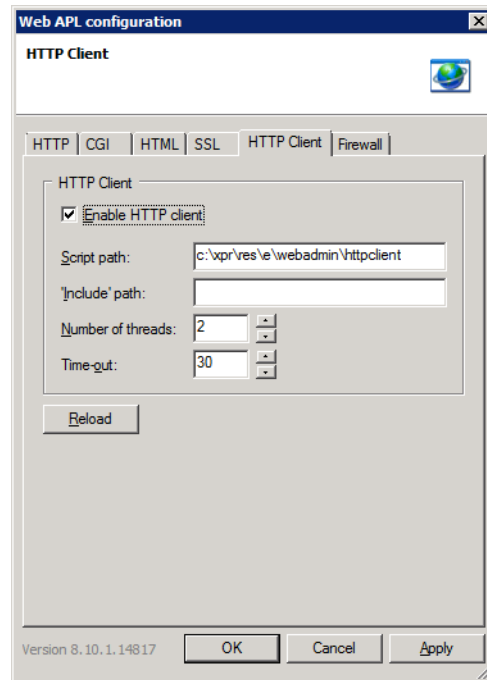
13.2.4.2 VeriSign Intermediate Certificate has expired

Secure Site Pro certificates by Verisign may have been signed with an "Intermediate Certificate" no longer valid. This causes the browser to issue a security warning to the users.

Via the Web server you can provide the browsers with a new version of this Intermediate Certificate though. Proceed as follows:

1. Open the following link in a browser:
<http://www.verisign.com/support/verisign-intermediate-ca/secure-site-pro-intermediate/index.html>
2. Follow the instructions on the displayed website to copy the shown certificate to a text file.
3. Save the text file in the directory `<XPR Server>\res\certs`. You can name the text file for example `VeriSignIntermediate.pem`.
4. Enter the name of the text file in the **Trusted certificates list** field.

13.2.5 HTTP Client Tab

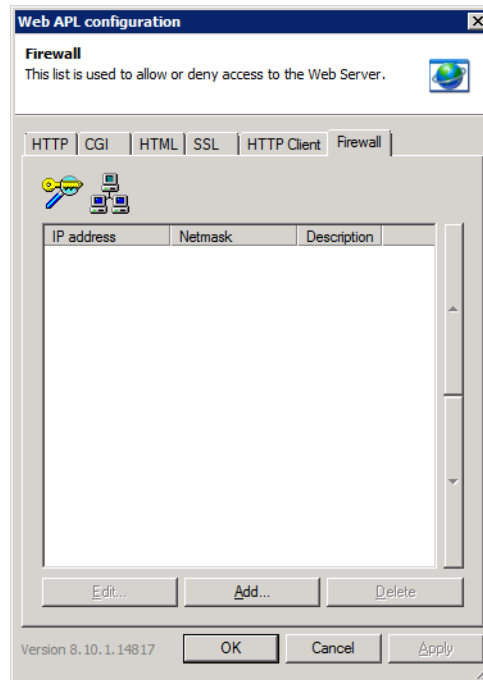


The HTTP client permanently integrated in the Web APL is controlled via transactions from another APL. Do not confuse it with the Web Assistant implemented as CGI protocol. This is to say that the Web APL acts as HTTP client and, for example, controlled by transactions, polls pages from another Web Server and evaluates these with the script specified here to return corresponding information. An example were the regular polling of stock exchange quotations. These transactions are passed on to a dedicated E-Script which executes the instructions.

This E-script or the compiled *.vo is entered including the path under **Script path** and possibly the path to the E-header files used is entered under **Include path**. The latter is only required if the script is not compiled. You should pay attention to the fact that when started the Web APL automatically regards all scripts found in the `<XPR Install>\res\WebAPL\` directory as CGI scripts. Thus, you should not store the HTTP Client script in this directory, but for example in `<XPR Install>\res\WebAPL\Client\`.

Via **nThreads** the number of connections the HTTP client can establish simultaneously is specified. In **Time-out** the period is set (in seconds) after which a connection is released when no data are received from the addressed Web server anymore.

13.2.6 Firewall Tab



Via this configuration tab additional safety measures can be taken. For certain IP networks access to the Web Server can explicitly be allowed or denied. This corresponds to the firewall handling for the TCP/IP APL described in [Section 15.2, “Firewall Mechanism”](#), on page 1028.

13.3 Standards

The Web APL supports the following standards:

RFC	Degree of support
1945	HTTP 1.0 (MUST and SHOULD only)
2595	SSL/TLS (so far supported by OpenSSL)

Table 35 Supported RFCs the Web APL

13.4 Enforcing SSL Accesses for the Web Assistant

You cannot configure the Web APL for exclusively using SSL. If you have configured SSL, though, and want to run all requests to the Web Assistant via SSL as far as possible, you can achieve this by modifying the file `<XPR Install>\res\WebApl\index.htm`.

In this file the following line must be adapted:

```
<meta http-equiv="Refresh" content="0; URL=/cgi_bin/webadmin$/start">
```

By modifying the URL, all HTTP requests shall be rerouted to https. To this, you need to enter a complete URL specifying the IP address respectively the computer's Fully Qualified Domain Name (FQDN) with the Web APL. With the FQDN `www.cycos.com`, the URL had to be specified in the above line as follows:

```
URL=https://www.cycos.com/cgi_bin/webadmin$/start
```

If a user does not enter the complete URL inclusive http (e.g. `http://www.cycos.com/cgi_bin/webadmin$/start`), every Web Assistant invocation will be rerouted to an SSL connection owing to this modification.

NOTE:

If you use the Web Message Access, you should adapt the URL used there as well. See [Section 16.7, “Web Message Access”, on page 1042](#).

13.5 Fax-printing Problems

The XPR server converts a fax to make it fit on one page. In case of fax printing from a browser, the default setting of one inch usually applies for the page margins. This shifts the browser fax-printout to the bottom right. Consequently, some sections are cut off and missing in the printout.

To circumvent this error, you can either adjust the page margins before printing the fax or the registry value [EMailFaxWidth \[REG_SZ\]](#). With a value of 730 the fax is further minimized and then completely printed out.

13.6 Customizing the Web Assistant Interface

IMPORTANT:

To utilize the options described in this chapter you need to have programming knowledge. Only modify the scripts if you know exactly what you are doing! You might render the Web Assistant interface inoperative by inconsiderate modifications.

Modified Web Assistant scripts are not part of the producer support and will be lost during the next server update.

This chapter includes an introduction to the options you have to modify the interface, and to the Web Assistant functionality.

Most Web Assistant pages are HTML forms. An HTML form as seen by the user who employs the Web Assistant is based on a file stored on the XPR server. This file contains, besides an HTML basic framework, special tags and wildcards.

The HTML files are found in the following directory:

```
<XPR Install>\xpr\res\WebApl\WebAdmin\html
```

When a page is invoked, a parser searches the HTML file for known tags and wildcards and replaces them dynamically with data (strings) delivered by a WebApl script in a CGI list. The parser was exclusively developed for the programming language E.

The parser is composed of two components:

- CGI functions for E-web scripting, which are implemented in the script itself (individual module `CgiList.e/XCgiList.e`)
- Special tags and character strings, which serve as wildcards for dynamic contents of the HTML page

13.6.1 Data Transmission between Browser and XPR Server

Transmission of data from a form to an E-script is handled using the POST/GET commands. The form data are then written in dynamic multilevel CGI lists.

Each element of such a list consists of a key/ name and an associated value. The value may be a string or another list.

Each of such lists can be sorted. The lists are arranged alphabetically.

CGI functions provide write and read access to single elements of such a list.

13.6.2 Wildcard

Wildcards are special tags and strings that are dynamically replaced by the parser with elements from a CGI list. Wildcards can also be used in JavaScripts, which are integrated in the HTML page. They cannot be used in JavaScripts that are present in separate files, though.

A string to be replaced by the parser must start with the at-character (@) and end on a semicolon (;). For example:

```
@Teststring;  
@Teststring;; (generates a string with attached semicolon.)
```

If an at-character is to be represented in the resulting page to display, for example, an e-mail address, the at-character must be used twice:

```
my.name@@company.com
```

13.6.3 Changing Web Assistant Default Settings

IMPORTANT:

You modify the `param.xml` at your own risk!

Modifications affect the entire Web Assistant. Support will not be provided after you have changed default settings.

The Web Assistant default settings are defined in the following files:

```
<XPR Install>\res\WebApl\Webadmin\param.xml  
<XPR Install>\res\WebApl\Webadmin\param.xml
```

These files define the default values of a number of parameters that determine the appearance and behavior of the Web Assistant.

There are two configuration files to prevent the customer-specific settings in the configuration file from getting overwritten. The contents of the configuration files is identical for the initial installation. The customer performs individual changes exclusively in the `param.xml`. The `default_param.xml` file remains untouched!

At the start, the respective component reads out the `param.xml` with the adjusted specifications first. Then the `default_param.xml` is read out. The parameters already read out in the customer-specific file are ignored when reading in the default file.

IMPORTANT:

The `default_param.xml` must not be removed as this may cause errors in the system.

In the ensuing sections we will go into the single parameters in the form of tables.

13.6.3.1 Appearance of the Interface Elements

By means of the parameters mentioned here you control the Web Assistant appearance. You can use them to adjust the Web Assistant to the colors common at your company (corporate identity). The following table lists all parameters relevant for colors, fonts and sizes.

Parameter	Meaning
bgcolor	Page background color. Default value: #FFFFFF
font	Font used. Default value: Arial, Helvetica
size	Font size. Default value: 2
font_size_note	Font size of fine-printed notes, for example in the voice mail settings. Default value: 1
text	Font color. Default value: #000000
TabColor1	Filling color for table rows in uneven position (first, third, fifth etc.). Default value: #B2E0E0
TabColor2	Filling color for table rows in even position (second, fourth, sixth etc.). Default value: #D9F0F0
rcb	This parameter is obsolete.
altfont	Font for alternative text, for example in routing rules. Default value: Courier, Arial
link	Font color for hyperlinks. Default value: #009999
vlink	Font color for already visited hyperlinks. Default value: #009999
alink	Font color of an active hyperlink. Default value: #009999
Settings for the navigation	
NavHighlightColor	Filling color of an inactive sub-item. Default value: #D9F0F0
NavTitSize	Font size of the category captions. Default value: 2
NavTitColor	Font color of the category captions. Default value: #009999
NavTitColorInactive	Font color of an inactive category caption. Default value: #C2C2C2

Table 36 Colors, Fonts and Sizes

Parameter	Meaning
NavSize	Font size of the sub-items. Default value: 2
NavTitContrCol	Filling color of an active sub-item. Default value: #FFFFFF
Settings for page titles	
TitFont	Font for titles. Default value: Arial, Helvetica
TitColor	Color for titles. Default value: #009999
TitSize	Font size for the title. Default value: 3
Settings for harddisk capacity representation	
DiskSpFree	Color for the representation of free hard disk capacity (). Default value: #009999
DiskSpOccu	Color for the representation of occupied hard disk capacity (<i>Special server settings -> Hard disk capacity</i>). Default value: #FF8F00
Settings for the <i>Special server settings -> APL</i> page	
AplRunning	Representation of the status of a started APL (<i>Special server settings -> APL</i>). Default value: #404CCC
AplStopped	Representation of the status of a stopped APL (<i>Special server settings -> APL</i>). Default value: #CC2125
user_data_font_color	This parameter is obsolete.
Colors of the log files	
F	Color for the log level <i>Fatal errors</i> . Default value: #FF8080
E	Color for the log level <i>Error</i> . Default value: #FF0000
W	Color for the log level <i>Warnings</i> . Default value: #FF8F00
I	Color for the log level <i>Info messages</i> . Default value: #008000
D	Color for the log level <i>Debug messages</i> without debug level. Default value: #000000
1	Color for the log level <i>Debug messages</i> with debug level 1. Default value #404040.
2	Color for the log level <i>Debug messages</i> with debug level 2. Default value #808080.
3	Color for the log level <i>Debug messages</i> with debug level 3. Default value #A0A0A0.
4	Color for the log level <i>Debug messages</i> with debug level 4. Default value #C0C0C0.
Colors for user graphs (obsolete)	
GraphColorMarker	This parameter is obsolete.
GraphColorSet	This parameter is obsolete.
GraphColorOtherwise	This parameter is obsolete.
GraphColorEmpty	This parameter is obsolete.
GraphColorBackgr1	This parameter is obsolete.
GraphColorBackgr2	This parameter is obsolete.

Table 36 Colors, Fonts and Sizes

Parameter	Meaning
GraphHeight	This parameter is obsolete.

Table 36 Colors, Fonts and Sizes

13.6.3.2 New User and Groups

The parameters mentioned here control the initial data that are stored to form a new user or group data record in the database.

In the parameters you can use variables, for example %user_id%. Such variables will be replaced with the actual value for each data record before they are stored in the database. The following variables can be used:

- %user_id%: Is replaced with the user ID.
- %voicebox%: Is replaced with the address to which a message waiting signal is sent.
- %tenant_name%: Is replaced with the tenant name. Relevant in multi-tenant environments only.
- %tenant_id%: Is replaced with the tenant ID. Relevant in multi-tenant environments only.
- %group_id%: Is replaced with the group ID.

The following table lists all parameters relevant for the default settings of new users and groups.

Parameter	Meaning
UserInit_MAILBOX	Name of the mailbox. Default value: %user_id%
UserInit_PREFERRED	Preferred address. Default value: MAILBOX
UserInit_GROUP	User group. Default value: USER
UserInit_CIT	Address to which a message waiting signal is to be sent. Default value: MWI/%voicebox%
UserInit_PASSWORD	Password of a new user. Default value: password
UserInit_NAME	Default value: %user_id%
TenantInit_NAME	Is required in a multi-tenant environment. Default value: %tenant_name%
Allow_DefaultPIN_LogIn	Determines whether logging on to the Web Assistant is permitted using the default PIN. Possible values: • yes: Logon using the default PIN is possible. • no: Logon using the default PIN is not possible. A user may then only log on via the TUI using the default PIN. Default value: yes
GroupInit_NAME	
GroupInit_ISGROUP	Determines that a group is registered as group. Default value: yes. This parameter should not be modified.

Table 37

Default Settings for new Users and Groups

Parameter	Meaning
DisableField_STAND-IN	Determines in which case the STAND-IN field is not displayed. The default value (PREFERRED=LN PREFERRED=EXCH) means that this field is not displayed if the PREFERRED field contains the LN value or EXCH.

Table 37 Default Settings for new Users and Groups

The following parameters determine which data must be contained in a mask before the data record can be saved:

Parameter	Meaning
CheckUserData_USER	Determines for the fields in the USER mask whether and which fields must be filled in. Default value: PASSWORD! PIN! GROUP! NAME!
CheckUserData_GROUP	Determines for the fields in the GROUP mask whether and which fields must be filled in. Default value: ISGROUP=YES NAME! PRIVILEGES!
CheckUserData_TENANT	Determines for the fields in the TENANT mask whether and which fields must be filled in. Default value: NAME!

Especially for the `CheckUserData_*` parameters, which all refer to the input masks in the user administration, you need to ensure that data have been entered before the data record is saved. For this purpose a parameter in which the mandatory data are defined exists for each input mask.

The check is controlled by means of a simple syntax, which has the following operators:

- = : must be equal
- ! : "not equal" respectively if no string follows the meaning is "must not be empty".
- | (pipe character): logical or
- & : logical and

For example, the default value of the `CheckUserData_USER` parameter means that the `PASSWORD` or the `PIN` field as well as the `GROUP` and `NAME` fields must not be empty.

In the `CheckUserData_GROUP` parameter it is defined that in the `ISGROUP` field the `YES` string must be entered and that the `NAME` and `PRIVILEGES` fields must not be empty.

13.6.3.3 Authentication

The following table lists all parameters relevant for the default settings of the authentication.

Parameter	Meaning
KnownHostName	See showpinforgotten . Here you can set the server name for the link in the first notification. This may be particularly required with cluster systems or when using DNS aliases. A mail with the new PIN is delivered after a click on this link in the first notification. As always, this PIN must be changed after its first use.
pinforgottenservice	Determines whether the PIN forgotten link shall use a specific service. See showpinforgotten . • EXCH: Send the message to the Microsoft Exchange address. • LN: Send the message to the Lotus Notes address. • SMTP: Send the message to the SMTP address. Attention: An example configuration is contained in the configuration file as comment. You can use this configuration by moving the end marker of the comment block --> in front of this example and behind the comment text.
showpasswordforgotten	Determines whether the Password forgotten link, which is possible in case of a connection to Lotus Notes or Microsoft Exchange, is displayed on the login page. Possible values: • yes: Link is displayed in case of a connection to Lotus Notes or MS Exchange. • no: Link is not displayed despite a connection to Lotus Notes or MS Exchange. Default value: yes
showpinforgotten	Determines whether the PIN forgotten link, which is possible in case of a connection to Lotus Notes or Microsoft Exchange, is displayed on the login page. Possible values: • yes: Link is displayed in case of a connection to Lotus Notes or MS Exchange. • no: Link is not displayed despite a connection to Lotus Notes or MS Exchange. Default value: yes You can activate this mechanism for messages via SMTP also. See pinforgottenservice .

Table 38

Default Settings of the Authentication

Parameter	Meaning
Use_Password_Guidelines	Determines whether the integrated password policies must be heeded when a user enters a new password. Possible values: • <code>yes</code>: The system checks whether a new password conforms with the password policies. • <code>no</code>: The system does not check whether a new password conforms with the password policies. Default value: <code>yes</code>
key_timeout_offset	Seconds that are deducted from the time still available until the user is automatically logged off after loading a page to balance possible latencies in the network. Default value: 5
DefaultDomain	Specifies the default domain. If the customer uses only one domain, the Windows domain need not be specified when logging on in the Web Assistant.
UseMailboxForSimplifiedWebAccess	When using the Web Message Access (see Section 16.7, "Web Message Access") you need to log on to the system if you wish to perform further actions after reading the message. You can do this either via the combination of user ID and password or via mailbox number and PIN. This value makes it easier for the user as the mailbox number is already entered and he/she only needs to specify his/her PIN. Possible values: • <code>yes</code>: Enter mailbox number. • <code>no</code>: Enter user ID. Default value: <code>yes</code>

Table 38 *Default Settings of the Authentication*

13.6.3.4 Date and Time Formats

The following table lists all parameters relevant for the default settings of the authentication.

Parameter	Meaning
Use12HourTimeFor	Comma-separated list of the languages in which the time is to be displayed in the 12-hour format. Default value: 2057, 1033
UseDateFormatDayMiddle	Comma-separated list of the languages in which the American data format is to be used. Default value: 1033
UseAmericanDateFor	Comma-separated list of the languages in which the American data format is to be used. Default value: 1033
UseAmericanTimeFor	Comma-separated list of the languages in which the American time format is to be used. Default value: 1033

Table 39 Date & Time

13.6.3.5 Default Language Settings

The following table lists all parameters relevant for the default language settings.

Parameter	Meaning
default_language	Fallback language. Independent from the server default language selected upon the installation. Default value: 2057
LangName_*	Connection between the clear text name of a language (for example GERMAN) and the language code (for example 1031). These parameters must never be modified!

Table 40 Default Language Settings

13.6.3.6 Filters for the User List in the User Administration

The following table lists all parameters relevant for the filters in the user list.

Parameter	Meaning
UserDataSearchFields	Database fields according to which the user list can be filtered in the user administration. Default value: S_LOGIN_WEB, E_LOGIN_WEB, DISABLED, NAME#, NAME, VOICE#, VOICE, PHONE#, PHONE, GROUP, ISGROUP Via the NAME# entry an index to the name field is created and searching occurs as described in the Web Assistant manual. If you remove the entry here, the search feature in the Web Assistant changes. The entered search string is then searched for anywhere in the Name field. Search string "r" would thus deliver all name entries that contain an "r". Since you cannot use an index with this type of searching, it is considerably slower than the default search!

Table 41 Filters for the User List in the User Administration

13.6.3.7 Message Settings

The following table lists all parameters relevant for message display and administration.

Parameter	Meaning
showhtmlbody	This parameter should not be modified. Determines whether or not HTML code contained in a message is processed. If this parameter is set to yes, JavaScript code contained in messages is also executed, which may represent a security risk. Default value: no.
Max_MsgsPerFolder	Determines the maximum number of messages that can be displayed. If the mailbox on the server contains more messages, only the latest messages until the defined number are displayed. Default value: 500
turned_fax	With the yes setting fax options appear under a displayed fax page with which you can rotate the fax page in the Web Assistant by 90°, 180° and 270°. Default value: no.

Table 42 Message Settings

13.6.3.8 CTI Settings

The following table lists all parameters relevant for CTI.

Parameter	Meaning
CTI_MaxAge	Determines the number in days
CTI_OptionUseSpeaker	Determines whether the telephone's hands-free option (dialing with hung-up receiver) is used when dialing from a CTI journal. Prerequisite is the connected telephone supporting this feature. Possible values: • 1: The hands-free option is used. • 0: The hands-free option is not used. Default value: 1

Table 43 CTI Settings

13.6.3.9 Address Book Settings

The following table lists all parameters relevant for the address book.

Parameter	Meaning
AB_PublicEnabled	Determines whether the public address book is active. Possible values: • 1: Public address book is active. • 0: Public address book is not active. Default value: 1
AB_PrivateEnabled	Determines whether the private address book is active. Possible values: • 1: Private address book is active. • 0: Private address book is not active. Default value: 1
AB_ColumnIds	Comma-separated list of columns that are displayed in the list view of the two address books. Default value: <code>name,phone,fax,mail</code>
AB_NAME_FIELDS	Name of the database field from which the name of a contact is read. Default value: <code>name</code>
AB_PHONE_FIELDS	Comma-separated list of database fields from which contact phone numbers are read. If several of the fields specified here contain data, all available data are displayed. Default value: <code>phone#,gsm#,privtel#</code>
AB_FAX_FIELDS	Comma-separated list of database fields from which contact fax numbers are read. If several of the fields specified here contain data, all available data are displayed. Default value: <code>faxg3#,privfax#</code>

Table 44 Address Book Settings

Parameter	Meaning
AB_MAIL_FIELDS	Comma-separated list of database fields from which contact e-mail addresses are read. If several of the fields specified here contain data, all available data are displayed. Default value: smtp
AB_C_CategoryIds	Comma-separated list of categories that are displayed on the details page of a contact. For each category specified here a parameter named AB_C_<category ID>_FIELDS must be configured, with <category ID> being a wildcard for the upper case category ID. Possible values: • common: The <i>common</i> category is displayed. • phone: The <i>phone numbers</i> category is displayed. • address: A category named <i>address</i> is displayed. Default value: common, phone, address There are two special attributes that cannot be directly mapped on a database field: • id: Can be used to display the XPR user name of the contact. • scope: Can be used to display whether the contact is a private or public one.
AB_C_COMMON_FIELDS	Comma-separated list of the database fields that are displayed in the <i>common</i> category. Default value: scope, id, name, smtp, preferred
AB_C_PHONE_FIELDS	Comma-separated list of the database fields that are displayed in the <i>phone</i> category. Default value: phone#, gsm#, voice#, faxg3#, privtel#, privfax#
AB_C_ADDRESS_FIELDS	Comma-separated list of the database fields that are displayed in the <i>address</i> category. Default value: addr1, addr2, company, division, zip, city, state, country
AB_CallFields	Default value: phone, phone#, gsm, gsm#, sms, sms#, privtel, privtel#
AB_MessageFields	Default value: faxg3, faxg3#, sms, sms#, privfax, privfax#, smtp

Table 44 Address Book Settings

13.6.3.10 Template Settings

The following table lists all relevant parameters for creating new users based on a template.

Parameter	Meaning
size_input_id	Determines the width for the ID entry fields. Default value: 33
size_input_voicebox	Determines the width for the voice mail number entry fields. Default value: 17
size_input_name	Determines the width for the user name entry fields. Default value: 55
number_of_new_users_by_template	Determines the number of lines and thus the number of users that may be specified in one go. Default value: 30
TEMPLATE_Show_Fields	Determines the fields displayed in the pop-up opened via the dotted icon next to a line. All fields with MASK DATA values can be used. Default value: FAXG3#, FAXG4#, GSM#, NAME, PASSWORD, PIN, PRIVEFAX#, PRIVTEL#, SMTP, VOICE#, SMS# ,mailbox, GROUP, CIT
TEMPLATE_Copy_User_Settings_Fields	Specifies the fields that are copied from the template to the new user. All fields with MASK DATA values can be used. Default value: GROUP, COUNTRY, STATE, CITY, ADDR1, ADDR2, ZIP, COMPANY, DIVISION, WEB_STARTPAGE, LANGUAGE_ID, NCO_GUI_PREFIX, NCO_TUI_PREFIX, NCO_GUI_CONN_PT, NCO_TUI_CONN_PT, NCO_LOCATION

Table 45

Template Settings

Parameter	Meaning
TEMPLATE_Copy_VM_Settings_Fields	Specifies the fields that are copied from the template to the new user. Possible fields: VM_PROTOCOL, VM_DEPUTY_NUMBER, VM_UO_MARK_URGENT, VM_UO_MARK_CONFIDENTIAL, VM_UO_MOBILITY, VM_UO_PROF_MODE, VM_UO_SHORT_PMP, VM_PRIV_PMP_LONG, VM_UO_INSTANT_DELETE, VM_UO_MARK_READ_AT_END, VM_UO_MSG_ASS_ON, VM_AC_PMP_SYS, VM_UO_HINT_AT_MSG_END, VM_UO_IBX_FILTER, VM_AC_PMP_SYS, VM_UO_IBX_SORT, VM_PRIV_MENU_REF_EXT, VM_PRIV_REC_INFO, VM_PF_AGE, VM_PF_MSG_TYPE, VM_PERSONAL_SORT, VM_ASR_HIGH, VM_ASR_LOW, VM_UO_ENH_GREETING, Default value: VM_PROTOCOL, VM_DEPUTY_NUMBER, VM_UO_MARK_URGENT, VM_UO_MARK_CONFIDENTIAL, VM_UO_PROF_MODE, VM_UO_SHORT_PMP, VM_PRIV_PMP_LONG, VM_UO_INSTANT_DELETE, VM_UO_MARK_READ_AT_END, VM_UO_MSG_ASS_ON, VM_AC_PMP_SYS, VM_UO_HINT_AT_MSG_END, VM_UO_IBX_FILTER, VM_AC_PMP_SYS, VM_UO_IBX_SORT, VM_PRIV_MENU_REF_EXT, VM_PRIV_REC_INFO, VM_PF_AGE, VM_PF_MSG_TYPE, VM_PERSONAL_SORT, VM_ASR_HIGH, VM_ASR_LOW, VM_PROGRAMMABLE_SHORTCUTS, VM_PROMPT_LEVEL, VM_VOLUME, VM_UO_ENH_GREETING
TEMPLATE_Copy_Notification_Settings_Fields	Determines which fields of the notification settings are copied from the template to the new user. Possible fields: • MWI • NOT_LAG • NOT_ACTIVE Default value: MWI, NOT_LAG, NOT_ACTIVE
TEMPLATE_Copy_Distribution_Lists_Settings_Fields	Determines which fields from the groups are copied from the template to the new user. Possible values: • PRIVATE_LISTS Default value: PRIVATE_LISTS
TEMPLATE_Copy_Fax_Forms_Fields	Determines which fields from the fax templates are copied from the template to the new user. Possible values: • SELECTED_FORM Default value: SELECTED_FORM

Table 45 Template Settings

Parameter	Meaning
TEMPLATE_Copy_Time_Profile_Fields	Determines which fields from the time profiles are copied from the template to the new user. Possible values: • TIME_PROFILE Default value: TIME_PROFILE
TEMPLATE_Copy_Mail_Tracking_Fields	Determines which fields from the mail tracking are copied from the template to the new user. Possible values: • SELECTED_OPTION Default value: SELECTED_OPTION
TEMPLATE_Copy_Forward_Access_Menu_Fields	Determines which fields from the forward access menu are copied from the template to the new user. Possible values: • INTERNAL_CALLERS • EXTERNAL_CALLERS • ALTERNATE_GREETING • WHEN_BUSY • AFTER_HOURS_GREETING Default value: INTERNAL_CALLERS, EXTERNAL_CALLERS, ALTERNATE_GREETING, WHEN_BUSY, AFTER_HOURS_GREETING
TEMPLATE_Copy_Misc_Fields	Other fields that are copied from the template to the new user. Possible values: • WEB_STARTPAGE Default value: WEB_STARTPAGE

Table 45

Template Settings

13.6.3.11 Miscellaneous

The following table lists all other parameters

Parameter	Meaning
ComAssistantAddress	In an integration with <i>ComAssistant</i> or <i>OpenScape Web Client</i> the URL for the corresponding invocation is entered here. Examples: • 10.10.1.41 • https://10.10.1.41:8443 • http://10.10.1.41:7789
ComAssistantCert	In an integration with <i>ComAssistant</i> or <i>OpenScape Web Client</i> you can specify here the <i>OpenScape Web Client</i> certificate optionally for a connection secured by SSL. The file specified here is searched for in the <code><XPR Install>\res\certs\</code> directory. You can use the openssl tool from <code><XPR Install>\SDKTools\</code> for obtaining the certificate. Via the invocation <pre>openssl cy s_client -connect <CAAddress>:<CAPort></pre> you receive a text output. In this output look for <pre>-----BEGIN CERTIFICATE-----</pre> and copy this portion until <pre>-----END CERTIFICATE-----</pre> into a file, e.g. <code>cacert.pem</code> . Copy this file into the above directory and enter the file's name here.
ComAssistantPort	In an integration with <i>ComAssistant</i> or <i>OpenScape Web Client</i> the port for the corresponding invocation is entered here. This is either 8443 for a connection secured by SSL or 7789 for an unsecured connection.
ComAssistantSSLMode	In an integration with <i>ComAssistant</i> or <i>OpenScape Web Client</i> you can use this parameter to control whether the reciprocal invocation occurs via https or http. Mixed invocation is not intended. The integration displays the voicemail settings and a journal of the <i>Web Assistant</i> voicemails in the <i>ComAssistant</i> or <i>OpenScape Web Client</i> . Possible values: • True: <i>ComAssistant</i> or <i>OpenScape Web Client</i> as well as <i>Web Assistant</i> are addressed via a connection secured by SSL. • False: <i>ComAssistant</i> or <i>OpenScape Web Client</i> as well as <i>Web Assistant</i> are addressed via http, thus an insecure connection.
cookie_lifetimedays	Determines the lifespan of the cookie in days. Default value: 6
DefaultProt	Determines the default voice mail protocol. Default value: PHONEMAIL

Table 46 Other Parameters

Parameter	Meaning
Distrib_UsersPerPage	Determines the number of entries in the Available users list upon creating or editing a group. Default value: 50
ergo_simple_tenant_profiles	You can determine the time profiles for Ergo via a selection field (default/advanced). If this option is set to <i>Yes</i> , the selection field offers appropriate options for all configured tenants of a multi-tenant environment.
HidePrivileges	Determines which privileges cannot be assigned to users who do not belong to any user group. Default value: SFT_GROUP, SFT_OWNER
HidePrivileges_USER	Determines which privileges cannot be assigned to users of the USER group. Default value: SFT_GROUP, SFT_OWNER
showhtmlbody	This parameter should not be modified. Determines whether or not HTML code contained in a message is processed. If this parameter is set to <i>yes</i> , JavaScript code contained in messages is also executed, which may represent a security risk. Default value: <i>no</i> .
SimplifiedMenuTree	If the parameter SimplifiedMenuTree has been set to <i>true</i> for PhoneMail, it will exclusively work with extended greetings. You need to set this parameter to <i>true</i> here too to adjust the appearance in the Web Assistant to this behavior. Default value: <i>false</i> . Attention: Please heed the use of small letters in the parameter's notation!
UserAdminHiddenMasks	Default value: <i>PROFILES</i>
WEB_STARTPAGE	Determines the default page displayed after login. May be overridden by a user setting. Possible values: • WEBASSISTANT: To administrators the Server settings > User administration and to normal users the Personal settings > User data page is displayed. • INBOX: The Mail Client > Inbox page is not displayed. Default value: WEBASSISTANT

Table 46

Other Parameters

13.6.4 Deactivating Web Assistant Features

The most simple way to disable a specific feature is to comment out the associated code using HTML comments:

```
<!-- This text is commented out -->
```

IMPORTANT:

Some HTML files contain a code that is only available for one of the two possible brandings. This code is in most cases imbedded in `xp_if` tags and uses the `@amlxpr` wildcard. Please mind these two tags when you comment out code sections.

Different tags are available for different scenarios. In the reference you find a description of all tags and their function (cf. [Section 13.6.5, "Reference", on page 966](#)).

If you need to write an individual code, you have to specify individual wildcards also. Since you can only modify the HTML files but not the WebAPL scripts, you must make sure that the wildcard name you use is unique and has not been allocated by another wildcard yet. For example, add you name token or your company's name to the desired wildcard name.

13.6.4.1 Example: Hiding the *Notification* feature in the `Nav.html` file

unchanged HTML page:

```
<xp_if condition="@NotApl | yes | eq">
  <!-- UsrNotification -->
  <xp_set name="menu_cmd" value="UsrNotification"><xp_set
name="menu_param" value="">
  <xp_set name="menu_anchor" value=""><xp_set name="menu_name"
value="@_lang[usrnäv][notify]">
  <xp_include block name="tab_menu">
</xp_if>
```

By commenting out the code section:

```
<xp_if condition="@NotApl | yes | eq">
<!--
  <!-- UsrNotification -->
  <xp_set name="menu_cmd" value="UsrNotification"><xp_set
name="menu_param" value="">
  <xp_set name="menu_anchor" value=""><xp_set name="menu_name"
value="@_lang[usrnäv][notify]">
  <xp_include block name="tab_menu">
-->
</xp_if>
```

By using the tag `<show ifequal>`:

The expression `ifequal="@my_company" to="nothing"` can never become true, since the script will never set a key value pair, so that the key `my_company` assumes the value `nothing`. Consequently, the condition is not true and the code between the opening and closing tag is not displayed.

```
<xp_if condition="@NotApl | yes | eq">
  <<!-- UsrNotification -->
  <show ifequal="@my_company" to="nothing">
  <xp_set name="menu_cmd" value="UsrNotification"><xp_set
name="menu_param" value="">
  <xp_set name="menu_anchor" value=""><xp_set name="menu_name"
value="@_lang[usrnäv][notify]">
  <xp_include block name="tab_menu">
  </show>
</xp_if>
```

By using the tag <show ifexists>:

The key `my_company` is not set within the script. Consequently, the condition delivers `false` and the code between the opening and closing tag is not displayed.

```
<xp_if condition="@NotApl | yes | eq">
  <!-- UsrNotification -->
  <show ifexists="@my_company">
    <xp_set name="menu_cmd" value="UsrNotification"><xp_set
    name="menu_param" value="">
    <xp_set name="menu_anchor" value=""><xp_set name="menu_name"
    value="@_lang[usrnav][notify]">
    <xp_include block name="tab_menu">
  </show>
</xp_if>
```

13.6.5 Reference

Name	Parameter1	Parameter2	Parameter3	Parameter4	closing tag
hide		ifequal ifexists	to		X
repeat	name	times	VALUE		X
set	name		VALUE		
show		ifequal ifexists	to		X
text	name		VALUE		X
xp_if		condition			X
xp_else					
xp_elseif		condition			
xp_unless		condition			X
xp_while		condition			X
xp_until		condition			X
xp_for	name	condition	VALUE	step*	X
xp_switch			VALUE		X
xp_case			VALUE		
xp_foreach	name		VALUE	key*	X
xp_set	name	condition	VALUE	else_value* else_remove*	
xp_checkbox	name	checked	VALUE		
xp_radio	name	checked	VALUE	display*	
xp_option		selected	VALUE	display*	
xp_block	name				X
xp_include	name			block file	
xp_compute	name	calculation			
xp_hidden	name*		VALUE	extract*	
xp_is_write					X
xp_no_space					X
xp_disp		condition	VALUE	level	

Table 47 Available tags

* optional

13.6.5.1 show / hide

Shows or hides specific data with arbitrary content.

Example:

```
<show ifequal="@amlxpr" to="yes"> ... </show>  
<show ifexists="@call_transfer"> ... </show>
```

```
<hide ifequal="@amlxpr" to="yes"> ... </hide>  
<hide ifexists="@call_transfer"> ... </hide>
```

Parameters:

ifequal ... to

Name of the variable. Value (text/number) of the variable

Boolean condition (true/false). Only if the condition delivers true, the text is displayed between the tags.

ifexists

Name of a variable

13.6.5.2 repeat

Simple loop to write data iteratively.

Example:

```
<repeat name="index" times="@languagecount" value="0"> ... </repeat>
```

Parameters:

name

Name of the variable inclusive the loop variable. Is initialized by the `value` parameter.

times

Number of repetitions

value

Start value

13.6.5.3 set

Sets a variable to a new value.

Example:

```
<set name="number" value="trusted_number@count";>
```

Parameter

name

Name of the variable. Is set by the `value` parameter.

times

Value (text/number) to which the variable is set.

13.6.5.4 condition (*calculation*)

calculation is an arithmetic/string expression that puts out a character string. The Reverse Polish Notation (aka. Postfix Notation) is used, which is calculated from the left to the right. Operators and arguments are separated from each other by the pipe character (`|`).

If numerical operators are used (`num_...`), a character string argument is converted into a number (under internal use of the `atoi()` function).

If logical operators are used (`not`, `and`, `...`), an empty argument or a 0 represents the Boolean value `false`.

condition is a Boolean condition. It is equal to `calculation`, but the result is converted into a Boolean value:

`false`, if the output string is empty `"0"`

`true`, in any other case

Available operators		Number of operands
<code>num_lt</code>	numerical "less than"	2
<code>num_le</code>	numerical "less than or equal"	2
<code>num_gt</code>	numerical "greater than"	2
<code>num_ge</code>	numerical "greater than or equal"	2
<code>num_eq</code>	numerical "equal"	2
<code>num_ne</code>	numerical "not equal"	2
<code>num_comp</code>	numerical "compare" (result: -1, 0, 1)	2
<code>lt</code>	less than	2
<code>le</code>	less than or equal	2
<code>gt</code>	greater than	2
<code>ge</code>	greater than or equal	2
<code>eq</code>	equal	2
<code>ne</code>	not equal	2
<code>cmp</code>	compare (-1, 0, 1) (cf. <code>strcmp()</code>)	2
<code>not</code>	logical NOT operator (false-> "0"/ true-> "1")	1
<code>and</code>	logical AND (false-> "0"/ true-> "1")	2
<code>or</code>	logical OR (false-> "0"/ true-> "1")	2
<code>xor</code>	logical XOR (false-> "0"/ true-> "1")	2

Table 48 Available Operators

Available operators		Number of operands
+	numerical addition	2
-	numerical subtraction	2
plus	numerical addition	2
minus	numerical subtraction	2
mul	numerical multiplication	2
div	numerical division	2
len	Length of a string (cf. <code>strlen()</code>)	1
dup	String duplication (cf. <code>strdup()</code>)	1
cat	String chaining (cf. <code>strdup()</code>)	2
sub	Substring extraction (cf. <code>substr(str, pos, len)</code>)	3

Table 48 Available Operators

Examples:

calculation	Result
"Hallo World dup len cat"	"Hallo World11"
"123456789 2 3 sub"	"345"
"32 2 div 3 mul"	"48"
"3 5 num_it not 1 or"	"1"
"@name 0 2 sub" (@name <- "John")	"Jo"

Table 49 Example of calculation

condition	corresponds in C to
"@count 3 num_lt"	(count < 3)
"12 @count + 5 num_ne"	((12 + count) != 5)
"@name Tom eq"	(strcmp (name, "Tom") == 0)
"3 5 num_it not 1 or"	(!(3 < 5) 1)
"@name John cmp -1 num_eq"	(strcmp (name, "John") == -1)

13.6.5.5 text

Is used for language-specific texts. For each supported language a corresponding XML file exists, which contains all language-specific texts as key value pair.

Example

```
<text name ="vm_settings" value="title_answering"> ... </text>
```

or

```
@_lang[vm_settings][title_answering];
```

Parameter

name

Name of the variable.

value

Value (text), with which the variable is filled from the language file.

13.6.5.6 xp_if

Simple `if` query. Known from C.

Example

```
<xp_if condition="@name | John | eq">
  @name;
</xp_if>
```

Output (if @name contains "John")

John

Equivalent in C

```
if (strcmp (name, "John") == 0)
    printf ("%s", name);
```

Parameter

condition

Boolean condition (true/false). Only if the condition delivers `true`, the text is displayed between the tags. See also [Section 13.6.5.4, “condition \(calculation\)”](#), on page 970.

13.6.5.7 xp_else

Is used with `xp_if`.

Example

```
<xp_if condition="@name | John | eq">
    Hello @name;
<xp_else>
    Bye @name;
</xp_if>
```

Output (if @name contains "Mark")

Bye Mark

Equivalent in C

```
if (strcmp (name, "John") == 0)
    printf ("Hello %s", name);
else
    printf ("Bye %s", name);
```

Parameter

None

13.6.5.8 xp_elseif

Simple `else if` condition. Also known from C.

Example

```
<xp_if condition="@name | Ted | eq">
  Bye @name
<xp_elseif condition="@name | Tom | eq">
  Hello name@
</xp_if>
```

Output (if @name contains "Tom")

```
Hello Tom
```

Equivalent in C

```
if (strcmp (name, "Ted") == 0)
    printf ("Bye %s", name);
else if (strcmp (name, "Tom") == 0)
    printf ("Hello %s", name);
```

Parameter

condition

Boolean condition (true/false). Only if the condition delivers `true`, the text is displayed between the tags. See also [Section 13.6.5.4, “condition \(calculation\)”](#), on page 970.

13.6.5.9 xp_unless

Opposite to an `if` condition.

Example

```
<xp_unless condition="@count | 5 | num_le">
    @count is bigger than 5
</xp_unless>
```

Output

```
7 is bigger than 5
```

Equivalent in C

```
if (!(count <= 5))
    printf ("%d is bigger than 5", count);
```

Parameter

condition

Boolean condition (true/false). Only if the condition delivers `false`, the text is displayed between the tags. See also [Section 13.6.5.4, “condition \(calculation\)”](#), on page 970.

13.6.5.10 xp_while

Simple `while` loop. Known from C.

Example

```
<xp_while condition="@test | aaaa | ne">
  <xp_set name="test" value="a@test">
    @test
  </xp_while>
```

Output (if @test was previously empty)

```
a
aa
aaa
aaaa
```

Equivalent in C

```
while (strcmp (test, "aaaa") != 0)
{
    strcat(test, "a");
    printf(test);
}
```

Parameter

condition

Boolean condition (true/false). Only if the condition delivers `true`, the text is displayed between the tags. See also [Section 13.6.5.4, “condition \(calculation\)”](#), on page 970.

13.6.5.11 xp_until

Opposite to a `while` loop. Repeated "if not `true`". Works like the `until` instruction from Perl.

Example

```
<xp_until condition="@test | aaaa | eq">
  <xp_set name="test" value="a@test">
    @test
  </xp_set>
</xp_until>
```

Output

```
a
aa
aaa
aaaa
```

Equivalent in C

```
while (strcmp (test, "aaaa") != 0)
{
    strcat(test, "a");
    printf(test);
}
```

Parameters:

condition

Boolean condition (true/false). Only if the condition delivers `false`, the text is displayed between the tags. See also [Section 13.6.5.4, “condition \(calculation\)”](#), on page 970.

13.6.5.12 xp_for

Simple `for` loop. Also known from C.

Example

```
<xp_for name="loop" value="3" condition="@loop | 7 | num_le">
  number = @loop;
</xp_for>
```

Output

```
number = 3
number = 4
number = 5
number = 6
number = 7
```

Parameter

name

Variable name inclusive a loop variable. Is initialized by the `value` parameter.

condition

Boolean condition (true/false). The entire expression is calculated with each loop run. The loop abandons at the first `false`. See also [Section 13.6.5.4, “condition \(calculation\)”, on page 970](#).

value

Number that is used for initializing the loop variable.

step (optional)

This value is added to the loop variable at the end of a loop run. If `step` is not defined, the loop variable will be raised by 1 each.

NOTE:

After 20,000 runs, loops abandon automatically to prevent infinite loops.

13.6.5.13 xp_switch

Simple `switch` instruction. Known from C, works with strings, though.

Example

```
<xp_switch value="@name">
  <xp_case value="Bond">
    My name is @name
  <xp_case value="Ted">
    Hello @name
  <xp_case value="John">
    Bye @name
  <xp_case>
    I don't know any @name
</xp_switch>
```

Output (if @name contains "Ted")

Hello Ted

Equivalent (in Pseudo-C)

```
switch (name)
{
  case "Bond":
    printf ("My name is %s", name);
    break;
  case "Ted":
    printf ("Hello %s", name);
    break;
  case "John":
    printf ("Bye %s", name);
    break;
  default:
    printf ("I don't know any %s", name);
    break;
}
```

Parameter

value

This value is compared with each `case` instruction. As soon as a match is found, the corresponding text will be parsed (displayed) after the `case` tag.

13.6.5.14 xp_case

Simple `case` instruction. Also known from C, works with strings, though.

Example

```
<xp_switch value="@name">
  <xp_case value="Bond">
    My name is @name
  <xp_case value="Ted">
    Hello @name
  <xp_case value="John">
    Bye @name
  <xp_case>
    I don't know any @name
</xp_switch>
```

Output

```
Hello Ted
```

Equivalent in C

```
switch (name)
{
  case "Bond":
    printf ("My name is %s", name);
    break;
  case "Ted":
    printf ("Hello %s", name);
    break;
  case "John":
    printf ("Bye %s", name);
    break;
  default:
    printf ("I don't know any %s", name);
    break;
}
```

Parameter

value

This value is compared with each `switch` instruction. As soon as a match is found, the corresponding text will be parsed (displayed) after the `case` tag.

13.6.5.15 xp_foreach

A loop like Perl's `foreach` instruction. Iterates via all list elemets.

Example (depends on the data)

```
<xp_foreach key="key" name="val" value="@data">
  @key = @val
</xp_foreach>
```

Output

```
0 = Tom
1 = John
2 = Rick
3 = Boris
```

Equivalent in C

```
for (i=0; i<data.length(); i++)
{
    std::string key = data[i].key;
    std::string val = data[i].value;

    printf ("%s = %s", key.c_str(), val.c_str());
}
```

Parameter

key (optional)

Name of the `key` variable. Is set to the name of each list element.

name

Name of the `name` variable. Is set to the name of each list element.

value

Should be a CGI list.

13.6.5.16 xp_set

Assigns a new value to a variable.

Example

```
<xp_set name="name" value="Ted" condition="@count | 3 |
num_eq">
```

Output

no visible result

Equivalent in C

```
if (count == 3)
    strcpy (name, "Ted");
```

Parameter

name

Variable name. Is, depending on `condition`, set to the value of `value` or `else_value`.

condition (optional)

Boolean condition (`true/false`). The variable is set to the value of `value` if the condition delivers `true`. Otherwise to the value of `else_value`.

value

Value (text/number) that the variable assumes in case of `true`.

else_value (optional)

Value (text/number) that the variable assumes in case of `false`.

else_remove (optional)

The variable is removed if `condition` assumes `false`.

13.6.5.17 xp_checkbox

Generates the HTML tag for a check box.

Example

```
<xp_checkbox name="@box" value="on" checked="@name | John |  
ne">
```

Output (if @box contains the string chk1 and @name contains the string Mark)

```
<input type="checkbox" name="chk1" value="on" checked>
```

Parameter

name

Name parameter of this HTML tag for a check box.

checked (optional)

Boolean condition. If `true`, the `checked` parameter is added to this tag. See also [Section 13.6.5.4, “condition \(calculation\)”, on page 970](#).

value

`value` parameter of the HTML tag for this checkbox.

13.6.5.18 xp_radio

Generates an HTML tag for an option field (radio button).

Example

```
<xp_radio name="@box" value="on" checked="@name | John |
ne">
```

Output (if @box contains the string chk1 and @name contains the string Mark)

```
<input type="radio" name="chk1" value="on" checked>
```

Parameter

name

Name parameter of this HTML tag for an option field.

checked (optional)

Boolean condition. If `true`, the `checked` parameter is added to this tag. See also [Section 13.6.5.4, “condition \(calculation\)”, on page 970](#).

value

`value` parameter of the HTML tag for this option field.

13.6.5.19 xp_option

Generates an `<option>` HTML tag.

Example

```
<xp_option value="on" display="option1" selected="@name |
Mark | eq">
```

Output (if @name contains the Mark string)

```
<option value="on" selected>option1</option>
```

Parameter

selected (optional)

Boolean condition. If `true`, the `selected` parameter is added to this tag. See also [Section 13.6.5.4, “condition \(calculation\)”](#), on page 970.

value

`value` parameter of the HTML tag.

display (optional)

This text is displayed between the opening and closing `<option>` tag.

13.6.5.20 xp_block

Anything between the opening and closing tag is saved in the parser cache, but neither edited nor displayed at runtime. `xp_include` can later be used to insert the saved text in the page and to parse it.

NOTE:

You can use `xp_block` as some kind of function invocation. The arguments of a function can then be set by means of `xp_set` tags.

Example

```
<xp_block name="block1">
```

```
</xp_block>
```

Output

No visible output

Parameters:**name**

Name of the save text block.

13.6.5.21 xp_include

Inserts a text block previously saved with `xp_block` and parses it. External HTML files can be loaded and parsed as well.

Example

```
<xp_include name=" block1" block>
<xp_include name="html/part.htm" file>
```

Output

The output depends on the content of the block or of the file.

Parameter

name

Name of the saved text block or the path to an HTML file.

block

Inserts a block.

file

Inserts an HTML file.

13.6.5.22 xp_compute

Performs a computation and assigns the result to a variable.

Example

```
<xp_compute name="len" calculation="@len | 100 | plus">
```

Output

No visible output

Parameter

name

Name of a variable. This name is assigned to the result of the computation.

calculation

A calculation like in a `condition` parameter. Delivers a string. In case of Boolean operations, `0` is `true` and `1` is `false`. See also [Section 13.6.5.4](#), “`condition (calculation)`”, on page 970.

13.6.5.23 xp_hidden

Using this tag a complete CGI list with its values can be written on an HTML page. The tag creates for each key in the list an `input` field with the parameter `hidden`. At the next POST/GET request this list will be automatically recompiled.

Example

```
<xp_hidden value="@data">
```

Output (depends on the content of the CGI list)

```
<input type="hidden" name="$data$name" value="Tom">
<input type="hidden" name="$data$age" value="23">
<input type="hidden" name="$data$sex" value="male">
<input type="hidden" name="$data$city" value="New York">
```

NOTE:

The `$` symbol is used as separator for this purpose. Therefore, never use it within `name` parameters.

Parameter

value

A CGI list.

It is possible to specify several entries for the `value` parameter. It is also possible to pack several CGI lists in a single list by using a `name` parameter. This is useful if data need to be "transported" via several pages. The `extract` parameter extracts the list again.

Example

```
<xp_hidden value="@data,@list,@user">
<xp_hidden name="container" value="@list,@data">
<xp_hidden value="@container " extract>
```

Output of the second example (depending on the list contents)

```
<input type="hidden" name="$container$list$1" value="+324">
<input type="hidden" name="$container$list$2" value="21">'
<input type="hidden" name="$container$list$3" value="-534">
<input type="hidden" name="$container$data$name" value="Tom">
<input type="hidden" name="$container$data$age" value="23">
<input type="hidden" name="$container$data$sex" value="male">
<input type="hidden" name="$container$data$city"
value="New York">
```

Parameter

value

A variable or a list. Several entries separated by comma are possible.

name (optional)

Name of a CGI list that contains all data (container).

extract (optional)

Extracts data from a container

13.6.5.24 xp_js_write

Converts HTML codes into JavaScript codes using the `document.write()` feature.

Example

```
<xp_js_write>
  <p>
    <input type="text" name="age" value="23" size="16">
  </p>
</xp_js_write>
```

Output

```
<script language="JavaScript">
document.write("<p>");
document.write("<input type=\"text\" name=\"age\" 
value=\"23\" size=\"16\">");
document.write("</p>");
</script>
```

13.6.5.25 xp_no_space

Deletes all blanks between HTML tags.

Example

```
<xp_no_space>  
  <p>  
    <b>  Hallo  </b>  
  </p>  
</xp_no_space>
```

Output

```
<p><b>Hallo</b></p>
```

13.6.5.26 xp_disp

Writes log information in the XPR monitor. The beginning of each message features the file name of the page (for example `webadmin.html`).

Example

```
<xp_disp value="@error_msg" level="warning"  
condition="@error|yes|eq">
```

Output

No visible output

Parameter

condition

Boolean condition (`true/false`). The log information is only written if `condition` assumes the value `true`.

value

The log information.

level

The log level. Must have one of the following values: `error`, `warning`, `info`, `debug`, `debug2`, `debug3` or `debug4`.

13.6.6 Adjusting the Web Assistant Interface for different User Groups

In order to provide different user interface layouts for different user groups, you can modify the respective HTML pages with special tags. These tags are no standard HTML tags.

With the help of the following text content can be displayed or hidden on the page:

```
<xp_if condition="">
...
<xp_else>
</xp_if>
```

The `condition` attribute must have the following structure:

```
<xp_if condition="@ui_group | USER | eq"></xp_if>
```

This condition becomes true, if the variable `@ui_group` is replaced with the value `USER` by the Web Assistant script. That means, that a user of the group `USER` has logged on.

The respective content that is to be displayed for this user group must be placed between the opening and closing tag.

Example: Modifying the interface

The following code prevents a user of the group `USER` from being able to modify their PIN.

```
<xp_if condition="@ui_group | USER | eq">
    <font face="Arial">You have no permission to change your PIN.</font>
<xp_else>
<font face="Arial"><b>Change PIN</b></font>&nbsp;&nbsp;&nbsp;
<input type="button" name="but_change_pin" value="Change PIN">
</xp_if>
```

The following code does not use an `xp_else` branching:

```
<xp_if condition="@ui_group | USER | eq">
    <font face="Arial">Sorry, no option to change your PIN.</font>
</xp_if>
```

13.7 Invoking XPR Functions from another Web Server

Most companies already use a Web server. Invocations of the XPR web server can be implemented in CGI scripts of this server, so that, for example, an SMS message can be sent in a default send form via the XPR server.

The Perl example will illustrate this basic functionality.

```
#!/perl/bin/perl

# Modules for CGI-, HTTP- and Browser-Object
use CGI;
use HTTP::Request::Common;
use LWP::UserAgent;

# Create CGI- and Browser-Objects
$cgi = new CGI;
$ua = LWP::UserAgent->new;

# read all Variables from form
$cgi->import_names();

# Send request to Web APL E-script routine "erp" with parameter "foo"
$r = $ua->request(POST 'http://server/erp', [foo=>$cgi::foo]);

# Print result via browser (here an error message)
print "Content-Type: text/html\n\n";
print $r->as_string();

exit 0;
```

Perl is much more suitable for such a simple task than C and related languages. It offers many efficient string functions and avoids the C-typical traps. A simple text editor is sufficient for creating executable Perl scripts.

A nice side effect of this proceeding is that the actual E-script parameters on the XPR side can be masked.

14 Short Message Service (SMS)

14.1 What is SMS?

The acronym **SMS** stands for **Short Message Service**. The short message service in **GSM** standard allows the transmission of short messages to mobile phone subscribers. This service can be compared with paging, but exceeds paging options owing to the guaranteed data transmission.

Depending on the type of connection, thus point-to-point connection or broadcast transmission, messages consisting of 160 or 93 characters can be sent. Transmission occurs digitally via circuit switched dial connections or with GSM via the packet switched control channel. The transmission rate is between 400 and 500 bit/s. The waiting time before transmission at the Short Message Service Center (SMSC) is between 5 and 10 seconds.

14.2 SMS and XPR

XPR provides three different, tailor-made SMS solutions to meet the various requirements in corporate divisions. These three solutions cover all characteristic requirements from the entry-level area to the professional high-performance area with direct provider coupling, which even enables the operation of the XPR server as independent message center.

These three solutions and their functionality will be briefly introduced in the following.

14.2.1 SMS via ISDN: The Entry-level Solution

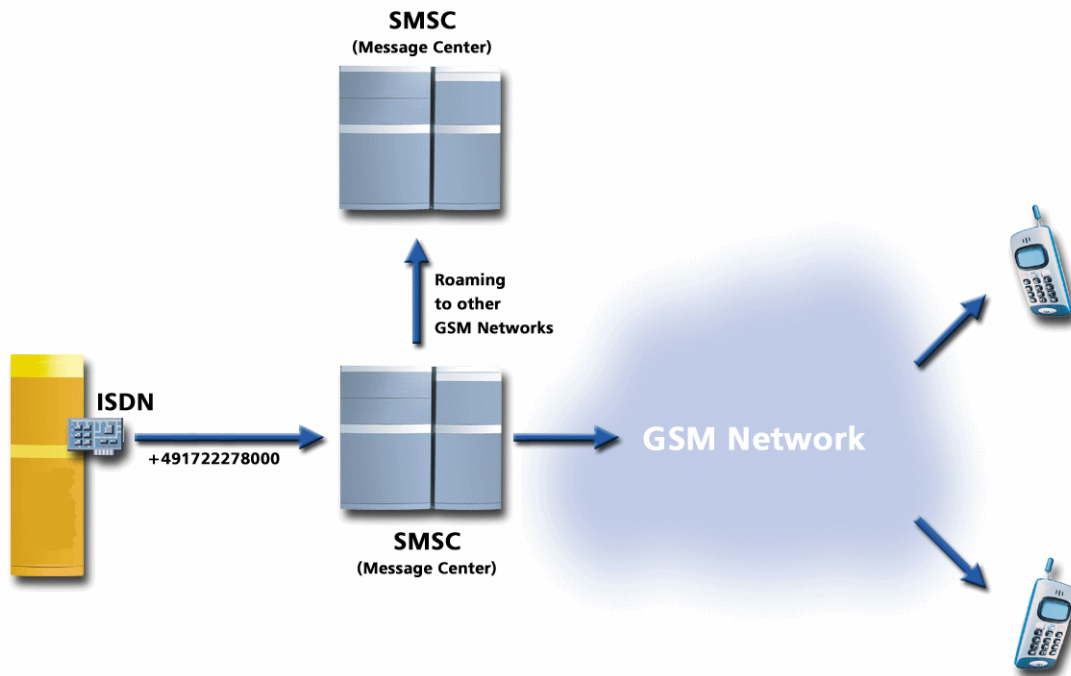
NOTE:

The explanations on connecting the SMS service to ISDN is found in [Section 10.4.19, "SMS \(TAP or UCP Protocol\)", on page 748](#).

For applications in which only a small number of SMS messages is sent, the ISDN APL offers the option to transmit these messages directly via **Short Message Service Center (SMSC)**. Either the EMI/UCP or the TAP protocol is used for this.

The following diagram outlines such a transmission:

Short Message Service (SMS)



If a short message is to be sent from the XPR server, the ISDN connector dials the configured message center (**Short Message Service Center**) and leaves the message there. The center then immediately tries to deliver the message. In doing so it can also pass the message on to further message centers if the recipient is at home in a GSM network that the message center cannot directly reach. If the recipient is not available (for example because the cell phone is switched off or the center in charge of the recipient's network cannot be reached), the message will be buffered for a specific period (usually 48 hours) and the delivery attempt repeated within this period several times. If the message could not be delivered during its maximum life span it becomes obsolete and is deleted from the message center. With this type of transmission the XPR server solely knows whether or not the message center has accepted the message. A message may be refused if, for example, the recipient number is definitely incorrect or the message center does not know any delivery path for this recipient. The ensuing status reports do not reach the XPR server since this would require a permanent connection between message center and XPR server.

SMS via ISDN is thus suitable as entry-level solution, since it normally does not require any extra hardware and contractual bindings to providers. Prices per message are in this transmission mode usually not very favorable and bulk discounts are mostly not possible owing to a missing contractual binding.

Depending on the protocol used and the message center, the XPR server can with this transmission type determine the short message originator address. This can be useful for e.g. calling the message's originator on his/her cell phone.

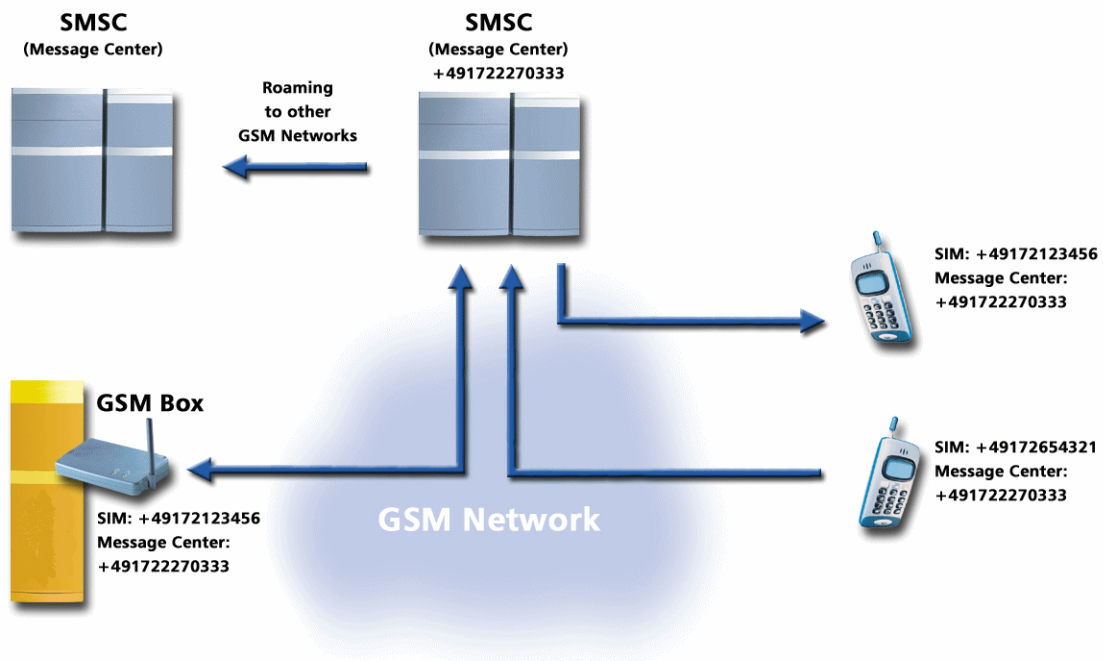
14.2.2 SMS via GSM Boxes

NOTE:

This connection type is in the XPR system administered and configured by the *SMS Connector*. The SMS Connector is described in [Section 14.5, “SMS Connector \(SMSIPAPL\)”](#).

Using this transmission type SMS messages are routed via GSM boxes (also called GSM adapters) connected to the XPR server. These GSM boxes are special mobile phone devices optimized for usage in server applications. Special cell phones equipped with data cable are suitable for this transmission type as well. The XPR server acts here as a normal mobile phone subscriber.

The following diagram outlines this transmission type:



The advantage of this type of connection is that messages cannot only be sent but also received. Furthermore, the conclusion of a mobile phone contract optimized for the SMS helps considerably reducing costs compared to the *SMS via ISDN* method.

Each GSM box receives an individual number to which messages can be sent via the implemented SIM board. Special recipient tokens in the message text enable an explicit addressing to XPR users. Contrary to the *SMS via ISDN* method an originator address can be defined, which is always the number of the implemented SIM board. Several GSM boxes can be used at one XPR server.

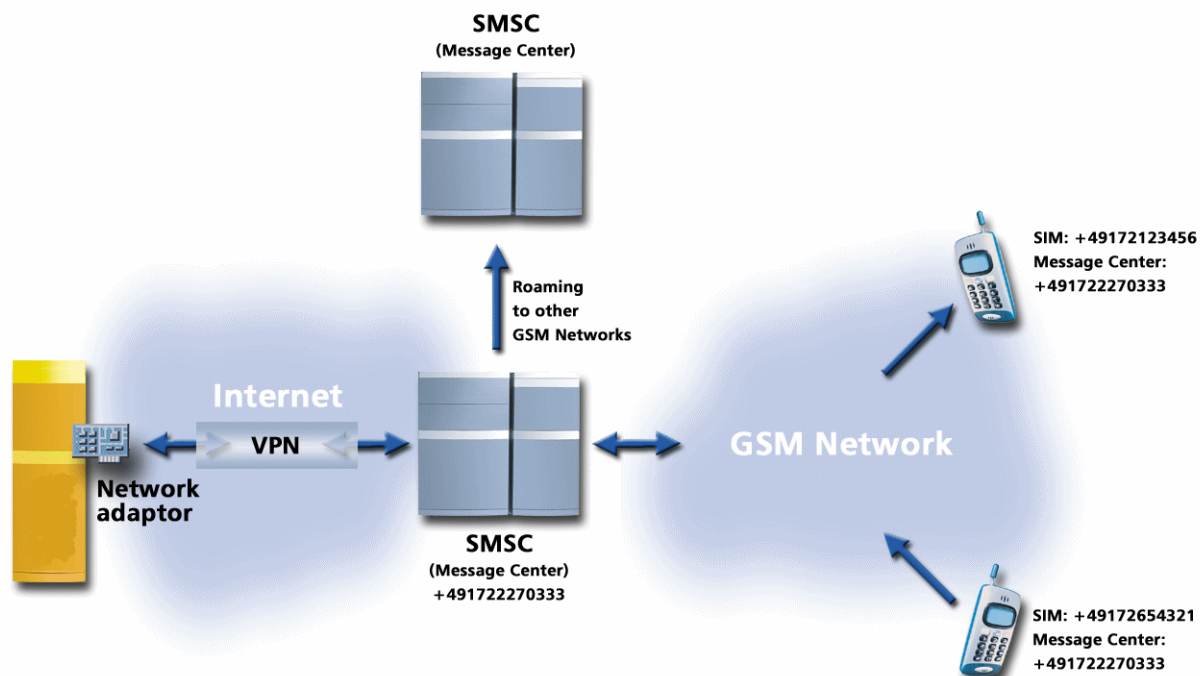
14.2.3 SMS via direct Provider Coupling

NOTE:

This connection type is in the XPR system administered and configured by the **SMS Connector**. The SMS Connector is described in [Section 14.5, “SMS Connector \(SMSIPAPL\)”](#).

The direct provider coupling is the most complete type of connection since it exploits all originator and recipient options. In addition it offers high performance and security as well as the lowest costs. The XPR server is connected via the TCP/IP protocol. Additional security can be reached by the implementation of a **Virtual Private Network** tunnel (VPN tunnels) between customer and provider.

The following diagram outlines this type of connection:



UCP or **SMPP** is supported as transmission protocol. The **SMS Connector** supports several connections to one or several providers. Each connection can be configured individually, so that the configuration can be performed without interrupting the service during operation. Extremely long SMS messages (up to 612 characters) are supported on the originator and recipient side as far as offered by the provider. The number of connections is restricted by external resources such as the size of the registry database for storing configuration data. In practical use such restrictions are unlikely to take any effect.

Furthermore, messages can be tracked since the protocol does not only deliver a mere confirmation of the message having been accepted or not but also more detailed information:

- **Delivery Notification:** The message was delivered.
- **Non-Delivery Notification:** The message could not be delivered.
- **Buffered Notification:** The message was buffered.

NOTE:

The features described in the following must be supported by the provider. Therefore consult your provider in case of doubt.

The following receiving models can be realized with the *SMS Connector*:

Receiving via rerouted number

In this case the provider assigns one or several mobile phone numbers to the connection. Short messages sent to these numbers do not arrive at a cell phone but are directly delivered to the *SMS Connector* by the message center via the connection. The destination address is subsequently determined in the XPR server and, if accessible, forwarded. In this way received messages are bundled and connections checked. In addition, XPR users can be directly addressed by a specially indicated recipient token.

Receiving via speed dialing code

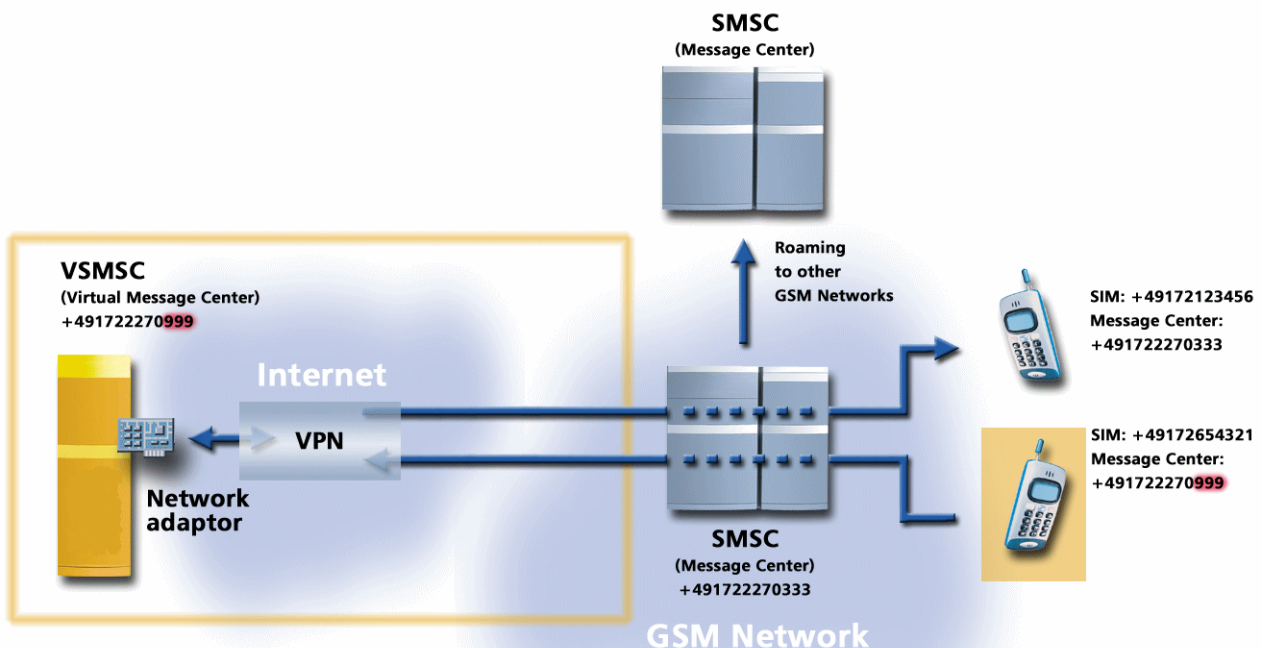
This is a special provider service, which couples a five-digit speed dialing code as recipient for short messages to the connection. This option is very popular, since it simplifies SMS message transmission and enables message services, subscriber services or premium services. Since the configuration of such a speed dialing code can always only occur in a radio network, such services are in most cases offered by so-called aggregation services. These are service companies that have reserved a large number of speed dialing codes at the various network operators and can therefore offer such a speed dialing number for the entire network.

VSMSC operation

This special type of connection exceeds the mere capability of receiving messages by far. **VSMSC** stands for Virtual Short Message Service Center, meaning that the connection represents an individual message center and receives an individual message center number.

Short messages are also sent by cell phones via a message center, the number of which has been preconfigured in the cell phone by the network operator or provider. If the XPR server is connected as VSMSC, it receives an individual message center number such as +491722270999. All SMS messages are then sent via the XPR server as VSMSC.

The following diagram outlines the function principle:



All this results in some interesting fields of application:

- **Process automation**

If e.g. a large number of gauging stations is maintained that include a GSM-compatible transmitter, this transmitter can be so configured that it always sends via the virtual message center. Examples are electricity meters, weather stations, vehicle monitoring, etc.

- **Corporate saving**

If a company has a large number of cell phones and the SMS is used a lot, all these devices can be reconfigured for the corporate message center. Short messages sent to the company are thus always free of charge, all others are sent via the SMS Connector at the negotiated, favorable prices by the XPR server after a security and identity check. This enables a higher cost transparency as well as considerable saving.

Both fields of application can also be combined.

14.3 Connection Type Comparison Overview

Feature	Comment	ISDN	GSM box	Provider
Sending		✓	✓	✓
Extra long SMS messages	Up to 612 characters.	✗	✓	✓
Special characters	Depending on the receiving cell phone and provider.	✗	✓	✓
Euro sign	Depending on the receiving cell phone and provider.	✗	✗	✓
Performance	Depending on the provider	300 SMS messages per hour	300 SMS messages per hour	30000 SMS messages per hour
Extended message tracking	The additional send reports: sent, saved, not saved.	✗	✓	✓
Adaptable originator recognition	If supported, then depending on the provider and contract.	✓	✗	✓

Table 50 Sending – SMS Features Overview

Feature	Comment	ISDN	GSM box	Provider
Editing		✗	✓	✓
Extra long SMS messages	Up to 612 characters.	✗	✓	✓
Special characters	Depending on the sending cell phone and provider.	✗	✓	✓
Euro sign	Depending on the sending cell phone and provider.	✗	✗	✓
Addressing via calling number		✗	✗	✓
Addressing via token in the message text		✗	✓	✓
Receiving via fixed calling number		✗	✓	✓
Receiving via speed dialing code		✗	✗	✓
Receiving as VSMSC		✗	✗	✓

Table 51 Receiving – SMS Features Overview

Feature	Comment	ISDN	GSM box	Provider
Number of connections per connector	Connections to message centers. With GSM each box represents a connection.	Depends on the number of B-channels	1	99 [*]
Daily reports	Per performance/ day.	✗	✓	✓
Total reports	Per performance/ total.	✗	✓	✓
Security restrictions	Option to restrict the maximum number of messages sent per day.	✗	✓	✓

Table 52 *Miscellaneous – SMS Features Overview*

* 99 connections are an arbitrary restriction not defaulted by the SMS Connector. If more connections are required, a test should be performed beforehand.

14.4 Sending SMS Messages

SMS messages can be sent from each client. Therefore enter the line `NVS : SMS / <mobile phone number>` as recipient address. `NVS :` might be omitted depending on the client that is used. If Communications is used as client, the addressing reads `<mobile phone number>[SMS]`.

Please note that, depending on the configuration, either the subject field or the message text is sent as SMS.

SMS message length is restricted to 160 characters, messages that exceed this restriction are not transmitted. Please also note that, depending on the configuration, user name, prefix and suffix may be added. This reduces the number of characters available to the user for the actual message. If the entire message comprises more than 160 characters, the originator is informed by report that it could not be sent.

14.5 SMS Connector (SMSIPAPL)

14.5.1 Installation

The SMS Connector is installed along with the XPR system. If an XPR system already exists and you want to add the SMS Connector, proceed as with installing another component in an existing XPR system.

The **SMS Connector** can be configured on the kernel node as well as on a satellite node.

NOTE:

In case of the UCP and SMPP protocols, no charges are entered in the GEB database. The messages are transmitted to the provider by IP. The call to the provider, which normally incurs charges that might be entered in the GEB database, is omitted.

NOTE:

The *ActiveXperts SMS and MMS Toolkit* was used for the GSM and SMPP protocols (<http://www.activexperts.com/xmstoolkit/>). We therefore recommend to consult the corresponding manual under <http://www.activexperts.com/files/xmstoolkit/manual.htm>.

14.5.2 Establishing and configuring a Connection

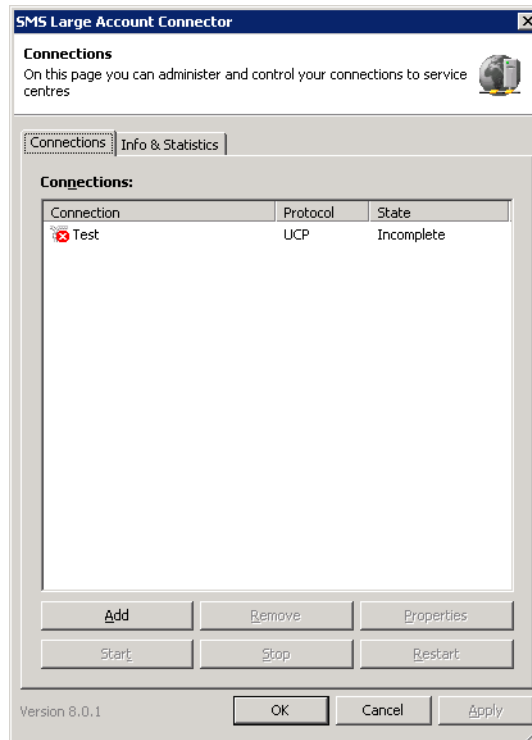
NOTE:

An administrator with *Service privilege* may configure the SMS Connector unrestrictedly.

The SMS Connector is initialized and configured via the **XPR monitor** settings dialog. In the XPR monitor open the **SmsIpAPL** option under **Settings** and doubleclick **Set options**.

14.5.2.1 Connections Tab

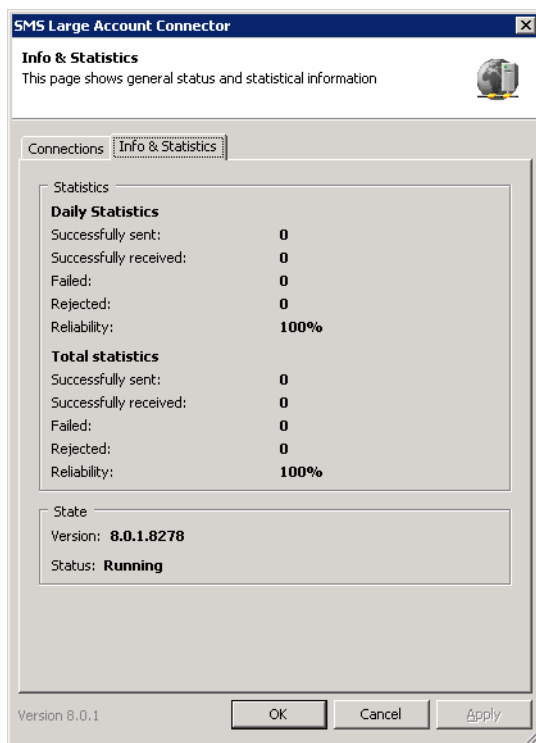
This tab shows all established connections via the SMS Connector. Displayed are merely the **Name** of the respective connection, the **Protocol** used and the **Status**. With the **Add** button you can generate new connections and delete them with **Remove**.



Furthermore you can modify the state of the selected connection by pressing the **Start** and **Stop** buttons. Clicking the **Restart** button initiates another start of the selected connection. The **Properties** buttons opens a new window in which the precise connection data can be set.

14.5.2.2 Info & Statistics

The SMS Connector configuration dialog opens. The **Info & Statistics** tab shows the data of all connections that have been established via this SMS Connector so far.



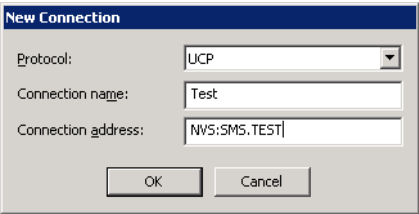
If you have established connections you can see the most important information on received and sent SMS messages in the top portion of the dialog. To be more precise, you are informed about the number of successful or failed in and outbound SMS connections.

You can also differentiate between a daily and a total evaluation. The **Reliability** aspect indicates the ratio of successful and failed SMS connections in percent. The higher the value, the more reliable is your SMS connection.

The bottom field shows the **Status** of the SMS Connector. Here you can see the SMS Connector's version and current state. This state may change if the SMS Connector is shut down during a configuration process.

14.5.2.3 Establishing a new SMS Connection

To generate a new connection, click on **Add** on the **Connections** tab to open the **New Connection** dialog.



Option	Description
Protocol	In this field you can select from the following protocols: • GSM • SMPP • UCP
Connection Name	Here you can assign an arbitrary name for the connection.
Connection Address	Enter the connection address in this field. At any rate you need to add a unique class to the NVS address. The class is the portion after the first dot.

To confirm your entries click **OK** and the connection will be listed in the **Connections** field. Now configure your new connection. See [Section 14.5.2.4, “Configuring a new SMS Connection”](#), on page 1010.

14.5.2.4 Configuring a new SMS Connection

Select the corresponding connection in the **Connections** field and click the **Properties** button. A new window appears in which you perform the precise connection settings. Depending on the protocol you receive a protocol-specific tab for the connection settings.

SMS Settings tab

The screenshot shows a window titled "Properties of line *TUCP*". Inside, there's a tab labeled "SMS Settings" with a sub-header "On this page you can specify the SMS behavior for this line". Below this are three tabs: "SMS Settings", "UCP Line Settings", and "Info & Statistics". The "SMS Settings" tab is active. It contains several sections: "Default originator number:" with an empty text box; "Default recipient address:" with a text box containing "NVS:DOC-MK/POSTMASTER"; a "Format" section with "Character set:" set to "Default IA5", "Long SMS mode:" set to "Strict (160 chars)", and "Recipient Limitation:" with two dropdown menus both set to "#"; a checkbox for "Prefix Originator Identification" which is unchecked; a "Delivery Notifications" section with three radio buttons ("None", "Default", "Specific") and three checkboxes ("Delivery notification", "Buffered notification", "Failed notification"), all of which are unchecked except for "None" which is selected; a "Size of index table:" with a text box containing "0"; "SMS prefix:", "SMS suffix:", and "SMS digest:" each with an empty text box. At the bottom, there are "OK", "Cancel", and "Apply" buttons. The version "Version 8.20.1" is displayed in the bottom left corner.

The **SMS Settings** tab describes the default settings for in and outgoing SMS messages. The following options can be configured:

Option	Description
Default Originator	This field defines the default originator address. Only digits are allowed here. If the sending user does not have any entries in the SMS and GSM database fields, the default set originator is used. Via the SmsOriginatorPropertyName [REG_SZ] registry value you can globally set a database field different from SMS for all configured connections.

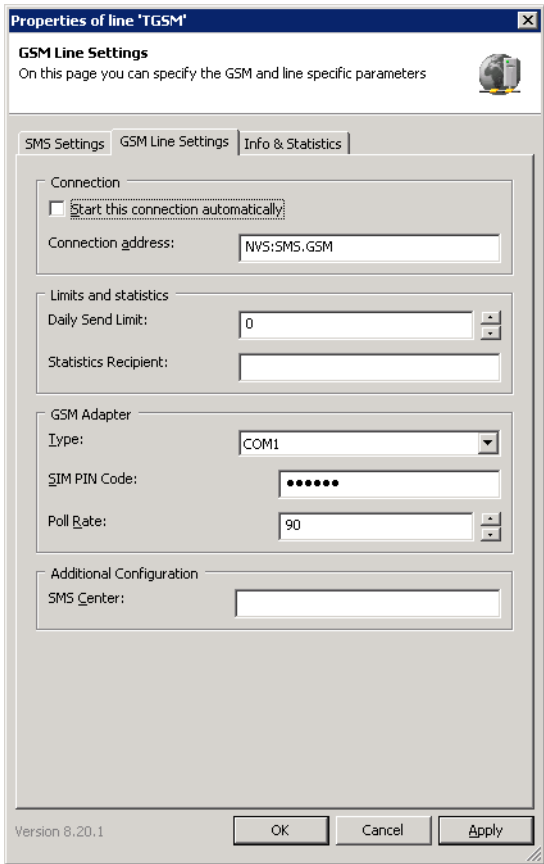
Option	Description
Default recipient address	Serves for specifying the default recipient NVS address. Postmaster is entered as predefined setting. If the information transmitted with the SMS message does not allow a recipient assignment, the default recipient is used. The precise usage of the default recipient is described in Section 14.5.4.1, "Determining the Recipient", on page 1024.
Fonts	Defines the font converter used. Possible values are: Standard IA5: Completely 3GPP-conformable GSM coding. VODAFONE-D: Font used in Germany by Vodafone in case of a provider connection via UCP.
Long SMS mode	The field defines the handling of extra long SMS messages (more than 160 characters). 8 modes are possible: Strict: If the SMS messages contains more than 160 characters it will not be sent. Split: An SMS message with up to 612 characters will be divided among up to four SMS messages. If the SMS message contains more than 612 characters it will not be sent. Concatenated: An SMS message with up to 612 characters will be divided among up to four SMS messages and sent as one. If the SMS message contains more than 612 characters it will not be sent. Based on these submessages a modern cell phone can display a single message again. Long: One big SMS message with up to 612 characters will be sent. This function must be supported by the provider. If the SMS message contains more than 612 characters it will not be sent. Short: The first 160 characters of a SMS message will be sent only. Further characters will be omitted. First Split: The first 612 characters of a SMS message will be divided among up to four SMS messages. Further characters will be omitted. First Concatenation: The first 612 characters of a SMS message will be divided among up to four SMS messages and sent as one. Further characters will be omitted. Based on these submessages a modern cell phone can display a single message again. First Long: The first 612 characters of a SMS message will be sent in one big SMS message. This function must be supported by the provider. Further characters will be omitted.
Recipient restriction	Character to identify the user with an incoming SMS. Besides the selectable characters you can also enter arbitrary ones. See Section 14.5.4, "Receiving SMS Messages", on page 1024.

Option	Description
Prefix Originator Identification	When you activate this option, each text of a sent SMS message is prefixed with a user ID. This user ID is either the e-mail address (database field SMTP) or, if this field is empty, the ID. If no user ID of the originator is known, the SMS message is not sent and a correspondingly negative report generated. This is a scenario that may emerge if, for example, messages are sent from foreign applications via the File Interface APL and the internal originator fields have not been correctly set. The net amount of available characters is reduced by the length of the determined user ID inclusive a colon and a conclusive blank. This may lead to SMS messages either being cut or not sent in the first place, though the sender has in his/her view not exceeded the maximum length. This feature has a legal background: If a company enables each user to send SMS messages via XPR, the recipient can only identify the messages if for each user a unique SMS or GSM number is entered in the user database. If co-workers abuse this feature, they can afterwards at least be identified.
Delivery Notifications – None	Do not request delivery notifications from the SMSC for sent messages.
Delivery Notifications – Default	It is up to the SMSC which notification types it uses for sent messages.
Delivery Notifications – Specific	This option offers a range of notification types for selection. Before this option is used the SMSC should be consulted since the feature is not always supported and may cause problems at the SMSC. • Delivery notification: The message center sends reports if the SMS message has been successfully transmitted. • Failed notification: The message center sends reports if the transmission of a SMS message has failed. • Buffered notification: The message center sends reports if SMS messages have been buffered because e.g. a recipient cannot be reached for the time being. The process will then be repeated within a specific time frame.

Option	Description
Size of index table	The delivery notifications sent by the SMSC cannot always be assigned to the SMS messages transmitted. To be more precise, the assignment occurs in the report via the specification of originator, recipient and a time stamp. Since the time stamp only has a resolution of one second, an assignment is not possible if more than one message is sent from the same originator to the same recipient within a second. The data required for delivery notification assignment are kept by the SMS Connector in an index table. If the size of this index table is 0, the delivery notifications are sent as message to the Statistics Recipient set. If the index table size is greater than 0, the attempt is made to determine the associating sent SMS message and to set the corresponding XPR state (OK, FAILED, DELAYED) for this message. If this is not possible owing to the small resolution of the time stamp, this report is sent as message to the Statistics Recipient again. Most SMSCs keep a SMS message up to two days, if a delivery is not immediately possible due to a cell phone switched off. Therefore an index table entry is deleted after two days. In a worst case scenario where a maximum of 1000 SMS messages is sent via the SMS Connector every day, the index-table size had to be set to 2000 (1000 SMS * 2 days), if all recipients had their cellphones switched off on these two days. In practice a significantly smaller index table should do.
SMS prefix	The text in this field will be prefixed to each SMS message. This reduces the number of freely available characters in the SMS message by the corresponding text.
SMS suffix	The text in this field will be attached to each SMS message. This reduces the number of freely available characters in the SMS message by the corresponding text.
SMS Digest	See Section 14.5.3, "The Digest Algorithm" , on page 1021.

GSM Line Settings tab

This tab defines the connection data. For SMPP connections see [SMPP Line Settings tab](#) on [page 1016](#). For UCP connections see [UCP Line Settings tab](#) on [page 1018](#).



The following configuration fields are available:

Option	Description
Start this connection automatically	Checkmarking this box makes sure that the connection is started automatically so that a manual start is not required. Otherwise you need to manually restart the SMS connection with each system reboot.
Connection Address	Serves for specifying the connection NVS address. The address must correspond to the NVS : <Service> . <Class> format. SMS is default set as <Service>.
Daily Send Limit	With this field you can set a security restriction by configuring a maximum limit for SMS messages to be sent. When 75% have been reached, a notification is sent to the Statistics Recipient .

Option	Description
Statistics Recipient	Enter a recipient here who receives the daily statistics as well as warnings. A warning shortly before reaching the send limit for a day. Another one, when the limit has been exceeded. This user also receives the delivery notifications if the correct recipient of the notification could not be determined.
Mailbox Type	With the GSM protocol, SMS messages can be sent via a GSM adapter or a modem-compatible GSM phone. Communication may occur e.g. via a serial interface, a USB port, a Bluetooth connection. We recommend to use the Windows Phone and Modem Options for the device, for example Standard 9600 bps Modem or Nokia 6310i Phone. If a Windows telephony device is used, the settings are checked via the <i>Windows Telephony Driver</i> and can be set via the Phone and Modem Options: • Open the Phone and Modem Options on the Control Panel. • Select the Modems tab. • Mark your modem and click on Properties. • You can now adjust the settings and select this modem here under Typ later. You can also directly select a COM port as alternative.
SIM PIN Code:	PIN number for SIM card.
Poll rate	Time interval in seconds in which the mobile phone device is to be queried for newly received SMS messages.
SMS Center:	Telephone number of the service center via which all SMS messages are to be sent. If the field remains empty, the service center stored on the SIM board is selected. The number is dialed as displayed. Thus no normalization takes place.

SMPP Line Settings tab

This tab defines the connection data.

Properties of line *TSMPP*

SMPP Line Settings
On this page you can specify the SMPP and line specific parameters

SMS Settings | **SMPP Line Settings** | Info & Statistics

Connection
☐ Start this connection automatically
Connection address: NVS:SMS.SMPP

Limits and statistics
Daily Send Limit: 0
Statistics Recipient:

Physical Connection
Service center: 1.2.3.4:1234
Reconnect Interval: 30
Retry Delay: 300
Keep Alive Time-out: 0
System Mode: Transmitter
Interface Version: v. 3.3

Credentials
ID: ID
Session Password:

Version 8.20.1

OK Cancel Apply

The following configuration fields are available:

Option	Description
Start this connection automatically	Checkmarking this box makes sure that the connection is started automatically so that a manual start is not required. Otherwise you need to manually restart the SMS connection with each system reboot.
Connection Address	Serves for specifying the connection NVS address. The address must correspond to the NVS : <Service> . <Class> format. SMS is default set as <Service> .
Daily Send Limit	With this field you can set a security restriction by configuring a maximum limit for SMS messages to be sent. When 75% have been reached, a notification is sent to the Statistics Recipient .
Statistics Recipient	Enter a recipient here who receives the daily statistics as well as warnings. A warning shortly before reaching the send limit for a day. Another one, when the limit has been exceeded. This user also receives the delivery notifications if the correct recipient of the notification could not be determined.

Option	Description
Message Center	In this field you need to specify the address of your provider's message center (SMSC) and the port number used. The address can either be entered as IP address or as qualified domain name and must be separated from the port number by a colon.
Reconnect Interval	Here you can define a period in seconds for the connector to wait after a termination of the physical connection. After this waiting period the connection will be re-established. The value must be between 5 and 3600 seconds.
Retry Delay	Here you can define a period in seconds for the connector to wait after an error that led to a connection breakdown. After this waiting period the connection will be re-established. The value must be between 10 and 86400 seconds.
Keep-Alive Interval	Here you can enter an interval in seconds. If the line does not show any activity for more than n seconds, a keep-alive package will be sent to the message center. In case of SMPP the connection is customarily kept open. Therefore, keep the 60-second default and change it only if the connection closes with this setting. In this case try a shorter interval setting.
System Mode	Here you can choose from the following options: • Transmitter/Recipient • Transmitter • Recipient The Transmitter/Recipient can only be set from version 3.4 of the SMPP interface.
Interface Version	Set the SMPP protocol version used. Supported are: • Version 3.3 • Version 3.4 • Version 5.0
ID	In this field you need to enter a unique speed dialing number or a number for the VSMSC. You can obtain these from your provider.
Session Password	You can obtain this password from your provider. It is stored encrypted in the registry.

UCP Line Settings tab

This tab defines the connection data.

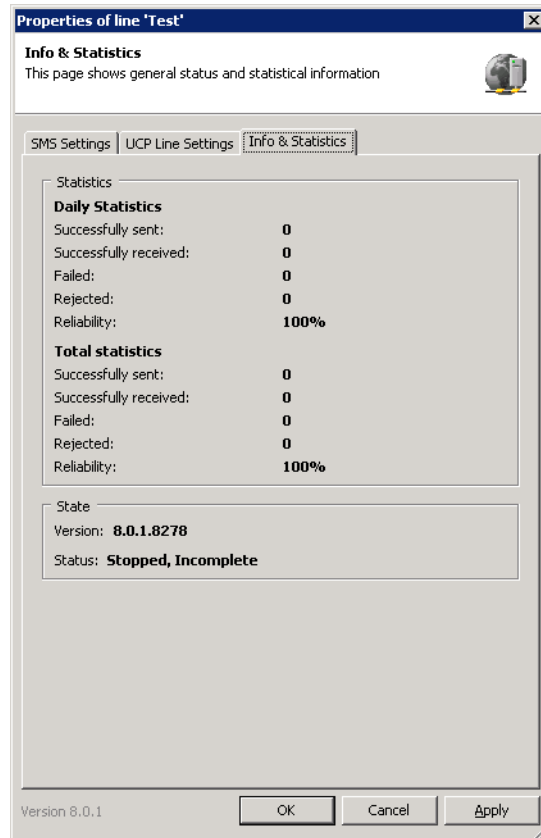
The following configuration fields are available:

Option	Description
Start this connection automatically	Checkmarking this box makes sure that the connection is started automatically so that a manual start is not required. Otherwise you need to manually restart the SMS connection with each system reboot.
Connection Address	Serves for specifying the connection NVS address. The address must correspond to the NVS : <Service> . <Class> format. SMS is default set as <Service> .
Daily Send Limit	With this field you can set a security restriction by configuring a maximum limit for SMS messages to be sent. When 75% have been reached, a notification is sent to the Statistics Recipient .
Statistics Recipient	Enter a recipient here who receives the daily statistics as well as warnings. A warning shortly before reaching the send limit for a day. Another one, when the limit has been exceeded. This user also receives the delivery notifications if the correct recipient of the notification could not be determined.

Option	Description
Message Center	In this field you need to specify the address of your provider's message center (SMSC) and the port number used. The address can either be entered as IP address or as qualified domain name and must be separated from the port number by a colon.
Reconnect Interval	Here you can define a period in seconds for the connector to wait after a termination of the physical connection. After this waiting period the connection will be re-established. The value must be between 5 and 3600 seconds.
Retry Delay	Here you can define a period in seconds for the connector to wait after an error that led to a connection breakdown. After this waiting period the connection will be re-established. The value must be between 10 and 86400 seconds.
Keep-Alive Interval	Here you can enter an interval in seconds. If the line does not show any activity for more than n seconds, a keep-alive package will be sent to the message center. This parameter is required for ITENOS connections. No other provider requires this functionality, so that this value should remain 0.
ID	In this field you need to enter a unique speed dialing number or a number for the VSMSC. You can obtain these from your provider.
Session Password	You can obtain this password from your provider. It is stored encrypted in the registry.

Info & Statistics tab

The **Info & Statistics** tab is the same window as the dialog at the configuration start. Therefore please refer to the **Info & Statistics** tab description for details. However, the properties in this window only refer to the respective connection which is particularly valid for the state reported. The dialog at the beginning of the configuration refers to information on all connections.



With a click on the OK button you return to the **Connections** tab. The previously configured connection must be **started** for the modifications to take effect.

14.5.3 The Digest Algorithm

The XPR server offers among other things the option to forward incoming messages as SMS message. This is particularly useful for MWI notifications created by the Notification APL or for forwarding e-mails. In this process it happens ever so often that rerouted e-mails reach a length that does not fit in the cellphone display. In this case the SMS protocol can intelligently shorten the message. The mechanism used for this purpose is the digest algorithm. It filters superfluous information (e.g. blank lines or greeting phrases) from messages to be sent as SMS message.

The manner in which the digest algorithm is to shorten messages is defined via various variables. The following variables are available for supplementing or modifying messages:

- { DATE }
Defines the current date.
- { DIGEST [, <Max>] }
Long messages to be sent can be shortened according to the Digest Algorithm. In doing so the attempt is made to remove non-information elements (such as blank lines or salutation phrases) from the text. Line breaks are converted into blanks.

The maximum length of the digest can be defined by the <Max> parameter. If the message text is longer, it is cut after <Max> characters and supplemented with '...' at the end.
- { FORMAT }
Defines the format of the original message (e.g. voice, fax or e-mail). This information is particularly interesting with message rerouting.
- { ORGNAME [, <Max>] }
Defines a legible version of the originator address. If e.g. an originator is contained in the speed dialing database, the actual originator name may be contained here instead of his/her phone number.

The maximum length of the address can be defined by the <Max> parameter. If the originator address is longer, it is cut after <Max> characters and supplemented with '...' at the end.
- { ORGNODE }
Defines the service type of the original message. This information is particularly interesting with message rerouting.
- { ORGUSER }
Defines the original originator address. This information is particularly interesting with message rerouting.

Short Message Service (SMS)

- {RECNAME[, <Max>]}
Defines a legible version of the recipient address. The maximum length of the legible recipient name can be specified by the optional entry <Max>. If the recipient address is longer, it is cut after <Max> characters and supplemented with '...' at the end.
- {RECNODE}
Defines which service has originally received the message. This information is particularly interesting with message rerouting.
- {RECUSER}
Defines the original recipient address. This information is particularly interesting with message rerouting.
- {SUBJECT[, <Max>]}
Defines the subject of the original message. This information is particularly interesting with message rerouting.

The maximum length of the subject information can be defined by the <Max> parameter. If the original subject is longer, it is cut after <Max> characters and supplemented with '...' at the end.
- {TEXT[, <Max>]}
Contrary to Digest, the message is not shortened here. This maintains the original formatting.

The maximum length of the digest can be defined by the <Max> parameter. If the message text is longer, it is cut after <Max> characters and supplemented with '...' at the end.
- {TIME}
Defines the current time.

Example:

The XPR server receives the following e-mail to be forwarded as SMS message to the relevant user.

Originator: john@far.com "John Smith"

Subject: We got the contract

Body:

Sunday evening, 06:45pm

Hi Mae,

At last we got the contract regarding your offer to the ABC inc.

Regards,

John

Since it would not be very useful to have this message displayed on a cellphone unchanged, we use the digest algorithm. We configure it in the following format:

{ORGNOME}: {SUBJECT,80} - {DIGEST,40}

In this definition, {ORGNAM} forms the originator name, {SUBJECT, 80} is the message subject limited to 80 characters and {DIGEST, 40} represents the message contents reduced to 40 characters. The result of our example thus reads:

```
John Smith: We got the contract - At last we got the contract  
regarding...
```


14.5.4 Receiving SMS Messages

SMS messages without special recipient ID in the body text are forwarded to the user entered in the **Default recipient address** field.

If an SMS message is to be directly sent to a specific user, the message text must contain a coding of this recipient. This is limited by the characters that have been configured under **Recipient restriction**. The coding can be placed in an arbitrary position within the SMS message body. The coding within the SMS text body corresponds for instance to one of the following patterns:

```
<Message text>*<Recipient>#<Message text>
<Message text><<Recipient>><Message text>
```

Examples:

```
*1234#Hello Mr Jones, ...
<Jane Miller>Hello Mr Jones, ...
```

14.5.4.1 Determining the Recipient

The SMS connector attempts to determine the recipient via the database field entered in the registry value **DBInField [REG_SZ]**. The text that can be found between the characters configured under **Recipient restriction** is taken from the received SMS message. The SMS will then be sent to the user who has entered this text in the referenced database field. Default value for this database field is SMS#.

If no recipient can be determined this way, then the default recipient is used.

IMPORTANT:

You need to write the name in capital letters. In the database, also the referenced field must exclusively contain capital letters. Please bear this in mind especially if no pure number field is used but e.g. the field SMTP.

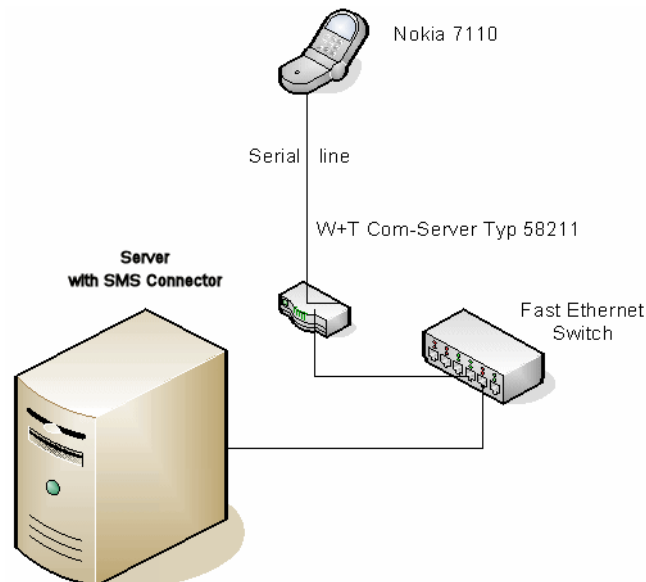
14.5.5 Messages with Attachments

The SMS Connector accepts any message. But only the message portion the MTA converts into text is sent in the scope of the maximum length set for the SMS message.

14.5.6 Serial Adapters for GSM (COM Server)

Serial adapters, also called COM server, represent a serial interface for using XPR SMS boxes and thus for using the SMS Connector. The SMS boxes need not be directly connected to a physical server interface, but can be arbitrarily connected to any position in the network by means of the adapters. This ensures a good network reception for cell phones, if no reception is possible at the place where the XPR server has been set up.

The adapters can be addressed and configured by a XPR server of the network. Each adapter with its Ethernet address, the configurable IP address and the assigned COM Port is a unique network element, with which the SMS Connector functions can be executed. The following graphic representation shows a rough example of how the different components can be connected.



How to install and configure the adapters depends on the use of a specific make and can be gathered from the manufacturer's operating instructions. Please also heed possible restrictions as regards the adapters' accessibility in the network.

The following adapters have been tested so far:

- Wiesemann & Thies: COM Server Typ 58211

14.5.7 Automatic Monitoring of the SMS Device

Every 30 seconds the SMS Connector checks whether the device for receiving and sending messages is in order. The following tests are performed:

- Test, whether the PIN is set in the device.
- Test, whether the device is ready to send or receive SMS messages.
- Test, whether the device is registered in the GSM network.
- Charge condition of the storage battery and readiness to serve.
- Signal quality: Received Signal Strength Indication (RSSI) and Bit Error Rate (BER)

If one of these five tests fails, the device is automatically rebooted and an internal error counter notched up. If no errors are detected with the next automatic check, the error counter is reset. Otherwise the counter is further notched up. If the number of checks set in [MaxRestartAttempts \[REG_DWORD\]](#) fails in succession, the following message is written in the Windows event log depending on [SnmpMode \[REG_DWORD\]](#):

There are technical problems regarding your SmsBox. Please verify as soon as possible.

This line is subsequently closed. You can set a period between the checks ranging from 15 to 300 seconds via [GsmDeviceCheckRate \[REG_DWORD\] \(GSM\)](#).

15 TCP/IP APL

The TCP/IP APL is a SMI transporter based on the TCP/IP protocol. A SMI transporter is required when an interconnection is made between two servers (Remote System Link), or when a connection is created between a client and a server.

XPR servers can be connected with this transport by Remote System Link. The MSP-based Windows client applications can also communicate with the XPR server via TCP/IP. Since TCP/IP is a protocol, which is used in wide area networks (WAN) such as the Internet, communication with the XPR server could also be worldwide if an Internet connection is available.

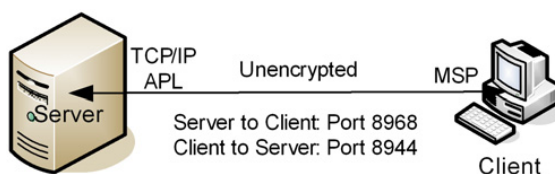
A configuration of this transport is in most cases not necessary since all required settings were performed during the TCP/IP network protocol installation under Windows.

NOTE:

An administrator with *service privilege* may configure the TCP/IP APL unrestrictedly.

15.1 Ports and Encryption used

The TCP/IP APL uses the ports 8944 and 1107 for the client access. Port 1107 is only supported for the update scenarios, since older MSP versions accessed the TCP/IP APL via this port. With active delivery from the TCP/IP APL to MSP-based client applications port 8968 is used. This type of communication is not encrypted. By means of a network sniffer you can play all data transmitted between server and client.



You can also communicate via a connection secured by SSL. On the server side, all corresponding requirements have already been met as a certificate has been configured for the STunnel program.

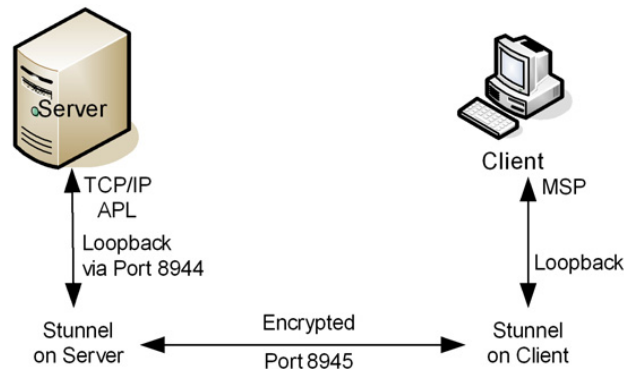
To activate this SSL encryption, you need to set the values [UseEncryption \[REG_DWORD\]](#) and [NatClient \[REG_DWORD\]](#) on the client appropriately. This encryption is not default set, so that the server can first be upgraded to the current version and subsequently all old clients still work. You can then set the two registry values in the course of the clients update.

NOTE:

Using SSL V2 and V3 is always disabled in the XPR server. TLS V1, V1.1 or V1.2 is always used.

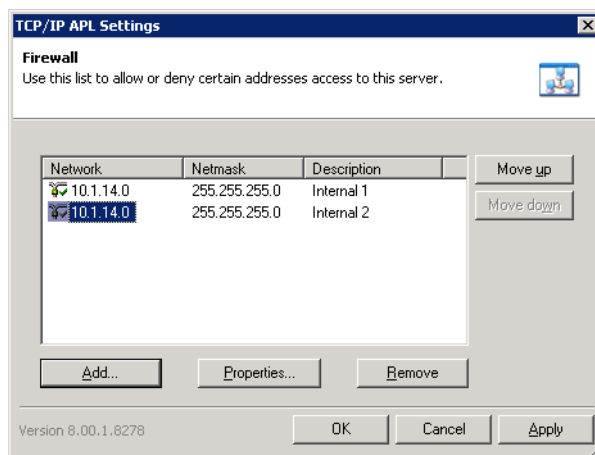
Furthermore, the load of upgraded systems should be watched, since via STunnel active delivery can no longer be performed by a connection setup from the server to the client. In conjunction with the [NatClient \[REG_DWORD\]](#) value the connection is not closed down any more and continuously loads the server.

For a connection secured by SSL, port 8945 is used. If you then lock port 8944 in the Windows firewall, clients without activated encryption will not be accepted any more.



15.2 Firewall Mechanism

After its installation, the TCP/IP firewall is disabled. This enables access from every computer to the server via TCP/IP.



If access is to be denied to specific computers or networks, this can be accomplished by forming a reference from the IP-Network address and Netmask. Through this reference, access can either be granted or denied. A description of the access type can also given for easy identification.

As soon as an entry is present in the dialog window, the behavior of the TCP/IP APL changes so that every computer (or network) must now be explicitly granted access to the server. The result is that normally only computers and networks are specified that are allowed access.

The reference list is sequentially searched from the first entry until a match is found. If a single computer from a network is to be allowed access to the server but the rest of its network denied access, then the computer reference must be inserted in the list prior to that of the network. By selecting the **Add** button, new references may be added to the list. An existing entry must first be selected and can then be modified via **Properties** or deleted via **Remove**. Repositioning an access reference within the list is accomplished through the use of the buttons **Up** and **Down**.

New settings are activated as soon as the **OK** or **Apply** buttons are selected. All changes to the settings are dynamically integrate, so that a restart of the TCP/IP APL is not necessary.

Examples

In the following examples an activated entry (access granted) is displayed with a "+" and a deactivated entry (access denied) through an "x".

- If access to the server is to be explicitly granted to all IP-addresses, then the following should be inserted into the reference list:

	IP address	Netmask
+	0.0.0.0	0.0.0.0

- To deny access to all IP-addresses the following entry is inserted into the reference list.

	IP address	Netmask
x	0.0.0.0	0.0.0.0

- A Class C network exists which has been divided into two logical networks. The “upper” network and the “rest of the world” are to be denied access to the XPR server.

Class C network: 194.77.158.0, Netmask: 255.255.255.0

Lower Network: 194.77.158.0, Netmask: 255.255.255.128

Upper Network: 194.77.158.128, Netmask: 255.255.255.128

The reference list then has the following entry:

	IP address	Netmask
+	194.77.158.0	255.255.255.128

- A Class C network exists which has been divided into two logical networks. The “upper” network and the “rest of the world” are to be denied access to the XPR server. The only exception is an additional XPR server from the “upper” network, that shall be allowed to access a Remote System Link.

Class C network: 194.77.158.0, Netmask: 255.255.255.0

Lower Network: 194.77.158.0, Netmask: 255.255.255.128

Upper Network: 194.77.158.128, Netmask: 255.255.255.128

XPR Server in the upper network:194.77.158.155

The reference list then has the following entry:

	IP address	Netmask
+	194.77.158.0	255.255.255.128
+	194.77.158.155	255.255.255.255

- In a Class C network all computers are to be granted access to the XPR server with the exception of one. and worldwide access is also to be deactivated.

Class C network: 194.77.158.0, Netmask: 255.255.255.0

Computer without access:194.77.158.166

The reference list then has the following entry:

	IP address	Netmask
x	194.77.158.166	255.255.255.255
+	194.77.158.0	255.255.255.0
x	0.0.0.0	0.0.0.0

Since all addresses that do not fall within the range of those through the combination of IP-address and Netmask will be denied access, the last entry may be omitted:

	IP address	Netmask
×	194.77.158.166	255.255.255.255
+	194.77.158.0	255.255.255.0

16 Notification APL

16.1 General Overview

The Notification APL provides functions used for creating notifications on any incoming messages. Notifications are server-generated and can be sent to arbitrary terminal devices to draw a user's attention to new messages. This may occur, for example, by MWI (Message Waiting Indication), SMS or the TUI (Telephone User Interface) calling the user (User Outcall). In the latter case you can also directly play the message or, for example, forward it to a local fax device. Via the Web Assistant you can freely define for which type of message a notification is generated and where it is to be sent to.

Especially when using True Unified Messaging (TUM) the Notification APL is the only option for sending new-message notifications to users. The corresponding APLs regularly retrieve the mailbox status and actively notify the Notification APL. The formerly used notification function of the MTA can only access messages available in the XPR database and does therefore not work in a True Unified Messaging environment. Reversely, the Notification APL always accesses the user inboxes via the TUM interface. In a Lotus Domino/Notes or Microsoft Exchange environment it thus mandatorily requires the APLs for access via TUM. With XPR server updates the Notification APL adopts the type of notification set in the CIT database field.

The Notification APL provides the following options for defining notifications:

- Notifications can be generated depending on the message type (e-mail, fax, voicemail).
- Within a definable period no further notifications occur once the user has been notified, even if new messages come in.
- Definition of a notification target. Several devices can be addressed parallel as well.
You can set two alternative target definitions that are activated in succession if the notification fails.
- For each message type you can define whether a notification is only generated with messages labeled "urgent".
- Definition of periods in which notifications are sent.

16.2 Operating Requirements

The CIT notification via the MTA is automatically shut down by the Notification APL. This MTA function can only be reactivated after uninstalling the Notification APL.

IMPORTANT:

On the initial installation the Notification APL particularly adapts the corresponding entries in the user database for signaling if these entries already exist for signaling via the MTA. In the event that you want to uninstall the Notification APL at a later date and reactivate the new message notification via the MTA, the user database adaptations must be manually canceled.

16.3 Notifications

The single notifications are summarized in a notification list. A list can contain a maximum of 99 entries per mailbox.

Each notification is internally mapped via the following structure: based on the message type and a time definition, notification target groups are selected. The target groups contain the notification targets. The notification targets are defined via service and address. Further targets can be specified here if the notification to the first target fails.

Which target address is eventually selected for the notification always depends on where the first valid entry is found in the process.

Message type

Selection for which type of message (e-mail, fax, voicemail or all) a notification is to be generated. In addition, notifications can be made dependent on whether an incoming message is labeled "urgent".

Time definition

- Determination of one or several periods in which notifications are to be sent within the course of a day (start/stop time).
- Determination on which days the notification is to occur.

Notification target groups

Here the (multiple) notification targets are stored.

Notification target

The first entry defines the preferred notification target. You can also specify additional devices as alternative targets here. The targets are addressed in succession if transmission to one device fails.

Destination

The service required for transmission is defined by the device entry (cellphone, MWI etc.). The device itself is specified by its address.

The following services can be used for addressing:

- Mobile phone (SMS)
- MWI/LED (MWI)
- E-mail (SMTP)
- Pager (PAGER)
- Ergo (User Outcall)
- Evo (User Outcall)
- PhoneMail (User Outcall)
- VMS (User Outcall)

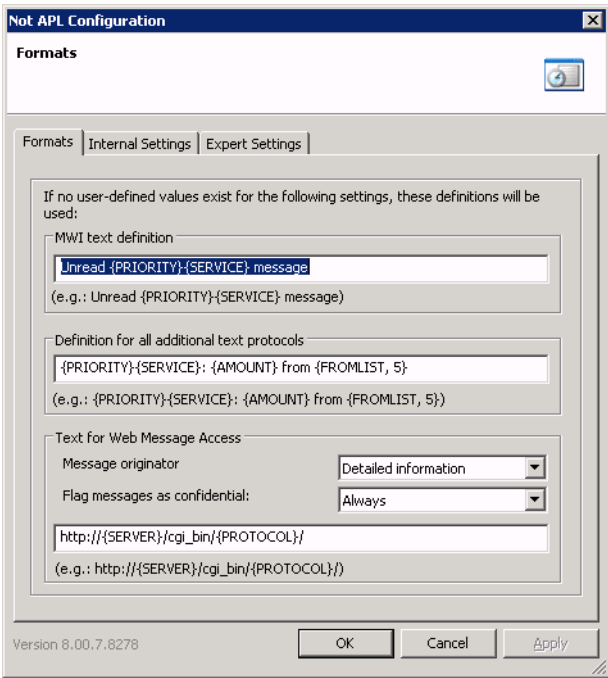
You find the XPR service used for the notification respectively User Outcall for voicemail systems in brackets. If, for example, another protocol than MWI is to be used for setting an LED on the telephone, this change must occur by a routing rule to be correspondingly created. See [Section 16.10, “Examples of Routing Rule Adaption”, on page 1045](#). In case of the MWI protocol an additional notification text is written in the telephone display if required.

16.4 Configuration

The Notification APL standard configuration is sufficient in most cases. The following reference provides an overview of the possible settings.

NOTE:
An administrator with *service privilege* only sees the **Formats** and **Internal Settings** tabs.

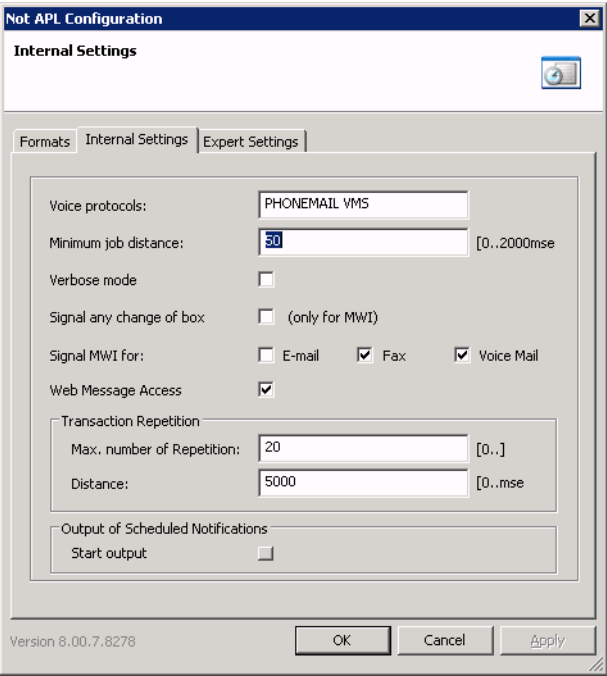
16.4.1 Formats



Option	Description
MWI text definition	This is the text string sent to the target address in case of notifications of type MWI. For a detailed description of the variables refer to Section 16.8, “SMS/E-Mail Notifications”, on page 1044 .
Definition for all additional text protocols	This is the text string sent to text-compatible target addresses in case of notifications. For a detailed description of the variables refer to Section 16.8, “SMS/E-Mail Notifications”, on page 1044 .

Option	Description
Text for Web Message Access	This is the URL that, in case of a notification for the Web Message Access, is sent to the recipient by SMTP along with an explanatory text. The variables {SERVER} and {PROTOCOL} must be modified when they deviate from the standard. {SERVER} is the XPR kernel computer IP address. If the Web APL is operated on a satellite, the corresponding IP address must be entered here. {PROTOCOL} is expanded to the Web Assistant. If you install the assistant under a changed protocol name, you can enter this name here. The URL is completed with the recipient and the ID of the message to be displayed, which are added in encoded format. If you have activated secure sockets in the Web APL, change the http to https here, so that messages can be accessed via a tap-proof connection. For more information see Section 16.7, “Web Message Access”, on page 1042.
Message originator	Originator of the notification for the Web Message Access. You can select Name, E-mail or Postmaster. For more information see Section 16.7, “Web Message Access”, on page 1042.
Flag messages as confidential	The notification for the Web Message Access can always be flagged as confidential or only depending on the original message. Confidential messages cannot be forwarded via the Web Assistant or by TUI. The behavior of other e-mail clients deviates from the one here described, so that there only an indication is displayed in most cases. For more information see Section 16.7, “Web Message Access”, on page 1042.

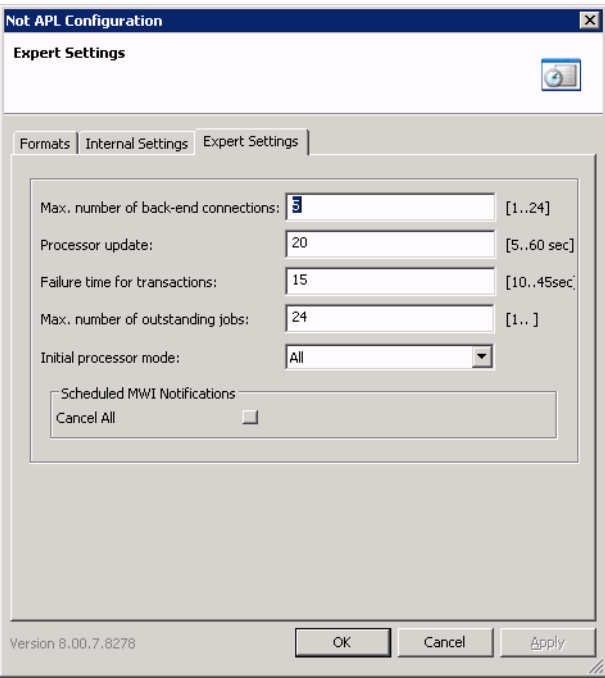
16.4.2 Internal Settings



Option	Description
Voice protocols	Enter here, separated with a blank each, the names of the voice-compatible protocols that may serve as target address for notifications. The Notification APL sends to these protocols a notification message of type voice. Without this setting a text message would be sent to the corresponding protocol. This message is then converted into Voice with configured text-to-speech. This also delivers the desired notification result by User Outcall. However, such notifications load the server with unnecessary, computing-intensive conversions.
Minimum job distance	Minimum period in milliseconds between two notifications by the Notification APL. To decrease the system load by the Notification APL you can mark up this value. On systems with a medium or high number of users, marking up should occur carefully since otherwise notifications may arrive delayed.
Verbose mode	In this mode the Notification APL becomes more extensive in all log output areas and the system load rises accordingly. This function should only be activated upon direct request by the development department.

Option	Description
Signal any change of box	MWI notifications are normally only sent with an increasing number of waiting messages and with no waiting message. When this option is activated, MWI notifications are also sent with each change in the monitored inbox. This enables, for example, counter indications on telephone displays that also change when e. g. a message is deleted. This setting is required e. g. for OpenStage phones at an OpenScape Voice if the Voicemail feature is active for this system. This type of counter indication is also enabled by the ABC-A APL for Alcatel 4400 PBXs or by the IP APL for Alcatel OXE 8.0 PBXs.
Signal MWI for E-mail	Via this switch you can influence the default settings for new users. If this option is set, the notification via telephone LED is automatically activated when a new e-mail comes in.
Signal MWI for Fax	Via this switch you can influence the default settings for new users. If this option is set, the notification via telephone LED is automatically activated when a new fax message comes in.
Signal MWI for Voice Mail	Via this switch you can influence the default settings for new users. If this option is set, the notification via telephone LED is automatically activated when a new voicemail comes in.
Web Message Access	Activates the Web Message Access. When a fax or voicemail comes in, you can use this feature to send a special notification to the recipient by SMTP. Via the special notification set under Text for Web Message Access , the recipient can then invoke the Web Assistant in simplified login mode to read or play the message there. An integration in the groupware available on the customer side is thus not necessary. See Section 16.7, "Web Message Access" , on page 1042.
Transaction repetition	
Max. number of Repetition	Maximum number of repetition attempts with sending transactions to the back-end. If, for example, the back-end lines are not yet ready at the Notification APL start, the monitor transactions would be resent. By means of 0 the repetition attempts can be deactivated.
Distance	Defines the waiting time after which a transaction is repeated.
Output of Scheduled Notifications	
Start output	All currently scheduled notifications are given out as XMR output on info level. The XPR monitor thus informs about pending notifications.

16.4.3 Expert Settings



Option	Description
Max. number of back-end connections	This option defines the maximum number of TUM sessions simultaneously opened by the Notification APL. These are needed to access the message store in True Unified Messaging environments via transactions. A TUM session may take, especially in Exchange and Lotus Notes environments, some seconds, in special cases even minutes. Therefore this value should, if at all, only carefully be modified and in small steps until the maximum value of 24 has been reached. Keep in mind that marking up this value leads to a larger number of opened sessions, which may increase the system load significantly. The reason is that for each session one thread is started. On the other hand you can, if performance problems should occur, gradually decrease this value (to a minimum value of 1) to set a compromise between system load and simultaneously opened TUM sessions. Normally the default should not be modified.
Processor update	Here you can set the time in which the APL-internal processor inquires whether a notification is due. This point in time, predefined by the user, is compared with the current UTC time, which results in the transmission time. So that no notification is missed, the transmission time must be less than 60 seconds. The default value of 20 seconds should not be modified. It makes sure that the processor checks the user mailbox three times a minute for notifications to be sent.

Option	Description
Failure time for transactions	Time in seconds that the Notification APL waits for a reply after a sent transaction. If you receive warnings of the type NotApl Backend W Monitor fetch of <AD47434> failed NotApl Backend E Monitor fetch of <AO38386> failed NotApl Processor W Monitor OFF request for in the XPR monitor, the most likely cause is a timeout of the back-end inquiry. In such cases try to mark up this value.
Max. number of outstanding jobs	This value limits the number of messages queuing up. In this way you can avoid a PBX overload.
Initial processor mode	The Notification APL never searches for unread documents as a matter of principle. This behavior does not depend on the applied back-end. Via a push mechanism the Notification APL learns directly from the back-end about new documents that have come in. The Notification APL itself is hence only a so-called monitor point on the mailbox which is actively notified by the back-ends about status changes in the mailbox. The internal Notification APL start behavior is set here via the value ResetMwi [REG_DWORD] . On systems with a large number of users the initial MWI status retrieval for setting the LED for all users can enormously increase the system load (setting All). By means of only real time the initial MWI status retrieval by the back-ends is ignored to avoid the high system load. Further notification types are performed anyhow. In such a case, the user does not receive any MWI signal for the first unread message. All following new messages will be signalized again. only normal leads to an exclusive handling of the back-end MWI inquiries at the start.
Scheduled MWI Notifications	Via a mouseclick on the Cancel All button all MWI notifications still to be sent are deleted from the send queue. Subsequently, the MWI stati of the users are not correct anymore, but a possible PBX overload can be relieved in this way.

16.5 Configuring Notifications

Contrary to the old MTA notification function the individual user privileges only partly determine which notifications can actually be activated. For the Notification APL the call privileges control whether a user may send an SMS message. The special privilege for notifications via SMS (`CIT_SMS`) is no longer considered and obsolete just like the other CIT privileges when notifications occur via the Notification APL.

Notifications are configured from the *Web Assistant*. How the user performs notification settings is described in the *Web Assistant*.

16.6 MWI Fallback Strategy

With initialized MWI the Notification APL browses the following database fields in succession:

- `CIT`
- `PHONE`
- `VOICE`

If the `CIT` field for a user should be empty, a number is searched for in the `PHONE` field. If no number is available there either, the last option is the `VOICE` field.

If several numbers have been assigned to a user in the respective field, the MWI notification goes to all entered numbers. For the allocation of several numbers the corresponding field must be assigned the MULTI flag. You find more information on this flag in [Table 5 on page 113](#).

16.7 Web Message Access

The Web Message Access enables an integration in each e-mail system that can receive and send SMTP messages. Instead of the actual message, merely a notification is sent with a URL by SMTP. The user clicks on the URL to invoke the Web Assistant via his/her browser in Web Message Access Mode and sees the message. Depending on the e-mail client setting, the URL is not displayed as link. In this case the user needs to copy the URL from the message to his/her browser to see the message. The user can also forward the notification with the URL for other recipients to see the message.

Editing or answering the message from within the Web Assistant requires a login. Without the login, the message is only displayed. If the administrator allows simplified Web access, the users can activate this type of access in their private settings. Then they only needed to log on with the first message since the required information is stored in the system via a cookie.

The notification is language-dependent and defined by the template `WEBUM_<LCID>.TXT` in the `<XPR Install>\Userdata\Notification` directory. `<LCID>` is the decimal Locale ID. The following values are currently supported:

<LCID>	Language (Country)
1031	German (Germany)
1033	English (USA)
1036	French (France)
1040	Italian (Italy)
1043	Dutch (Netherlands)
1046	Portuguese (Brazil)
1055	Turkish (Turkey)
2057	English (United Kingdom)
2070	Portuguese (Portugal)
3082	Spanish (Spain)

Table 53 Supported LCIDs with Notification APL Text Notifications

The text of the template file can be arbitrarily adjusted, but it is important that the `{WEBUM_URL}` variable is contained in this file. This variable is replaced with the URL via which you can see the actual message in the Web Assistant.

To activate the Web Message Access, you need to activate the **Web Message Access** option on the **Internal Settings** page.

If an administrator wants to allow users to immediately edit these messages without having to log on again for each message, the following steps must be performed:

1. Logging on in the Web Assistant as administrator (member of the administrator group).
2. Under **Server settings > Web Access Security > Decision for simplified web access** activate the **Allow simplified web access** option.
3. Each user is now enabled to activate the **Simplified web access** option under **Personal settings > user data**.

NOTE:

The users must receive their messages via the Mail APL and must have an SMTP address. We therefore recommend the setting `MAILBOX` in the `PREFERRED` field. The Web Message Access is not supported for users who deploy a TUM integration.

16.8 SMS/E-Mail Notifications

It is possible to generate language-dependent texts for notifications to SMS and e-mail addresses. When these language-dependent versions are available, they are used instead of the registry default. These texts are stored as files in the `<XPR Install>\Userdata\Notification` directory. For SMS these texts have the file name `SMS_<LCID>.TXT`; for SMTP the file name `SMTP_<LCID>.TXT`. `<LCID>` is the decimal Locale ID. See [Table 53 on page 1043](#).

NOTE:

The available files `SMS_<LCID>.TXT` must be customized with the voice mail system callback number for each installation.

It is also possible to store user-dependent text files. These are stored in the same directory and have the file name `SMS_<User ID>.TXT`, or `SMTP_<User ID>.TXT`. So that these text files can be taken for the respective user, an entry of the format `<User ID>.TXT` must be made in the user's `CITFILE` database field. If required, this database field is to be supplemented since it is not present in the standard form. In the event that an entry of the format `SMS_<User ID>.TXT` is stored in this database field, this file will only be used for SMS notifications; SMTP notifications still use the default. This works also vice versa: If you define the SMTP notification user-dependently, the language-dependent version is used as SMS notification. If this version is not available, the default from the registry is reverted to.

The following variables can be used in the text file:

Variable	Meaning
{AMOUNT}	Number of unread messages referring to a service.
{FROM}	Originator of the last received unread message referring to a service. The variable {ORGNAME} can also be used.
{FROMLIST}	List of the originators of unread messages referring to a service.
{PRIORITY}	Generates a ! for messages of high priority.
{SERVICE}	Service of the unread messages this notification refers to. The variable {ORGNODE} can also be used.
{SUBJECT}	Subject of the last received unread message.
{TO}	Message recipient. The variable {RECNAME} can also be used.

Table 54 Variables with Notification APL Text Notifications

Each variable except {FROMLIST} can be restricted to a maximum number of characters by an optional length specification. Via {SUBJECT, 50} for example a subject with more than 50 characters would be cut accordingly. In case of {FROMLIST, 2} the specification refers to the number of displayed originators.

If a notification is to occur for several services simultaneously because e.g. a new voicemail as well as a new e-mail has come in, one line is generated per service. In the event that an SMS becomes too long, the sending APL is responsible for dividing or cutting it.

If the notification is an SMTP notification, the subject informs you about the type of the incoming messages. If you have received e.g. a voicemail as well as an e-mail, the subject would be "Notification service: VOICE SMTP".

16.9 Configuring a Repeat Strategy for User Outcall

With the User Outcall function the TUI protocols defined in a telematic APL are for outbound use, thus call a subscriber. So that this call is successful, the set repeat strategy of these protocols should be checked and adapted if required.

Repeat strategy default are three attempts in a 60 seconds interval, then two attempts in a 120 seconds interval and another attempt after 300 seconds. If the user to be notified made a ten-minute call, all of these attempts would be futile as he/she could not be reached.

16.10 Examples of Routing Rule Adaption

If the MWI protocol addressed by the Notification APL is actually never used for signaling but e.g. the CIT_BASIC protocol provided by the V.24 APL, the routing rules are to be extended by the corresponding rule. For CIT_BASIC e.g.:

```
NVS:MWI.*/*=NVS:CIT_BASIC.*/*
```

Since internal XPR operation always occurs with the international calling number format, this format may have to be cut to the internal format for the transmission to the PBX. Example:

```
NVS:MWI.*/+492404901*=NVS:MWI.*/*
```

or

```
NVS:MWI.*/+492404901*=NVS:CIT_BASIC.*/*
```

In some cases only a specific number of subscribers may have to be furnished with such a rule since these subscribers are connected to another PBX. One solution is the introduction of a new user data field (e.g. USED_PBX), which needs to be filled in for these special subscribers so that the modified routing rule can take effect:

```
NVS:MWI.*/*=NVS:MWI.*/* [FLAG=NOPREFERRED]
NVS:MWI.*/* [RECD (USED_PBX) =HP4000] =NVS:CIT_BASIC.*/*
```

An MWI job to MWI/123 is modified exactly when a subscriber has the settings

```
MWI: 123
USED_PBX: HP4000
```

16.11 Problems with MWI via ISDN

Some HiPath PBXs issue error reports when the MWI signal is switched off. This occurs with MWI via ISDN. In such cases [IgnoreMwiOffResponse \[REG_DWORD\]](#) should be set to 1.

16.12 Problem with MWI LED

The MWI LED may signal unread messages, though none are available. This can be caused by an undefined state with some PBXs after a reboot. Therefore, when you log in via PhoneMail, VMS or the Web Assistant, a check is performed as to whether new messages have actually come in. If no new messages are available, the MWI LED is switched off and a defined state achieved in this way.

17 CTI APL

This chapter provides information on the following topics:

- [What is CTI?](#)
- [The CTI APL](#)
- [Technological Concepts for the CTI APL](#)
- [Example of a CTI Link Setup \(CSTA\)](#)
- [Connection to a HiPath 4000](#)
- [Redundant Connection to OpenScape Voice with geographic Node Separation](#)
- [Configuration Reference](#)
- [Optimizing the CTI APL Starting Behavior](#)
- [PBXs in the CTI Environment](#)
- [Tips and Tricks](#)
- [Standards supported in the CTI APL](#)

17.1 What is CTI?

The term CTI (Computer Telephony Integration) summarizes all functions that realize a logical link between data and telephone services. In the most simple case this can be, for example, starting a defined PC application when a call arrives at the telephone terminal device of the same workstation. This scenario can be extended at will by linking an incoming call to more complex, computer-based processes. Such processes can include, for example, the display of caller-specific information on the computer screen.

The other way round, from computer to telephone, is possible as well. A good example is the setup of a communication connection to a telephone user from a computer application. The simplest form of such an application is a so-called dialer.

17.2 The CTI APL

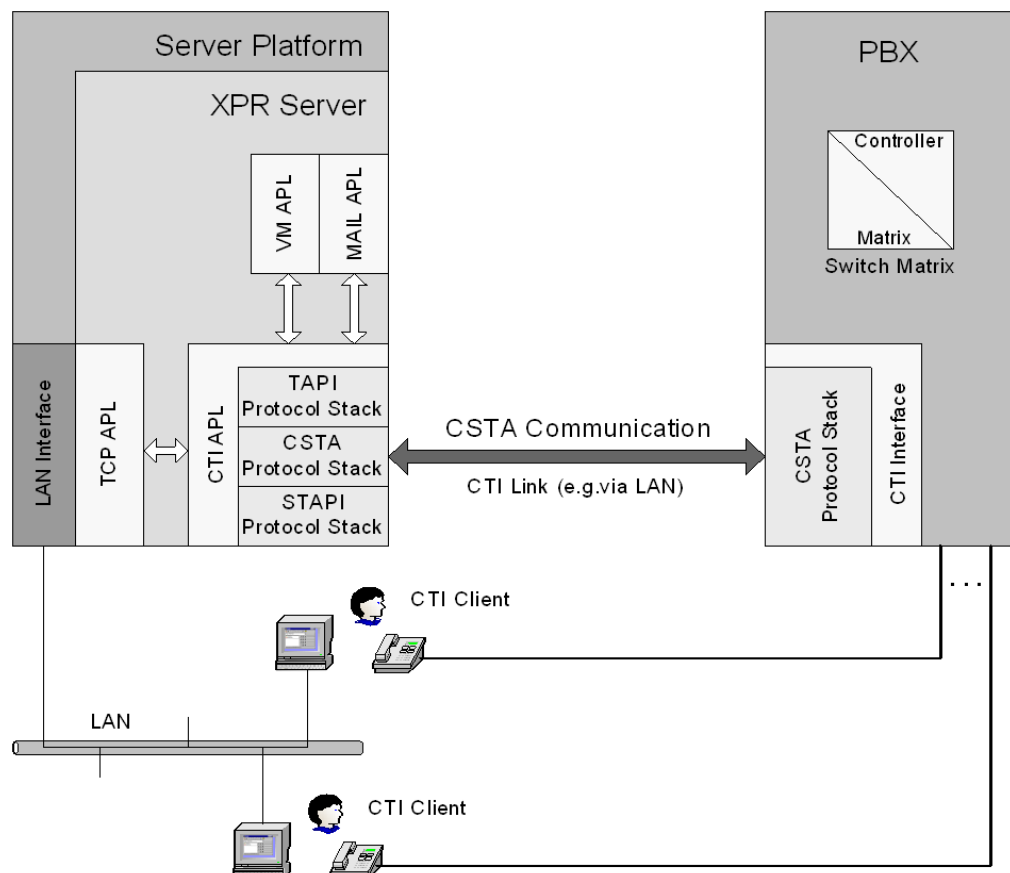
CTI functions are realized via so-called CTI interfaces that are configured between the components of the telecommunication and data systems technology.

Via respective CTI commands they enable:

- control of telephone devices and connections,
- monitoring of telephone devices and connections,
- representing the collected information on telephone devices and connections at a PC workstation.

CTI interfaces have been mostly standardized by now. Thus, they enable the control of communication systems of different manufacturers. The respective realization standards of the standardization boards are not binding anyhow. Therefore, the feature range of each CTI interface depends on its individual manufacturer's implementation.

Let's have a look at the principle structure of a CTI solution with the XPR server. The connection to the PBX is in this case realized via the CTI protocol CSTA.



In an XPR environment the CTI APL communicates with corresponding CTI clients. It accepts CTI controlling information. This information defines the way telephone devices and communication connections of attached PBX systems are monitored and controlled.

The CTI clients in the XPR server environment include for instance:

- optiClient
- Dialer in Communications and Outlook
- Mail APL for the implementation of a CTI journal
- VM APL for contact center environments

The respective PBX systems are connected via so-called CTI links, which can be realized on the basis of different CTI interfaces – e.g. CSTA. Via these, control information is transmitted from the XPR server to the PBX and monitoring information from the PBX to the XPR server. The latter will then be transmitted to the CTI clients to be displayed.

For a better understanding of the applied mechanisms in a CTI environment the next section explains various technological concepts in detail.

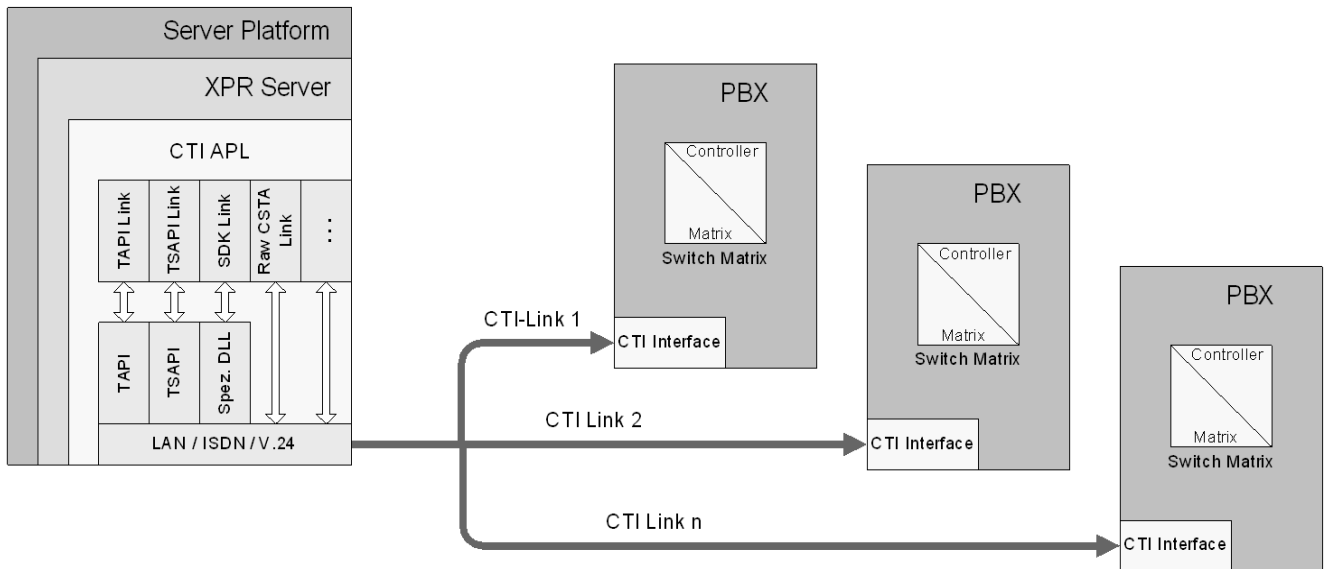
17.3 Technological Concepts for the CTI APL

This chapter provides information on the following topics:

- [CTI Protocol Interfaces](#)
- [CTI Transport Interfaces](#)
- [CTI Transactions](#)
- [CTI Features](#)
- [Device Profiles](#)
- [Multi PBX “AutoLearn” Mode](#)
- [Access Privileges](#)

17.3.1 CTI Protocol Interfaces

The following figure gives an overview of the CTI interfaces implemented in the XPR server.



Various interface protocols are available for CTI connections. The most important ones are:

- CSTA (Computer Supported Telecommunication Applications)
- TSAPI (Telephony Services Application Programming Interface)
- TAPI (Telephony Application Programming Interface)

Let's have a closer look at these interfaces in the following section.

17.3.1.1 CSTA

The CSTA protocol is the most common CTI protocol interface at the moment. CSTA was developed by ECMA (European Computer Manufacturers Association) as standard for coupling computers and PBXs and determines structure and type of messages.

For the time being CSTA (Computer Supported Telecommunication Applications) exists in three different phases, which are not downwardly compatible, though. They are described in the following standards:

- CSTA Phase I (ECMA 179/180)
- CSTA Phase II (ECMA 217/218)
- CSTA Phase III (ECMA 269/285)

17.3.1.2 TSAPI

IMPORTANT:

If several PBXs are to be connected via TSAPI, a multilink-compatible TSAPI driver must be used.

TSAPI (Telephony Services Application Programming Interface) was developed by Novell and AT&T and is based on CSTA (Phase I). TSAPI also defines commands and parameters via which PBX and telephone device features can be controlled.

17.3.1.3 TAPI

IMPORTANT:

If several PBXs are to be connected via TAPI, a multilink-compatible TAPI driver must be used.

TAPI (Telephony Application Programming Interface) implements a programmable, network-independent CTI interface under Windows operating systems.

The following TAPI interfaces are currently used:

- **TAPI 3.1**
Is based on the H.323 Telephony Service Provider (TSP) shipped with Microsoft Windows XP. With TAPI 3.1 the TSP also supports the Supplementary Telephony Services described in the H.450 standard. Supplementary Telephony Services define additional services to the Basic Telephony Services, e.g. holding, parking, alternating and conferencing.
- **TAPI 3.0**
Is either based on H.323 TSP shipped with Microsoft Windows 2000 (e.g. for Innovaphone IP 400), or the producer delivers a corresponding TSP for their system.
- **TAPI 2.1 with wave interface**
Here as well the manufacturer needs to supply a corresponding TSP. Compared to versions 3.0/3.1, TAPI 2.1 is not based on H.323.

Depending on the TAPI version used, possible features may be restricted. Version 2.1 for example does not support Fax-Over-IP (FoIP-T.38).

TAPI interface usage, as described above, occurs with an additional software module - the TAPI Service Provider (TSP). The TSP is the connecting link between the hardware-independent TAPI interface and the hardware of the communication network and represents thus a driver for the transport technology used. Queries posed by the TAPI to the TSP are converted by the TSP into operations to control the connected hardware.

In this function this module defines the scope of performance supported via the TAPI interface. Beyond that, communication- and hardware-specific details remain hidden from the application itself with this concept.

To support manufacturer-specific features with PBXs, PBX manufacturers often deliver individually adapted TAPI service providers along with their PBXs. The TSP supplied along with Windows, implementing the above H.323 standard, can be used as an alternative.

17.3.2 CTI Transport Interfaces

Mainly LAN (TCP/IP) or ISDN media is used as transport interfaces for the CTI protocols. Older protocols use e.g. serial interfaces (V.24) in addition.

17.3.3 CTI Transactions

We know now that the CTI communication is enabled via CTI protocols such as CSTA on the basis of CTI commands that are defined in the respective protocol standards. The XPR server uses a similar approach for the CTI communication with its CTI clients – the so-called CTI transactions.

CTI transactions are system messages that are transmitted in a very short time. They contain control commands or monitoring information, depending on the data that is transmitted. They either refer to a call or a telephone device. Accordingly, a transaction either receives a referencing Call ID or Device ID.

The Call ID is a connection reference automatically created by the CTI entities of the XPR server, if an incoming or outgoing communication connection is recognized. In the case of the Device ID this is the telephone number of the corresponding telephone device.

Different CTI transactions can either be referenced via a Call ID or a Device ID. The implementation determines which of these two options is used. A pure device ID implementation becomes a problem if telephone devices in the CTI environment support more than one call at a time. In this case connection-specific transactions can no longer be uniquely referenced via the device ID.

The following table gives an overview of the CTI transactions of the XPR server available at the moment. It lists the available transactions, their usage and possible reference type (C=Call ID, D=Device ID).

Transaction	Use	Reference
ALTERNATE	Alternating between	C D
ANSWERCALL	Accept incoming call	C D
CALLDATA*	Transmit data with call (Call-Attach-Data)	C
CALLSTATE	Request the current call state	C
CONFERENCE NEXT	Set up a conference connection ("blind")	C D
CONFERENCE HOLD	Set up a conference connection ("controlled")	C
CONSULTATION TO	Consultation	C D
DEFLECT TO	Call diversion for specific callers	C D
DISCONNECT	Hanging up	C D
DISPLAY	Display on the telephone display	D
DISTURB	"Do not disturb" on	D
DISTURB OFF	"Do not disturb" off	D
DISTURB SHOW	Request "Do not disturb" state	D
DIVERSION TO	Call diversion of a telephone device on	D
DIVERSION OFF	Call diversion of a telephone device off	D
DIVERSION SHOW	Request call diversion of a telephone device	D
FORWARD TO	Blind transfer of a call to another device.	C D
FORWARD HOLD	Call forward with previous consultation call	C
HOLD	Hold a call	C D
HOLD OFF	Retrieve "parked" call	C D
MONITOR	Set monitor point for a telephone device	D
MONITOR OFF	Delete monitor point for a telephone device	D
MONITOR SHOW	Request monitor point for a telephone device	D
PHONESTATE	One-time request of telephone device state	D
PICKUP	Active call acceptance by a third party	C D

Table 55 *CTI Transactions of the XPR Server*

* Is currently not used under TSAPI by the XPR server.

17.3.4 CTI Features

CTI provides different features for controlling and monitoring PBX systems and telephone devices. The most important ones are:

- Control of telephone devices (accept call, show display information etc.)
- Control of telecommunication connections (initiating connection setup, conferences, “park calls”, “alternate” etc.)
- Monitoring telephone devices by setting monitor points within the PBX

To enable these features some additional technological concepts are required in addition to the already described CTI transactions. Let's have a closer look at them in this section.

17.3.4.1 Set Monitor Points

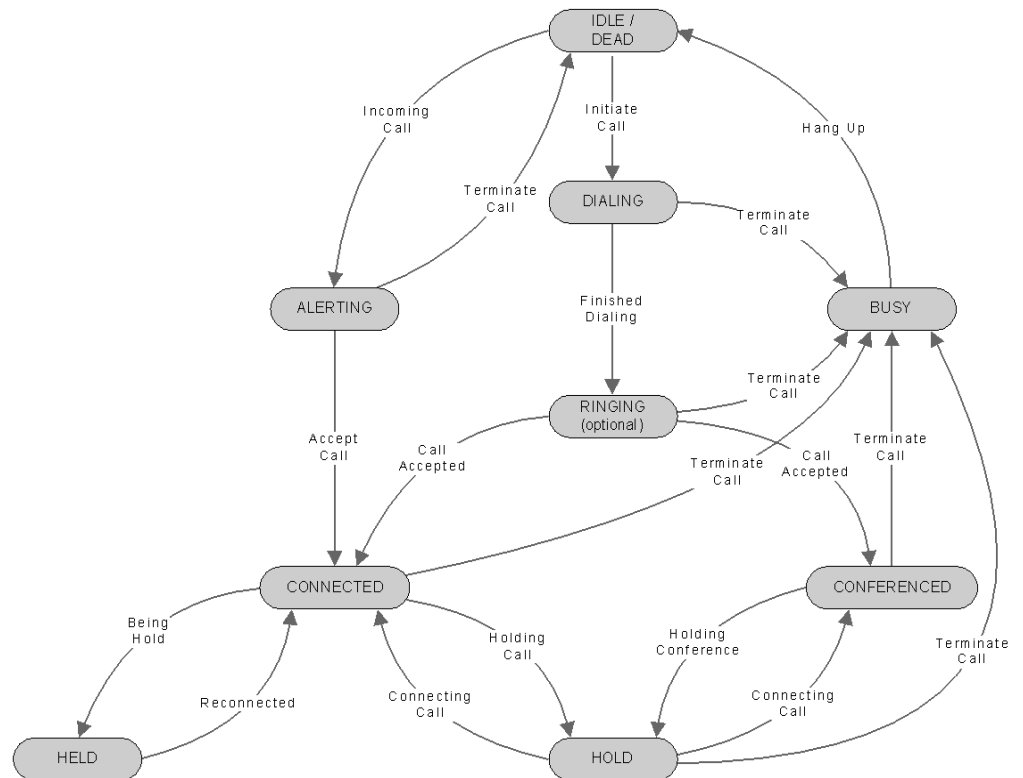
In each CTI environment it is important to be able to control and monitor the state of the corresponding telephone device from the PC workstation. Main issue of this functionality is the CTI interface.

To be able to display the current state of the corresponding telephone device in the CTI client of a PC workstation, the CTI server - in our case the XPR server – must be informed about this state. This original information can only be provided by the PBX the corresponding telephone is connected to.

This CTI communication can be optimized, meaning that not for all telephone terminal devices connected to the PBX the corresponding status is transmitted all the time. To achieve this differentiation, the XPR server defines so-called monitor points in the PBX. By way of defining such a monitor point the XPR server advises the active PBX that it wants to be continuously informed about the status of the corresponding telephone terminal device. One monitor point must be defined in the PBX for each telephone terminal device to be monitored.

17.3.4.2 XPR Connection Model

Concerning the control functions of communication connections or telephone devices we will have a look at the XPR call model first. Since this model does not represent potential restrictions of telephone devices, not all illustrated states and actions are possible with each device. However, the following figure gives an overview of the possible life time of a communication connection.



The figure shows the different states a communication connection of the XPR server can have, as well as the actions that cause status changes. The illustrated states are transmitted in the XPR server via the CTI transaction **MONITORSTATUS**. Thus e.g. the state of any telephone device can be transmitted to a CTI client at all times. The transaction **MONITORSTATUS** is e.g. sent to the clients having set a monitor point on a telephone device that is to be monitored for each change.

The following states are defined for the XPR server:

Status	Description
IDLE/DEAD	Waiting
ALERTING	Ringling (at the called party)
DIALING	Dialing
RINGING	Ringling (at the calling party)
CONNECTED	Connected
HELD	On hold
HOLD	Hold
CONFERENCED	Conference
BUSY	Busy

Table 56 Status of the XPR Connection Model

After we have now regarded the possible connection states of the XPR server, the question arises how these correlate with the CTI transactions described before.

Therefore we consider the actions that are also represented in the call model. They describe the events that causes passing from one connection state to another. Moreover, it indirectly describes which state changes are not possible at all (these states are not linked in the call model by an action). These actions are closely related to the CTI transactions that are finally nothing but instructions to the XPR server to execute certain actions.

Let's have a look at three examples for the assignment of actions and transactions:

Status Alteration	Action	Transaction
Connected > Hold	Holding Call	HOLD
Hold > Connected	Connecting Call	HOLD OFF
Ringling > Connect	Call Accepted	ANSWERCALL

Table 57 Examples of Assignments of Actions and Transactions

17.3.5 Device Profiles

We have read a lot about controlling and monitoring at telephone devices in the previous sections. Manufacturers of PBX systems often offer a variety of telephone devices for their communication system that normally differ significantly concerning features they support. This fact has of course a great influence on the support of the CTI features discussed above. How, for instance, is a display message to be shown at a telephone device if this device does not provide a display at all?

Furthermore, perhaps it is not desired that all subscribers in a PBX are to use all technically possible features via CTI.

To accommodate such individual circumstances in an XPR CTI environment it is possible to configure individual device profiles. These can then be assigned to the diverse telephone devices of the corresponding PBX systems.

NOTE:

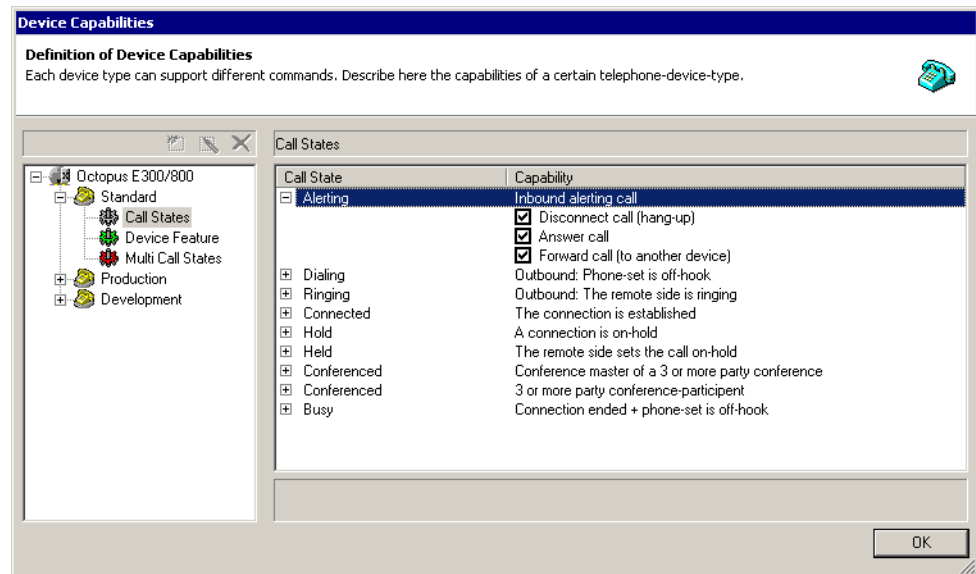
The CTI APL device profiles are currently evaluated and supported by the CTI client optiClient only.

In a device profile settings in the three sections Call State, Feature and Multi Call States can be made.

NOTE:

The release of a feature only makes sense if the respective telephone device and the PBX support this feature.

The XPR server contains already default profiles that specify exactly such features that are supported by the associated PBXs as things are now. These profiles cannot be edited.



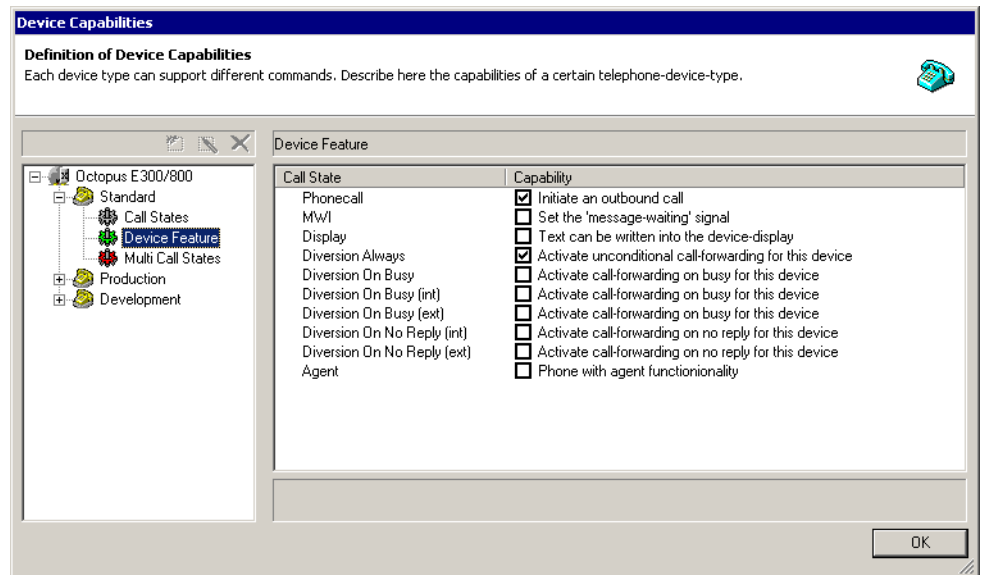
These settings allow the release of CTI-controlled actions that can be executed during an existing call state.

Example:

If an incoming call is signaled at a telephone device with the default profile illustrated above (Alerting), the subscriber is able to

- reject the incoming call (disconnect connection),
- accept the incoming call or
- divert the incoming call to another device.

Feature

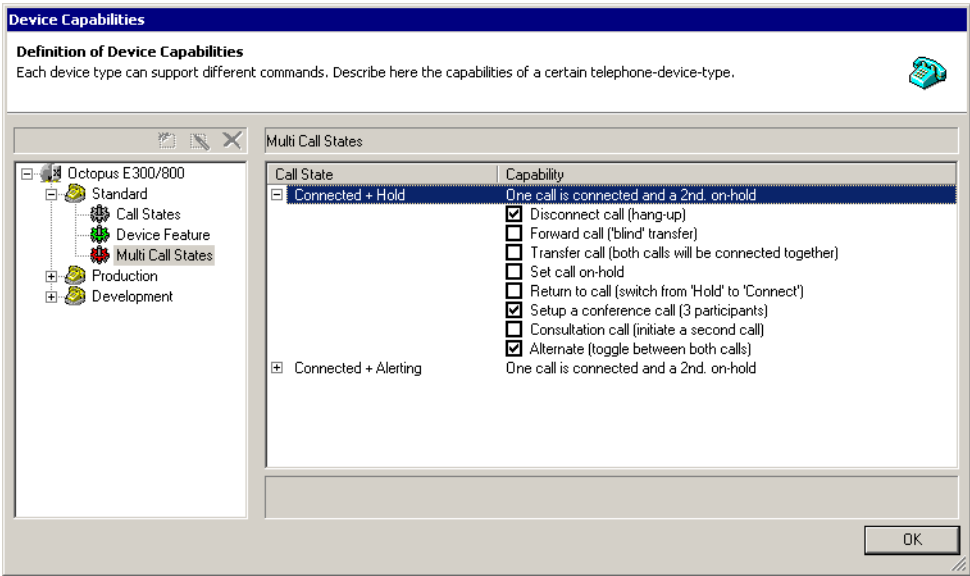


Configuring features enables the release of CTI-controlled actions that can be executed at a telephone device.

Example:

It is possible to signalize an outgoing call via CTI to a telephone with the features defined above. On the contrary, it is not possible to set the MWI signal via CTI.

Multi Call States

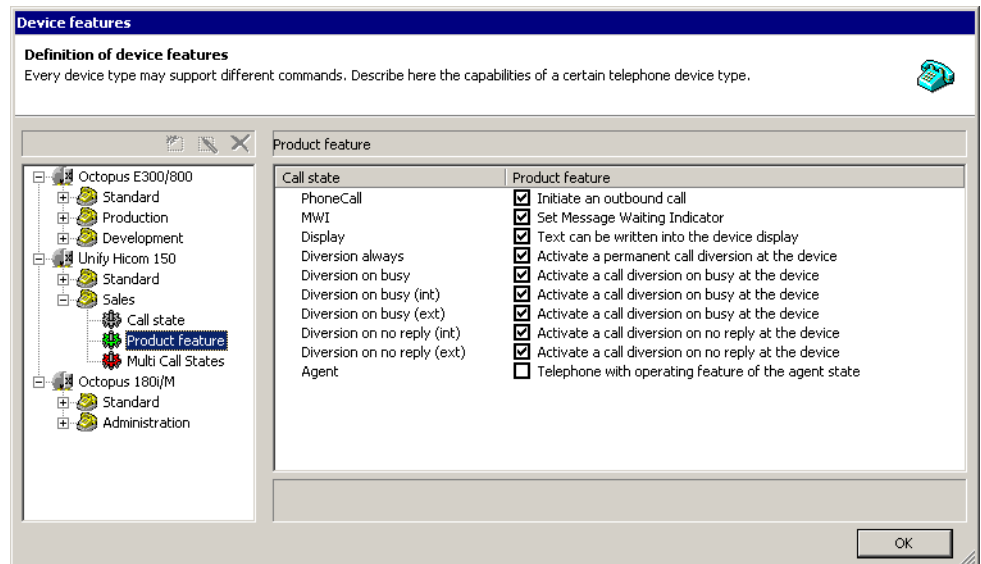


Multi Call States describe the actions that can be executed at a PBX with several calls that exist at the same time.

Example:

A user at a telephone device with the default profile illustrated above is connected to a subscriber who is, however, in the hold state (*Connected + Hold*). In this state it is possible at this telephone to close this connection or initiate a conference via CTI. With this profile it is not possible in this state to initiate “blind” forward via CTI.

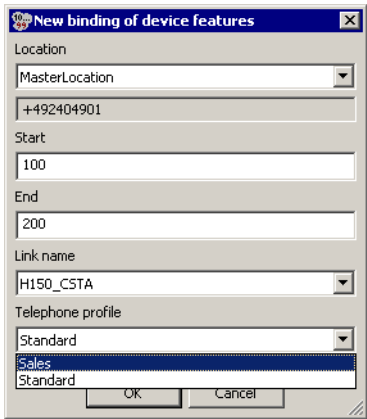
Let's have a look at the device profiles and their assignment to telephone devices in a more complex sample environment.



We have a CTI environment with three PBX systems. The Octopus E300/800 supplies the production and development areas of our sample company. In addition, the Hicom 150 supplies the sales personnel, and the Octopus 180i/M mainly the management. Accordingly, the system administrator has created corresponding device profiles to the respective PBX systems. As an example we have a look at the features of the device profile *Sales*. This profile is to be assigned to all telephone devices of the sales personnel.

If we have a look at the features that are to be controllable via CTI, we can see that important sales features are activated for these devices. These include, for instance, the various call diversions and the possibility to initiate external calls.

The device profiles created like this can subsequently be assigned to the desired telephone devices of the respective PBX systems in the CTI APL. Let's have a look at the assignment of the device profile *Sales*:

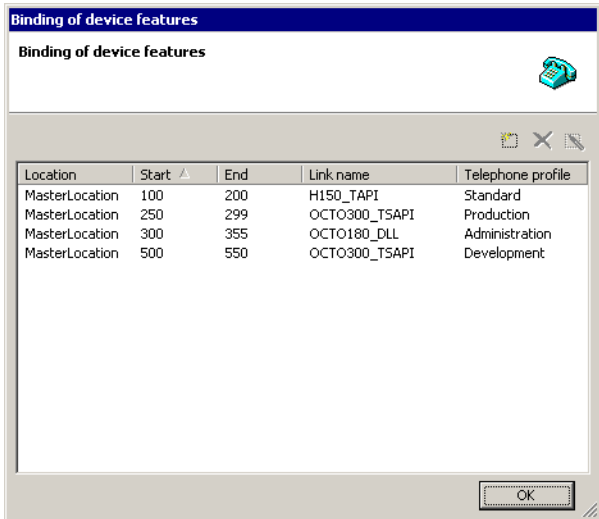


We see the profile assignment for the extensions 100 to 200 of the site with the extension 490240490183. The Hicom 150 PBX with CTI channel *H150_CSTA* has been selected, under which the telephone profiles display among other things *Sales* for selection.

NOTE:

Please notice that a previously configured profile is only displayed for selection, if the corresponding **Link name** has been selected previously.

After the telephone profiles *Sales*, *Production*, *Administration* and *Development* have been assigned, the following structure might e.g. unfold:



17.3.6 Multi PBX “AutoLearn” Mode

The Multi PBX “AutoLearn” mode realizes a learning algorithm, with the help of which the XPR server determines at which CTI link a defined telephone device can be reached. The information found is then stored and from now on available for setting monitor points or for the setup of communication relations via CTI.

The “learning” of the Multi PBX “AutoLearn” algorithm is based on setting temporary monitor points. These will be deleted in the respective PBX after a searched telephone device has been found.

Multi PBX “AutoLearn” allows thus to connect several PBX systems to one XPR server. Furthermore, the network-wide unique extensions can be distributed arbitrarily to the connected PBX systems with regard to CTI functionality. The XPR server behaves as in an environment with only one PBX for the existing CTI clients.

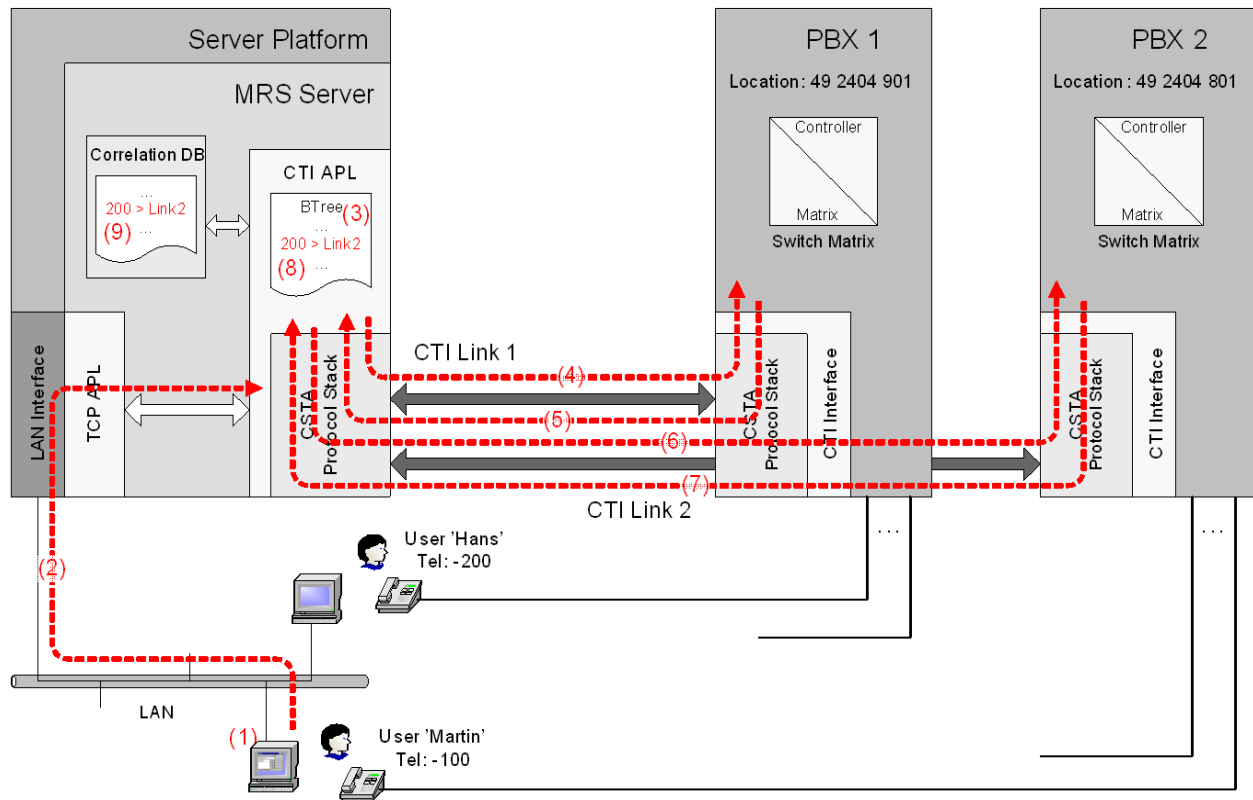
IMPORTANT:

If several PBXs are to be connected via TAPI, TSAPI or via a special SDK, the corresponding multilink-compatible drivers must be used.

Let's have a look at this algorithm's functionality with the help of a simple example. We select the establishment of a communication relation between two parties. Setting a new monitor point is performed similarly.

Functionality of the Multi PBX “AutoLearn” algorithm

On the basis of the following figure we will learn about the Multi PBX “AutoLearn” algorithm of the XPR server in a simple CTI environment. This example is limited to the steps important for us. We will not consider the CTI transactions actually exchanged between the systems in detail.



We presume that the represented environment has just been installed and no CTI communication has taken place as yet. Thus, the “AutoLearn” entries in the Correlation Database as well as in the BTree of the CTI APL are empty. The CTI links between the XPR server and the PBX systems take place via the CSTA protocol in our example. The functionality of other CTI links, also mixed ones, is the same.

We assume that user Martin starts a dialer application at his computer workstation to establish a telephone connection to user Hans whose device is connected to the PBX of another site.

Let's see what happens.

1. Martin has the extension **100**, dials the extension of user Hans with the help of the GUI of his started dialer and starts the connection setup.
2. The request is sent via LAN to the CTI APL of the XPR server.

3. The CTI APL's task is now to send the desired connection request to the PBX Martin's telephone device is connected to. Therefore it checks whether already an entry with the phone number **100** exists in the APL-specific BTree. Such an entry would define the CTI-link to the PBX searched for (see 8). However, this entry does not exist, since we regard the first CTI action of the examined server installation.
4. Therefore the CTI APL tries to set a temporary monitor point for the extension **100** via the CTI link 1 in the PBX 1 to identify the correct PBX.

IMPORTANT:

The “learning” of the Multi PBX “AutoLearn” algorithm is based on the setting of monitor points. If all monitor licenses are already in use for a PBX, no telephone device of this PBX can be “learned” by the Multi PBX “AutoLearn” algorithm.

5. The extension **100** is apparently not known to the PBX 1. This is signaled to the CTI APL by an error message for the monitor request.
6. After this first failed attempt the CTI APL tries to set the temporary monitor point for the extension **100** via the CTI link 2 in the PBX 2.
7. The desired extension is known to this PBX. It sets the desired monitor point accordingly and informs the CTI APL about it.
8. The CTI APL stores the information that the subscriber with the phone number **100** respectively **49 2404 801100** can be reached via the CTI link 2 in its internal BTree. The same entry is also mirrored in a corresponding section of the Correlation Database. Since the BTree content is lost during a restart of the CTI APL, the last BTree version can be reestablished from the thus mirrored information.
For the next CTI request by subscriber Martin the BTree entry can directly be accessed. Searching the single CTI links is omitted.

We leave the connection setup that is to follow here and consider some details concerning the Multi PBX ‘AutoLearn’ mode.

Dialing an 'incomplete' phone number

In the default setting the Multi PBX 'AutoLearn' algorithm expects the transmission of a destination phone number in normalized form. In this case only the CTI-links to PBX systems with identical location information are searched for the desired subscriber.

If the Multi PBX 'AutoLearn' algorithm is also to work with extension information only and with no unique addressing of a location, the registry value [*MultiPBXAutoLearnModeWithoutLocation \[REG_DWORD\]*](#) can be set. In this case all existing CTI links are searched for the desired extension.

Cf. [Section E.5.1](#), "[MultiPBXAutoLearnModeWithoutLocation \[REG_DWORD\]](#)", on page 1724.

Dialing a non-existing phone number

If a CTI request is started by a non-existing subscriber, the Multi PBX 'AutoLearn' algorithm searches all respective CTI links one after another. As the phone number cannot be successfully assigned to the CTI link, the CTI APL sends a message that the respective subscriber cannot be reached.

A corresponding connection request or the setting of a static monitor point would fail in this case.

Modifications in the known BTree assignment

If an already "learned" extension moves from one location to another, the respective entry in the BTree or in the Correlation Database is maintained at first. During the next CTI request from this phone number, access on the basis of this existing entry fails. Then the Multi PBX 'AutoLearn' starts the original search algorithm for unknown subscribers again. The outdated entry in the BTree and in the Correlation Database is then updated.

Extension distribution in a CTI environment

The extensions in a CTI environment can be distributed arbitrarily on the PBX systems connected with the XPR server. However, they must be network-wide unique for all devices that are administered by the XPR server via CTI features.

Supported PBX systems in a CTI environment

Multi PBX 'AutoLearn' supports all PBX systems as far as they provide a CTI interface that is compatible with the CTI APL of the XPR server. Detailed information can be found in the Hardware Compatibility List (HCL) of the XPR server.

Applied CTI interfaces in a CTI environment

All combinations of CTI interfaces provided by the XPR server are supported.

IMPORTANT:

If several PBXs are to be connected via TAPI, TSAPI or via a special SDK, the corresponding multilink-compatible drivers must be used.

CTI environment with several locations

Multi PBX 'AutoLearn' can also administer PBX systems of different locations (different country code, area code, access number) and/or with differing dialing parameters (e.g. external line prefix).

Extra administration effort

No extra administration effort is necessary for Multi PBX 'AutoLearn'. Each PBX is connected to the XPR server via a CTI link with the desired CTI protocol. The individual parameters of the respective PBX are assigned to it.

17.3.7 Access Privileges

The CTI APL uses access privileges that control the users' permission to monitor telephones. Such access privileges are configured in the XPR client Communications.

The access privileges are divided in two areas:

- **Default privileges**
These are valid for telephones for which no further privileges have been specified under the individual privileges.
- **Individual privileges**
These are valid for individually defines telephones only.

17.3.7.1 Default Privileges

The default privileges are administered in the Default privileges folder of the XPR client Communications. Default privileges can be based on:

- Individual users entitled to monitor a terminal device
- Individual user groups entitled to monitor a terminal device
- Pseudo users (\$OWNER)
- Pseudo user groups (\$GROUP : <group name>).

\$OWNER and \$GROUP are used as follows:

- `$OWNER`
If this entry exists in the default privileges, every user may monitor their individual primary telephone.
- `$GROUP : <name>`
The `$GROUP` entry can be compared with a call transfer group in PBXs. It defines which users may monitor each others telephones. The description *Name* can be freely selected and serves solely to administer the `$GROUP` entry in the correlation database.
At least one sub-entry must be added under a `$GROUP` entry. Such a sub-entry must either correspond to the name of a user group or consist of the first letters of a user group name or different user group names.

Example:

There are the user groups: BG10, BG11, BG2, BG3.

Under the default privileges exists the entry: `$GROUP : ACL`.

To this entry are assigned: BG1 , BG3.

With these settings the users of the BG10 user group may monitor each others telephones. Also the users of the user group BG11 may monitor each others telephones. The same applies for the users of user group BG3.

Please note: telephones may not be monitored from one group to another. Thus not among the users of user group BG10 and BG11.

17.3.7.2 Individual Privileges

Individual privileges may be based on:

- Individual users entitled to monitor a terminal device
- Individual user groups entitled to monitor a terminal device

If individual privileges are defined for a telephone, the default privileges are no longer valid for this device.

Manual *Communications* explains how to configure access privileges.

17.4 Example of a CTI Link Setup (CSTA)

NOTE:

For the CTI APL configuration the NCO configuration files of the XPR server are accessed via the NCOAdmin. Please make sure that the NCOAdmin used and the NCO configuration files are of the same version.

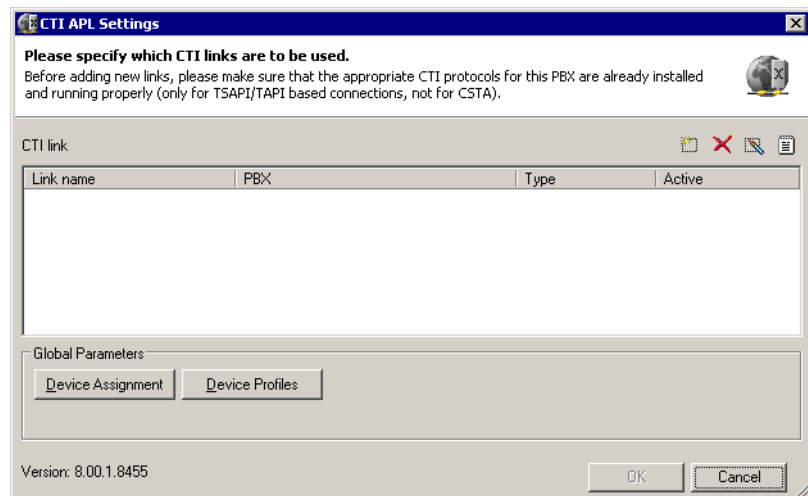
If this is not the case, an alarm message at the beginning of the CTI configuration indicates this incompatibility.

In this section the basic setup for the CTI protocol CSTA is described. We merely contemplate here the configuration of the XPR server.

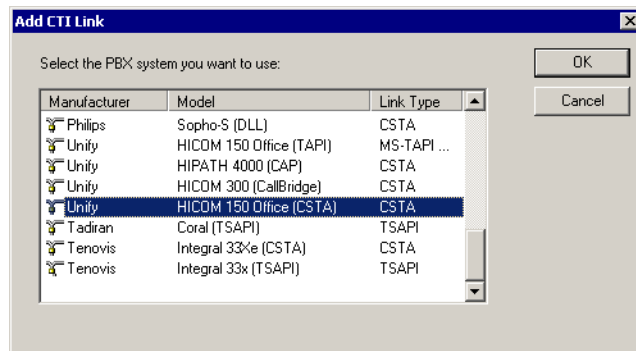
You can obtain installation instructions for the applied PBX and other required components, which may have to be additionally installed on the XPR server system, from the respective documentations of the PBX manufacturer.

How to set up a CSTA-CTI connection in the XPR server:

1. Start the XPR server and the XPR monitor.
2. In the *Components* window of the XPR monitor select **CtiApl > Set Options**.
3. Select the **Add** button in the tool bar of the configuration dialog *CTI APL Settings* to add a new CTI link.



4. Select the desired entry from the displayed list of supported PBX systems. For our example we use the PBX **Hicom 150 Office (CSTA)**.

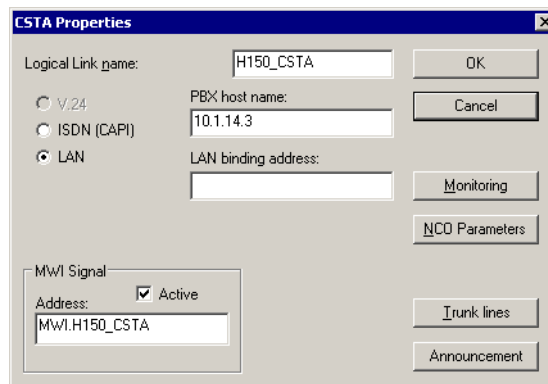


5. Save your settings by clicking on the **OK** button.
6. We adopt the name suggested in the **Logical Link name** field.

IMPORTANT:

The connection name that was defined here must be **unique**. The XPR server composes the associated logical line from it.

This address has then the format `NVS:CTI.<logical link name>`.



7. Enter the IP address in the **PBX Hostname** field under which the LAN interface of the applied PBX can be reached.

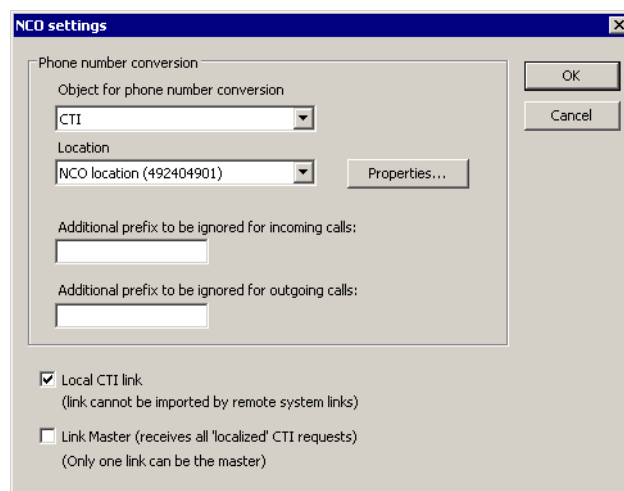
IMPORTANT:

The PBX and the XPR server should be in the same LAN segment. If this is not the case, correct routing between the respective systems must be provided.

NOTE:

If a service to resolve host names is available in the TCP/IP network used, also the PBX host name can be entered here.

8. Select the **NCO Parameters** button.
9. Make sure that **CTI** has been selected as **Object for phone number conversion**. Thus the CTI default rules and the location for phone number conversion that has been configured in CTI NCO are activated for this PBX.

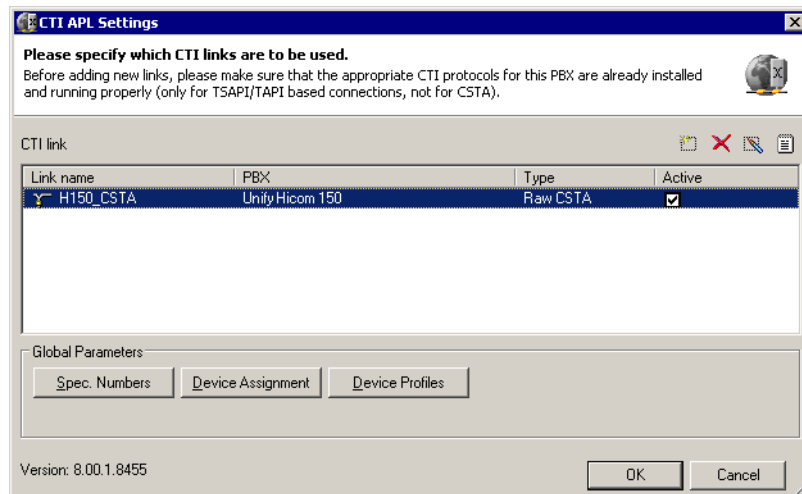


NOTE:

It is also possible to use other location information for phone number conversion for the respective PBX than those configured in CTI-NCO. Therefore select the respective location with the desired information under **Location**.

The location of the selected object for phone number conversion is always set under **Location** by default.

10. Close the *NCO settings* dialog with the **OK** button.
11. Then also close the *CSTA Properties* dialog with the **OK** button.
12. Make sure that the newly configured CTI link in the **Active** column is activated.



13. Then also close the *CTI APL Settings* dialog with the **OK** button.
14. If also on the PBX side all required settings have been made, the logical line `NVS:CTI.<logical link name>` and maybe also `NVS:MWI.<logical link name>` in the Logical Lines window of the XPR server will change to status **ready**.

Congratulations. You have now configured a new CTI link under the CSTA protocol.

17.5 Connection to a HiPath 4000

NOTE:

For the CTI APL configuration the NCO configuration files of the XPR server are accessed via the NCOAdmin. Please make sure that the NCOAdmin used and the NCO configuration files are of the same version.

If this is not the case, an alarm message at the beginning of the CTI configuration indicates this incompatibility.

In this section we describe the configuration of a CTI connection between the HiPath 4000 and the XPR server. We merely contemplate here the configuration of the XPR server and the CA4000 connector. For configuration instructions as regards the PBX used please refer to the corresponding PBX documentation.

The CTI connection configuration is divided into the following sections:

- [Installing the CA4000 Connector](#)
- [Configuring the CA4000 Connector](#)
- [CTI APL Configuration](#)
- [HiPath 4000 with E.164 Number Format](#)

17.5.1 Installing the CA4000 Connector

NOTE:

The *Connectivity Adapter* of the CAP V3 is required for HiPath 4000 as of V5. From this release the *Connectivity Adapter* is also called *CAP Inside*.

Before you can configure the XPR server CTI APL, you need to install and configure the CA4000 connector on the XPR server. How to set up the CA4000 connector:

1. Start the `setup.exe` setup file of the CA4000 connector. You find the file on the XPR product data carrier for HiPath 4000 V4 and for HiPath 4000 V5 in the folder `XpressionsInstall\Drivers\Connector-CA4000\HiPath 4000 CSTA`.

IMPORTANT:

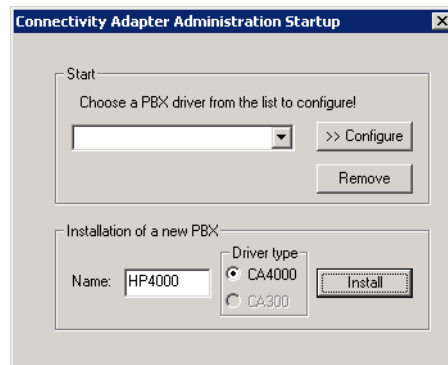
The CA4000 connector may terminate with the error message *1607: Unable to install InstallShield Scripting Runtime*, if you invoke the setup file via network. In this case, copy the `Connector-CA4000` directory to the XPR server and perform the `setup.exe` setup file from there anew.

2. Install the CA4000 connector by following the setup wizard instructions.

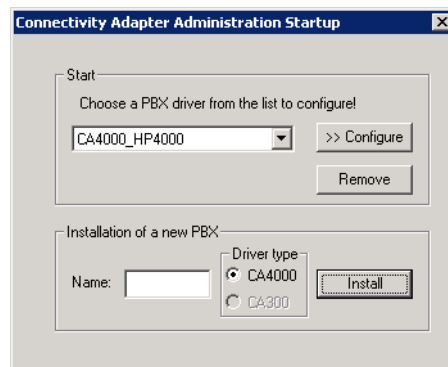
17.5.2 Configuring the CA4000 Connector

After you have installed the CA4000 connector, you need to configure it for the connection to the HiPath 4000 in the CA4000 administrator. Proceed as follows:

1. On the XPR server start the CA4000 administrator via **Start > All Programs > HiPath CTI > CAP > CA Admin.**
2. In the **Name** field specify the name for the new PBX connection – for our example *HP4000*.

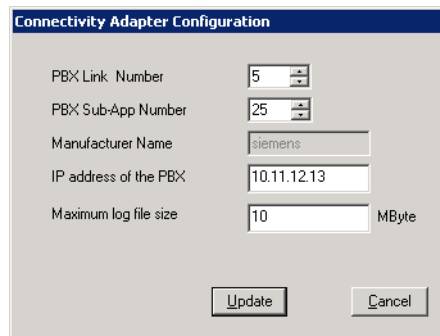


3. Select **Install** to define the new PBX connection. The new PBX connection appears in the PBX drivers field – in our example under the name *CA4000_HP4000*.



4. Select **Configure** to configure the new PBX connection. Subsequently, the CA4000 administrator user interface opens.
5. In the main menu bar select the entry **Configuration > Connectivity Adapter**. The configuration dialog for the new PBX connection opens – in our example for *CA4000_HP4000*.

6. In the **IP address of the PBX** field enter the IP address under which the HiPath 4000 can be reached.



The 'Connectivity Adapter Configuration' dialog box contains the following fields and values:

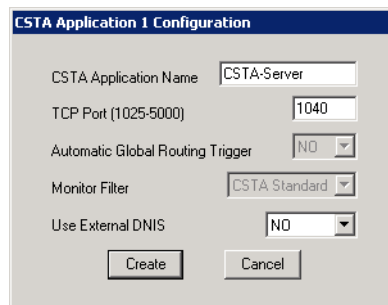
Field	Value
PBX Link Number	5
PBX Sub-App Number	25
Manufacturer Name	siemens
IP address of the PBX	10.11.12.13
Maximum log file size	10 MByte

Buttons: Update, Cancel

7. Select **Update** to copy the new setting.

You have thus configured the connection between the CA4000 connector and the HiPath 4000. Next, we configure the connection between the CA4000 connector and the XPR server. Continue as follows:

8. In the CA4000 administrator main menu bar select the entry **Configuration > ASCE App > New**. The configuration dialog for a new CSTA application opens.



The 'CSTA Application 1 Configuration' dialog box contains the following fields and values:

Field	Value
CSTA Application Name	CSTA-Server
TCP Port (1025-5000)	1040
Automatic Global Routing Trigger	NO
Monitor Filter	CSTA Standard
Use External DNIS	NO

Buttons: Create, Cancel

9. In the **CSTA Application Name** field enter the name for the new application – in our example *CSTA-Server*.

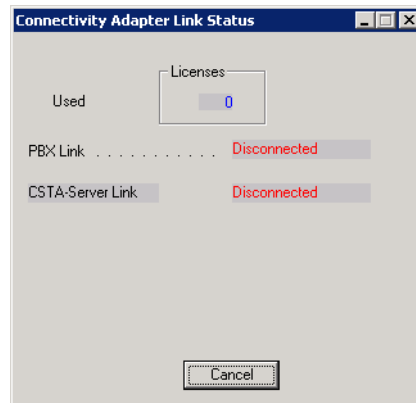
IMPORTANT:

If other connections are already configured via the CA4000 connector in your system environment, you may need to configure another, previously unused port number in the **TCP Port** field.

10. Select **Create** to copy the settings for the new application.
11. On the computer system, restart the **Connectivity Adapter** service. This installs the CA driver required for the new application.

12. A status window now displays whether the connection between CA4000 connector and PBX respectively between CA4000 connector and the XPR server works correctly.

The connection to the PBX (PBX Link) should already operate troublefree at this point. This requires the HiPath 4000 to be correctly configured as well. If no connection can be established between the systems involved, the status display may appear as follows:

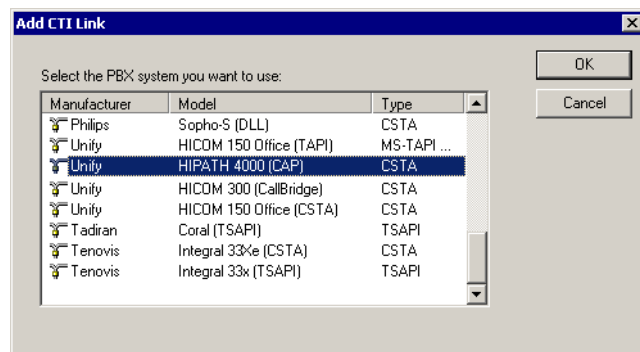


You have thus performed all required CA4000 connector settings.

17.5.3 CTI APL Configuration

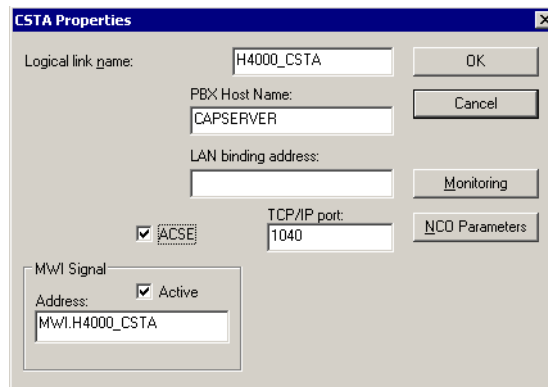
After you have installed and configured the CA4000 connector, you now need to configure the CTI APL. Proceed as follows:

1. Start the XPR server and the XPR monitor.
2. In the *Components* window of the XPR monitor select **CtiApl > Set Options**.
3. Select the **Add** button in the tool bar of the configuration dialog *CTI APL Settings* to add a new CTI link.



4. Insert a new CTI link of the type *HIPATH 4000 (CAP)*.

5. In the **PBX host name** field, enter for this channel the host name of the computer system on which you have previously installed the CA4000 connector.



6. In the **TCP/IP port** field enter the number of the TCP port that you have previously configured in the CA4000 connector for the connection.
7. Activate the **ACSE** option for Hipath 4000 as of V5.
8. Copy the settings with **OK**.

After the CTI APL configuration the status window of the CA4000 connector should display that the connection to the PBX (PBX link) as well as the connection to the CTI APL (CSTA server link) works correctly.

The CTI connection between XPR server and HiPath 4000 is thus operable.

17.5.4 HiPath 4000 with E.164 Number Format

The HiPath 4000 supports the E.164 number format on the CSTA interface as of V6R2. In complex environments this facilitates keeping track and operating. Two steps are required to enable OpenScape Xpressions V7 using this feature:

- First, the feature must be activated in the Hipath 4000.

This requires reconfiguring the CSTA Connectivity Adapter used by XPR. Select this adapter. Move to the Advanced configuration page. Set the line E164_NUMBER_FORMAT to 1. The Connectivity Adapter will be rebooted automatically.

If the line E164_NUMBER_FORMAT is missing, execute an add line, set the value to 1 and save it. The Connectivity Adapter will be rebooted automatically.

- Second, the NCO rules must be adjusted on the XPR server.

The HiPath 4000 always sends and expects the E.164 number with a leading + sign. That is no problem for inbound numbers as NCO can handle this.

Outbound numbers require adjustments to the NCO. The CTI localization rule “use international number type” with the switch “UseTypeInternational=true” results in a normalized number without leading + sign. To add a leading + sign here, the rule must be changed from “\$1” to “+\$1”.

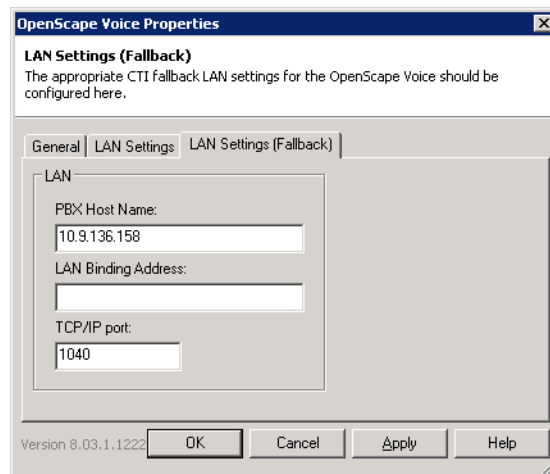
17.6 Redundant Connection to OpenScape Voice with geographic Node Separation

If you connect an OpenScape voice system with geographic node separation via a CSTA link to the XPR server, you can configure the connection redundantly. Besides the usual primary link settings you define a redundant CSTA link in the CTI APL. This redundant CSTA link has the following settings:

- The redundant host name of the OpenScape Voice system or its redundant IP address
- The redundant binding address of the OpenScape Voice system (optional)
- The TCP port for the redundant CSTA link.

The redundant CSTA link becomes active as soon as the OpenScape Voice system cannot be reached under the primary link settings any more. If the OpenScape Voice system cannot be reached under the redundant link settings either, the CTI APL takes turns in the attempt to reach the OpenScape Voice system under the primary and the redundant link settings.

You configure the redundant link settings of the OpenScape Voice system in the CTI link settings for the OpenScape Voice system.



17.7 Configuration Reference

NOTE:

To view and edit the CTI APL settings you need to log on to the XPR monitor with a user account that has the supervisor privilege.

Users with the service privilege may only see the **CTI APL Settings** configuration dialog and cannot perform any settings in there.

NOTE:

For the CTI APL configuration the NCO configuration files of the XPR server are accessed via the NCOAdmin. Please make sure that the NCOAdmin used and the NCO configuration files are of the same version.

If this is not the case, an alarm message at the beginning of the CTI configuration indicates this incompatibility.

NOTE:

The XPR monitor transmits settings made in the CTI APL configuration dialog to the CTI APL only after **all** windows of the configuration dialog have been closed. If individual options or settings are not displayed in current form in the CTI APL configuration dialog, simply close the dialog completely. After opening it again, all current information is available.

In this chapter you receive information about the possible CTI APL setting options:

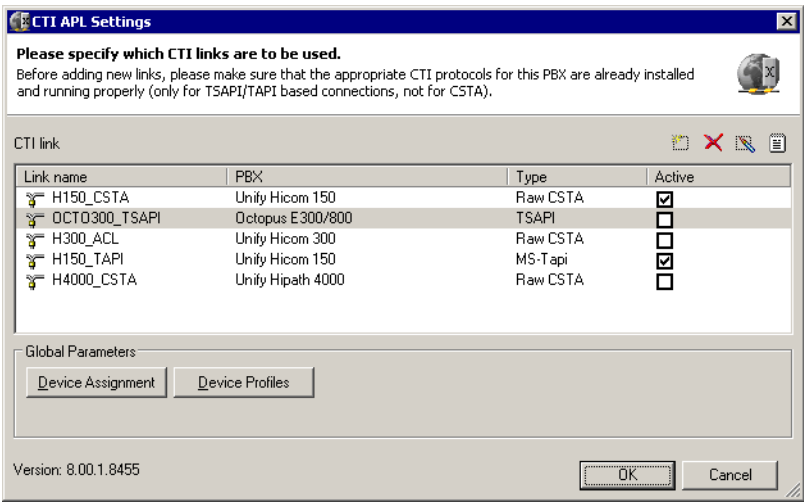
- [CTI APL Settings](#)
- [Logging](#)
- [Assignment of Device Features](#)
- [Terminal Device Features](#)
- [CSTA Settings](#)
- [TSAPI/CSTA Link Properties \(TSAPI\)](#)
- [MS-TAPI Properties \(TAPI\)](#)

All represented dialogs can be reached via the menu item **CtiApl > Set Options** of the *Modules* window in the XPR monitor. The exact path is documented individually for each dialog.

Some settings depend on the type of the applied CTI protocol. In these cases the respective configuration dialogs are listed repeatedly. A supplement in the form *CSTA*, *TSAPI* or *TAPI* in the dialog heading indicates the respective CTI protocol.

17.7.1 CTI APL Settings

The basic dialog of the CTI APL settings lists all configured CTI links of the CTI APL. Via the **Add**, **Remove** and **Edit** icons in the tool bar they can be administered accordingly. The **Logging** icon in the same place leads to the logging settings (cf. [Section 17.7.2, “Logging”, on page 1085](#)).



Moreover, the following features are provided:

Device Assignment

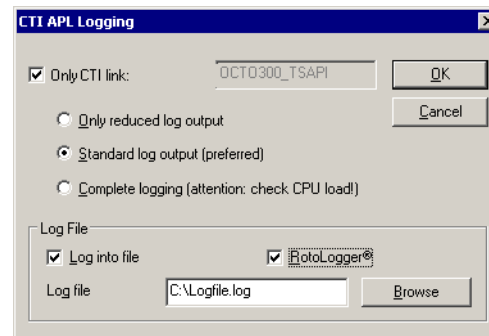
Leads to the assignment of device features (cf. [Section 17.7.3, “Assignment of Device Features”, on page 1087](#)).

Device Profiles

Leads to the configuration of device features (cf. [Section 17.7.4, “Terminal Device Features”, on page 1091](#)).

17.7.2 Logging

The CTI APL supports logging for configured CTI links.



The following features are provided:

Only CTI link

Defines that only the displayed CTI link is logged.

If this option is not activated, logging data for all configured CTI links is collected and stored.

Only reduced log output

Opens a logging monitor with preset parameters for CTI APL logging with reduced logging information.

Standard log output

Opens a logging monitor with preset parameters for CTI APL logging with extended logging information.

Complete logging

Opens a logging monitor with preset parameters for CTI APL logging with complete logging information.

Logging

The CTI APL supports the logging of monitor data in one or several log files. It is possible to choose between simply writing in a log file or using the RotoLogger. The RotoLogger enables writing the CTI logging data to a file system with several files that are filled with logging data according to the round robin system. The default settings of the RotoLogger works with 10 files sized 5120KB each.

Via the options **Log into File** and **RotoLogger** the following logging behaviors can be selected:

Log into File	RotoLogger	Logging behavior
Inactive	–	No logging takes place.
Active	Inactive	Output of logging data in a file which continuously grows.
Active	Active	Output of the logging data in a file system with 10 files of 5120KB content each.

Log file

Defines the log files or the file system where the logging data is stored. For a file system under RotoLogger the labels `Part 1` to `Part 10` are attached to the indicated file name.

Browse

For indicating a file it is possible to select a directory and a logging file via the **Browse** button.

17.7.3 Assignment of Device Features

Can be reached via: **CtiApl > Set Options > Devices-Assignment**

NOTE:

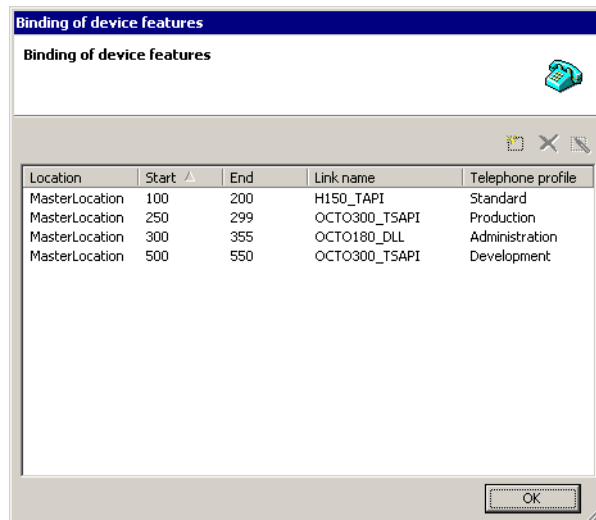
The CTI APL device profiles are currently evaluated and supported by the CTI client optiClient only.

It is possible to assign individual features to selected telephone devices (cf. [Section 17.3.5, "Device Profiles", on page 1059](#)).

This dialog lists all configured assignments of telephone devices and features. Via the **Add**, **Remove** and **Edit** icons in the tool bar they can be administered accordingly.

IMPORTANT:

The devices for which the respective features are to be defined in *one* entry must be within a coherent extension number range.



Moreover, the following features are provided:

Location

Defines which location the telephone devices of the respective device are assigned to.

Start

Via appropriate extension number ranges and the location you define for which telephone devices the features of an entry are valid. **Start** defines the beginning of such an extension number range.

End

Via appropriate extension number ranges and the location you define for which telephone devices the features of an entry are valid. **End** defines the end of such an extension number range.

Link name

The diverse features (phone profiles) are administered in the CTI APL according to the respective PBX or its CTI link. The CTI link belonging to the desired phone profile is specified under **Link name**.

Telephone profile

The diverse features (phone profiles) are administered in the CTI APL according to the respective PBX. Under **Telephone profile** the assigned phone profile is specified.

17.7.3.1 New Device-Feature Assignment

Can be reached via:

CtiApl > Set Options > Devices Assignment > Add/Edit

NOTE:

The CTI APL device profiles are currently evaluated and supported by the CTI client optiClient only.

It is possible to assign individual features to selected telephone devices (cf. [Section 17.3.5, "Device Profiles", on page 1059](#)). In this dialog you can create new device profiles or edit existing ones.

IMPORTANT:

The devices for which the respective features are to be defined in *one* entry must be within a coherent extension number range.

NOTE:

Under **Link name** only those CTI links are displayed that have been assigned to the selected location during the CTI link definition.

Cf. [Section 17.7.5.2, "NCO Settings \(CSTA\)", on page 1099](#).

Under **Telephone profile** only those profiles are displayed that have been assigned to the CTI link selected in the **Link name** field during the profile definition.

Cf. [Section 17.7.4, "Terminal Device Features", on page 1091](#).

The following features are provided:

Location

Defines the location the telephone devices of which are to be assigned a device profile. This entry defines which CTI links are displayed for selection in the **Link name** field.

In addition to the actual site name, its assigned phone number is also displayed.

Start

Via an appropriate extension number range you can define which telephone devices of a location are assigned to the respective device features. **Start** describes the beginning of such an extension number range.

End

Via an appropriate extension number range you can define which telephone devices of a location are assigned to the respective device features. **End** describes the end of such an extension number range.

Link name

Defines the CTI link the devices of which are to be assigned the desired phone profile. The choice of CTI links to be selected depends on the selected location.

Telephone profile

Specifies the phone profile to be assigned to the defined telephone devices. The choice of phone profiles to be selected depends on the selected channel name.

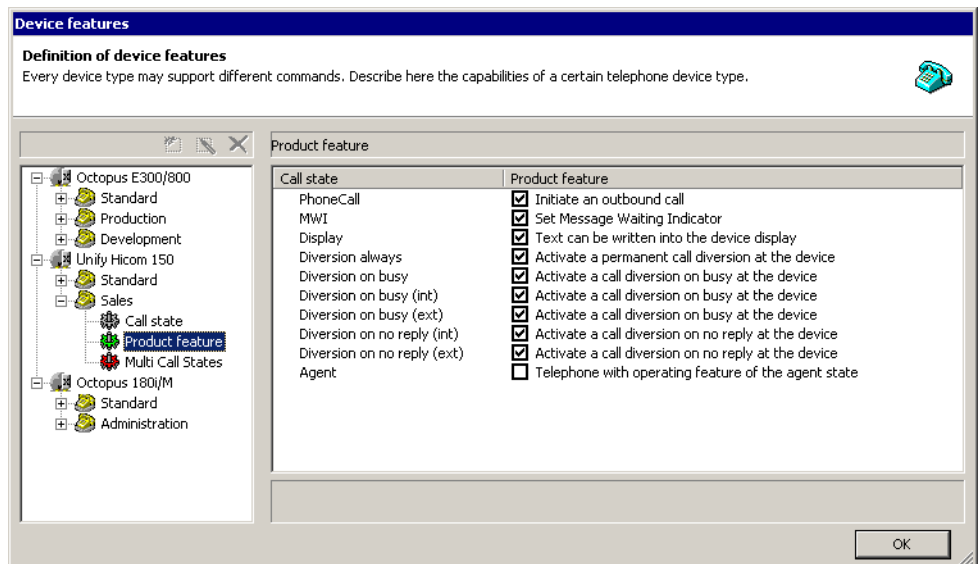
17.7.4 Terminal Device Features

Can be reached via: **CtiApl > Set Options > Device-Profiles**

It is possible to assign individual features to selected telephone devices (cf. [Section 17.3.5, "Device Profiles", on page 1059](#)). This dialog lists all configured device profiles that can be assigned to the telephone devices of the corresponding PBXs (cf. [Section 17.7.3, "Assignment of Device Features", on page 1087](#)). Via the **Add**, **Remove** and **Edit** icons in the tool bar they can be administered accordingly.

NOTE:

Device profiles can only be removed if they are not listed in a device assignment.



Moreover, the following features are provided:

Menu item *Call state*

Displays the call states of a device profile entry on the right hand side of the dialog. Here it is possible to define individual settings for new or already existing device profile entries.

Menu item *Product feature*

Displays the product features of a device profile entry on the right hand side of the dialog. Here it is possible to define individual settings for new or already existing device profile entries.

Menu item *Multi Call States*

Displays the multi call states of a device profile entry on the right hand side of the dialog. Here it is possible to define individual settings for new or already existing device profile entries.

17.7.5 CSTA Settings

Can be reached via: **CtiApl > Set Options > Add/Edit**

This dialog defines the settings the CTI APL requires for the basic CTI communication via the respective CSTA-CTI link.

The following features are provided:

Logical Link name

The logical link name helps the XPR server with the logical addressing of the CTI link. The logical address is composed of `NVS : CTI .` followed by the name defined here.

The example displayed above results in the logical address

`NVS : CTI . H150 _CSTA.`

IMPORTANT:

The connection name defined here must be **unique** because of its reference character.

PBX host name

This field indicates the IP address or the host name of the connected PBX.

NOTE:

If a service to resolve host names is available in the TCP/IP network used, also the PBX host name can be entered here.

V.24 / ISDN (CAPI) / LAN

The options **V.24**, **ISDN (CAPI)** or **LAN** define the transport medium that is to be applied for the CTI communication.

LAN binding address

If the XPR server system is provided with several LAN boards (NIC), the LAN board to be individually used can be specified for each CTI link.

IMPORTANT:

If the **LAN binding address** field is empty in a multi-NIC-environment, the first LAN card transmitted from the WinSocket of the Windows operating system to the XPR server is used.

Since the result from this is unpredictable, we recommend in a multi-NIC-environment to always specify one of the existing LAN cards via its IP address.

MWI Signal Active

It is possible to signalize newly incoming messages to users via an MWI message (Message Waiting Indicator) at the telephone device. Possible display formats of such an information are e.g. setting the MWI LED or a note in the respective telephone device display.

For this feature another logical line must be initialized by the CTI APL between the PBX and the XPR server MTA. Via this line a corresponding notification is sent to the user in case of a newly received message. The **Active** option causes the CTI APL to set up this additional logical line.

NOTE:

This option must not be set when connecting OpenScape Voice.

NOTE: In case of a HiPath 4000 the MWIInterrogate feature must be disabled.

MWI Signal Address

So that an MWI message of the XPR server can be addressed for the appropriate telephone, it must be forwarded to the PBX with an address of the format `MWI.<CTI-Link>/<Phone number>`. In the **MWI Signal Address** field the part `MWI.<CTI-Link>` is defined.

The example displayed above results in the MWI signal address `MWI.H150_CSTA`.

NOTE:

This entry field can only be edited when the **MWI Signal Active** option is selected.

Monitoring

Leads to the monitoring parameters (cf. [Section 17.7.5.1, “Monitoring Parameters \(CSTA\)”, on page 1097](#)).

NCO parameters

Leads to the NCO settings of the CTI link (cf. [Section 17.7.5.2, “NCO Settings \(CSTA\)”, on page 1099](#)).

Trunk lines

Leads to the trunk lines configuration (cf. [Section 17.7.5.3, “Trunk Lines \(CSTA\)”](#), on page 1101).

NOTE:

You can only configure trunk lines for selected PBX systems (e.g. for the Hicom 150).

Greetings

Leads to the greeting ports configuration (cf. [Section 17.7.5.4, “Announcement Ports \(CSTA\)”](#), on page 1102).

NOTE:

You can only configure trunk lines for selected PBX systems (e.g. for the Hicom 150).

17.7.5.1 Monitoring Parameters (CSTA)

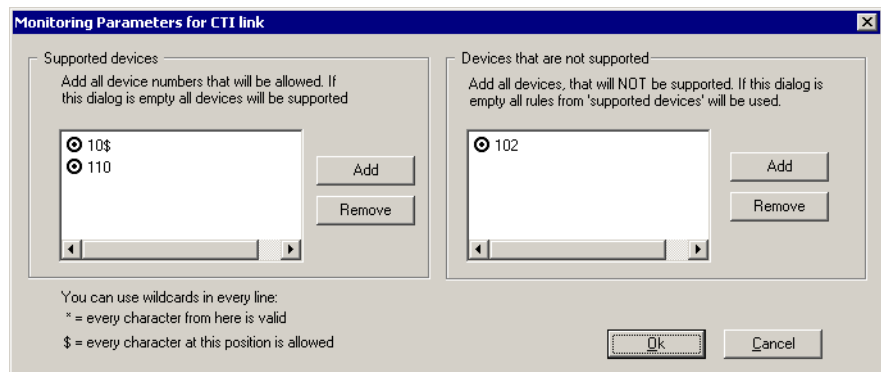
Can be reached via: **CtiApl > Set Options > Add/Edit > Monitoring**

This dialog gives an overview of possible CTI access to telephone devices. It is possible to release devices dedicatedly for setting monitor points or lock them dedicatedly.

To cover complete extension number ranges with one entry it is possible to use the wildcards * and \$ in entries.

With this applies:

- * – Allows an arbitrarily long string with any characters at the defined space
- \$ – Allows exactly one arbitrary character at the defined space



Moreover, the following features are provided:

Supported devices

Lists all devices or device ranges which can be administered with the help of CTI functionality.

IMPORTANT:

If no entries are indicated here, all telephone devices can be administered with the help of CTI functions. It is possible to configure additional restrictions in the **Devices that are not supported** section.

Devices that are not supported

Lists all devices or device ranges which may in no case be administered with the help of CTI functions.

IMPORTANT:

If no entries are displayed here, only the entries defined under **Supported devices** are analyzed.

Add

Inserts a new entry in the **Supported devices** section or **Devices that are not supported** section.

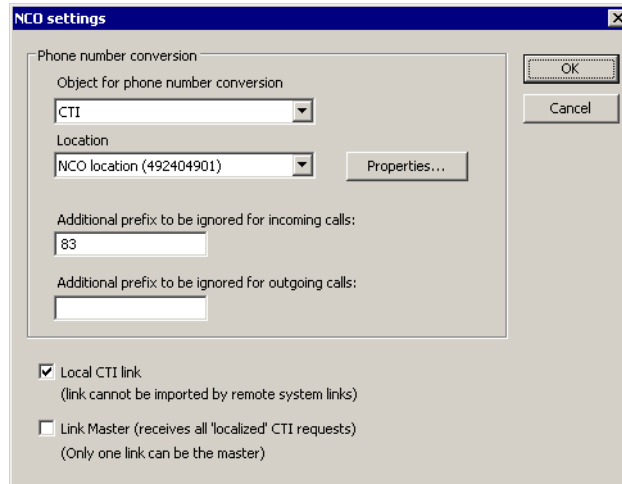
Remove

Removes an existing entry from the **Supported devices** section or **Devices that are not supported** section.

17.7.5.2 NCO Settings (CSTA)

Can be reached via **CtiApl > Set Options > Add/Edit > NCO Parameters**

This dialog serves for the configuration of site information in a CTI environment with several PBX systems. In this case several site parameters such as area code or subscriber code can be configured for several CTI links.



The following features are provided:

Object for phone number conversion

Defines the NCO that is used for the phone number conversion of the respective CTI link.

Location

If different locations are used in a CTI environment with different location information, manual location information can be assigned to each CTI link. This setting is preferred in the location information of the NCO that has been selected under **Object for phone number conversion**.

NOTE:

By default, the location of the selected object for phone number conversion (NCO) is always set under **Location**.

Properties

Leads to the **Location** tab of the NCO configuration. It is possible to edit existing locations here or to create new ones. Cf. [Section 9.9.5, "NCO Locations", on page 447](#).

Additional prefix to be ignored for incoming calls

Some PBX systems do not forward normalized phone numbers to the XPR server in transactions. Instead, possible additional phone number information precede a phone number (e.g. an external prefix or a tie trunk number). Anyhow, the XPR server might not be able to normalize the phone numbers correctly.

In such a case leading digits can be discarded for all incoming target numbers on the respective CTI link via this option.

If no additional settings are made in the **Additional prefix to be ignored for outgoing calls** option, the entry made here is not only valid for target but also originator numbers.

Additional prefix to be ignored on outgoing calls

Some PBX systems do not forward normalized phone numbers to the XPR server in transactions. Instead, possible additional phone number information precede a phone number (e.g. an external prefix or a tie trunk number). Anyhow, the XPR server might not be able to normalize the phone numbers correctly.

In such a case leading digits can be discarded for all incoming originator numbers on the respective CTI link via this option.

If no entry is made here, the entry of the option **Additional prefix to be ignored for incoming calls** is applied.

Local CTI link

Several XPR servers can be networked via so-called Remote System Links (RSL). Logical lines of a XPR server are represented on another server which is connected via RSL, so that this remote server can also access it.

Via the **Local CTI link** option you can define in this context that the respective CTI link is not mapped to those XPR servers that are connected via an RSL.

Link Master

The XPR server does not evaluate this setting any further.

17.7.5.3 Trunk Lines (CSTA)

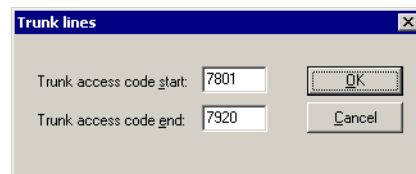
Can be reached via:

CtiApl > Set Options > Add/Edit > Trunk lines

For some PBX systems it is possible to monitor trunk lines as well as telephone devices. In this dialog trunk lines to be monitored can be specified.

IMPORTANT:

All trunk lines to be monitored must be within a coherent phone number range.



The following features are provided:

Trunk access code start

Defines the phone number of a trunk line describing the beginning of a phone number range of trunk lines to be monitored.

Trunk access code end

Defines the phone number of a trunk line describing the end of a phone number range of trunk lines to be monitored.

17.7.5.4 Announcement Ports (CSTA)

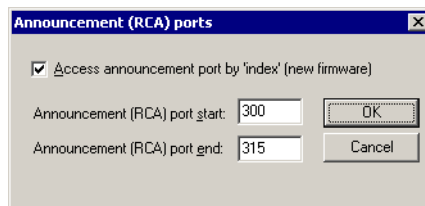
Can be reached via: **CtiApl > Set Options > Add/Edit > Announcement**

Some PBX systems support analog announcement ports for playing voice messages. Depending on the PBX it might be possible to control these ports.

The addressing type of these announcement ports depends on the applied PBX. Index-based or phone number-based addressing is possible. If index-based addressing is supported, announcement ports can be specified in this dialog on the basis of their index so that they can be monitored.

IMPORTANT:

All announcement ports to be monitored must be within a coherent phone number range.



Moreover, the following features are provided:

Access announcement port by 'index'

With this option you can define if the announcement ports are addressed via their index or their phone number. If the option is activated, the addressing is based on the index. If the option is deactivated, the addressing is based on the phone number. In the second case no further entry is possible in this dialog.

Announcement (RCA) port start

Defines the index number of an announcement port describing the beginning of an index block of trunk lines to be monitored.

NOTE:

This entry field is only active if the option **Access announcement port by 'index'** is selected.

Announcement (RCA) port end

Defines the index number of an announcement port describing the end of an index block of trunk lines that are to be monitored.

NOTE:

This entry field is only active if the option **Access announcement port by 'index'** is selected.

17.7.6 TSAPI/CSTA Link Properties (TSAPI)

IMPORTANT:

If several PBXs are to be connected via TSAPI, a multilink-compatible TSAPI driver must be used.

Can be reached via: **CtiApl > Set Options > Add/Edit**

This dialog defines the settings the CTI APL requires for the basic CTI communication via the respective TSAPI-CTI link.

The following features are provided:

Logical link name

The link name defined here helps the XPR server with the logical addressing of the CTI link. The logical address is composed of `NVS:CTI`, followed by the name defined here.

The example displayed above results in the logical address `NVS:CTI.TSAPI`.

IMPORTANT:

The connection name defined here must be **unique** because of its reference character.

PBX

Here the PBX type of the connected PBX is displayed automatically.

Login ID

For the CTI communication with a PBX via TSAPI an access account must be configured in the applied PBX. Enter the account name in the **Login ID** field. With this name the CTI APL logs on to the PBX for the CTI communication.

PBX name

Defines a server ID which the CTI APL forwards to the PBX during the login procedure. As far as possible this field is already preset with useful default values. However, depending on the PBX further adaptations are required here. The Octopus E-300/800 requires as last portion of this name for example the Windows name of the XPR server computer on which the CTI APL runs.

Password

If the access account configured in the PBX is secured by a password, this must be entered in the field **Password**. The CTI APL forwards this information to the PBX before the communication and thus authenticates for access.

Confirm password

If an entry has been made in the field **Password**, this must be repeated here. Since the two fields **Password** and **Confirm password** are displayed 'hidden' in the dialog, this second confirmation entry is to prevent unintentional wrong entries.

NCO parameters

Leads to the NCO settings of the respective TSAPI-CTI link. The settings here correspond to those of the CSTA protocol (cf. [Section 17.7.5.2, "NCO Settings \(CSTA\)", on page 1099](#)).

Advanced

Leads to the advanced CTI settings (cf. [Section 17.7.6.1, "TSAPI/CSTA Advanced Settings \(TSAPI\)", on page 1106](#)).

NOTE:

The extended settings are only available if value **1** is set for the registry key [UseOldTSAPIStack \[REG_DWORD\]](#).

This registry value may only be modified by the service personnel of the producer or their official partners.

Monitoring

Leads to the monitoring settings of the respective TSAPI-CTI link. The settings here correspond to those of the CSTA protocol (cf. [Section 17.7.5.1, "Monitoring Parameters \(CSTA\)", on page 1097](#)).

17.7.6.1 TSAPI/CSTA Advanced Settings (TSAPI)

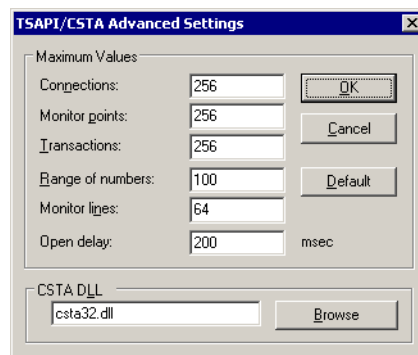
IMPORTANT:

The extended settings are only available if value **1** is set for the registry key [UseOldTSAPIStack \[REG_DWORD\]](#).

This registry value may only be modified by the service personnel of the producer or their official partners.

Can be reached via: **CtiApl > Set Options > Add/Edit > Advanced**

This dialog defines some basic parameters and advanced CTI settings for the communication with the connected PBX.



The following features are provided:

Connections

TSAPI drivers normally allow only a number of CTI links limited by the licenses. In the **Connections** field this individual system restriction can be forwarded to the XPR server to optimize the resources for the CTI link setup.

Monitor points

PBX systems normally allow only a number of monitor points limited by the licenses. In the **Monitor points** field this individual system restriction can be forwarded to the XPR server to optimize the resources for setting monitor points.

Transactions

The TSAPI stack administers all current transaction relations in a list that is restricted in its length. For this reason, the XPR server can only set up a restricted number of transactions to the connected PBX at the same time. This restriction applies especially to the setting of monitor points.

Example:

In a CTI environment 30 users exist who have activated their TrayPhone client and have added 10 extensions to their TrayPhone event bar.

If all users start their computers at the same time in the morning, this results in 300 transaction relations. This value exceeds the default setting of 256. As a

result, the 'first' 25 users will see all states of the extensions in Trayphone. The 26th user will only receive 6 states (the rest of the extension is marked with a red exclamation mark, the limit of 256 is reached) and no state at all is displayed for the remaining users.

Transactions defines the maximum number of transaction relations that can be administered via the applied TSAPI stack.

Range of numbers

Under TSAPI it is possible to set static monitor points in a coherent phone number range.

The setting in the **Range of numbers** field defines the maximum range size of monitor points. Therefore no oversized ranges can be indicated for setting monitor points.

Monitor lines

For each established logical CTI link a line entry is generated in the window *Physical Lines* of the XPR monitor.

The entry in the **Monitor lines** field limits the number of these displayed line entries. In environments with a very large number of CTI lines this setting prevents that the XPR server has to deal with too much performance loss by the line display in the XPR monitor.

Open delay

As soon as the XPR server has started a CTI link, it begins to set all required monitor points in the connected PBX. The XPR server sends the respective CTI commands often faster than PBX systems can process them. For this reason, a delay time can be defined here in milliseconds. It is waited by the XPR server between two CTI commands to set monitor points.

CSTA DLL

A routine library is provided for the TSAPI interface by the PBX manufacturers. Their storage location must be known to the CTI APL. Since it is always stored at a defined storage location depending on the manufacturer, this information is automatically preset during the selection of the PBX.

Browse

Via this interface another file path could be defined for the `CSTA.DLL`.

Default

Resets all modified settings to their respective default value.

17.7.7 MS-TAPI Properties (TAPI)

IMPORTANT:

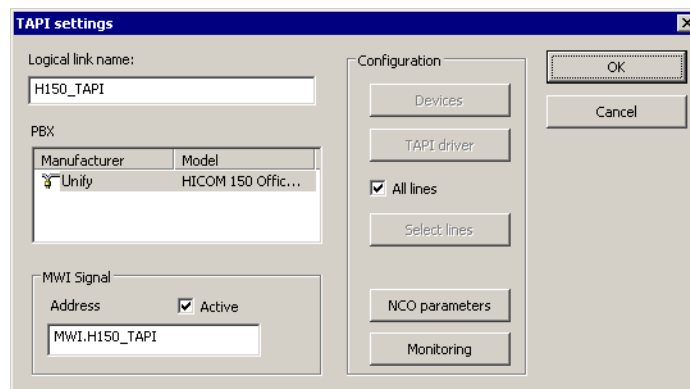
If several PBXs are to be connected via TAPI, a multilink-compatible TAPI driver must be used.

Can be reached via: **CtiApl > Set Options > Add/Edit**

IMPORTANT:

Before you can configure a TAPI-based CTI connection, you need to install the TAPI driver for the relevant PBX on the XPR server system.

This dialog defines the settings the CTI APL requires for the basic CTI communication via the respective TAPI-CTI link.



The following features are provided:

Logical Link name

The link name defined here helps the XPR server with the logical addressing of the CTI link. The logical address is composed of `NVS : CTI .` followed by the name defined here.

The example displayed above results in the logical address `NVS : CTI . MSTAPI`.

IMPORTANT:

The connection name defined here must be **unique** because of its reference character.

PBX

Displays the PBX whose settings are currently edited.

MWI Signal Active

It is possible to signalize newly incoming messages to users via an MWI message (Message Waiting Indicator) at the telephone device. Possible display formats of such an information are e.g. setting the MWI LED or a note in the respective telephone device display.

For this feature another logical line must be initialized by the CTI APL between the PBX and the XPR server MTA. Via this line a corresponding notification is sent to the user in case of a newly received message. The **Active** option causes the CTI APL to set up this additional logical line.

MWI Signal Address

So that an MWI message of the XPR server can be addressed for the appropriate telephone, it must be forwarded to the PBX with an address of the format `MWI.<CTI-Link>/<Phone number>`. In the **MWI Signal Address** field the part `MWI.<CTI-Link>` is defined.

The example displayed above results in the MWI signal address `MWI.H150CSTA`.

NOTE:

This entry field is only active when the **MWI Signal Active** option is selected.

Devices

Via this button the configuration dialog of the applied and normally manufacturer-specific TAPI driver is opened. Here respective adaptations for the TAPI communication between the XPR server and the PBX can be made.

For further information on the required TAPI settings please refer to the manufacturer documentation of the TAPI supplier.

NOTE:

This button is only active if a TAPI driver has been installed in the XPR server system, and if this has been started as service in the Windows operating system.

TAPI driver

With this button the phone and modem options of the Windows operating system are opened. Here respective adaptations for the phone and modem communication between the XPR server and the PBX can be made.

NOTE:

This button is only active if a TAPI driver has been installed in the XPR server system and if this has been started as service in the Windows operating system.

All lines

The CTI APL supports setting monitor points via TAPI drivers. For this purpose it uses the information about terminal device lines determined by the TAPI driver used.

If the **All lines** option is active, the CTI APL sets a monitor point for each terminal device line determined in the TAPI driver.

NOTE:

If you use the Cisco CallManager feature “Shared Line Support”, the CTI APL may monitor only one terminal device line for a phone number. Using the “Shared Line Support” you should therefore not activate the **All lines** option. Determine the terminal device lines to be monitored individually via [Select lines](#) instead. If you select several terminal device lines to be monitored for one phone number, the CTI APL monitors always only one terminal device line.

Select lines

Leads to the selection of TAPI lines for the respective CTI link (cf. [Section 17.7.7.1, “Select TAPI Lines \(TAPI\)”](#), on page 1111).

NOTE:

This button is only active if the **All lines** option has not been selected.

NCO parameters

Leads to the NCO settings of the CTI link. The settings here correspond to those of the CSTA protocol (cf. [Section 17.7.5.2, “NCO Settings \(CSTA\)”](#), on page 1099).

Monitoring

Leads to the monitoring parameters of the CTI link. The settings here correspond to those of the CSTA protocol (cf. [Section 17.7.5.1, “Monitoring Parameters \(CSTA\)”](#), on page 1097).

17.7.7.1 Select TAPI Lines (TAPI)

Can be reached via:

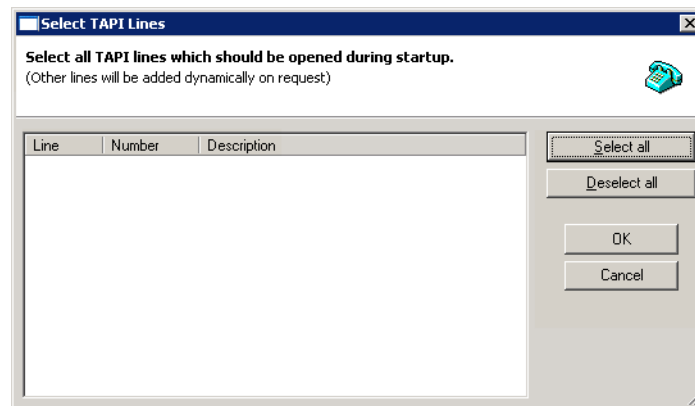
CtiApl > Set Options > Add/Edit > Select lines

NOTE:

This dialog can only be selected if the **All lines** option is not selected in the TAPI settings.

The CTI APL supports setting monitor points via TAPI drivers. For this purpose it uses the information about terminal device lines determined by the TAPI driver used.

This dialog specifies for which of the terminal device lines defined in the TAPI driver a monitor point is actually set after the start of the respective CTI channel.



The following features are provided:

Select all

For all terminal device lines defined in the TAPI driver a monitor point is set.

NOTE:

If you use the Cisco CallManager feature “Shared Line Support”, the CTI APL may monitor only one terminal device line for a phone number. Using the “Shared Line Support” you should therefore not activate all terminal device lines.

If you select several terminal device lines to be monitored for one phone number, the CTI APL monitors always only the terminal device line listed first.

Deselect all

All displayed marks are canceled.

17.8 Optimizing the CTI APL Starting Behavior

On booting the CTI APL, monitor points are set in the connected PBX to supervise various telephone devices, trunk lines or tie lines. Monitor points are set by different sources.

These sources are:

- The Mail APL
The Mail APL defines independently all users with activated CTI journal during a reboot. Therefore it exports those users from the Correlation Database for whom the CTIJOURNAL database field is set. It makes the CTI APL set monitor points for those in the respective PBX.
- The CTI APL
The CTI APL defines during a reboot independently all users that have been learned via the AutoLearn algorithm before. Therefore it exports the content of the `<Server Name>/$Perform/CTI` domain from the Correlation Database.
- Arbitrary clients
For example optiClient.

The APLs set the monitor points as quickly as possible. This may lead to overlapping and a delayed setting of monitor points in the PBX, possibly resulting in client time-outs.

To avoid this problem, the following parameters have been introduced in the registry. Via these, the starting behavior of the CTI APL can be optimized.

Optimizing the CTI APL starting behavior

The following registry values are available for optimizing the startup behavior of the CTI APL:

- **CtiJrnLoadDelay [REG_DWORD]**
Defines the time interval during which the Mail APL sends monitor points to the CTI APL in milliseconds.
This parameter belongs to the registry entries of the Mail APL and is stored under the key `<XPR Install>\MailAPL`.

From our experience, the following values work well with efficient PBX systems (e.g. Alcatel 4400 or Hicom 300E) regarding the CTI APL startup behavior.

Parameter	Value	Description
CtiJrnLoadDelay	300	The Mail APL sets a monitor point every 300 ms.

The send queue state can be examined on the basis of the following logging messages of the CTI APL:

- When entered *in* the send queue:

```
15.14:... CtiApl PBX AL4200 1 new sendpacket queued. '9' packets in the send queue.
```

- With sending *from* the send queue:

```
15.14:... CtiApl PBX AL4200 1 queued packet send on Ch '0'. '9' packets in the send queue.
```

Only a few entries in the send queue is an ideal state.

17.9 PBXs in the CTI Environment

A current list of supported and tested PBXs is found in the hardware compatibility list, which is part of the release notes.

17.10 Tips and Tricks

17.10.1 Debug Filter Usage

IMPORTANT:

If all log filters are switched on at the same time, the XPR monitor may no longer be able to deal with the accumulating information and thus no longer put out single messages in the log window. Consequently, log messages could be interpreted wrongly.

Therefore never activate all log filters at the same time!

1. For monitoring events and commands the topics *<link name>* with “Debug 1” and in addition *CSTA <link name>* with “Debug 2” are suited very well.
 2. To examine malfunctions of single PBX variables, *CstaL6 <link name>* with “Debug 4” is the best filter.
 3. With interface problems all *TCP <link name>* or *ISDN <link name>* filters and, in addition, all *PBX<link name>* filters should be activated.
 4. The info-message *mrs with PBX connected* with the “PBX<link name>” topic means that the connection to the PBX has been established. If the CTI link does nevertheless not declare itself READY, the login procedure should be examined by activating all filters with the *PBX<link name>* topic.
-

IMPORTANT:

Before activating this option, you must find out for how many XPR users in *Communications* the **CTI Journal** option has been activated.

The reason is that setting many monitor points may influence the PBX performance negatively. Furthermore, PBX systems normally only support a limited number of monitor points that can be configured at the same time. The number of monitor points to be set automatically should be complementary with this behavior.

17.10.2 Error-Search Tools

When you look for CTI connection errors, the following tools are particularly suitable:

- **CtiTest**
CtiTest is a tool for testing the CTI features of the XPR server.
You find detailed information about using this tool in [Section 32.2, “CtiTest”, on page 1503](#).
- **Phone**
This tool is available for free to test the communication via TAPI 2.1 and TAPI 3.x service provider. It can be obtained, for example, under the following address: www.julmar.com.

17.11 Standards supported in the CTI APL

IMPORTANT:

Protocol standards may contain optional features. Such features need not necessarily be implemented in a standard-conformable system. Depending on the optional features a producer enables, the range of features of different protocol implementations may vary.

The following table lists standards supported by the CTI APL.

- CSTA Phase I (ECMA 179/180)
- CSTA Phase II (ECMA 217/218)
- CSTA Phase III (ECMA 269/285)
- TAPI 2
- TSAPI

18 CSTA APL

18.1 What is CSTA?

CSTA is the acronym for **C**omputer **S**upported **T**elecommunications **A**pplication and for the time being the most common CTI protocol interface. It was developed by ECMA (European Computer Manufacturers Association) as standard for coupling computers and PBXs and determines CTI messages and their structure.

The CSTA protocol consists of a core (call control model) and a large number of possible expansions. Furthermore, CSTA does not only serve as interface but also as guideline for implementing CTI protocols. PBX and CTI application providers use CSTA as basis for their individual developments, since CSTA can be flexibly adjusted to different specifications. The CSTA APL makes sure that CSTA-based CTI applications can be connected to any PBX supported by the XPR server and are able to execute CTI functionality by means of the XPR server.

NOTE:

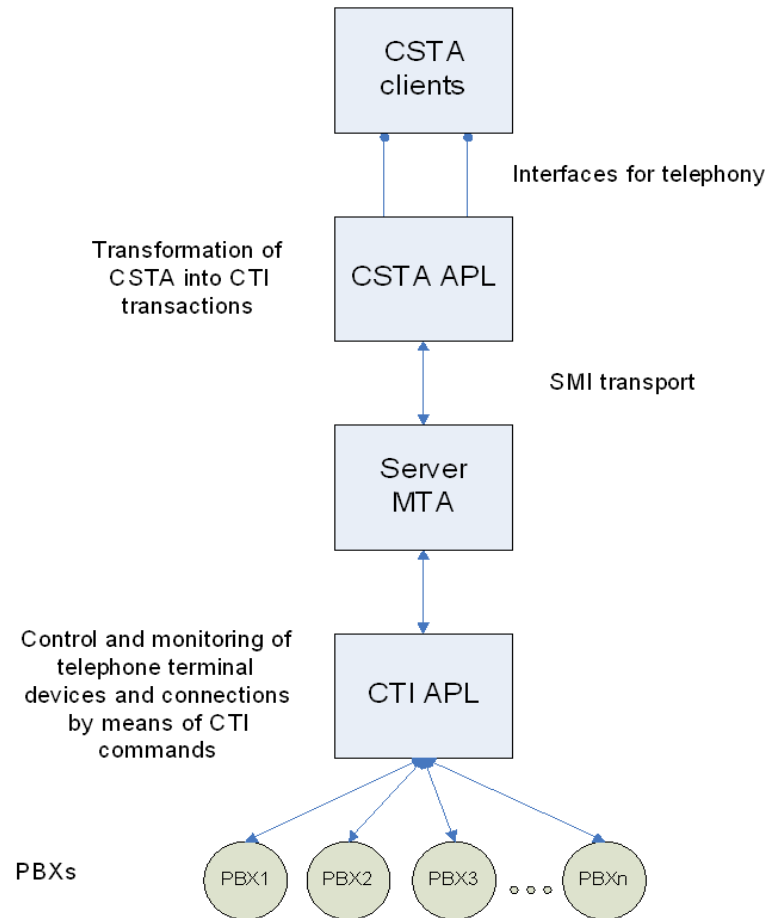
In the *Release Notice* document you learn which PBXs are supported by the XPR server.

18.2 CSTA APL Functionality

The CSTA APL serves for successfully connecting CTI applications that communicate via CSTA to the PBXs supported by the XPR server. These CTI applications are also called CSTA clients. Supported CSTA clients are:

- OpenScape Web Client

The following illustration shows how the CSTA APL fits in the XPR system:



The CSTA clients communicate with the CSTA APL by means of the CSTA protocol. In this process the internal XPR connection model is mapped. See [Section 17.3.4.2, “XPR Connection Model”, on page 1057](#).

The CSTA APL compiles the CSTA protocol in CTI transactions. The CTI transactions are delivered to the MTA within the XPR server. The MTA sends the CTI transactions to the CTI APL.

The CTI APL communicates with the actual PBXs in their respective communication protocol. This abstracts the communication between PBX and CSTA client. Consequently, special functions of a specific PBX may not be available in the CSTA client.

On the other hand, applying the process described here enables PBXs that do not support CSTA themselves to collaborate with CSTA clients.

The CSTA clients require the IP address and the port number of the XPR server to connect to the CSTA APL.

You find continuative information about CTI and the XPR connection model as well as about the CTI APL functionality in [Chapter 17, “CTI APL”](#).

18.3 CSTA APL Configuration

In the XPR monitor open the CSTA APL configuration dialog in the window for managing the XPR server modules. The dialog features the tabs **Phone Numbers** and **Connectivity**.

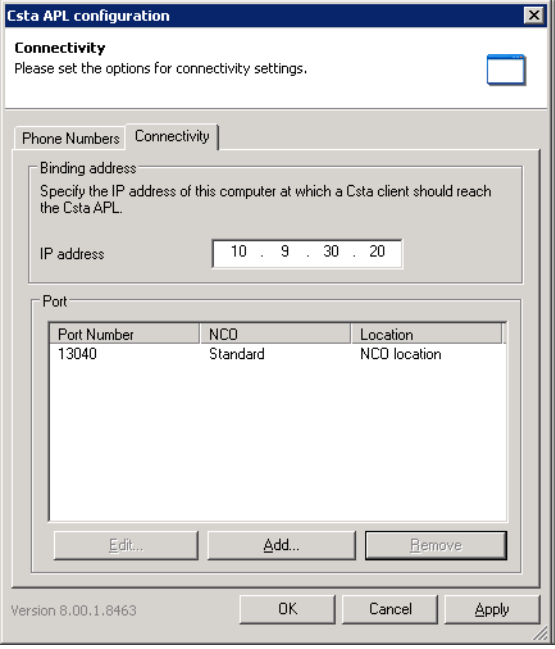
18.3.1 Phone Numbers Tab

The screenshot shows a Windows-style dialog box titled "Csta APL configuration". It has two tabs: "Phone Numbers" (selected) and "Connectivity". The "Phone Numbers" tab contains the following elements:

- A header section with the title "Phone Numbers" and the instruction "Please set the options for contact center applications." followed by a small blue square icon.
- A section titled "Special phone numbers:" with the instruction "Specify the phone number of the comfort transfer application." and a text input field labeled "Phone number".
- A section with the instruction "Specify the standard parking phone number and the real phone number." and two text input fields labeled "Virtual phone number" and "Real phone number".
- A section titled "Redirection time-out:" with the instruction "Time after which a redirected caller is returned to the original phone if the call is not accepted." and a text input field labeled "Time-out (sec)" containing the value "10".
- At the bottom, there is a version string "Version 8.00.1.8463" and three buttons: "OK", "Cancel", and "Apply".

This dialog is obsolete, because the configurable XPR functions are not supported anymore.

18.3.2 Connectivity Tab



The image shows a Windows-style dialog box titled "Csta APL configuration". It has two tabs: "Phone Numbers" and "Connectivity", with "Connectivity" currently selected. The "Connectivity" tab contains the following elements:

- A header section with the title "Connectivity" and the instruction "Please set the options for connectivity settings." followed by a small blue square icon.
- A "Binding address" section with the instruction "Specify the IP address of this computer at which a Csta client should reach the Csta APL." Below this is an "IP address" field containing the text "10 . 9 . 30 . 20".
- A "Port" section containing a table with three columns: "Port Number", "NCO", and "Location".

Port Number	NCO	Location
13040	Standard	NCO location

Below the table are three buttons: "Edit...", "Add...", and "Remove". At the bottom of the dialog box are the "OK", "Cancel", and "Apply" buttons, and the version number "Version 8.00.1.8463" is displayed on the left.

Here you can configure how CSTA clients can connect the CSTA APL. Enter the **IP address** of the XPR server on which the CSTA APL is installed. On the predefined port 13040 connects, for example, *OpenScape Web Client*. This client always requires normalized numbers. Further ports can be added if required. Based on these specifications CSTA clients can be connected with the CSTA APL of the XPR server.

19 The LDAP APL

19.1 What is LDAP?

The LDAP APL provides the so-called **Lightweight Directory Access Protocol**, **LDAP** for short, to browse and edit entries in directory services. It is a further development of the access protocol Directory Access Protocol (DAP), which is based on the directory service **X.500**. X.500 describes an early standard that, based on the OSI reference model, is to administer a world-wide, distributed directory. However, as regards speed and overhead, X.500 did not make the grade anymore.

LDAP includes the following advantages:

- LDAP is an open standard.

Since LDAP is an open standard of the Internet Engineering Task Force (IETF), it can be unrestrictedly used by any developer and company.

- LDAP offers a universal design for directory services.

LDAP is based on the definition of so-called schemas. A schema is an object oriented concept, which also supports heredity. Therefore, schemas specialized for individual requirements can be derived from standard schemas the IETF has agreed upon.

- LDAP is a simple protocol.

An important aspect about LDAP as successor to the more complex DAP was the development of a simple protocol that is easy to implement and easy to use. Most programming languages support LDAP as well as most operating systems.

- LDAP allows a distributed architecture.

By way of replication it is possible to keep parts or the entire LDAP server on physically separated computers several times.

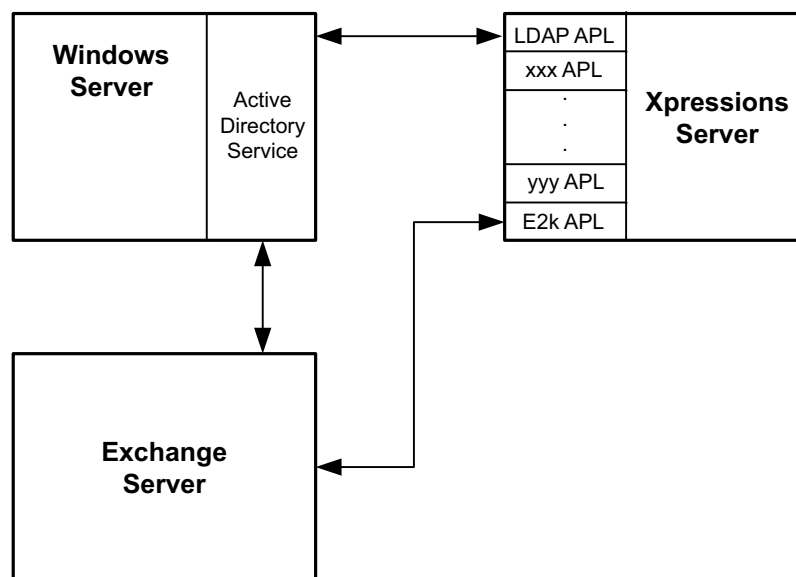
- LDAP enables the integration of security concepts.

19.2 LDAP and XPR

The LDAP protocol enables the XPR system to connect to a directory service. Such a directory service is represented by the Microsoft Active Directory. Microsoft Exchange for example stores all directory information in the Active Directory. The following is an example of the connection of a directory service to XPR.

The figure shows the interaction of LDAP APL in the XPR system, Active Directory and Microsoft Exchange server. The LDAP APL has been designed for this structure, but the Microsoft Exchange server is not required for the information replication between XPR and Active Directory. So if the LDAP APL is connected to the Active Directory without Microsoft Exchange, you can omit the lower portion of the figure.

The LDAP communication protocol can thus be used to read out information of a directory service such as Microsoft Active Directory and to transfer the information to the XPR system.



For this purpose a separate connection to the Active Directory via the LDAP APL is required. It is in charge of enabling a relation between the Active Directory attributes and the data relevant for XPR. The correct assignment is thus created. Since manual adaption of the database fields is relatively laborious, the effort is minimized by performing the basic configuration via the import of a standard configuration file (xxx.lcf).

NOTE:

The LDAP APL only serves to replicate user data - the DS pattern is not extended or modified.

The LDAP APL is so conceived that it can additionally access other systems

supporting the LDAP protocol. Such systems are, for example, Novell NDS, Netscape Directory Server and DirX. The LDAP APL is thus not fixed to the Active Directory.

19.3 The theoretic LDAP Structure

The following sections deal with the main features of the LDAP structure and proceedings. These theoretical explanations are useful for configuring the LDAP APL.

Directories

A directory is a list of information on objects in a specific order. On each object detailed information can be retrieved. Directories serve mostly for searching and administering directory entries.

Example:

In a phone directory, the objects are the subscribers, the order is alphabetic, and the detailed information to be obtained is address and telephone number.

The term 'Yellow Pages' is often used to characterize the way in which a directory is used. In reality, directories found on computers are much more flexible than those on paper. A directory cannot only be browsed according to default criteria such as second names in alphabetic order, but also based on specific individual criteria.

19.4 The logical LDAP Model

So that the LDAP can be used, it is important to understand its logical structure. The logical LDAP structure can be divided into the four areas **Information**, **Naming**, **Function** and **Security**.

19.4.1 The LDAP Information Model

The LDAP information model describes what directory entries look like and how they are structured.

19.4.1.1 Objects and Attributes

The total amount of information in a directory is called **Directory Information Base** (DIB). These items of information are usually not fully visible to the normal user. The DIB consists of single **Entries** that share an interrelationship. An entry is an amount of information on a single **object**. Entries represent in most cases objects from reality.

Example:

A phone directory has entries for subscribers, a library catalogue contains entries for books, a university directory features entries for students, lecturers, employees and so on.

Entries are composed of an **attribute** collection. Each attribute has an **attribute type** and an **attribute value** with **one or several values** (single or multi value). **Mandatory** attributes must appear in each entry. **Optional** attributes may be missing in entries. Attributes can also occur in an entry several times. The so-called **matching rules** define how entries are compared.

19.4.1.2 Object Classes

Each entry in an LDAP directory describes an **object**, thus a definite entity of an **object class**. An object class is a generalized description for this and congenial objects. The object class has a list of mandatory and optional attributes.

RFC 2252 defines that LDAP object classes can either be:

- **Abstract**,
- **Structural** or
- **Auxiliary**.

Abstract object classes are only used to derive other object classes from them. They serve exclusively as super class or “template”. They represent a comfortable way to define attribute collections that are bequeathed to all structural classes derived from them. `top` is such an abstract object class. There are no abstract object class entries.

Entries must always belong to a **structural** object class. Most object classes are of structural nature, therefore the default setting for object classes is `structural`.

Auxiliary object classes can be used to bind the same attributes to different entries. Such an “auxiliary object class” might serve e.g. to supplement entries with special attributes. An entry must, however, not exclusively be created from this auxiliary object class, but must the attributes defined in it additionally feature to those of a structural object class.

Example:

`Christmas cookies` could be an abstract object class. All Christmas cookies have specific common attributes, “the” Christmas cooky as definite instance does not exist. From `Christmas cookies` a structural object class `shortbreadcookies` can be derived, which inherits all `Christmas cookies` attributes and receives its individual characteristic attributes in addition. As auxiliary object class an object class `withchocolatecoating` could be defined. There are no objects that are exclusively generated from `withchocolatecoating`. Structural object classes such as `shortbreadcookies` or `gingerbread` may supplement their instances by the auxiliary object class `withchocolatecoating` as desired attribute.

19.4.1.3 The Schema

The object classes of a directory server are stored in a summarizing description, the **schema**. A schema thus describes which object classes are permitted in a directory, which attributes they must have, which attributes they may have, which syntax must be used for the attributes, and which matching rules apply.

Example:

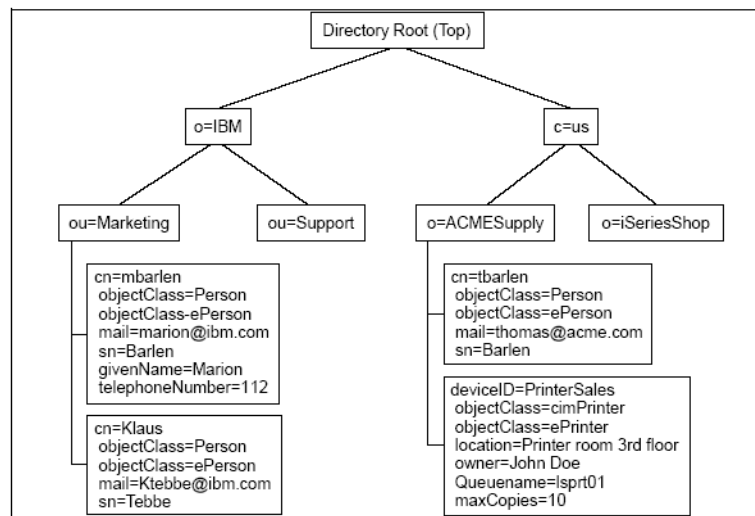
A schema might define an object class `person`. The `person` schema might mandatorily dictate that a person must have an attribute for their second name. This attribute be `surname`. At the same time the schema determines that this attribute must be a string of letters. The `person` entry may optionally have an attribute `telephoneNumber` for its telephone number, which may be a string of digits, blanks and hyphens.

19.4.2 The LDAP Naming Model

The naming model describes how information is identified and addressed.

Each entry is uniquely identified via its **Distinguished Name (DN)**. The DN describes where exactly an entry can be found within a directory hierarchy. It is thus a “fully qualified” name for an entry. Entries can have **parent, children and peer entries**. The relationship between the entries is clarified in the below tree structure. Parent entries are above and children entries are below the respective entry. Peer entries are on the same level.

The DN consists of a number of parts, the **Relative Distinguished Names (RDNs)**. Such names correspond approximately to a path specification in the operating system, which is composed of the directory and subdirectory names. The hierarchy is represented in a directory tree **Directory Information Tree (DIT)**. All names in a directory represent **namespace**.



As example for this graphic the Distinguished Name of the entry person Klaus in the marketing department of the company IBM is depicted: `cn=Klaus, ou=Marketing, o=IBM`. Relational Distinguished Names such as `cn=Klaus` form the DN.

19.4.3 The LDAP Function Model

LDAP defines different operations to find, read out and edit entries:

- Searching for entries that fulfill specific criteria
- Adding entries
- Deleting entries
- Modifying entries
- Modifying (relocating) the Distinguished Name (DN) or the Relative Distinguished Name of an entry
- Comparing entries

19.4.4 The LDAP Security Model

The security model explains how information is protected from unauthorized access.

LDAP determines how items of information is exchanged between LDAP client and server as messages. In these messages the operations are specified by the entries that the client wants to execute on the server (searching, editing, deleting etc.). The server's reply and the data format in which the information is transmitted in the messages is defined. Since TCP/IP is a connection-oriented protocol, connections must be established, sessions managed, and connections also be shut down again.

How LDAP server and client interact:

1. The client establishes a session with the LDAP server. This action is called **binding**. Access to the directory server occurs as anonymous user (anonymous bind), via an uncoded login with user name and password (simple bind) or via an encoded SSL connection (strong authenticated bind).

NOTE:

Using SSL V2 and V3 is always disabled in the XPR server. TLS V1, V1.1 or V1.2 is always used.

2. The client may then perform its operations on the LDAP server, for example reading out or editing entries. Searching is one of the most common operations on LDAP servers. The client may look for data according to freely selectable search criteria.
3. When the client is finished, it closes the session. This is called **unbinding**.

19.5 Directory Services

LDAP is an open Internet standard allowing access to directory services. The use of LDAP enables cooperation of Active Directory with the directory services of other suppliers. As component of Active Directory Interfaces (DSI), the Active Directory support of LDAP comprises an LDAP supplier object. The Active Directory Interfaces support the LDAP application programming interfaces for C, defined in the RFC 1823 Internet standard.

Other directory service applications can be adapted to access Active Directory information via DSI and LDAP.

A directory service is similar to a database in its functionality, so that the term Data Repository is often used. But it differs from traditional relational databases in the following respects:

- A directory is more specialized in **finding and reading out information** than in writing new information.
- **Searching** is one of the major operations in directory services. A directory service therefore provides advanced search features. Consequently, directories must be able to process a large number of search requests; they are optimized for the **read access**. Write access is often restricted to the administrators or owners of a specific information unit. Directories are not suitable for filing information that often changes.
Example: Information on network printers may be contained in a directory, but the highly dynamically changing printer queue information is misplaced there.
- Directory services are so conceived that they are **site-independently**. If a server does not keep an information locally, it will either forward the client “to the colleague in charge” or have the client application transparently access it. The server uses the advantages of technologies for distributed storing and data replication, which allows an efficient scaling.
- Directory services store information in **Entries** and not in rows of a table (records). An entry can additionally have **attributes**, which would be a field in a database. Entries can be all sorts of objects: persons, printers, rooms etc. The basic data structures of an LDAP directory, altogether called **scheme**, can be extended according to local requirements.

Some directory services will now be introduced, most of all the Microsoft Active Directory and the Novell eDirectory. The functions of these services is generally the same as they only differ in few structural aspects.

19.5.1 Microsoft Active Directory

The Microsoft Active Directory is based on the concepts of the X.500 and integrated in the Windows Server product lines. Typical of AD is the partitioning in domain, domain tree and domain forest. A domain is identified by a unique name and forms the smallest organizational unit in the entire structure, the latter one being called domain forest. Via the domains specific information can be accessed. Single domain structures consisting of a root domain and subdomains, are also called domain trees.

Servers are called domain controllers and administer the directory of the individual domain. Beyond that the domain controller administers selected attributes of objects of all other domains of the entire structure. These attributes are in most cases attributes often used such as the first and second name in search requests and defined in the *global catalog*. The global catalog task to enable logging in at the network at all and to perform search processes in the entire structure. All domain controllers are equal, so that a directory change can be performed on every domain controller. The multi-master replication makes sure that these modifications are copied to all domain controllers of the domain.

There are however some domain controllers in charge of specific modifications alone. These special server roles are summarized under the term FSMO. For example the scheme master administers modifications to the Active Directory scheme.

Some Active Directory features differ from the X.500 concepts. Firstly, there are no independent auxiliary object classes. Their attributes are integrated in the structural object classes instead but do not appear as value. These auxiliary object classes cannot be searched for or these selected entries cannot be added. Secondly, RDN must be available as single value. Finally, attributes or object classes cannot be removed anymore, they can at the most be deactivated when being added to the scheme.

19.5.2 Novell NDS eDirectory

The first Novell Directory Server (NDS) version was no X.500 directory service but strongly oriented towards the X.500 concepts. The NDS operated with individual protocols, so that with the LDAP introduction LDAP operations had to be converted into NDS-compatible commands. This lead to significantly reduced NDS performance.

To avoid the loss of market shares and to become platform independent, Novell performed a restructuring that considered NDS the key component in the new Novell product architecture. With renaming the NDS to Novell eDirectory, new features were implemented that lead to a versatile and flexible replication architecture. So-called *filtered replicas* were enabled that only replicate a subset of non-confidential attributes. These attributes can then be made public to all servers. Furthermore, an index of attributes not registered so far is automatically generated. This increases the request performance. *Subtree* partitions enable each host to administer several partitions with eDirectory.

19.5.3 Further Directory Services

There are further directory services supporting the LDAP. To mention are DirX, Domino Directory Server and Netscape Directory Server.

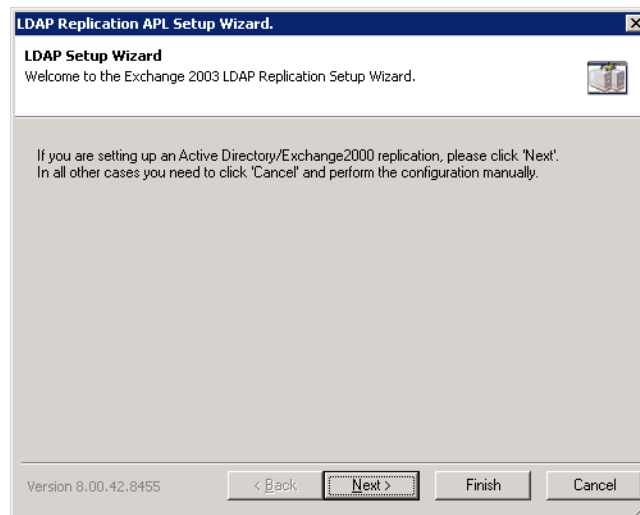
19.6 Installing the LDAP APL

19.6.1 LDAP APL Installation for Microsoft Exchange Server

Installation of the LDAP APL for Microsoft Exchange Server is embedded in the XPR server setup. If a new XPR server is to be set up for Microsoft Exchange Server, the LDAP APL must be integrated in the installation for selecting the E2k APL. The LDAP APL installation procedure in this case is described in the *Microsoft Exchange Gateway* manual.

19.6.2 LDAP APL Installation for other Directory Services

If the LDAP APL is required to access other directory services, specific presettings need to be performed for Microsoft Exchange with the installation. Since these presettings are not required for connecting the LDAP APL without Exchange Connector, the installation can be terminated at an appropriate stage. This happens as soon as the LDAP installation wizard appears with its welcome window.



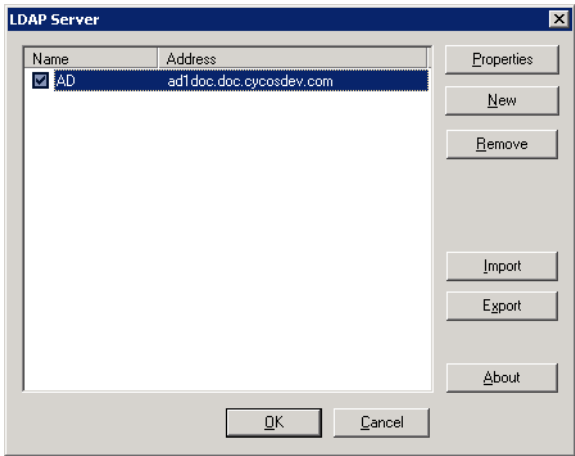
Click on **Next** to start the installation for the Exchange version. To install the LDAP APL for other directory services, select **Cancel**. The LDAP APL will then be installed but without copying any presetting for Microsoft Exchange Server.

Accessing other directory services requires an individual LDAP APL configuration, performed after the first LDAP APL start via the configuration in the XPR monitor. Configuration modifications should be exported as lcf file to secure the settings.

Note that for special configurations the script language E may be required. This is the case when e.g. complex filter mechanisms are needed for data replication.

19.7 LDAP Settings

The ISDN APL is configured through use of the XPR monitor. The configuration dialog is started by double clicking the **Set Options** entry in the Modules window under **LDAPApI/Settings**.



NOTE:
An administrator with *service privilege* can only invoke the Properties of an existing connection. Of this connection he/she only sees the **Login** and **Search** tabs.

This first dialog **LDAP Server** serves general administration purposes. The names and IP addresses of already existing LDAP servers are listed here. From here you can define further LDAP servers and modify the settings of already existing ones. In use is the server that features a check mark before the name entry.

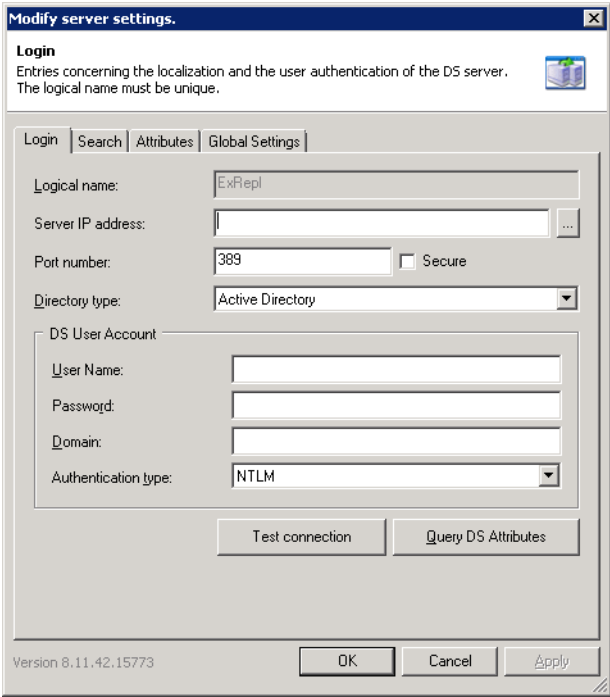
The buttons in this dialog have the following significance:

Field	Meaning
Properties	If an arbitrary configuration entry is selected, the actual configuration dialog Edit server settings is opened via this button. In there you find four tabs used for LDAP configuration. See Section 19.7.1, “The “Login” Tab”, on page 1136 .
New	Further LDAP servers can be added using this button. When you enable it you are taken to the New server settings configuration dialog. To define the LDAP configuration here, fill in the four tabs Login , Search , Attributes and Global Settings . See Section 19.7.1, “The “Login” Tab”, on page 1136 .
Remove	Deletes a selected LDAP connection.

Field	Meaning
Import	Branches to the file selection window "Open an LDAP Configuration File". Here you can enter an existing configuration file (format: *.lcf). After the configuration data import you are taken to the Login tab in the "New server settings" window to perform modifications possibly required.
Export	If stored as *.lcf file, a configuration with the current settings can be saved.
Info	Displays the version number of the LDAP APL. This should always be specified with error notifications or support requests.

19.7.1 The “Login” Tab

Here all information on this DS server is displayed. In the top portion you find the assigned LDAP configuration name, the IP address, the port number and the addressed directory type of the LDAP server. Thereunder, entry lines for user identification data are available. With the exception of the name assigned with the reconfiguration you can edit settings for DS server localization and the access privileges.



NOTE:

A name can only be changed with redefining the server settings.

The functions of the input fields on the **Login** tab are as follows:

Field	Meaning
Logical name:	Serves to assign an unambiguous name to a new LDAP configuration. If you have already opened an existing DS server configuration via Properties , the previously assigned name is displayed. This name can subsequently not be changed anymore.
Server IP address	In this entry line you can specify the valid DS server IP address (either the qualified host name or the numeric address), or the IP address of the selected entry is displayed. If you have opened an existing configuration, the IP address of the selected configuration is displayed. To simplify the process, click the selection button  to search the entire network for the desired DS server.

Field	Meaning
Port number	Entry field for displaying the currently set port or to modify the port number.
Secure	This option changes the port used for this connection automatically to 636 and encrypts the communication via the certificate delivered by the server by SSL. See also Section 19.13, "Secure LDAP Connection" .
Directory type	This menu allows the selection of either <code>Active Directory</code> , <code><unknown></code> and <code>DirX</code> . For Microsoft Exchange Server set <code>Active Directory</code> here. The other options refer to LDAP connections to other systems.
User name	The name of the user account provided with the corresponding access privileges to the directory service is entered or displayed here.
Password	This entry field is for definition of the password associated with the above user account.
Domain	Field for the entry of the domain associated to the above user account.
Authentication type	The definition of the authentication type must be set to <code>NTLM</code> (NT Lan Manager) for connecting to the Active Directory Service. The alternatives <code>SIMPLE</code> and <code>Negotiate</code> are intended for other directory systems. Remark: When you log in with the authentication type <code>SIMPLE</code> , the user name must be entered as Distinguished Name (DN). Example: <code>uid=admin,ou=administrators,ou=TopologyManagement,o=NetscapeRoot</code>

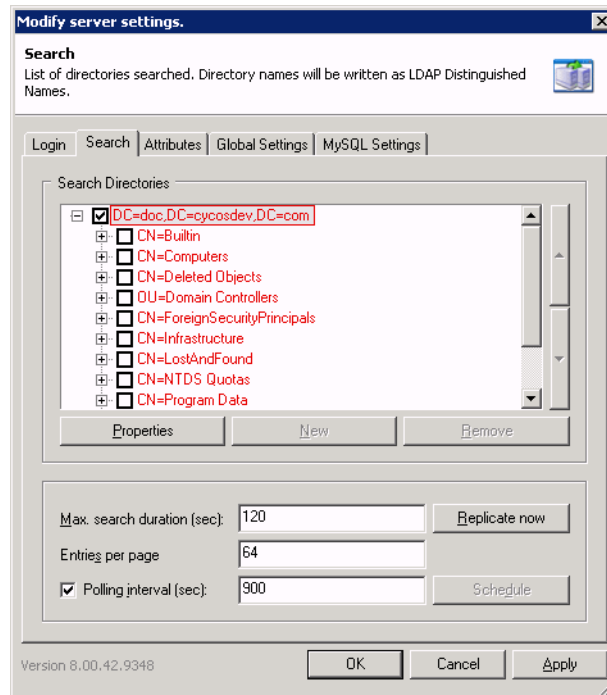
Thus all data significant for DS server selection are entered and can be verified via **Test Connection**. You are informed about the status of the connection to the DS server by a corresponding message. In case of an error, more detailed information is put out if possible.

With a click on **Query DS Attributes**, transmission of the DS attributes can be manually initiated. Otherwise, the DS attributes are read out from the selected DS server via recurrent automatic queries and listed on the **Attributes** tab. See **Polling interval** respectively **Schedule** on the **Search** tab. This process can be observed in the XPR Monitor as well.

19.7.2 The “Search” Tab

General considerations

The **Search** tab is used to define directories or user entries that are to be integrated in the replication process. Here you must explicitly select the containers that include users whose attributes are to be replicated. The containers or user entries in the search directory are color highlighted according to the search depth set.



The **Search Directories** portion displays the directories of the entire DS tree. You can expand the tree to display the single user entries. The desired directory is selected by setting the corresponding ticks next to the branching node of the tree.

- **Black entry:** Only the attributes of the users defined in the respective container object are replicated.
- **Blue entry:** Only the user attributes of the first level below the selected container will be replicated.
- **Red entry:** The entire subtree will be included in the replication.

An implemented logic prevents a redundant replication. An error message is issued when a new selection includes an already existing one. If you confirm this message with **Yes**, the new setting becomes active and the old one is automatically adapted. **No** restores the state before the modification.

Annotation on selecting users whose attributes are to be replicated: If in a larger organization all users have been defined in one container and attribute replication is required for a subset of these users only, the selection process may become

relatively protracted when all users have to be selected individually. In this case filter rule definition can be applied to specify the selection. Another option is to define the users intended of replication in a special container.

The two arrow icons on the right margin of this window serve to modify the directory sequence in the represented list. For this purpose, simply select the corresponding container or the container object to be moved with a click. The desired new position is then reached by upward or downward movement. In this way you can customize the replication priority since otherwise, with several selected directories, the processing sequence is from top to bottom.

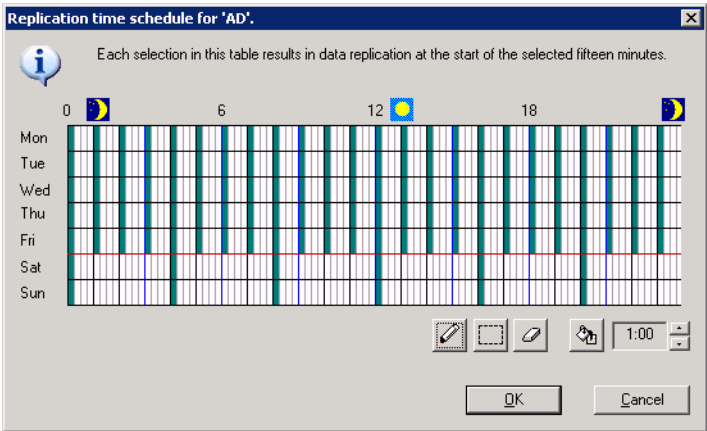
Replication settings

The buttons and entry fields in the bottom section of the dialog define the temporal replication process.

Field	Meaning
Polling interval	Each entered number value x starts the replication after x seconds (for example: with an entry of 12 the next replication starts after 12 seconds). Default after the installation is 0 seconds. Thus replication is at first deactivated so that it does not occur uncontrolled. Instead of via a polling interval, replication can also be performed via a schedule definition. Deactivate the checkbox next to the Polling interval entry to automatically activate the Schedule button. Schedule definition is described further below. If you want regular replication via a polling interval and no valid time value has been entered yet, an error message informs you accordingly.
Max. search duration	This value determines the maximum duration of a replication. Any numeric value x ($x > 0$) entered there terminates the replication when this value has been reached after x seconds.
Entries per page	A timeout problem may occur if extremely large data amounts need to be replicated. In such a case you can use this entry to set the number of data records transmitted per transmission unit. A 0 means that all data records are to be transferred in one cycle. Any other numeric value limits the number of data records.
Replicate now	Via this button you can start this process manually. You can also achieve this by invoking a URL. See Section 13.2.2.4, "Replication Trigger for LDAP" , on page 936.
Schedule	If you do not specify a poll interval you can set a schedule instead. In this case you need to enable this button and generate a week profile in which the replication times are defined. Replication can be set in 15-minute steps for each weekday.

NOTE:

If replication is to occur via schedule and no settings have been made there, no replication takes place. No error message is put out on this.



After opening the schedule you can edit the replication times. The following tools are available:

Icon	Function
	Serves to arbitrarily enter replication times in the schedule.
	Selection tool for marking sections in the week profile.
	With the eraser function you can remove single replication times from the week profile. If an entire area has previously been selected with the selection tool, the replication marks within the marked area are maintained in case of replication mark deletion.
	Is used to define a replication time for a whole week if replication is to occur each day at the same time in the same interval. The intervals can be specified in the entry field next to this icon.

The New, Remove and Properties buttons

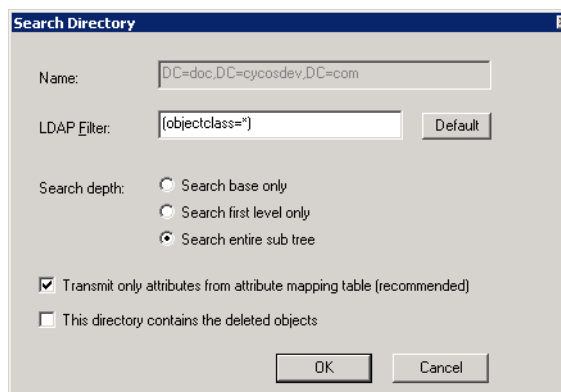
NOTE:

The options **New** and **Remove** are only required with manual configuration of a directory of the type *<Unknown>*. During a connection to a Microsoft Active Directory these features are automatically executed.

Via **New** further nodes (e.g. additional domains) can be integrated in the search directory list. The node to be added is integrated as subfolder under the previously selected folder. For this purpose the above dialog is opened as well to enable the name definition and the performance of the corresponding settings.

Via **Remove** you can hide entire directories or single directory entries in the display.

After clicking on **Properties** you can view and modify the search directory settings.



The settings for new nodes align themselves to three parameters required for searching by means of LDAP.

1. The **Name** specifies the **search base** or the starting point of the search run within the directory hierarchy. Under **Name** the search base is displayed as node of the DS branch or entered, if it is to be newly defined.
2. The **LDAP Filter** field specifies the **search filter** that determines the conditions for searching the data records (objects), so that special criteria can also be searched for. In the **LDAP Filter** field the search filter can be restricted to specific attributes. The default filter `objectclass=*` replicates all entries, though. Any complex logical filter¹ is conceivable. After changing the filter you can click on the **Default** button to switch to the `objectclass=*` filter again.
3. The **search area** indicates which part of the directory starting from the search base is to be searched. The search area can be set for the selected object via the **Search depth** option:
 - **Search base only**
Attributes of the users defined in the respective container object are replicated only.
 - **Search first level only**
The user attributes of the first level under the selected containers are replicated only.
 - **Search entire sub tree**
The entire sub tree is involved in the replication.

By means of the **Transmit only attributes from attribute mapping table** field you can define that only the entries listed on the **Attributes** tab are to be transmitted. This setting is recommended since it optimizes IP transmission (only attributes needed most are transmitted).

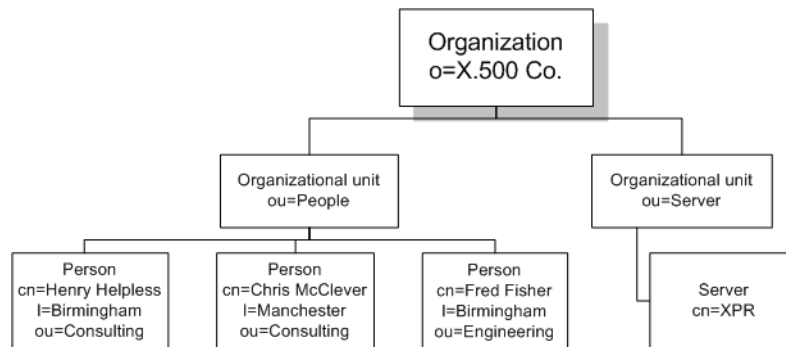
1. See also: Implementing LDAP, Mark Wilcox, Wrox Press Ltd. 1999, ISBN 1-861002-21-1

If the **This directory contains the deleted objects** field has been selected, the elements of the directory specified in the **Name** field are interpreted as “deleted” (in the DS “Deleted Objects”). Deleted means here that these objects are merely hidden.

The settings are copied with **OK**, **Cancel** terminates the previously described process without performing any modifications. Simultaneously you are taken back to the **Search** tab.

Example:

Based on the following graphic the search process is introduced as example.



In the process represented, all personnel data of the fictive company X.500 Ltd. in Birmingham are to be selected.

- The search base (Name) is: `ow=Persons, o=X.500 GmbH`
The search starts at the node `ow=Persons`
- Search filter (LDAP filter): `(&(objectless=Person)(l=Birmingham))`
All objects of type *Person* are taken where the attribute *l* (locality) has the value *Birmingham*.
- Search area (search depth): *Entire subtree*
The entire tree under `ow=Persons` is searched, this means also all possibly available deeper levels. Since in this model no deeper levels exist, the specification *First level* would also be possible.

As result two employees at site Birmingham are put out with their attributes.

Example: Only replicate a distribution list

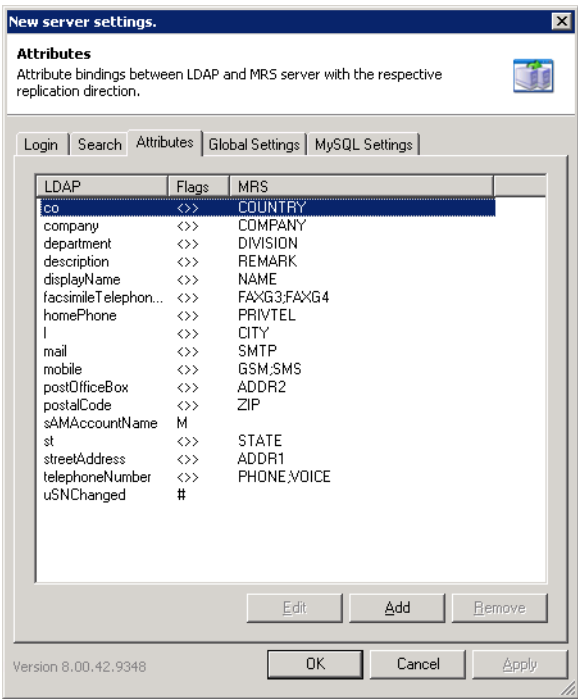
Instead of replicating all members of a CN or OU, you can also create a distribution list and then replicate only its members. This method is particularly simpler if the members are distributed in a security group or via the OU.

Enter the following string in the **LDAP Filter** field and select **Search entire subtree**:

```
(memberof=cn=unify,ou=unified users,OU=ITSupport,DC=xpr,DC=bg)
```

On the **Search** tab, select the topmost path, which should be the DC path. The LDAP APL is to search the entire customer domain from the top to find all users of the distribution list.

19.7.3 The "Attributes" Tab

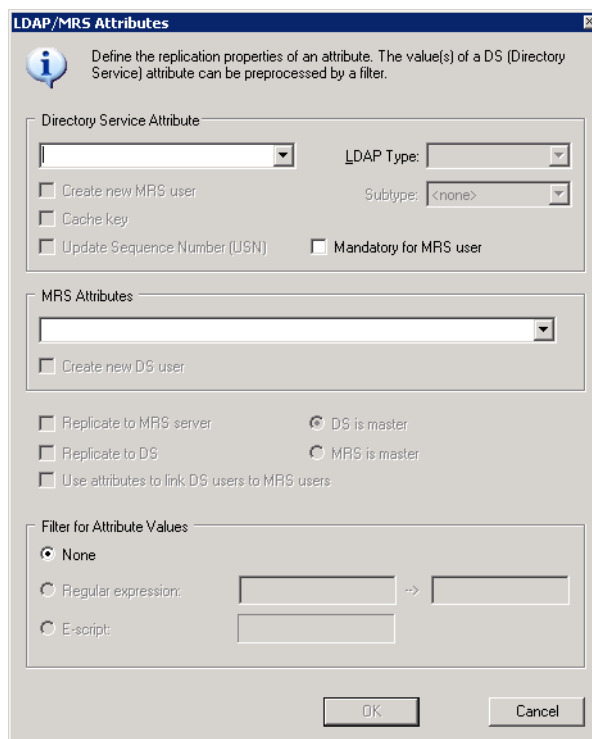


The central window of the **Attributes** tab lists the DS attributes, the corresponding XPR data fields and the set flags. They are already defaulted by way of basic configuration or configuration file import.

The “extensionData” attribute is of special significance. The XPR data fields assigned to this DS attribute are precisely the same fields that are to be found on the XPR settings tab. Another field can be added to the XPR settings tab by editing this attribute.

When you click on the **Edit** button, settings for selected attributes can be changed and via **Add** further attributes are selected, assigned and various attribute parameters set.

The following figure shows an empty mask for selection of a new attribute and its assignment to an XPR attribute. Different parameters such as the use of attributes, replication etc. are additionally set.



LDAP/MRS Attributes

Define the replication properties of an attribute. The value(s) of a DS (Directory Service) attribute can be preprocessed by a filter.

Directory Service Attribute

Directory Service Attribute: LDAP Type:

☐ Create new MRS user Subtype:

☐ Cache key

☐ Update Sequence Number (USN) ☐ Mandatory for MRS user

MRS Attributes

MRS Attributes:

☐ Create new DS user

☐ Replicate to MRS server ☒ DS is master

☐ Replicate to DS ☒ MRS is master

☐ Use attributes to link DS users to MRS users

Filter for Attribute Values

☒ None

☐ Regular expression: →

☐ E-script:

OK Cancel

The attribute to which the following settings relate is selected and displayed in a combo box in the **Directory Service Attribute** area. Next to this name field you find the data type in the gray **LDAP Type:** field. Thus you are informed whether the type is a string variable (**str**), an integer variable (**int**) etc. Thereunder, another field is placed to display the **Subtype:** if there is another differentiation in subtypes as e.g. in case of an Octets type.

The check boxes in this part of the window have the following functions:

Description	Function
Create new MRS user Flag: M	This attribute should be used when a new XPR user is to be created. The value of this LDAP attribute is used as user ID on the definition of new XPR users. If the Use attributes to link DS users to MRS users option is not active, the value also serves for directly linking a LDAP data record to the data record of an XPR user with this name.
Cache key Flag: K	Integrates an attribute in the cache (for faster access). An XPR user once found would be directly found via the cache key with each following search and his/her data were available faster.
Update Sequence Number (USN) Flag: #	The USN is an update ID that is upgraded to DS attributes with each search request by XPR attributes. When this check box is active, only data records having a larger USN-ID than the one generated with the last search run are replicated.

Description	Function
Mandatory for MRS user	Defines that this attribute is mandatory for an XPRuser. If this option is set, a user is only defined if the attribute is filled in. In other words, if the attribute entry is deleted, all users that do not have this attribute entry will be deleted with the next replication.

Thereunder, you find the **MRS Attribute(s)** list field for assigning the above selected DS attribute to the corresponding XPRdatabase field. All XPRdatabase fields are listed here so that each DS attribute can be mapped on each XPRfield.

The associated check box allows using this attribute if a **new DS user** is to be created (flag: D). This option is currently not available.

The check boxes coming next determine the replication direction. You can alternatively replicate to the XPRserver (**Replicate to MRS server**, flag: >), to the directory service (**Replicate to DS**, flag: <) or to both simultaneously (both characters are then displayed as flag: < >). If a reciprocal replication is desired, you need to define one of the two servers as the superordinate one. This is done via activation of the **DS is master** or **MRS is master** switches.

Through activating the checkbox **Use attributes to link DS users to MRS users** (flag ~) you can directly relate a DS user to an XPRuser via attributes. In this way you can create indirect links. For example, with DS attribute `proxyAddresses`, XPR attribute `EXCH` and activated option, all DS data of a user are assigned via the value of the DS attribute `proxyAddresses` to the XPRuser who has the same contents in the `EXCH` database field.

Via the switches you can set in the **Filter for Attribute Values** field you can manipulate the attributes in different ways. Depending on the complexity of the manipulation, this can either be done per filter or by an E-script. E-scripts are programs for establishing e.g. complex filters.

The following setting options are available:

Settings	Function
None	The filter function is deactivated.
Regular expression	This activates two entry fields for regular expressions. The entry field on the left hand side is for entering a regular expression, for which the attribute value must be valid. The entry field on the right hand side indicates, how this attribute value is to be replicated to XPR. This is particularly useful if an LDAP attribute contains more than one value. Here you can use a regular expression to directly filter out a specific value.
E-Script	Entry field for the name of the e-Script to be applied to the DS attribute.

Example

Definition example of an attribute's replication properties with usage of the **Regular expression** filter function.

The screenshot shows the 'LDAP/MRS Attributes' dialog box. The 'Directory Service Attribute' is set to 'proxyAddresses' and the 'LDAP Type' is 'str'. The 'MRS Attributes' section shows 'EXCH'. The 'Filter for Attribute Values' section has 'Regular expression' selected, with the expression 'MRS:%t' and the replacement '%1'. The 'Replicate to MRS server' checkbox is checked, and 'DS is master' is selected. The 'OK' and 'Cancel' buttons are at the bottom.

LDAP/MRS Attributes

Define the replication properties of an attribute. The value(s) of a DS (Directory Service) attribute can be preprocessed by a filter.

Directory Service Attribute

proxyAddresses LDAP Type: str

☐ Create new MRS user Subtype: <none>

☐ Cache key

☐ Update Sequence Number (USN) ☐ Mandatory for MRS user

MRS Attributes

EXCH

☐ Create new DS user

☒ Replicate to MRS server ☒ DS is master

☐ Replicate to DS ☐ MRS is master

☐ Use attributes to link DS users to MRS users

Filter for Attribute Values

☐ None

☒ Regular expression: MRS:%t -> %1

☐ E-script: AdRepl

OK Cancel

The entries in the above dialog have the following significance:

1. All entries of the directory attribute `proxyAddresses` are filtered.
2. The regular expression `MRS:%t` filters all character strings starting with `MRS :` and continuing with any character string. `%t` serves as wild card for an arbitrary, not empty chain of characters without blanks. The `%1` on the right hand side assumes the first parameter from the left hand side and hence corresponds to `%t`.

19.7.3.1 Regular Expressions

Several subpatterns can generally be specified in the regular expression of the left hand side. On the right hand side the n-th subpattern of the left hand side can then be selected with `%n`.

The length of the adapted character string can be restricted by inserting `[x]` directly after the `%` character. `x` corresponds to the maximum length of the adapted character string here. Example:

```
MRS:%t/%d -> %[4]1\\%2
```

This regular expression adopts up to four characters after the `MRS :` and attaches a `\` to these. Finally, all digits that follow the `/` on the left hand side are attached.

The following example is to filter each value with 3 digits minimum and adapt the last three digits of this value. Finally, these 3 digits are preceded by an 8.

```
[0-9]*<[0-9]{3}> -> 8%1
```

IMPORTANT:

Please note the specific meaning of some characters such as the `%` character on the right hand side. To deactivate the specific meaning of these meta characters, you must precede them with a `\`.

Further information about regular expressions can be found in [Section 7.4.4.1, "Regular Expressions", on page 248](#).

The settings performed become valid with a click on **OK** and you are simultaneously taken back to the **Attributes** tab. Newly selected and edited attributes are added at the bottom of the list.

19.7.3.2 E-Script

If you are provided with a developer package for E-scripts, you can make further modifications. Please consult Professional Services on this, which you can reach via your sales partner.

The E-script exports 2 features for the LDAP APL:

```
export int NewMrsUser(const char *user)
{
}

export int FilterLdapAttribute(const eatt_t *pA, const vals_t *pV, unsigned *pf)
{
}
```

The feature `NewMrsUser` is invoked for each XPR user that is newly created and is to set some default values such as `PASSWORD`, `PIN`, `GROUP`, etc.

The filter feature is invoked for each LDAP attribute where the **filter for attribute values** is set to **E-script**. It enables any edition of this value. This also includes setting default values, if the LDAP attribute should be empty. In the default script `ExRepl.e` detailed examples for some cases are given.

Example of setting a default value for the LDAP attribute `mail`:

```
export int FilterLdapAttribute(const eatt_t *pA, const vals_t *pV, unsigned *pf)
{
    char defaultMail[] = "xyz@nowhere.un";

    match ( &me, pA->name ) {
    case "mail":
        if ( strlen(pV->u.sv[0]) == 0 )
            cb_addvalue(sizeof defaultMail, defaultMail);
        }
    }
```

19.7.3.3 Extending XPR Attributes

Another example shall explain how to add new fields to the user data (in “Active Directory Users and Computers”) on the **MRS Settings**² tab.

IMPORTANT:

If additional XPR attributes are defined here for the DS server, data replication to the XPR server may lead to the deletion of XPR-significant data fields. When you replicate an empty XPR data field, it probably deletes (overwrites) a data field filled in.

Therefore, MRS data fields must not be left empty when defining a user.

1. For this purpose select the **Set Options** function in the XPR monitor under LDAP APL.
2. Next, mark the desired server in the list of possible LDAP servers and enable the **Properties** button.
3. In the opening window **Edit server settings** switch to the **Attributes** tab and select the **extensionData** entry from the attributes list.
4. After clicking **Edit** all entries of the **extensionData** directory attribute are displayed in the **LDAP/MRS Attributes** dialog.
5. From the selection window for **MRS Attribute(s)** a data field can now be selected via the associated checkbox. With a click on **OK** the attribute is additionally integrated in the user settings of **Active Directory Users and Computers**.

Cancel terminates the process and modifications already performed are disregarded. A click on either button simultaneously takes you back to the **Attributes** tab.

If the attributes are defined by the configuration file, then these are listed on the **Attributes** tab with the already existing assignment to the XPR system. This means that the relevant XPR data field assigned to the attribute shown is displayed. There are various flags between the attribute name and the XPR data fields which already provide information about how certain attribute or replication parameters are set. In detail the following flags or a combination of flags can be set:

Flag	Significance for the selected attribute
M	The attribute is used when a new XPR user is to be created.
D	The attribute is used when a new DS user is to be created. This option is currently not available.
K	Integrates an attribute in the cache (for faster access).

-
2. This configuration tab is added by installing the MMC SnapIn.

Flag	Significance for the selected attribute
#	This flag indicates that the search run is only performed from the last replicated records.
<	Replicates this attribute to the DS server (XPR as master). This setting can be used for example if a new Microsoft Exchange server is to be docked to an existing XPR server. All XPR data are then replicated into the AD.
>	Replicates this attribute to the XPR Server (DS is master).
<>	Replication in both directions.
<>>	Replication in both directions with AD as master.
<<>	Replication in both directions with XPR as master.
~	This flag shows that the directory service user is linked directly with an XPR user by means of the attribute.

The **Edit** button enables the modification of the attribute parameters of a selected entry at a later date. When you click it, the **LDAP/MRS Attributes** dialog opens with the entries made for the selected attribute. You can adapt entries and save them as described above.

19.7.3.4 Attribute Settings for additional LDAP Servers

As attributes for additional LDAP servers, e.g. additional subordinate domains, are not automatically preset, they must be configured as follows:

1. Select the first server in the **LDAP Servers** window and export its settings to a file by means of the Export button. The changes for the new server must now be made in this file.
2. Open this file with the editor, modify the entries for the DC domain controller and for the containers CN and possibly OU to be replicated. Back up the changes in a file.
3. This file is now imported in the **LDAP Server** window. In the following the same specifications are demanded for the new server as already described in [Section 19.7.1, “The “Login” Tab”](#). The **Search** and **Global** tabs must now be additionally filled in. Enter the same settings here as for the first server.

19.7.3.5 Multivalue-Field Specials

A user database field can include several values via the MULTI attribute. This is used, for example, to assign several phone numbers to a user but only one mailbox. With such fields the first entry is stored in the primary field (e.g. `PHONE`) and all further entries in the associated fields with the corresponding numbering (e.g. `PHONE.01`, `PHONE.02`, etc.). For such multivalue fields there is, besides the primary field, another one with attached “.” (e.g. `PHONE` and `PHONE.*`), which is offered for replication and represents exclusively the non-primary fields.

On the directory service side a differentiation is also made between attributes that can only include one value (e.g. `telephoneNumber` with Active Directory) and such attributes that can host several values (e.g. `otherTelephoneNumber` with Active Directory).

The following types of replication for multivalue fields can be configured:

- LDAP single value to XPR multivalue field.
The single value is written in the primary field.
Example: `telephoneNumber` to `PHONE`
- LDAP multivalue to XPR multivalue field.
All values are written in the XPR multivalue field 1:1.
Example: `otherTelephoneNumber` to `PHONE`
- LDAP multivalue to XPR multivalue field.
All values are written in the XPR multivalue field. The primary field remains untouched. Example: `otherTelephoneNumber` to `PHONE.*`

19.7.3.6 Dial Number Replication Restrictions

For dial numbers there is the normalized field with `DNO` attribute and the legible one with `DNOREAD` attribute each. The last mentioned field always receives the same name with attached `#` character as the one with the `DNO` attribute according to convention. Replication of fields with `DNOREAD` attribute is not supported. The normalized format must be replicated at any rate.

19.7.3.7 Excluding Fields from Replication

Via the registry value [MRS-NonSyncAtts \[REG_MULTI_SZ\]](#) you control whether modifications performed to attributes in the LDAP directory are to be copied to the database only in case of initial attribute creation. This can be useful for the `PASSWORD` respectively `PIN` fields. The PIN can, for example, be changed via a TUI or the Web Assistant. After the recreation the PIN changed by the user should not be overwritten by the directory service anymore.

19.7.3.8 Creating Fields with Default Values

Via the [DefaultMRSValues \[REG_MULTI_SZ\]](#) registry value you can input a default value for XPR attributes that must be filled in but are not to be maintained by the LDAP directory. You can thus default, for example, a value for the PIN attribute, which is written upon the creation of new users.

19.7.4 The “Global Settings” Tab

Modify server settings.

Global Settings
Global settings for attributes, e.g. you can set one side to 'read-only', or use a previous USN, to repeat replication.

Login | Search | Attributes | **Global Settings** | MySQL Settings

Directory Service (DS)

- ☒ Write changes to DS
- ☒ Save USN

USN:

MRS Server

- ☒ Write changes to MRS
- ☒ Save Update ID
- ☒ Create new user in MRS
- ☐ Delete users from MRS

Update ID:

E-Script

Name:

Tenant

Name:

Version 8.00.42.9348

OK Cancel Apply

On the **Global Settings** tab additional, more detailed settings can be performed.

This tab is divided into three portions.

- Settings referring to the Directory Service,
- Settings that concern XPR.
- A selection window to invoke an E-script.

The settings in the **Directory Service (DS)** and **MRS Server** portion are performed analog for the directory service and XPR side.

Field	Meaning
Write changes to DS or Write changes to MRS	Modifications can either be saved in the directory (DS), in the XPR system (MRS) or in both.
Save USN or Save Update ID	With the modifications copied by closing the LDAP settings the USN (Update Sequence Number) and/or the UID (Update ID) is upgraded. Here you can determine whether this is desired for one of the two or for both. The corresponding values are stored in the registry. Both IDs make sure that replication processes performed at a later date can start from a certain flag rather than all over again.
Create new user in MRS	New users in the directory can also be created on the XPR server.

Field	Meaning
Delete users from MRS	Via this check box, deleting of user entries can optionally be suppressed (removing the tick) for test purposes as well. If no folder exists for deleted objects and no attribute has been set as cache key , deletion of the XPR users does not work. In such a case the LDAP APL cannot recognize whether the XPR user has been created by replication from the directory service or by direct generation on the XPR server. Since the LDAP APL in the latter case must not delete the XPR user, deletion always remains undone. Remedy is produced by setting one of the attributes as cache key .
Entry fields: USN and Update ID	By means of these entry fields replication can be started from a certain USN or update ID. In doing so it should always be clear what has been replicated with the entered UID or update ID.

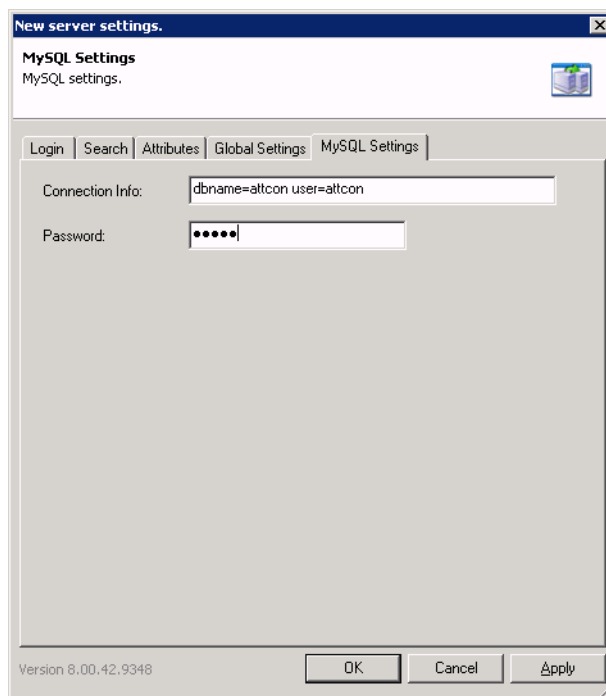
The **E-Script** section serves for selecting an E-script that can be used for automatically editing the attributes. The active E-script “AdRepl” sets the predefined values for the standard replication in case of an Active Directory connection without Microsoft Exchange.

An E-script may act as complex filter via which, for example, a phone number normalization can be performed. Also special actions for creating a new XPR user are enabled. Selection of e-scripts is performed via the pull-down list. E-scripts already available are usually in the `<XPR Install>\res\ldap` directory.

The **Tenant** section enables the selection of a tenant within a multi-tenant system. Using the LDAP APL you can bind an Active Directory to a tenant. You find a precise description of the function and structure of multi-tenant systems in the **Multi-Tenant** section of the *Multi Tenancy* manual.

19.8 The “MySQL Settings” Tab

Here you can enter the user entries for the *Attendant Console* by Ostertag Systemhaus via the LDAP APL in the MySQL database used by the *Attendant Console*.



To this, specify in the **Connection Info** field the database table and the user for access to this database table of the MySQL database used by the *Attendant Console*.

The format is: `dbname=<database> user=<User ID>`

Further parameters allowed in the **Connection Info** field are `host` and `port`. Please heed the syntax, since e.g. `Port` or `User` would lead to an error. The MySQL table used is always the `tab_names` table defaulted by the *Attendant Console*.

In the **Password** field enter the password of the just specified user in hidden form. This password is required to access the MySQL database.

The connection occurs directly via the MySQL API library, no ODBC drivers are needed. If this connection is configured, replication is performed exclusively with the MySQL database. You do not find this data in the Correlation then!

19.8.1 Assigning Attributes

Owing to an architectural restriction, the MySQL fields cannot be assigned via the **Attributes** tab, since the GUI always accesses the Correlation database there. The assignment must therefore occur manually in the [AttributeMap \[REG_MULTI_SZ\]](#) registry value. A possible assignment of the LDAP attributes `telephoneNumber`, `givenName` and `sn` would be e.g.:

```
uSNCreated:IDPHONE:0,str:toM,cor,key,mstM:none  
uSNCreated:VAR1:0,int64:toM:none  
givenName:FIRSTNAME:0,str:toM:none  
sn:LASTNAME:0,str:toM:none  
telephoneNumber:PHONE:0,str:toM:none
```

An LDAP attribute must be assigned to the `IDPHONE` field. This assignment must be marked as `cor`. In this way this field is used to link the LDAP users to the MySQL users.

Assignments to the MySQL fields `PHONE`, `LASTNAME` and `VAR1` are mandatory. Each combination of these fields must be unique. This restriction results from the definition of the table schema of the MySQL database.

If you execute the assignment as described here, set the **LDAP filter** to `(objectclass=person)` on the **Search** tab of the **Properties**.

19.9 LDAP and MWI

The notification APL must be informed about a user's MWI settings. The administrative clients *Web Assistant* and *Communications* have an implemented functionality for creating users with working MWI settings.

The LDAP APL and its replication mechanism cannot be considered administrative client in this sense, though. It establishes a 1:1 assignment between a directory and the XPR server. There is no default for a special handling of user data for notifications. Therefore, no MWI is active in case of replicated users.

To activate the telephone LED as MWI for users, we recommend an additional link between the phone number and the CIT field via a rule of the following type:

```
telephoneNumber:CIT:0,str:toM:rule:"%t":MWI/%1
```

With this strategy you can establish different connections with the LDAP APL to, for example, configure MWI only for a special group of people.

19.10 Configuration in Connection with the Netscape Directory Server

The following descriptions only refer to the LDAP APL settings in the XPR system. For the Netscape Directory server configuration the corresponding administration manuals must be referred to. The LDAP APL configuration with other directory services mostly concerns the settings in the **Login** configuration dialog.

If you have an LDAP APL configuration file you can import it in the **Login** window to copy specific presettings. The advantage is that you need not modify or fill in each field and add each single attribute for replication yourself. You cannot use any Microsoft Exchange or Active Directory configuration file, because the attribute descriptions are partly different from those of the Netscape Directory server.

On the **Login** configuration dialog you need to change the **Directory type**, the **Authentication type** and the **User name**. The other specifications correspond to your specific values. The significance of these fields can be gathered from [Section 19.7.1, "The "Login" Tab", on page 1136](#).

Field	Entry
Directory type	For Netscape Directory server select the DirX entry.
Authentication type	For Netscape Directory server select the SIMPLE entry.
User name	With defining the authentication type SIMPLE you need to enter your user name as Distinguished Name (DN). Example: uid=admin,ou=administrators,ou= =TopologyManagement,o=NetscapeRoot

The field for the domain is gray and cannot be modified, since with specifying the authentication type **SIMPLE** the domain need not be indicated.

In the other configuration tabs you need to perform the settings according to the explanations in the previous [Section 19.7, "LDAP Settings", on page 1134](#).

On the **Search** tab you need to enable the **Properties** button and enter the search base under **Name**. With the initial search you should enter the topmost node of your directory structure, so that the entire structure is introduced to the system. This would be for example: `DC=Servername,DC=local`.

IMPORTANT:

Make sure that the **Pollintervall** receives a value greater 0.

On the **Attributes** configuration tab no attributes are displayed for mapping, if you do not have an lcf configuration file that imports presettings. Attributes for mapping can be generated via the **Add** button ([Section 19.7.3, "The "Attributes" Tab", on page 1144](#)). Before you can add the attributes, you need to **Query DS**

Attributes in the **Login** tab.

NOTE:

If you do not use a configuration file for the import of presettings you need to enter attributes yourself. Make sure that you configure an attribute that defines new XPR users. With Netscape DS select the **nsUniqueID** attribute and select **Create new MRS user** with a tick. The attribute receives in the list flag **M**.

You can check your entries by enabling the **Test Connection** and **Query DS Attributes** buttons on the **Login** tab. The **Replicate now** button on the **Search** tab can be used for testing the configuration and the successful connection as well. Reports that confirm the successful replication or error reports appear in the **XPR monitor**.

19.11 LDAP APL Configuration without Microsoft Exchange

The LDAP APL configuration and replicating data from the Active Directory without a Microsoft Exchange server connection can be done offhand. There is a `AdRepl.lcf` configuration file in the `<XPRinstall>\res\LDAP` directory that you can import in the **Login** tab. In this way you can insert specific presettings such as a certain number of attributes in the LDAP APL for replication.

On the **Login** configuration tab, leave the settings as with configuring using a Microsoft Exchange server. The **Directory type** remains `Active Directory` and the **Authentication type** `NTLM`. The significance of the other fields is explained in [Section 19.7.1, “The “Login” Tab”, on page 1136](#).

On the **Search** tab you need to enable the **Properties** button and enter the search base under **Name**. With the initial search you should enter the topmost node of your directory structure, so that the entire structure is introduced to the system. This would be for example: `DC=Servername,DC=local`. The structure of the directory is copied when you close the configuration and editing tab with **OK** and open them again by means of **Edit settings**. [Section 19.7.2, “The “Search” Tab”, on page 1138](#) explains the significance of the fields.

IMPORTANT:

Make sure that the **Pollintervall** receives a value greater 0.

On the **Attributes** configuration tab only attributes are displayed for mapping that you have imported by means of the `AdRepl.lcf` configuration file. Further attributes for replication can be generated via the **Add** button ([Section 19.7.3, “The “Attributes” Tab”, on page 1144](#)).

On the **Global Settings** tab assign the `adrep1` value to the **E-Script** field, which sets predefined values for the direct connection to the Active Directory. The `ExRepl` value is intended for a Microsoft Exchange connection and should not be set for this reason.

Further settings under **Global Settings** have not been made and can be activated with a tick. For the field significance refer to [Section 19.7.4, “The “Global Settings” Tab”, on page 1153](#).

You can check your entries by enabling the **Test Connection** and **Query DS Attributes** buttons on the **Login** tab. The **Replicate now** button on the **Search** tab can be used for testing the configuration and the successful connection as well. Reports that confirm the successful replication or error reports appear in the **XPR monitor**.

19.12 Monitoring the LDAP APL Activities

Via the XPR monitor you can precisely observe which actions are currently carried out by the LDAP APL. The following short instruction shows you the path to this display:

1. Generate a new log window.
1. In the XPR monitor drag the  gearwheel icon  LdapApl from the <Topics> branch of the “Modules of <<XPR server name>” dialog to the log window you have created.
2. In the **Logging display properties** dialog now open you need to set the data you want to have displayed.
3. Verify the settings via the apply button.
4. Then confirm with OK.

The selected LDAP APL activities are now logged in your log window.

Further setting options are introduced in [Chapter 6, “XPR Monitor”](#).

19.13 Secure LDAP Connection

19.13.1 Prerequisites

19.13.1.1 General Prerequisites

The certificate should be issued by a CA that the domain controller and the LDAPS clients trust. Trust is established by configuring the clients and the server to trust the root CA to which the issuing CA chains.

NOTE: The prerequisites apply to both Domain Controller and Xpressions.

19.13.1.2 Domain Controller

To enable LDAPS, you must install a certificate that meets the following requirements:

- The LDAPS certificate is located in the Local Computer's Personal certificate store (programmatically known as the computer's MY certificate store).

- A private key that matches the certificate is present in the Local Computer's store and is correctly associated with the certificate.
- The private key must not have strong private key protection enabled.
- The Enhanced Key Usage extension includes the Server Authentication (1.3.6.1.5.5.7.3.1) object identifier (also known as OID).
- The Active Directory fully qualified domain name of the domain controller (for example, DC01.DOMAIN.COM) must appear in one of the following places:
 - The Common Name (CN) in the Subject field.
 - DNS entry in the Subject Alternative Name extension.

NOTE: You must use the Schannel cryptographic service provider (CSP) to generate the key.

For more information please visit:

<https://support.microsoft.com/en-us/help/321051/how-to-enable-ldap-over-ssl-with-a-third-party-certification-authority>

19.13.1.3 Xpressions

On Xpressions you have to modify the following LdapApl Server settings at **Login** tab:

- **Ip Address:** use the FQDN instead of an IP Address
- **Port Number:** mark the Secure Box

19.14 The RFCs

The following RFCs specify version 3 of the LDAP³. XPR uses the LDAP API, which was originally defined by Netscape and also provided by Microsoft for Windows. The following RFCs are only supported insofar as this support occurs by the LDAP API.

19.14.1 RFC 2251: Lightweight Directory Access Protocol (v3)

The LDAP described in this document is designed of the access to a X.500 directory without requiring the resources of a X.500 Directory Access Protocol (DAP). This protocol aims most of all for the management and browser applications to enable the read/write access to directories. When this protocol communicates with a directory service that addresses an X.500 protocol, it is to be considered a complement to the X.500 DAP.

19.14.2 RFC 2252: LDAP: Attribute Syntax Definitions

The contents of the AttributeValue fields in the protocol elements are required as Octet strings. This document defines a syntax set for LDAP v3 and the rules according to which attribute values are represented as Octet strings by these syntaxes. This document defines attribute types that support LDAP server.

19.14.3 RFC 2253: LDAP: UTF-8 String Representation of Distinguished Names

In an X.500 directory, *distinguished names* (DN) are used as primary keys to enable entries in the directory. *Distinguished Names* are coded in the X.500 protocol in ASN.1. This string representation should be used in LDAP as well. This specification defines a string format to represent names based on commonly used names and capable of representing each DN.

3. The RFCs can be found under the URL <http://www.ietf.org/rfc.html>.

19.14.4 RFC 2254: The String Representation of LDAP Search Filters

The LDAP protocol defines a presentation of search filters that can be transferred to a LDAP server. Some applications may find it useful to employ a common way of presenting such filters in a legible format suitable for humans. This document therefore defines a string format legible for humans for LDAP search filters. Beyond that this document replaces RFC 1960.

19.14.5 RFC 2255: The LDAP URL Format

This document describes an “LDAP Uniform Resource Locator Format”. This format describes LDAP search operations to retrieve information from an LDAP directory. This document replaces RFC 1959. Furthermore, it renews the LDAP URL format for LDAP/v3.

19.14.6 RFC 2256: A Summary of the X.500 User Schema for use with LDAPv3

This document offers an overview of the attribute types and object classes that were defined by the ISO and ITU-T committees in the X.500 protocol. Here, those are particularly considered that are used for the directory clients. This is surely the scheme for LDAP/X.500 directory used most. This document contains neither attributes for the administration of X.500 servers nor attributes handled by other ISO/ITU-T documents.

20 HiPath User Management

20.1 The HiPath User Management

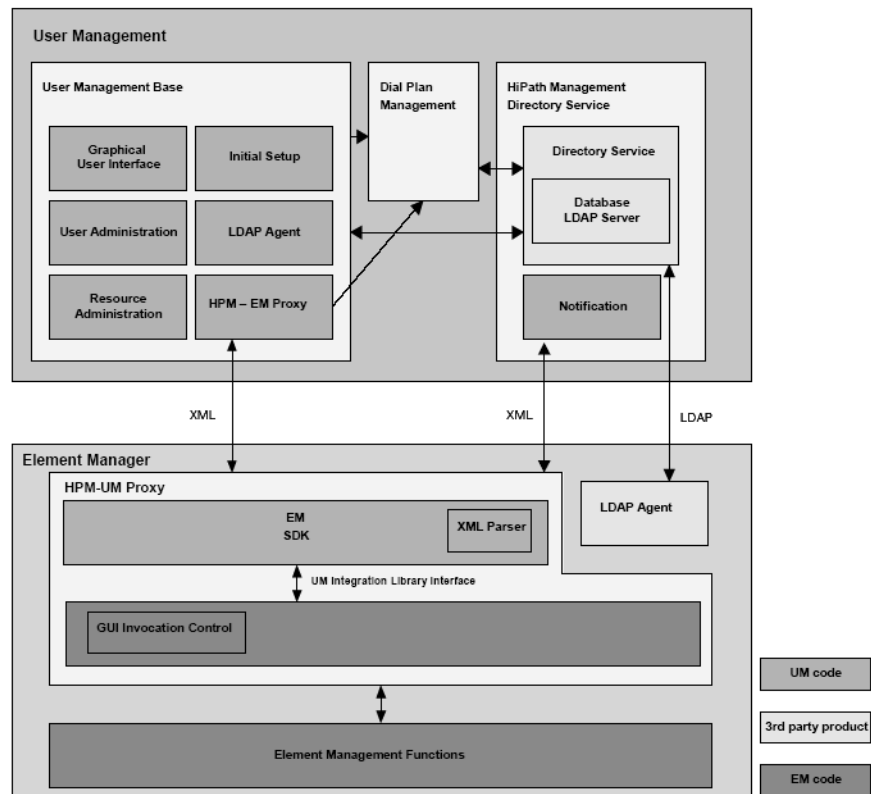
With the help of the **HiPath User Management System** (HPM-UM), user data can be administered and stored independently from their data format. The HPM-UM has mostly been designed for very large communication networks to enable an efficient, decentralized control of the user administration. The HPM-UM is configured in XPR with the help of the HPM APL. The following table shows the most important components of the HPM-UM.

Component	Description
HPM-UM Base	Provides the basic functionality of the user and resources administration. A graphic interface is provided for the execution of operations and requests. An element manager (EM) proxy enables the connection to the element managers, whereas an LDAP agent establishes the connection to the directory service.
Element Manager	For each HiPath platform of the network there is a specific module, the Element Manager, via which the respective platform is configured and monitored. Examples are the HiPath 3000 Manager and the HiPath 4000 Manager. The XPR system is also an element manager as component via the HPM APL. Tasks that all element managers have in common are compiled under the HiPath Management Applications module. This includes the HiPath Fault Management for network monitoring and the HiPath Accounting Management responsible for the cost input.
EM SDK	The Element Manager Integration SDK synchronizes the HPM-UM Base and element managers. Modifications in the HPM-UM Base are passed on to the element managers and vice versa, so that the data of both components are always up-to-date.
Directory Service	The directory service serves for saving and retrieving user data. It can either be integrated in the HPM-UM system or connected as component from another supplier (e.g. Microsoft Active Directory). The LDAP protocol connects an external directory service with the HPM-UM Base and with the Element Manager.
LDAP Agent (optional)	An LDAP agent exists in the HPM-UM Base and the element managers, if the integrated directory service is not used.

Table 58 Components of the HiPath User Management Systems

Fast communication with the element managers allows the assignment of the most various resources to the users. The resource types are, for example, the telephone number, the fax ID and the e-mail address. These resources represent a user and are called mailbox.

The HPM-UM system is not only compatible with HiPath products, but also to other suppliers, so that the provision and co-ordination of user data is ensured.



The figure is a rough overview of the HPM-UM system structure. The **User Management Base** serves for administering the user data filed in the **Directory Service**. The Directory Service does not need to derive from the HiPath group but can also be a third-party product, such as the Microsoft Active Directory. User data from the UM system can thus be imported into the Directory Service or exported.

The single user resources are saved in the **element managers**.

20.2 Definition and Function of the HPM APL

IMPORTANT:

Up to now, creating, removing and modifying user information has only been possible from the HPM-UM system to the XPR system. User data replication from the HPM APL to the HPM-UM system is only possible manually. See [Section 20.5, “The Connection of XPR Server and HPM-UM”](#).

The **HPM APL** has been conceived to integrate the XPR server in the **HiPath User Management System** (HPM-UM). Since this application serves an efficient and clear decentralized administration, it has been created for immensely large systems.

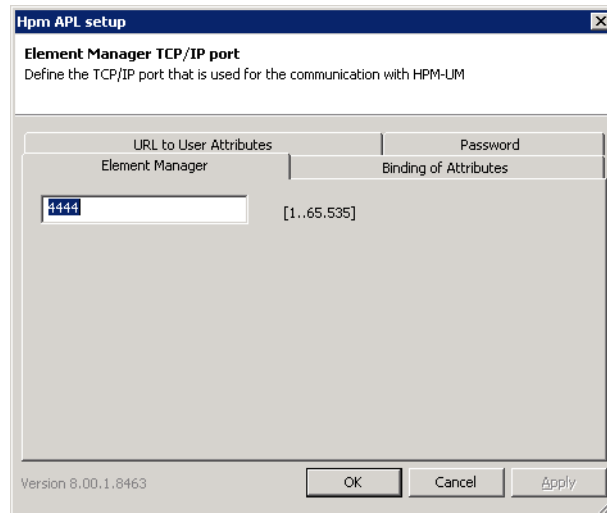
The HPM APL operates as an HPM-UM element manager between the XPR server and the HPM-UM system. It accepts requests from the HPM-UM server and returns the requested data. The HPM APL communicates with the XPR server to create users with all required data, modify or delete them. The data are either user-defined information and resources or notifications. The respective resources are called **mailbox** in the HiPath User Management.

From the XPR server's point of view a mailbox can either be a telephone number or the voicemail system assigned to a user (PhoneMail or VMS). Several mailboxes can be assigned to an XPR user. This assignment is automatically stored in the database field PHONE. This field should not be changed manually.

20.3 Configuration

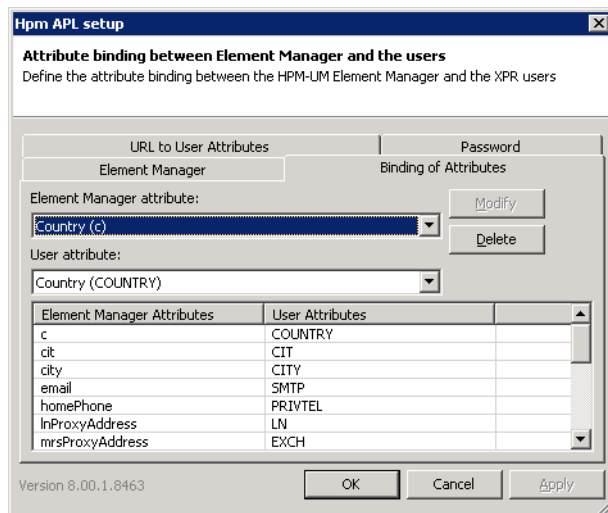
Open the HPM APL configuration as usual via **Set Options** in the XPR monitor.

20.3.1 Element Manager



This tab only provides a single field for entering the **port number** of your HPM APL. You establish the connection between your HiPath User Management and the HPM APL as element manager with the help of this port number. That means the port number must correspond to the HiPath User Management configuration.

20.3.2 Binding of Attributes



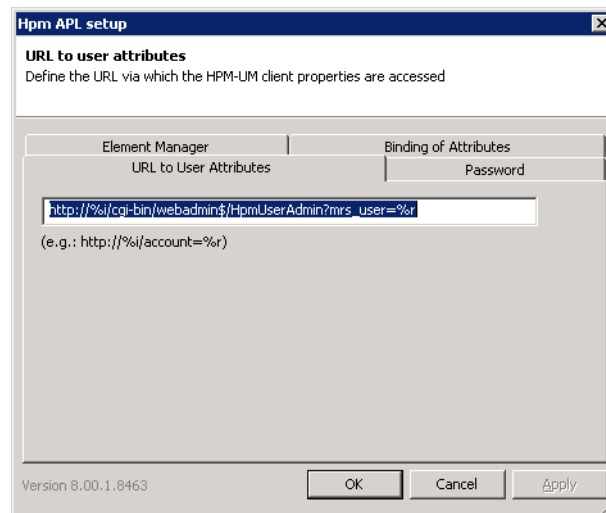
In this window you can synchronize the user attributes in the Element Manager of the HPM-UM system with those in the XPR system. The HPM-UM acts as master. Changes on the XPR server side are thus not transmitted to the HPM-UM and will be overwritten during the next synchronization.

Some attribute assignments that you can modify, delete or supplement are already defaulted in the list. Select the corresponding pair of attributes in the list. Both attributes appear in the two fields above the list. Using the scrollbars you can now select predefined values in both windows and refer them to each other. You can select only attributes though that have not been linked to another attribute yet, since otherwise no unique assignment could be assured.

A click on the **Modify** button either changes already existing assignment pairs or creates new ones. Enabling the **Delete** button removes the selected attribute pair.

The modifications do not become valid until the **OK** or **Apply** button is clicked.

20.3.3 URL to User Attributes



This tab provides the possibility to set a URL to invoke the **Web Assistant**. In this way you can open the corresponding information about a certain user from within the HPM-UM in the Web Assistant. Enter the valid address of your Web Assistant to be provided with this function. The default settings are normally sufficient. Only more complex systems with a Web APL on a satellite require an adjustment.

There are different variables that are charged by the HPM-UM:

- %i represents the IP address of the resources manager. This is the system the HPM APL is running on.
- %r represents the resources ID and is transferred as user ID.
- %s stands for the network name of the resources manager computer. When this variable is saved in the HPM APL, it is already stored as IP address.

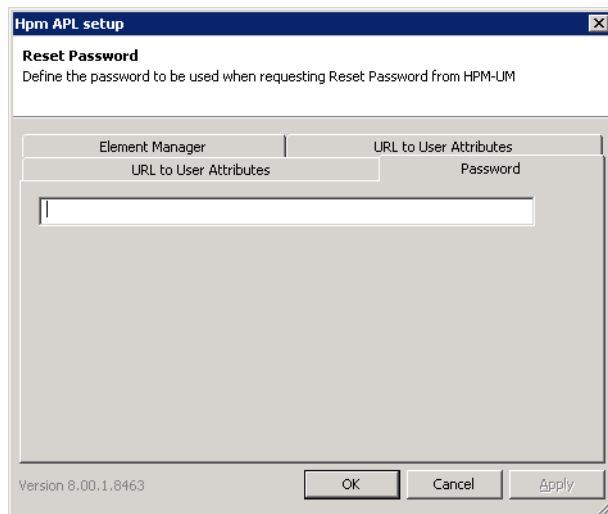
IMPORTANT:

If the Web APL is installed on a satellite system, the fixed IP address must be entered instead of the variable %s.

With a click on **OK** or **Apply** the modifications become valid.

20.3.4 Password

IMPORTANT: This configuration tab is only relevant to HpmApl connections to legacy HPM-UM (Hipath Management - User Management) systems. It has no effect when connected to UC systems.



This password is set for a user, if the **Reset Password** option is invoked for a user in the HPM-UM.

20.4 Attributes

The following is a list of the attributes used. The only mandatory attribute is `NAME`, whereas all other attributes are optional.

Attribute Name	XPR Name	Description
SN	NAME	Name of the user.
l	LANGUAGE_ID	Language selection
ou	COMPANY	Company
org1	DIVISION	Department
street	ADDR1	Street
postalcode	ZIP	Zip code
st	STATE	State
C	COUNTRY	Country
homephone	PRIVTEL	Private telephone number
xprCostInfo	COSTINFO	Information on cost centers/charges

Attribute Name	XPR Name	Description
xprConUser	CONUSER	For ComAssistant integration. See <i>Unified Communications Act Now</i> manual.
xprTimezone	TIMEZONE	Time zone

20.5 The Connection of XPR Server and HPM-UM

20.5.1 Replication Directions

Regarding replication you need to differentiate between two options. On the one hand there is the replication from one HPM-UM to an XPR server and on the other hand the one from an XPR server to an HPM-UM. The first option is effected automatically, whereas the second one needs to be performed manually.

The automatic replication direction runs from the HPM-UM to the XPR server. To be more precise, user data are automatically transferred from the HPM-UM to the XPR server and maintained there. If you have an HPM-UM and configure an additional XPR server, all user data of the HPM-UM is transferred to the XPR server via the system.

Vice versa user data from an XPR server to an HPM-UM can only be transferred manually. If thus an XPR server already exists and you install an HPM-UM, you have to upload all user data manually from the XPR server to the HPM-UM. See [Section 20.5.2, “Transferring User Data from the XPR Server to the HPM-UM”](#). Likewise, you need to manually transmit data from XPR to the HPM-UM, if further directory services are connected to the XPR server. This could be, for example, Lotus Domino or an Active Directory. Data replication between XPR server and a directory service may occur bi-directional, i.e. data are automatically replicated between XPR and directory service in both directions. User data are transferred to the HPM-UM only manually, though.

For this reason we recommend to create and maintain user data exclusively in the HPM-UM. In this way the XPR server and possibly further directory services are automatically updated.

20.5.2 Transferring User Data from the XPR Server to the HPM-UM

If you have already set up an XPR server and install an HPM-UM, you need to upload all user data manually from the XPR server to the HPM-UM. Only then will the user data be available in the HPM-UM. An automatic replication from XPR to HPM-UM does not take place.

The manual transmission from an XPR server to HPM-UM will be described in the following section. If the user data in the XPR server and in the HPM-UM have the same up-to-dateness, we recommend to exclusively use the HPM-UM for user data maintenance in the future. This will automatically adjust the data in the XPR system.

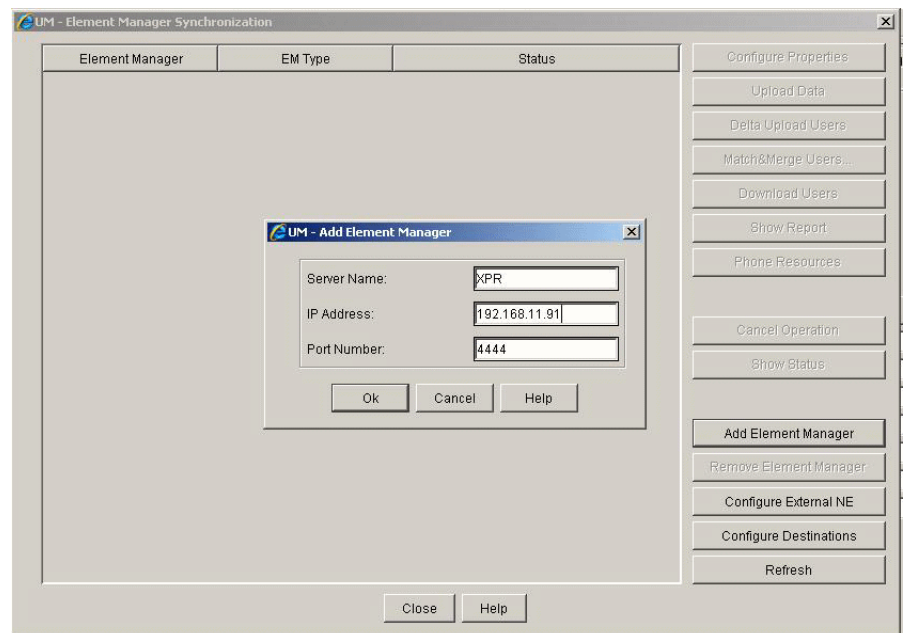
NOTE:

For information about setting up, configuring and operating the HiPath User Management, please consult the associated operating instructions for the administrator.

This feature is executed via the graphic user interface (GUI) of the **HPM-UM**, so that you need to start the GUI. You start the HiPath User Management via the **HiPath Desktop**.

The XPR server is connected to the HPM-UM via the **Element Manager Synchronization**. This setup window is opened via the **Tools** menu. Perform the following steps to configure a new element manager:

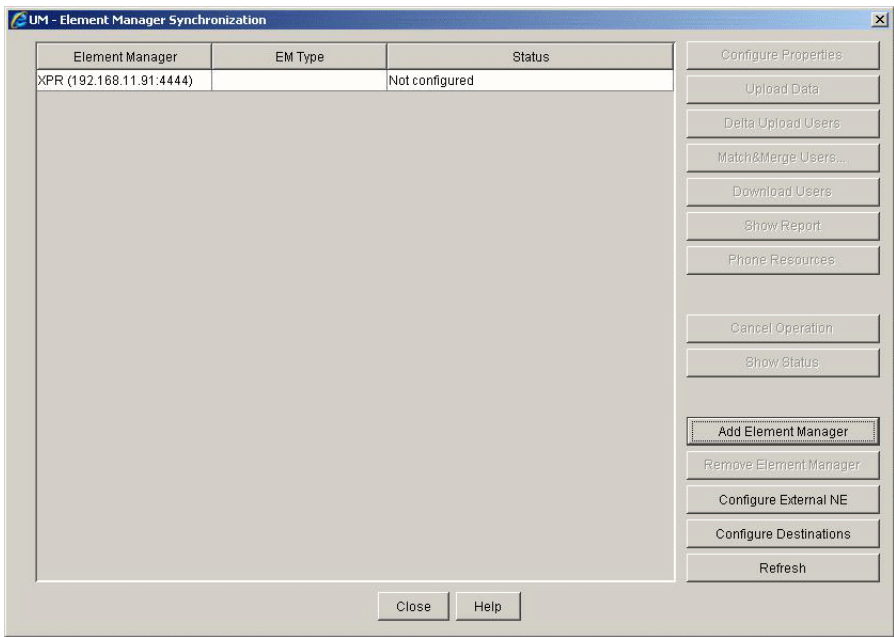
1. A list with the element managers connected so far appears. To add the XPR server as element manager, click the **Add Element Manager** button.



2. Another dialog opens in which you enter the **Server Name**, the **IP Address** and the **Port Number**. The port number corresponds to the entry that you have performed in the **Element Manager** tab in the configuration pages of your XPR server's HPM APL. The port number used is normally 4444.

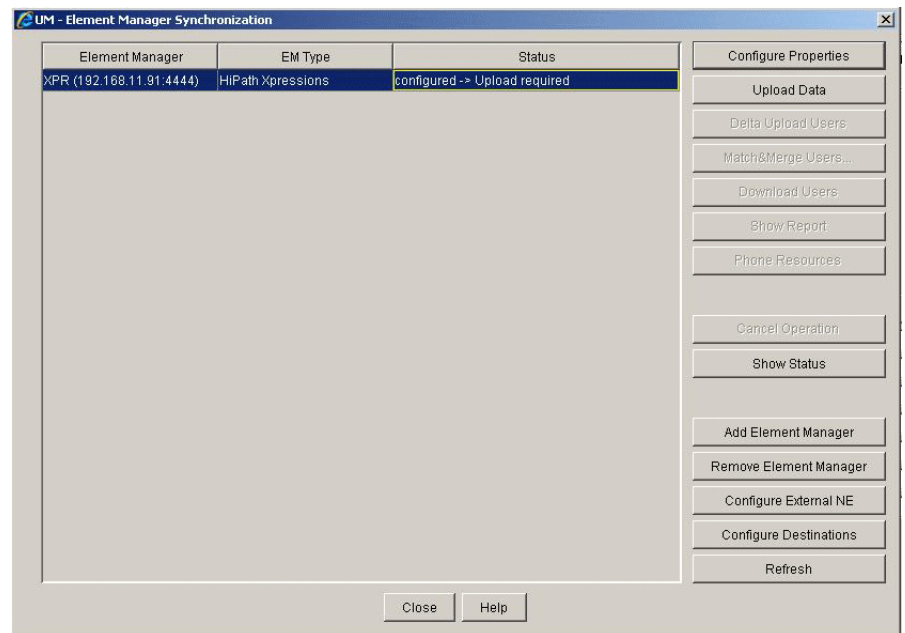
Confirm your entries with **OK**.

Your XPR server now appears in the list of the **Element Manager Synchronization** window.



- After this step the Element Manager is **not configured** yet. This message appears in the **Status** column. To completely configure the Element Manager, click on the **Upload Data** button. The Element Manager properties are now read in (**Status: Upload data (retrieve EM data)**).

If you have newly connected your XPR server as element manager, no user data have yet been loaded from the XPR server to the HPM-UM. Therefore, the XPR server status is still set to **configured => Upload required**.

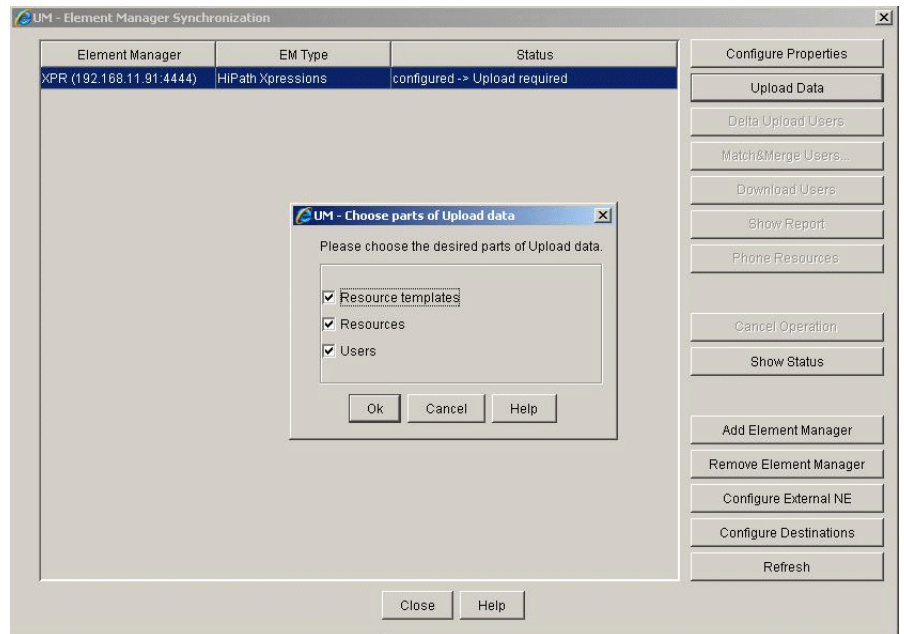


4. Before you can upload the Element Manager user data to the HiPath User Management, you need to specify the rules for data match&merger. Click on the **Configure Properties** button.

Another dialog opens, in which you can determine different properties and rules for the so-called *Match and Merge* of data. Here you can define, for example, a key attribute or the names interpretation. You find detailed information about the single rules in the administrator manual of the HiPath User Management. Confirm your specifications with **OK**.

5. You return to the dialog for **Element Manager Synchronization**.
If no **Status** representing the current state of your Element Manager is displayed, you can have it determined and indicated with the **Show Status** button.

6. A click on the **Upload Data** button initiates the actual data upload to the HiPath User Management. Another dialog opens in which you can select the different data elements used for the upload.

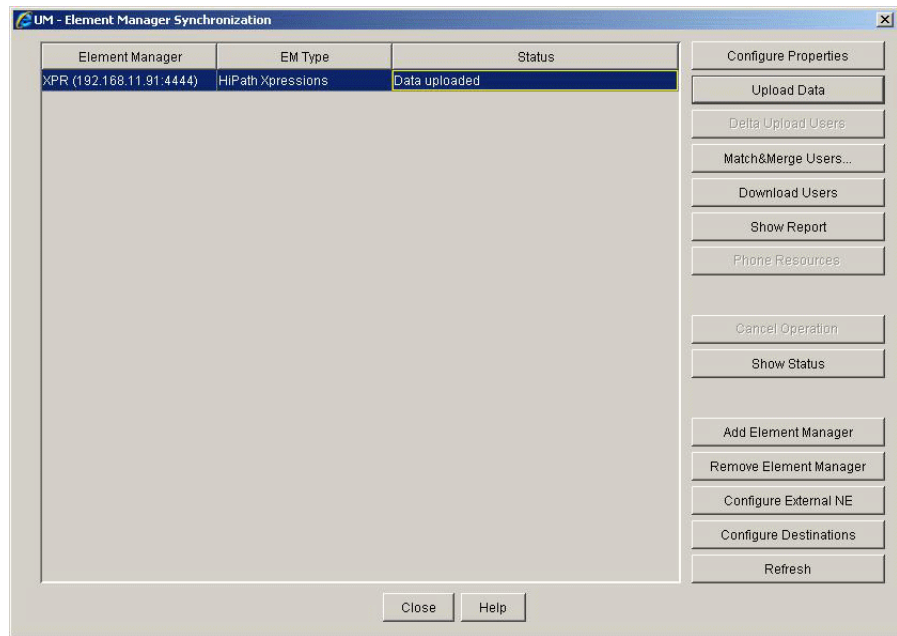


Select the **Resource templates**, **Resources** and **Users**. When you click on the **OK** button to confirm the selection the XPR server user data are loaded in the HPM-UM.

The data upload occurs in two steps. In the first step the uploaded users are matched to the HiPath User Management users according to the defined rules. In the second step the uploaded users are merged in the HiPath User Management according to the defined rules.

Depending on the size and number of user data this process may take some time. During the process the status changes to the display **Uploading data**.

7. If all user data have successfully been transferred, the XPR server status changes to **Data uploaded**. This means that the same data are available to you in the XPR server as well as in the HPM-UM.



NOTE:

If the data upload fails, the **Uploading failed** status display appears. You need to click the **Show Status** button to receive an error report and to restart the upload process.

8. The uploaded data as well as the match&merger status are displayed in the **UM-Match&Merge Element Manager Users** dialog. You reach this dialog by pushing the **Match&Merge Users...** button in the **UM-Element Manager Synchronization** dialog.

UM - Match&Merge Element Manager Users

Uploaded Element Manager Users

View: ☐ Search Criteria ☐ User ☒ User List

Status	Last Name	First Name	Primary Phon...	Mail	Resources	PINs
Unidentified	Administrator					
Unidentified	Company					
Unidentified	Garcia	Andy				
Unidentified	Joulie	Angelina				
Unidentified	Postmaster			postmaster@qus-c...		
Unidentified	System					

1/6

Match Users Create New UM User Ignore User Resolve Conflict Unmatch User Merge All Users

Display Mode Match Mode

Already existing HiPath User Management Users

View: ☒ Search Criteria

Last Name:

First Name:

Middle Name:

Gender:

PINs | Configuration Requests | Call Accounting | HiPath Applications
 Organization | Address | Alternate Address | Communication | Resources

Select Organization...

Organization:

Search Limit: 300 Search

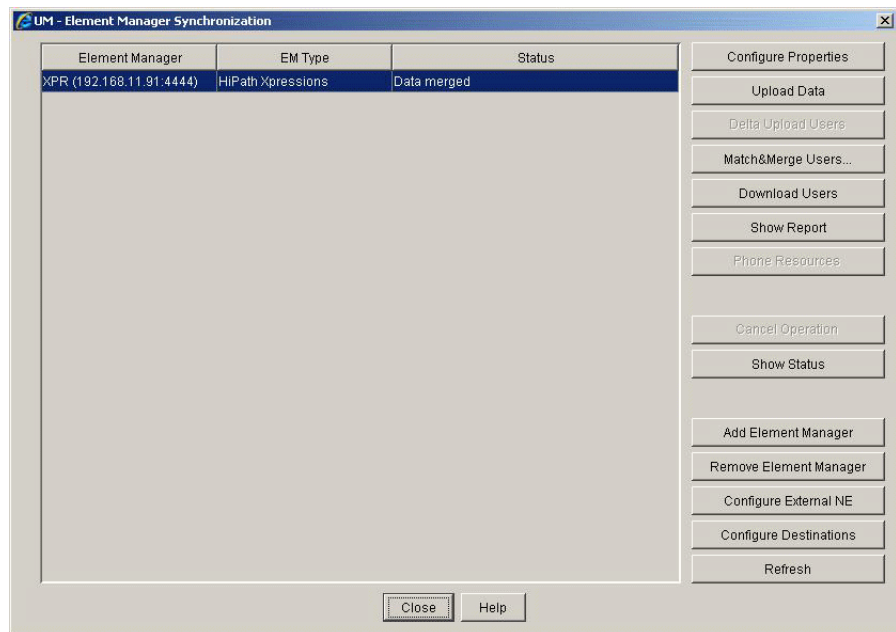
Close Help

After **matching** the Element Manager user data the data must now be **merged**. In the process the following cases must be distinguished:

- Based on the set rules, the user data could not be matched with any user in the HiPath User Management (status **Unidentified**). Such users can either be created as **new users** in the HiPath User Management or be **manually** matched with an existing user.

- a) A new user is created by selecting a user and pressing the **Create New UM User** button. The uploaded data are then used to create a new user in the HiPath User Management. By means of the **Merge all users** button all uploaded, unidentified users are created in the HiPath User Management as new users.
- b) The manual match is performed by selecting the associated HiPath User Management user and pushing the **Match Users** button. This may result in a **conflict** that is to be handled as if the match had occurred automatically according to the set rules (see next point).
- The user data from the mailbox could be matched with a user in the HiPath User Management based on the set rules (for example by matching with a unique key attribute such as *email* or *telephone number*). Depending on whether the user attributes differed, such users are assigned the status **No conflicts** or **Conflicts**. Conflicts can be resolved with a click on the **Resolve Conflict** button. You can decide whether to copy the XPR attributes (by selecting **uploaded User attributes precedence**) or to maintain the HiPath User Management attributes (by selecting **UM attributes precedence**).

When you have merged all uploaded data in the HiPath User Management, click the **Close** button to return to the **UM-Element Manager Synchronization** dialog. The Element Manager status must have switched to **Data merged**.



You can now complete the UM-Element Manager synchronization with a click on the **Close** button.

You return to the main dialog of the HPM-UM and are in the **Search Criteria** view. Click on the **Search** button and you receive a list of all uploaded user data in the **User List** view. The respective users with the most important attributes as well as status and configuration are displayed. The data are sorted according to the **Last Name** attribute, which is also considered a primary key.

Siemens HiPath User Management - Microsoft Internet Explorer

Address: <http://10.1.12.129:3043/apps/Hipath-UM/index.sso?user=root&role=Administrator&key=i7knbnae0m8m#>

HiPath User Management

User Management

User View Tools Help

View: ☐ Search Criteria ☐ User ☒ User List ☐ New User

Last Name	First Name	Primary Phon...	Mail	Resources	PINs	Status	Configuration
Administrator	Administrator					Newly Created	
Company	Company					Newly Created	
FRAN	FRAN					Newly Created	
Guest	Guest					Newly Created	
JOHN	JOHN					Newly Created	
Postmaster	Postmaster		postmaster@rd-de...			Newly Created	
System	System					Newly Created	

1/7 Save Revert New Copy Delete

Search complete Internet

When you select a user and change the **View** to **User**, you receive a precise representation of the data of the single user.

The screenshot shows the HiPath User Management application window. The title bar reads "HiPath User Management". Below the title bar is a menu bar with "User", "View", and "Tools". A "View:" dropdown is set to "User". The main area is divided into two panes. The left pane contains a form for user details: Last Name (FRAN), First Name (FRAN), Middle Name, Gender (dropdown), Salutation, Title, Language (dropdown), and Display Name. The right pane contains a tabbed interface with four tabs: "PINs", "Configuration Requests", "Call Accounting", and "HiPath Applications". The "Configuration Requests" tab is active, showing fields for Organization, Address, Alternate Address, and Communication. Below these tabs is a form for user communication details: Phone #, Primary Phone #, Internal Phone #, Home Phone # (49240490179898), Mobile Phone # (49240490112452), Fax #, Mail, User Account (FRAN), User Password (*****), Windows Domain, and Windows Account.

In the left window portion, some general specifications of the user are found. The right portion hosts several tabs that may contain various information. The **Communications** window, for example, delivers information about telephone numbers, e-mail address and fax number of a user.

You can modify existing as well as empty fields. With **Save** you can save your modifications. Via the **Revert** button you can set your modifications back to the state after the last saving of data. **New** defines a new user that must at least have a surname by **Last Name**. **Delete** deletes a user while **Copy** copies user data.

If you have modified the data records of the HPM-UM or the HPM APL during the course of time, you have to synchronize your data in the HPM-UM and in the XPR server. Proceed similarly to the description at the beginning of this section, by opening the **Element Manager Setup**, selecting the **XPR Server** in the list, and then clicking on **Match&Merge Users** .

21 Presence APL

21.1 Functions

The Presence APL provides multifarious application options. As regards functionality we generally differentiate between the control and display of profiles respectively user status and the transfer of specific data to the XPR system. In addition it serves as server for the Instant Messaging feature of optiClient.

The control and representation of profiles respectively status of users refers to the management of so-called presence settings. Each user can display information on his/her current status for other users. For example, information about the user's whereabouts (workstation, home) or the phone number under which the user is available can be displayed. We differentiate here between a status automatically generated by the system (online status), and a profile that each user can manually modify and activate (presence profile). Users can perform the settings on these profiles in client applications such as Communications.

Transfer of specific data to the XPR system means on the one hand that calendar data are copied from Lotus Notes or Microsoft Exchange, and on the other hand the current user status is synchronized in the Live Communications Server (LCS) with the user status in the XPR system. The calendar data from Lotus Notes and Microsoft Exchange are stored as presence profile ("Appointment"). The user status in the Live Communications Server is stored as current online status in the XPR system. With a specific user status in the LCS, a specific presence profile is partially activated in the XPR system besides the online status. The data transfer is configured in the XPR monitor.

According to this differentiation of the Presence APL functionality we will first explain the control and representation of user profiles in [Section 21.2, "User Profile and Status Administration"](#). Then follows in [Section 21.3, "Data Replication"](#) the data transfer to the XPR system. Finally Instant Messaging and web conferences will be dealt with in [Section 21.4, "Instant Messaging"](#) and [Section 21.5, "Web Conferences"](#).

21.2 User Profile and Status Administration

Like the Microsoft MSN Messenger, the Presence APL displays the status of logged-in users. The XPR server Presence APL communicates with clients via an individual protocol, so that also the status of users not logged in at a client are shown.

The Presence APL can display a status and a profile of a user:

- **Online status:** This status indicates whether or not a user is logged in at the system. Furthermore, a period can be specified in which the user is logged in but has not become active in the system. In this way you can check whether or not a logged-in user is currently at his/her workstation. You find an overview of possible online status in [Section 21.2.1, "The Online Status"](#).
- **Presence profile:** The presence profile comprises a profile that each user can freely set to provide information about his/her current status (for example, on business trip, appointment, or in the office). Beyond that, further information such as comments, the location and a phone number under which a user can be reached can be added. Contrary to the MSN Messenger this presence profile can also be active when a user is not logged in at the XPR system. You find an overview of possible presence profiles in [Section 21.2.2, "The Presence Profile"](#).

While the online status depends on the presence or activity of the user, he/she can individually define each presence status themselves. Each user can modify and display this information for other users via client applications such as Communications. Such data are only displayed statically and *cannot* be used for further functions such as automatically forwarding to a specified phone number. You can activate each presence profile either manually via a client application like Communications, or automatically by a created time profile.

The following graphic shows an example of an information display according to a user's status.

Administrator
Working at home

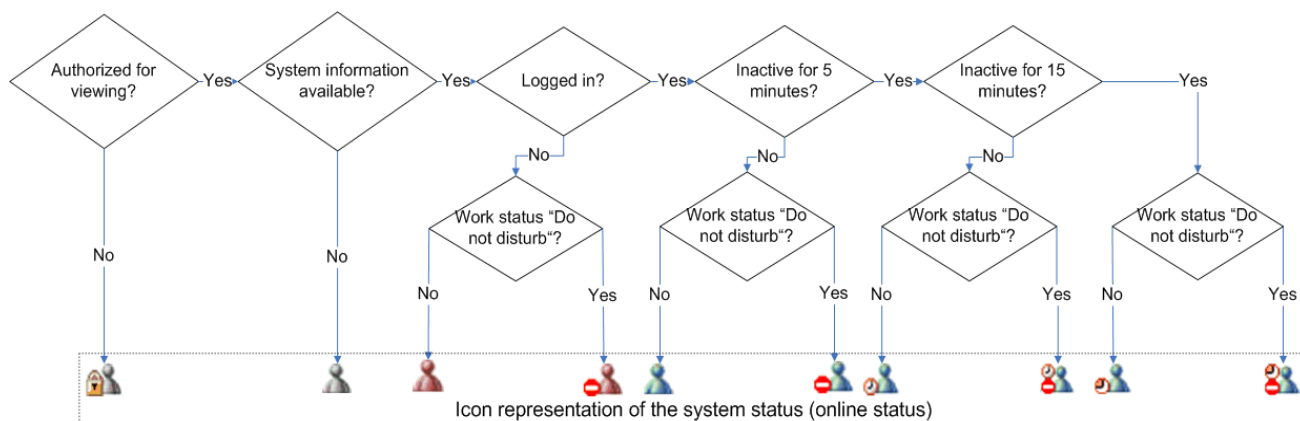
Birthday

Online status: Online
Please do not disturb
Private Comment: No congratulations, please!
Location: Testuser City
Next Profile: On business trip from Tomorrow,
08:00 to Tomorrow, 23:00
Phone: 0240490186100
Since: 16:16
☒ Notification 'Online' state
GUI

The Presence APL distributes the status information of the users among XPR server and clients by means of transactions. These transactions describe the communication between XPR server and clients. The data stored in the XPR server database are distributed among the clients by the Presence APL in regular, short intervals. In this way the displayed information is continuously updated. No external protocols are required for the Presence APL functionality.

21.2.1 The Online Status

The graphic represents the online status display options.



Each diamond depicts a branching of possible online stati. Each branching eventually ends with an arrow in an online status with specific properties. The specified symbols correspond to the representation of a user's online status in the display.

First we need to find out whether the corresponding system information and necessary access privileges are available. If they are not, this fact will be displayed as online status. In the event that both, information and privileges, are available, a query is made as to whether the user is logged in or off. Besides the pure login or logoff status, further specifications are possible. You can additionally indicate whether a user has selected the "Busy" property in an arbitrary presence profile, and whether the user has been inactive in the system for 5 or 15 minutes already. All information is represented in one icon.

The single icons for displaying the online status and the respective explanation are contained in the following table.

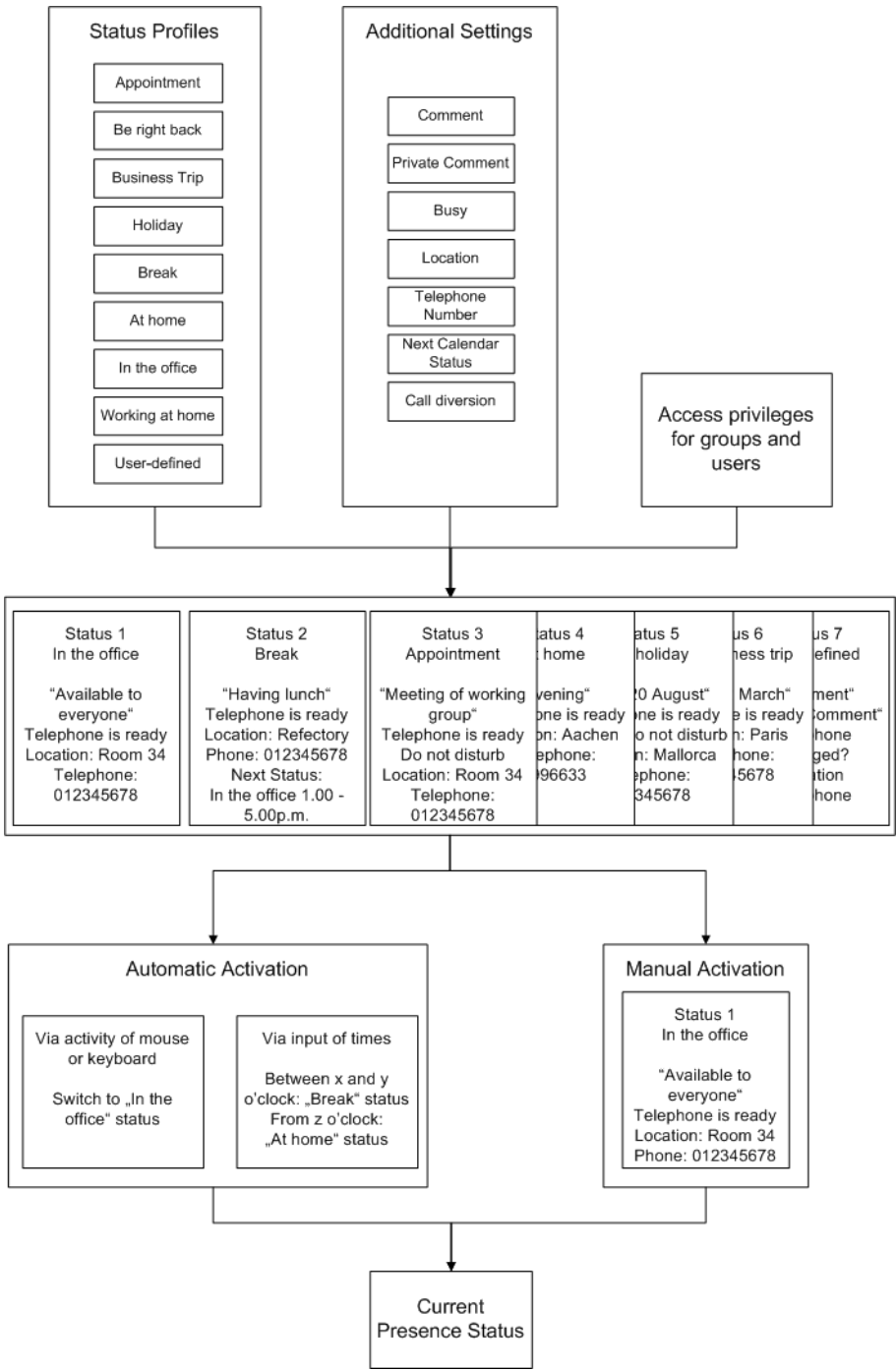
Icon	Description
	This icon indicates that the user is logged in at the system.
	User is logged in at the system. For five minutes the system has not registered any user activities.
	User is logged in at the system. For five minutes the system has not registered any user activities. Setting of a presence profile with the property "Do not disturb".
	User is logged in at the system. For at least 15 minutes the system has not registered any user activities.
	User is logged in at the system. For at least 15 minutes the system has not registered any user activities. Setting of a presence profile with the property "Do not disturb".
	User is logged in at the system. Setting of a presence profile with the property "Do not disturb".
	User is logged out of the system.
	User is logged out of the system. Setting of a presence profile with the property "Do not disturb". This is possible since presence profiles may also be active if the respective user is not logged in at the system.
	There is no system information on this user.
	No permission to display status information.

21.2.2 The Presence Profile

The following table contains the icons of the single predefined presence profiles. In addition, user-defined presence profiles are possible, which can be allocated with an individual icon.

Icon	Description
	Appointment
	Be right back
	On business trip
	Holiday
	At home
	Break
	In the office
	Working at home
	User-defined (no individual icon selected)

The following graphic demonstrates the presence profile representation.



Each possible presence profile may contain a specific number of additional **properties**. The properties, such as location or comment, are optional except for the display that indicates whether a user's line is busy. In other words, these properties are only displayed if they have assigned a value (this may also be a standard value). The display of these properties as well as of the presence status

itself depends on assigned **access privileges**. Groups or single users can be denied the display of single properties or of the entire profile. An arbitrary number of profiles can be created.

Each currently used presence profile is either activated manually by the user or automatically by specific temporal settings. Manual activation may be permanently valid or temporarily limited. Automatic activation is reserved for specific presence profiles. This means that only the presence profiles *In the office*, *At home* and *Break* can be automatically activated. Presence profiles may also be active when the respective user is not logged in at the system.

21.2.3 Settings in Client Applications

Since the Presence APL serves for transmitting the so-called presence profile of a user, it can only be used with client applications that use this presence profile of a user. The Presence APL functionality is supported by applications such as Communications or optiClient.

The Presence APL enables defining specifications on the individual online status and presence profile and displaying them for others. In the same manner it is possible to be informed about the corresponding profile of others.

As regards a user's profile entries, a wide range of setting options is available. In clients with presence support such as Communications you are given access to the **Presence Settings**, in which the individual presence profile can be specified.

NOTE:

You find a comprehensive description of the presence settings for the respective client application in the appropriate manual, for example in the *Communications* manual.

The “Current Profile” tab

In these presence settings the user selects his/her current presence profile as well as its properties. Specific properties may contain predefined values, while other properties may have arbitrary values.

This tab displays the currently active work status that you have predefined and its settings. You can temporarily modify the predefined status via the configuration and entry options available here. If the active-profile entries performed here differ from those predefined for this profile ([The “My Profiles” tab](#)), the field descriptions appear in red after you have opened the settings dialog again. In addition, a warning message is displayed in the bottom section of the dialog.

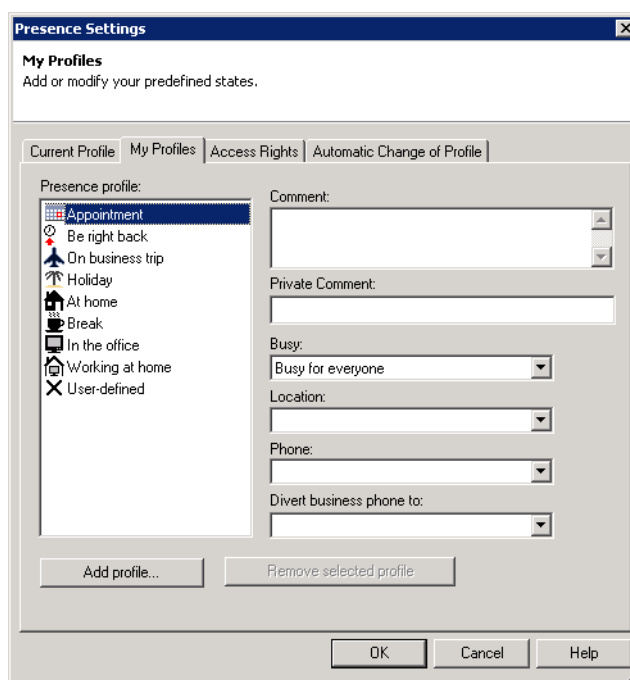
The screenshot shows the 'Presence Settings' dialog box with the 'Current Profile' tab selected. The dialog has a title bar with a close button. Below the title bar, there is a section titled 'Current Profile' with a note: 'Select the state you are currently in. Please note that changing the settings below will not modify the original properties of the state.' Below this, there are four tabs: 'Current Profile', 'My Profiles', 'Access Rights', and 'Automatic Change of Profile'. The 'Current Profile' tab is active. It contains a section 'Activated profile' with a dropdown menu showing 'In the office'. Below this is a section 'Settings for the selected profile' with several fields: 'Comment' (a text area), 'Private Comment' (a text area), 'Busy' (a dropdown menu showing 'Not busy'), 'Location' (a dropdown menu), 'Phone' (a dropdown menu), and 'Divert business phone to:' (a dropdown menu). At the bottom right of the settings section is a button labeled 'Next Profile...'. At the very bottom of the dialog are three buttons: 'OK', 'Cancel', and 'Help'.

The “My Profiles” tab

For each predefined presence profile such as *Holiday*, *In the office*, *At home*, *Break*, *Appointment*, *Be right back*, *Working at home*, *On business trip* or *User-defined*, profile properties can be assigned as well as individual profiles created. The properties of a profile are automatically activated upon selecting this profile as current profile.

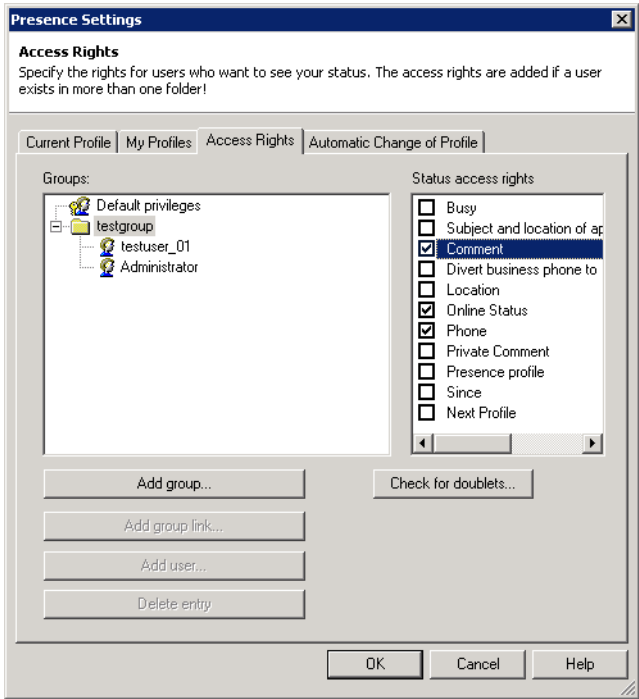
NOTE:

In case of a profile change (automatic or manual) and a possible diversion number change, the phone diversion is only updated if the diversion number of the current profile (see [The “Current Profile” tab](#)) and the one for the activated profile previously match. This also means that if you have configured a diversion for your phone and this diversion differs from the one defaulted via the active profile, no modification takes place when the profile is changed.



The “Access Rights” tab

Specific access privileges enable the display and hiding of information for groups or users.

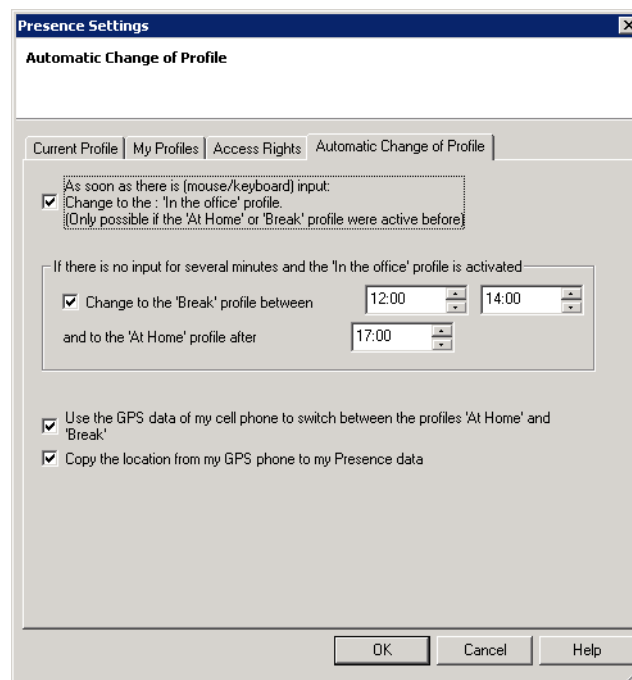


The “Automatic Change of Profile” tab

Selecting various options allows an automatic activation of a user's presence profiles:

- If you select the presence profile “At home” or “Break”, the system will know by entry via mouse or keyboard that the user is at his/her workstation. The profile switches automatically to the “In the office” status.
- You may specify a period in which the “Break” presence profile is automatically activated. In addition, you may define a time from which the “At home” presence profile is automatically valid.

With these options you can have the activation or the switch to specific presence profiles automatically initiated.



The information on the respective stati appears in static format, for example as tooltip.



A screenshot of a tooltip window with a yellow background and a thin black border. The text inside is as follows:
Administrator
Working at home

Birtday

Online status: Online
Please do not disturb
Private Comment: No congratulations, please!
Location: Testuser City
Next Profile: On business trip from Tomorrow,
08:00 to Tomorrow, 23:00
Phone: 0240490186100
Since: 16:16
☒ Notification 'Online' state
GUI

You can set an automatic notification if the respective user has not set the **Busy** property to “Busy for all” or “Please do not disturb” anymore. Notifications can be set as messages arriving via SMS, business phone, cellphone and as information displayed on the PCs graphical user interface. Messages by SMS, business telephone or cellphone require a phone number each to ensure a correct functionality. Such phone numbers can be configured in, for example, Communications.

NOTE:

The set presence profile and the associated properties are exclusively displayed. They do not have a direct function. Thus, you cannot reroute the telephone to the voicebox or have the telephone switched to busy.

21.3 Data Replication

To copy appointments from the calendar of MS Exchange or Lotus Notes and online stati from the Live Communications Server (LCS) of a user to the XPR system, the XPR monitor configuration tabs are used.

21.3.1 Settings in the XPR Monitor

Open the configuration dialog of the Presence APL in the XPR monitor.

Two tabs are available for configuring the Presence APL. The **TUM Calendar** tab enables settings for transmitting calendar data from Lotus Notes or Microsoft Exchange to the presence profiles of XPR users. On the second tab, **Live Communications Server**, you can make specifications for the data transfer from the LCS to the XPR system. You can only transfer data from the Live Communications Server to the XPR system but not from the XPR system to the LCS.

NOTE:

An administrator with *service privilege* may configure the Presence APL unrestrictedly.

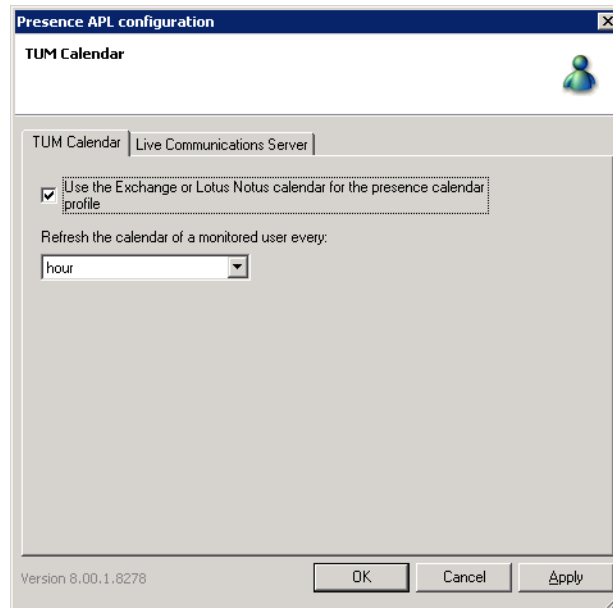
21.3.1.1 The TUM Calendar

On this tab you activate the transfer of a user's calendar data from Microsoft Exchange or Lotus Notes to the XPR system. In the XPR system, the data are automatically stored in the presence profiles in a way that an appointment copied from MS Exchange or Lotus Notes is defined as **Appointment** presence profile of a user in XPR.

In this process, the **Comment** property of the presence profile is allocated with the **subject** of the transferred appointment.

The **Location** property of the presence profile adopts the content of the **location** specification of the copied appointment.

The remaining presence profile properties are filled with the default values for the **Appointment** presence profile and do not require special access privileges.



Use the Exchange or Lotus Notes calendar for the presence calendar profile

Via this option you activate or deactivate copying calendar data from Microsoft Exchange or Lotus Notes to the XPR system. The data transfer is deactivated by default.

Refresh the calendar of a monitored user every

Here you specify in which interval data from the Microsoft Exchange respectively Lotus Notes calendar is replicated to the presence profiles of an XPR user. A one-hour interval is set by default. You can select the intervals *30 minutes*, *1 hour*, *2 hours*, *3 hours*, *4 hours*, *6 hours* and *12 hours*. You can only perform this setting if you allow the copying of calendar data. Otherwise this field is shaded gray.

21.3.1.2 The Live Communications Server Tab

On this tab you activate the replication of LCS data to the XPR system and perform settings for the access data to the LCS.

IMPORTANT:

The Live Communications Server query allocates port 5060, which is also required for SIP. A simultaneous use of this query in combination with an SIP connection of the IP APL is therefore not possible. If such an SIP connection is to be established, LCS server usage must not be activated here!

Using this transmission you can transfer the online status of a user from the LCS to the XPR system. With specific LCS values, a presence profile is additionally activated in the XPR system. This replication occurs at runtime, so that modifications in the LCS are immediately transferred to the XPR system. Data transfer from the XPR system to the LCS is currently not possible!

NOTE:

If a user activates copying the LCS data to the XPR system, all other users with the corresponding access privileges may see the data of this user's presence profile.

Requirements

The replication feature is only possible if the following **LDAP APL** attributes are replicated from the LCS to the XPR system:

- The LCS attribute `msRTCSIP-UserEnabled` must be replicated to the XPR attribute `SIP_SUPPORT`. This attribute states whether the user is authorized for using SIP. SIP is a communication protocol used for setting up connections.
- The LCS attribute `msRTCSIP-PrimaryUserAddress` must be replicated to the XPR attribute `SIP`. This attribute specifies the user's SIP address (SIP URI). This SIP address can be used like an e-mail address or a phone number as unique address to connect to a user.

For such proceedings, open the LDAP APL configuration page in the XPR monitor. On the *Attributes* tab you need to click on *Add* and select the listed attributes. You find further information about the LDAP APL in [Section 19.7.3, "The "Attributes" Tab"](#).

Configuration

In the **Use the LCS server for retrieving presence information** field you can activate or deactivate the LCS data transfer to the XPR system. This option must be active, otherwise the other fields cannot be configured.

The **Login name** requires the name that the user specifies when logging on to the LCS system.

In the **User Name** field you need to enter the name the user has in the LCS.

The **Password** field refers to the password of the user for logging in to the LCS system.

By means of **Server name or IP address** you localize the LCS and establish a connection between LCS and XPR system.

Data transfer

When data are transferred from the LCS, the system must adapt information to the values of the online status in the XPR system. The following table shows how the single data are transferred from the LCS system to the XPR system.

For better orientation you can use the graphic and table from [Section 21.2.1, "The Online Status"](#). Please obtain a description of the LCS fields from the corresponding Live Communications Server manual.

LCS Field	XPR Field	Description of the XPR Fields
"Online"	XPR-online	The value of the XPR-online field is set to "true" and states that the user is logged in at the system.

LCS Field	XPR Field	Description of the XPR Fields
"Offline"	XPR-online	The value of the XPR-online field is set to "false" and states that the user is not logged in at the system.
"Away"	XPR-idle-long	The user is logged in to the system (XPR-online is set to "true"), but for 15 minutes no user activity has been registered.
"Out to lunch"	XPR-online + XPR-Profile BREAK	The user is logged in at the system (XPR-online is set to "true"). In addition, the "Break" presence profile is active.
"Be right back"	XPR-online-idle + XPR-Profile BE_RIGHT_BACK	The user is logged in at the system, but for 5 minutes no activity has been registered. Furthermore, the "Be right back" presence profile is active.
"Busy"	XPR-online-busy	The user is logged in at the system (XPR-online is set to "true"). In addition, however, the "Please do not disturb" property of a currently active presence profile is specified.
"On the phone"	XPR-online-busy	The user is logged in at the system (XPR-online is set to "true"). In addition, however, the "Please do not disturb" property of a currently active presence profile is specified.
"Idle"	XPR-online-idle	The user is logged in at the system (XPR-online is set to "true"), but for 5 minutes no user activity has been registered.
after 10 Minutes of "Idle"	XPR-online-idle-long	The user is logged in to the system (XPR-online is set to "true"), but for 15 minutes no user activity has been registered.

21.4 Instant Messaging

The Presence APL serves as server for the Instant Messaging functionality of the XPR server. As client, optiClient is always used. Connecting other Instant Messaging servers is not intended.

The requests and short text messages of Instant Messaging are sent as transactions via the Presence APL. The presence status is considered here as well, so that a request is automatically rejected if the *Do not disturb* presence status is set.

21.4.1 Transactions

21.4.1.1 Invitation for Instant Messaging

Transaction

```
IM_INVITE CALLER=<AID> CALLEE=<BID> [PARTIES=<CID>{,<CID>}]
[SESSION=<SID>]
```

Parameters:

CALLER=<AID>

<AID> is the user ID of the inviting user.

CALLEE=<BID>

<BID> is the user ID of the invited user.

PARTIES=<CID>{,<CID>}

List of users already involved in this Instant Messaging session. <CID> is a user ID. <AID> and <BID> are not contained in the list. If no further users take part in the Instant Messaging session, this parameter will be omitted.

SESSION=<SID>

<SID> is the session ID of this Instant Messaging session. This parameter is only sent if an existing session is to be expanded, otherwise the session ID is created by the Presence APL.

Reply

```
IM_INVITE STATUS=<STATUS> SESSION=<SID> PARTY=<BID>
```

Parameters:

<STATUS>

Whether the invited user has accepted the invitation. Can be OK (accepted), ERROR (some problem), DENIED (rejected) or DND (presence status was set to *Do not disturb*).

<SID>

<SID> is the session ID of this Instant Messaging session.

<BID>

<BID> is the user ID of the invited subscriber used for the correlation with the original transaction.

21.4.1.2 Leaving Instant Messaging

Transaction

IM_BYE PARTY=<AID> SESSION=<SID>

Parameters:

PARTY=<AID>

<AID> is the user ID of the subscriber who leaves the session.

SESSION=<SID>

<SID> is the session ID of this Instant Messaging session.

Reply

IM_BYE STATUS=<STATUS> SESSION=<SID>

Parameters:

<STATUS>

Can be OK or ERROR (some problem).

SESSION=<SID>

<SID> is the session ID of this Instant Messaging session.

21.4.1.3 Sending Instant Messaging Data

Transaction

IM_DATA PARTY=<AID> SESSION=<SID> TEXT="<Text>" [CR]

Parameters:

PARTY=<AID>

<AID> is the user ID of the author.

SESSION=<SID>

<SID> is the session ID of this Instant Messaging session.

TEXT="<Text>"

<Text> is the text written by the author. This text is coded in UTF-8. Inverted commas and the backslash are marked by a prefixed backslash. The string may contain a maximum of 510 bytes. If required, a text is cut up in several consecutive transactions.

CR

This parameter marks the end of a section. If a section consists of only one transaction, this parameter must also be set.

Reply

IM_DATA STATUS=<STATUS> SESSION=<SID>

Parameters:

<STATUS>

Whether the data could be sent. Can be OK (accepted), ERROR (some problem) or GONE (all other subscribers have left the session).

SESSION=<SID>

<SID> is the session ID of this Instant Messaging session.

21.4.1.4 Notification in Case of a joining Subscriber

Transaction

IM_JOINED PARTY=<AID> SESSION=<SID>

Parameters:

PARTY=<AID>

<AID> is the user ID of the joining subscriber.

SESSION=<SID>

<SID> is the session ID of this Instant Messaging session.

Reply

IM_JOINED STATUS=<STATUS>

Parameters:

<STATUS>

Always OK.

21.4.1.5 Notification when a Subscriber leaves the Instant Messaging Session

Transaction

IM_LEFT PARTY=<AID> SESSION=<SID>

Parameters:

PARTY=<AID>

<AID> is the user ID of the subscriber who leaves the session.

SESSION=<SID>

<SID> is the session ID of this Instant Messaging session.

Reply

IM_LEFT STATUS=<STATUS>

Parameters:

<STATUS>

Always OK.

21.5 Web Conferences

An invitation for a web conference is also sent as transaction to the Presence APL. It is basically a special Instant Messaging transaction. The following transactions are used:

21.5.1 Invitation for a Web Conference

Transaction

```
WEB_INVITE CALLER=<AID> CALLEE=<BID> [PARTIES=<CID>{,<CID>}]
[CONFERENCE=<CONFID> ] [WEBSESSION=<WSID>] [PASSWORD=<PWD>]
[DURATION=<Seconds>] [REMAINING=<Seconds>]
```

Parameters:

CALLER=<AID>

<AID> is the user ID of the inviting user.

CALLEE=<BID>

<BID> is the user ID of the invited user. This parameter is mandatory since it is required by the Presence APL for forwarding the invitation to this user.

PARTIES=<CID>{,<CID>}

List of users already involved in this web conference. <CID> is a user ID. <AID> and <BID> are not contained in the list. If no further users take part in the web conference, this parameter will be omitted.

CONFERENCE=<CONFID>

<CONFID> is the conference ID used for a web conference by the Conference Planning Service.

WEBSESSION=<WSID>

<WSID> is the session ID for web conference.

PASSWORD=<PWD>

<PWD> is the password for the web conference.

DURATION=<Seconds>

<Seconds> is the scheduled duration of the web conference in seconds.

REMAINING=<Seconds>

<Seconds> is the remaining time for this web conference. This period may deviate from the originally scheduled duration, if somebody is invited for an already ongoing web conference.

Reply

WEB_INVITE STATUS=<STATUS> PARTY=<BID>

Parameters:

<STATUS>

Whether the invited user has accepted the invitation. Can be OK (accepted), ERROR (some problem), DENIED (rejected) or DND (presence status was set to *Do not disturb*).

<BID>

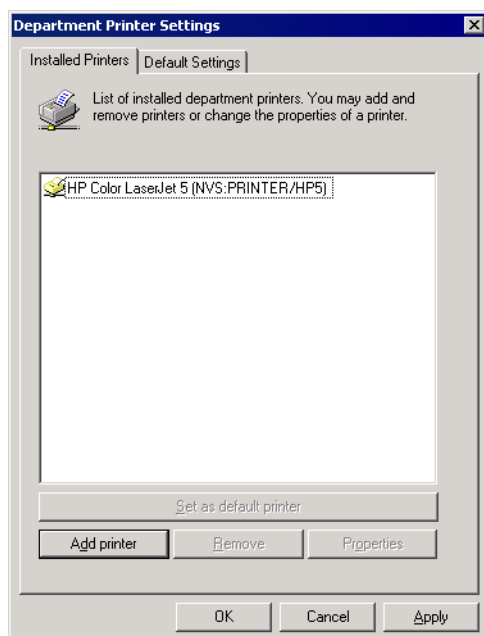
<BID> is the user ID of the invited subscriber used for the correlation with the original transaction.

22 Print APL

Copies from incoming and outgoing documents can be automatically created and sent to a printer through the Printer APL. The configuration is performed from the XPR monitor as usual. To this, select in the modules window under **Settings** the **Print APL** and doubleclick **Set Options**.

NOTE:

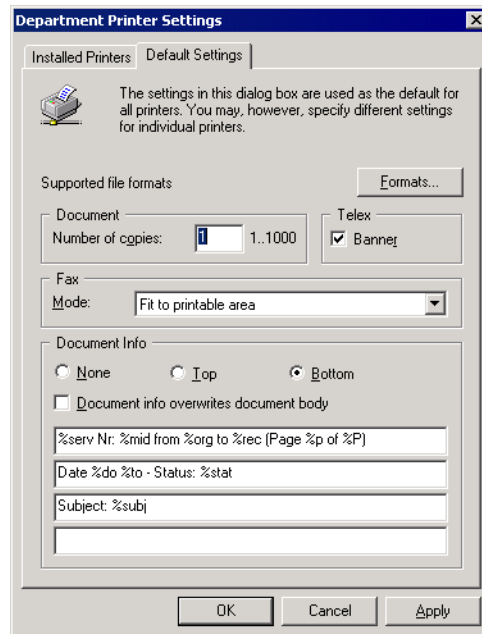
An administrator with *service privilege* may configure the Print APL unrestrictedly.



On the **Installed Printers** configuration tab all currently installed printers are displayed. New printers are installed through use of the **Add printer** button. Obsolete printers can be removed from the list through use of the **Remove** button.

Any one of the installed printers can be declared as the **default printer**. This printer would be used, if the *Carbon Copy Rules* in the MTA were set to *Incoming fax documents are copied to the default printer*. In this way all incoming fax documents would automatically be put out on this default printer. The yellow printer symbol denotes the current default printer.

22.1 Printer Settings



Number of copies

The default number of copies to be printed is entered in this field.

Telex banner

When activated, a telex banner with the word “Telex” is printed in the right and left-hand margins of the document. The printed document would then have the appearance of a “real” telex message. The XPR server does not support its own telex devices, but can access the telematic server NVS (based on Real Time Unix QNX) over a remote system link. For printing, a special telex font must be installed.

Fax mode

The following options are available:

- Fit to printable area. This option makes extra-long fax pages appear very small!
- Fit printable area. Fax documents that exceed the length of the printable area as a result of resizing are continued on a second page. In the case of continuous form fax documents, the document is logically split into several printable areas when printed.
- Fit to printer resolution. The size of the fax printout depends on the printer resolution, and consequently printing is faster.

- Optimize printable area width. This option is based on the premise that the left and right margins of a fax are normally blank. This portion of the fax can be disregarded without any loss of the text by printing.
- Optimize printable area. This option is principally the same as the above one with the exception that the entire page width is used (A4 or US Letter). Areas outside the Windows printer driver's "printable area" are also used.

Document info

In the lower portion of the dialog positions can be defined in which document information is to appear. This can either be printed at the Top, Bottom, or not at all. If a portion (upper or lower) of the incoming fax document is normally free of text, this area could be used for printing the document information. When the Document info overwrites document body option is enabled, document information will be inserted at the selected location and run into the body of the document when necessary.

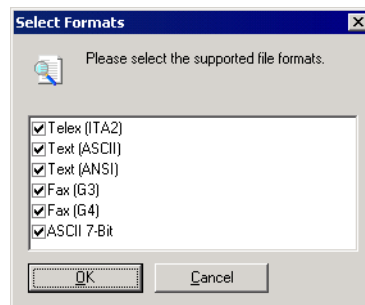
The information to be printed can be entered in the four input fields. The following variables can be used for displaying the document information.

Variable	Meaning
%cost	Charge costs.
%costid	Cost center.
%do	Date of receipt on server.
%dr	Date of the report. The report is generated after completion of the document transmission.
%frm	The format, e.g. ASCII, Fax G3, etc.
%fullname	The complete user name or, if it is unknown, something like "Unknown User" (language dependent).
%len	Document length in bytes.
%mid	The message ID.
%oid	Originator ID e.g with a fax.
%oorg	Original originator for documents that are rerouted.
%orec	Original recipient for documents that are rerouted.
%org	Message originator.
%p	Actual page number.
%P	Total number of pages in document.
%rec	Message recipient.
%rid	Recipient ID e.g with a fax.
%serv	Transport service used.
%stat	Detailed message status.
%subj	Message subject.
%succ	Success or failure of the send job: Undefined, Unknown, OK, ERROR, REJECT, REPEAT or DELAYED.

Variable	Meaning
%to	Time of receipt on server.
%tr	Date of the report. The report is generated after completion of the document transmission.
%units	Number of units where one unit costs, for example, 12 cent.
%worg	NVS address of the originator.
%wrec	NVS address of the recipient.

22.1.1 Supported File Formats

Via the **Formats** button the file formats accepted by the Print APL can be set.



If the MTA passes on a file for printing, it is converted into one of the printable formats listed here.

NOTE:

If the Print APL is to be used for the printing of e-mails with attachments, the method should be used for printing attachments: Register **FG3** and **FG4** only as formats. The MTA will convert e-mails with attachments to one of these fax formats. If the application converter supports the document format of these attachments, they will be printed.

22.1.2 Printer Properties

In most cases each printer uses the **default settings** described above. If this behavior is not desired, deactivate the **Use default settings** option before performing the desired settings in the bottom portion of the dialog.

The **Printer:** field is provided for entering a line name for the XPR monitor. The printer name used by XPR in the addressing is entered as **Name:**. This name must also be entered in a user database under `PRINTER` if this user wants to print copies of his/her documents according to the *Carbon Copy Rules*.

IMPORTANT:

The Print APL does not allow the installation of a printer the name of which contains the string: `FAX G`. This prohibits the inefficient usage of the XPR fax printer driver.

If documents are to be automatically sent to a departmental printer, then a set of *Carbon Copy Rules* must be defined. Therefore define a *Carbon Copy Rule* via the MTA setting pages that creates this copy and sends it to the Print APL. The flag `NOPREFERRED` should be set in this rule, so that copies are not detoured by the preferred rule.

Example:

```
NVS:*.*/*[ORG=NVS:FAXG3.*/*;FLAG!=CARBONCOPY;FLAG!=NOPREFERRED]=
    NVS:PRINTER/<DB>[FLAG=NOPREFERRED]
NVS:*.*/*[ORG=NVS:FAXG4.*/*;FLAG!=CARBONCOPY;FLAG!=NOPREFERRED]=
    NVS:PRINTER/<DB>[FLAG=NOPREFERRED]
```

All incoming fax G3 and G4 documents (whose `CARBONCOPY` and `NOPREFERRED` flags are not set) would be sent to a printer, when a printer from the Print APL is entered in the `PRINTER` field of the recipient's user database.

22.2 Security Aspects

Accessing a network printer almost always requires the corresponding privileges. To furnish the Print APL with these privileges you can run this service in the security context of a user account that has the access privileges.

As administrator call the service administration and in the service properties access the **Log On** tab to specify the corresponding user account with the associated password.

With this user account log in at the server once and connect the desired network printer. Subsequently, you can also check whether the user is really permitted to print.

You can recognize such an access problem e.g. by the following line in the XPR server log file:

```
23.11:49:17.884 PrintApl Printer E StartDoc failed (Access is denied.)
```

23 Direct Print (LPR APL)

The LPR APL serves for outputting documents via the LPR protocol according to RFC 1179 to a large number of congenial printers or multi-purpose devices. To this, the LPR APL registers a line `NVS : LPR` of the format `TIF_BMP` with the MTA. By way of this format selection, any document sent by the MTA to the LPR APL is transferred as TIFF. In this connection, the MTA may initiate an external conversion to, for example, PDF of the document to be put out. See [Section A.3, “Graphic Formats”, on page 1586](#).

For the document output, the user merely needs to know the associated printer. The respective printer is made known by its IP address being entered in the LPR field. Via appropriate routing rules it is then possible to print out, for example, reports about sent fax messages.

The printers are introduced to the LPR APL not until they address this APL. The printer queues are thus dynamically established and broken down again as required. A large number of such multi-purpose devices can be relatively easily managed in this way.

23.1 Configuration

A configuration modification is normally not required. But if you want to change, for example, the repeat strategy, you need to do this via the registry. See [Section E.11, “Entries of the LPR APL”, on page 1777](#).

23.2 Internal Database

The LPR protocol demands for each print job a unique ID between 0 and 999. Therefore, the LPR APL memorizes the ID used last for each printer ever addressed in an internal database.

Furthermore, the currently active printer queues and their stati are mapped here from the LPR APL view. The possible stati of a printer queue are `Idle`, `Print`, `Shutdown` and `Sleep`.

After the LPR APL shutdown, the IDs are stored in the `LprApl.jobnr` file, so that they are available again at the next startup.

23.3 Structure of the Display in the XPR Monitor

Under the direction of the LPR APL, all printers are displayed in the XPR monitor that currently print out a document. This display is structured as follows:

```
lpr: <IP address> mid<MIDD> [<MIDH>]: > <Queue>
```

The *<IP address>* determines the printer. *<MIDD>* is the message ID of the printed document as decimal number. *<MIDH>* is the message ID of the printed document as hexadecimal number. *<Queue>* is the number of documents that are currently in the printer queue for this printer.

23.4 Structure of the Log Output

All LPR APL outputs are structured as follows:

```
[<IP address>]mid[<MIDH>] <report>
```

The *<IP address>* enables the assignment of output and printer. *<MIDH>* is the message ID of the printed document as hexadecimal number. The log output can later be very easily searched and filtered according to such criteria.

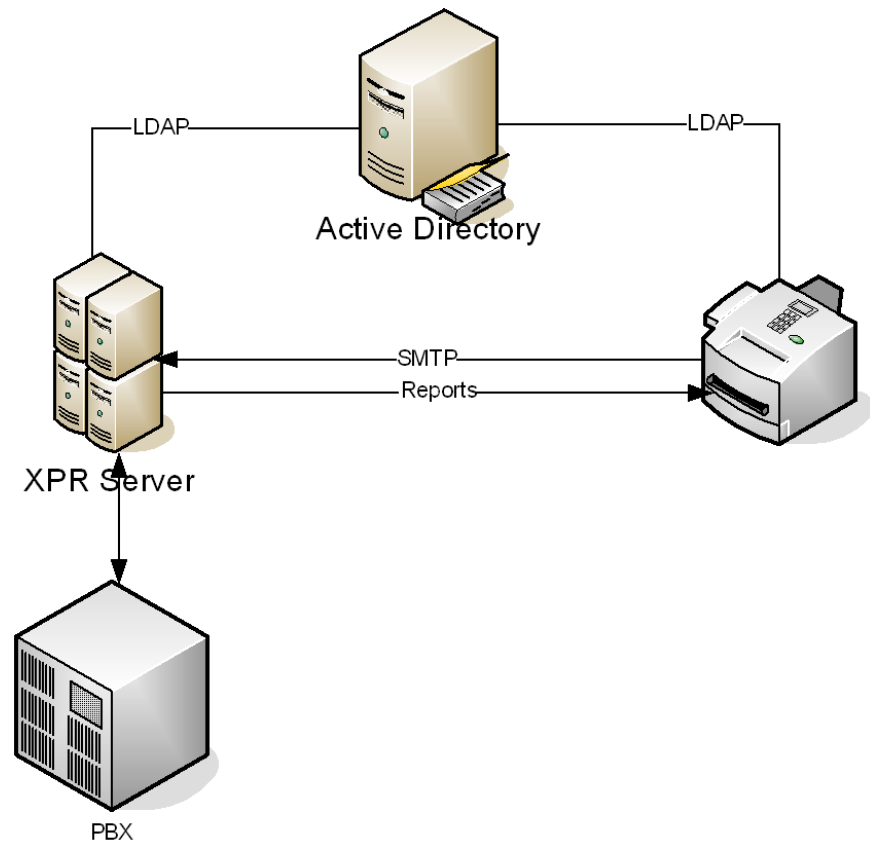
23.5 Debug Transaction

You can send the following transaction to the line `NVS:LPR:`

```
DEBUG PRINTER=<IP address> FILTER=[ON|OFF]
```

After receiving this transaction the LPR APL writes the content of the internal database as information in the XPR log. The parameters `PRINTER` and `FILTER` are optional. Via `PRINTER` you can restrict the output to a specific printer. Via `FILTER` you can restrict the output to the printers for which a job exists in the printer queue (`ON`) in the moment of the transaction.

23.6 Example Scenario



Each department has a multi-purpose device for scanning, faxing and printing. The users can log on to one of these multi-purpose devices. Their data are checked against a company directory by LDAP. Subsequently, a scanned fax is transferred to the XPR server by SMTP and sent by the server. Connecting the multi-purpose devices to the telephone network is thus not required.

The user is known to the XPR server via an LDAP replication, so that he/she, as originator, has the necessary privileges on the XPR server.

The report about sent fax messages can now be put out by carbon copy rules via the LPR APL on the printer that the user has entered in the `LPR` database field. Example:

```
NVS: *.*/* [TYPE=REPORT; SUCCESS=FAILURE; FLAG!=FLAG1] =
                                NVS:LPR/
<ODB> [FORM=report.failure; FLAG=FLAG1, NOREPORT]
NVS: *.*/* [TYPE=REPORT; SUCCESS=OK; FLAG!=FLAG1] =
                                NVS:LPR/<ODB> [FORM=report.ok; FLAG=FLAG1]
```

This scenario can be expanded with a groupware connection, where the reports are delivered by e-mail. Since the routing rules need to be adjusted at any rate, cooperation with the Professional Services should be sought in such scenarios.

24 V.24 APL

With the help of the V.24 APL XPR servers can be linked via Remote System Link (SMI protocol). Practically, this connection today takes place via TCP/IP or perhaps via ISDN. Furthermore, the V.24 APL enables transmission, reception, and operational readiness (Fax-on-Demand Server) of fax G3 over class 2 fax-modems, as well as polling from other Fax-on-Demand servers. In contrast to the Telematic APL functionality, massive limitations exist here, so that in practice the V.24 APL is no longer installed for sending and receiving fax messages.

The V.24 APL is often used for MWI signalization of new messages to Hicom 300 or Ericsson MD 110 PBXs. We recommend MWI signaling at Hicom 300 via the ISDN APL with Cornet-N.

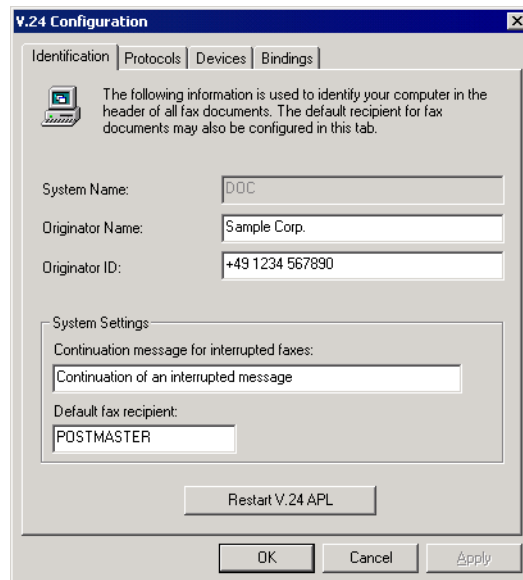
A list with all supported modems can be found in the Hardware Compatibility List (HCL) of the XPR server.

The configuration is performed from the XPR monitor as usual. The configuration dialog is started by double clicking the **Set Options** entry in the Modules window under **<V24Apl/Settings>**.

NOTE:

An administrator with *service privilege* may configure the V.24 APL unrestrictedly.

24.1 Identification



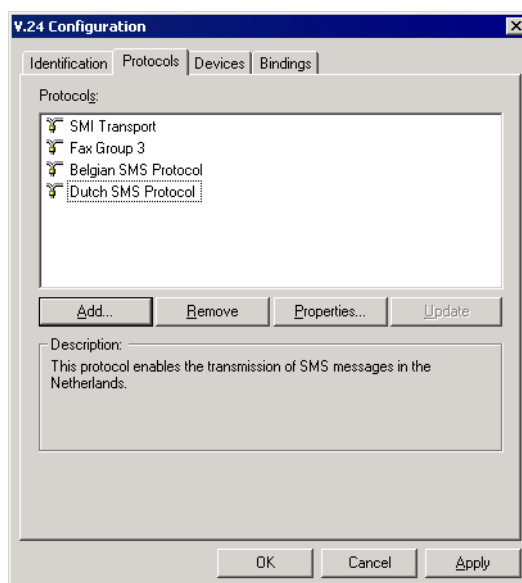
On this page default values especially for Fax G3 are configured. These are the **Originator name** (header) and the **Originator ID** that are both displayed above of a sent fax message, if the corresponding fields are empty in the user database. Furthermore, a sender receives these data on his receipt.

In the dialog entry **Continuation message for interrupted faxes:**, a text message is inserted in the page header informing the recipient that the fax transmission is being continued. If during a fax transmission the connection is interrupted, a retransmission attempt will be made. The message "Continuation of an interrupted message" would be affixed to the remaining transmission.

Enter the user ID in the **Default fax-recipient** field, to which all incoming fax messages are routed. This entry is required since analog modem technology prohibits direct inward dialing/routing to various users.

The button **Restart V.24 APL** is used for executing a restart of the APL. This option should only be used as a "last resort" when the modem blocks or can only be addressed after manually switching it off and on. Since the modem is not recognized as cleared and re-initialized by the V.24 APL after a hardware reset, a restart of the V.24 APL must be executed.

24.2 Protocols

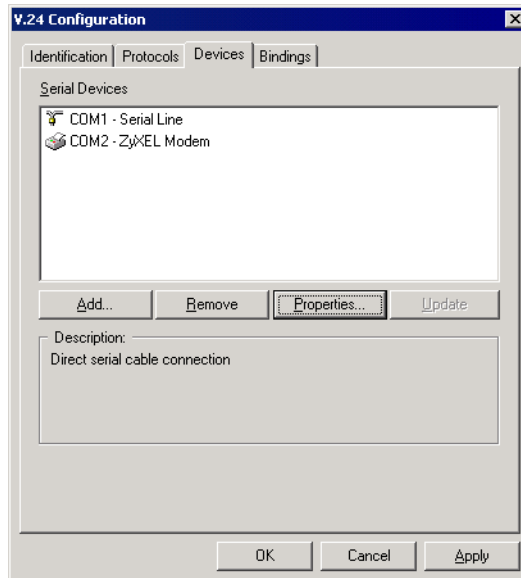


Here protocols are selected that can be connected to a device later on. Through use of the button **Add**, new protocols may be inserted into the list. Protocols that are not included in the standard package can be installed from another data medium. Removal of a selected protocol is done with the button **Remove**. The protocol can be easily re-inserted in the list at a later time.

Some protocols require further configuration in order to function properly. Settings for the installed protocols can be configured through use of the **Properties...** button.

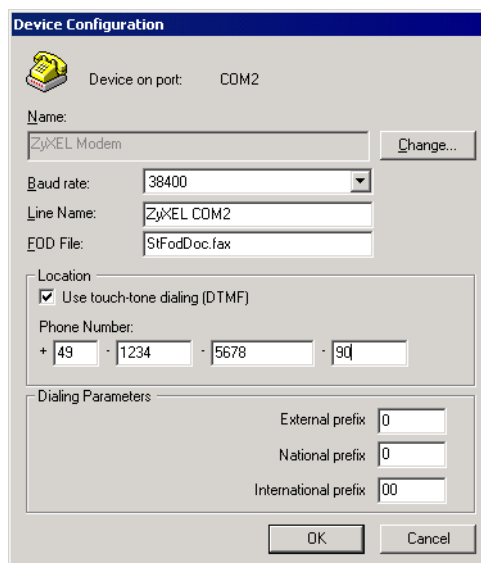
For the **Hicom CIT message signal** you need to enter the sequences for switching on and of the Message Waiting Indicator (MWI) in a Hicom PBX.

24.3 Devices



In a manner similar to that of the protocols, devices (modems) connected to a serial port can be added or removed with the **Add...** and **Remove** buttons. Various standard modems as well as a serial-line for connecting computers is included in the standard delivery. If a modem is used which is not included in the standard delivery, an adapted driver-script may be installed from disk or an equivalent data medium.

The type of device can be easily recognized by the symbol proceeding the device name. The printer symbol indicates a fax-modem, a telephone denotes that the device is a data-modem, and the line with a node indicates a serial line. Configuration of the various devices is done through use of the **Properties...** button.



The **Change...** button allows the modification of driver-scripts, if e.g. new devices connected are to the serial port. In the dialog entry **Baud rate:** the transmission speed between the computer and the modem is defined. The value entered here should always be higher than actual transmission speed so that any on-line data compression can be executed.

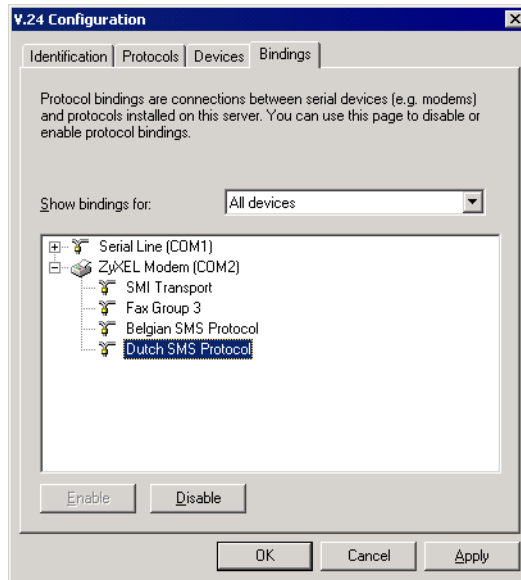
The description entered in the dialog entry **Line Name:**, will be displayed in the XPR Monitor.

Since direct inward dialing is not supported by analog modem lines, only one document per modem may be used as a **FOD File:** for fax-on-demand applications. This file must be stored in the directory <XPR

Install>\userdata\sford\faxfiles\ as with those of ISDN fax-on-demand applications.

In the **Dialing Parameters** section the **External prefix** to be dialed for external connections, the area code for local calls (**National prefix**) and an international dialing number (**International prefix**) can be entered in the appropriate fields. The last two entries are required for correct dialing within the area code and for international calls. Pulse or tone (DTMF) dialing can be selected with the option **Use touch-tone dialing (DTMF)**. In the **Phone Number:** field the complete dialing number is given in international notation. The first entry is the country code without any proceeding zeros, then the area code (also without proceeding zeros), the telephone number, and the extension number of the modem.

24.4 Bindings

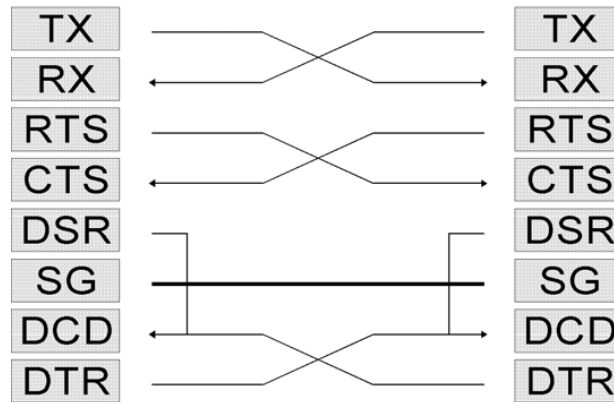


In the configuration tab Bindings, protocols are bound to the various serial devices. At first all protocols are attached to each device that is installed and supported. In the event a device should not support a specific protocol, the protocol can be selected and disabled through use of the **Disable** button. In a like manner the protocol can be reactivated through selection of the protocol and subsequent selection of the **Enable** button.

In the field **Show bindings for:** the display is either sorted by devices or protocols in the window.

24.5 V.24 Dedicated Lines

A null modem cable is used for client coupling over dedicated V.24 lines. All handshakes must be wired:



NOTE:

The client connection via a V.24 dedicated line is only mentioned here for compatibility reasons for the no longer supported XPR Client 2.50.

25 MWI to Alcatel 4400 (ABC APL)

The ABC APL serves as interface to the Alcatel 4400 PBX for notifying a user about new messages (MWI). When new messages are available, the LED at the Alcatel system telephone is activated. Reading the messages deactivates the LED again. No further functions are supported.

The name ABC APL derives from the applied Alcatel protocol ABC-A. Communication with the PBX occurs via LAN by means of TCP/IP.

NOTE:

If newer telephones of series 40x8 or 40x9 are used, MWI must be deployed via SIP or QSIG, since these telephones do not work via the ABC-A protocol anymore.

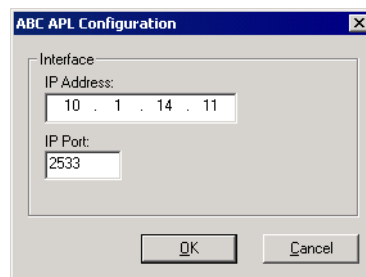
To read or manipulate messages, a user should employ common client products such as Outlook, Communications, Web Assistant, etc. or call his/her mailbox.

NOTE:

An administrator with *Service Privilege* may configure the ABC APL unrestrictedly.

The ABC APL must first be configured once via the configuration dialog in the XPR monitor, so that the Alcatel 4400 MWI service can be used. Proceed as follows:

1. Open the configuration dialog of the ABC APL in the XPR monitor.



2. Enter the PBX **IP Address** and, if required, the **IP Port** number for the ABC-A protocol. The port number is normally 2533.
3. Save the settings with **OK**.

Prerequisite for message waiting indication is an entry for each user in the **CIT** database field of the correlation database. This entry contains the routing address of the Alcatel PBX for the MTA with the corresponding extension. The MWI address of the ABC APL is: **MWI . 4400**. A complete entry for a user with extension 123 thus reads: **MWI . 4400/123**.

25.1 Telephone Display Support

To have the type (e-mail, fax, voicemail, SMS) and number of new messages displayed on the telephone, the [SignalAnyChange \[REG_DWORD\]](#) switch must be activated in the Notification APL via the registry. This occurs automatically with the initial ABC APL start.

Since this mechanism in the Notification APL leads to an increased system load, this switch can be deactivated when this feature is not required.

The displayed text for the message type can be changed via the registry values [DisplayNameEmail \[REG_SZ\]](#), [DisplayNameFax \[REG_SZ\]](#), [DisplayNameSMS \[REG_SZ\]](#) and [DisplayNameVoice \[REG_SZ\]](#).

25.1.1 Waiting-Message Retrieval

When you press the LED, the correct number of waiting messages is displayed. After you have pressed the system key under this entry again, the type and number of messages appears in the display. By hanging up or pushing the **Back** key you terminate the menu.

25.2 Several PBXs

To address several PBXs a connection must be established to each of these systems. The ABC APL can only address one system each. The problem can be averted by installing the implemented APL under a different name as service under Windows several times.

Register the ABC APL from the `<XPR Install>\bin` directory with the following command line call once more:

```
ABCApl install -name=ABCApl2
```

For each further registration the parameter `-name=<Name>` is adapted. Via the `<Name>` parameter the key in the registry for this entity of the ABC-A APL is adapted as well as the name defined, under which the entity is displayed in the XPR monitor. In this way both can be configured separately, thus the IP address of the respective PBX entered.

The logical line must be individually adapted for each further ABC APL entity, which can only be done via the registry. Modify the [LogicalLineClass \[REG_SZ\]](#) value for this purpose.

Attach the entry `ABCApl2` to the list for automatically starting the new service in the registry under `HKLM\Software\Wow6432Node\PP-COM\MRS\Services\` in the value [Access Protocol Layers \[REG_MULTI_SZ\]](#).

The logical line class must be additionally maintained in the user `CIT` field, so that a new message notification is routed to the correct PBX. Thus `MWI . 4400/4711` instead of `MWI/4711`. Important is the direct assignment to a specific PBX via a distinguishable class.

IMPORTANT:

When using the Web Assistant for configuring notifications, this entry is always made there without class.

MWI to Alcatel 4400 (ABC APL)

26 DB APL

26.1 Introduction

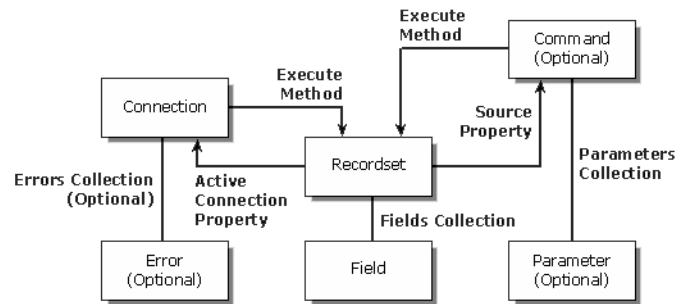
The DB APL provides a link to databases that operate on the basis of ActiveX Data Objects (**ADO**). By means of the DB APL, SQL commands of XPR server components are forwarded to the addressed data sources. For this purpose, ADO are used that can also use already configured ODBC drivers for data source queries.

ADO describes a Microsoft database interface that enables safe access to many common databases such as Oracle, Microsoft Access or Microsoft SQL Server. ADO is the successor to Data Access Objects (DAO).

The ADO data model consists of the following six components:

- **Connection (connection object):** This component contains the location and name of the addressed database and acts as some kind of “gateway” for the other components. Specifying this component is mandatory.
- **Error (error object):** Error objects are optional and are attached to the connection object, if several errors occur simultaneously.
- **Command (command object):** The command object is optional as well. It is used for executing database commands such as `UPDATE`, `CREATE TABLE` or `INSERT INTO`.
- **Parameter (parameter object):** This component is also optional and provides supplementary information with the execution of command objects.
- **Recordset (recordset object):** Each execution of database commands leads to data record objects, which contain the query results.
- **Field (column object):** Each data record object consists of a number of fields that represent one column of the data display.

The following graphic clarifies the correlation of the single components:



ADO is based on the OLE DB provider, which defines the access to a database and its version. The ODBC driver often used, which contains descriptions on data sources and thus on the connection setup with data sources, is no longer required. If, however, this driver has already been installed for linking up with a data source, it will with ADO usage be called by the OLE DB provider. The ODBC driver will consequently send the desired SQL commands to the data source.

NOTE:

You find further information on the ADO principle and fields of application on the MSDN Internet pages.

The DB APL uses ADO to access existing ODBC drivers and data sources. For example, by means of the DB APL the Application Builder and the associated VOGUE protocol can be used to configure database queries during an application. The DB APL represents an interface between application and database, since the database queries are controlled here. The corresponding SQL commands are executed in the application and not in the DB APL.

26.2 Requirements and Compatibility

26.2.1 Requirements

Microsoft Data Access Components (MDAC) with at least version 2.7 is required. MDAC contains different components for data access.

26.2.2 Compatibility

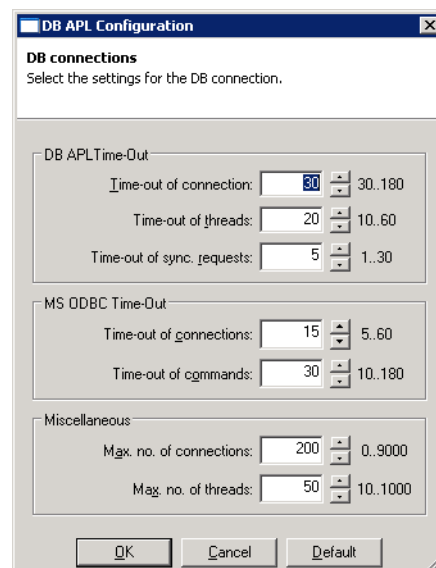
A general compatibility to any database cannot be guaranteed. The release notes list the systems that are respectively tested and released after successful test runs.

26.3 Configuration

NOTE:

An administrator with *service privilege* may configure the DB APL unrestrictedly.

The DB APL configuration tab can be invoked in the XPR monitor. In the **modules window** of your XPR servers select the **DB APL** entry and doubleclick **Set Options**. The following dialog opens:



This dialog is divided into the three sections **DB APL Time-Out**, **MS ODBC Time-Out** and **Miscellaneous**. To save your entries click the **OK** button. With a click on the **Default** button all fields are reset to their default values. During the configuration please pay attention to the minimum and maximum values of the single fields.

26.3.1 DB APL Time-Out

This section contains three configuration fields that refer to the link between application and DB APL:

Field	Description
Time-out of connection	If a connection such as the Vogue protocol with the DB APL is not used by an application for some time, the DB APL closes this connection. This period of inactivity is set here and may range from 30 to 180 seconds. Default value: 30 seconds.
Time-out of threads	A thread is an execution string within a process. Threads save resources and are more efficient than entire processes. They are used with the connection to the database. The DB APL uses a so-called threadpool via which the respective queries of an application to the DB APL and the replies are processed. A thread not used longer than specified here will be released again. This value should not be greater than the Time-out of connection value. The period that can be set here may range from 10 to 60 seconds. Default value: 20 seconds.
Time-out of sync. requests	Synchronous requests describe a specific type of database transactions where an ensuing transaction is not started until a reply from the database has been received. In this field you set the period available for processing transactions until the application issues an error message. The possible values range from one to 30 seconds. Default value: 5 seconds.

26.3.2 MS ODBC Time-Out

This portion holds two fields for configuring the connection of ODBC driver and DB APL:

Field	Description
Time-out of connection	If a connection of the DB APL with a database is not used for some time, the ODBC driver closes this connection. This period of inactivity is set here and may range from 5 to 60 seconds. Default value: 15 seconds.
Time-out of commands	Here you set the temporal limit for transmitting SQL commands between DB APL and ODBC driver, which are forwarded to the data source. The corresponding value may range from 10 to 180 seconds. If a database operation takes a long time, this value should be scaled up. Default value: 30 seconds.

26.3.3 Miscellaneous

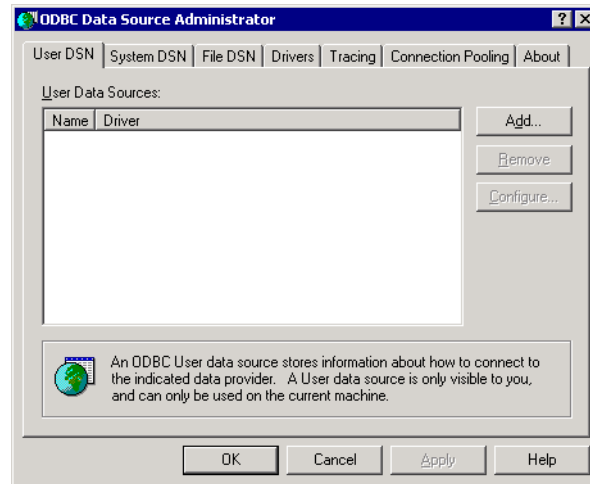
In this section you can configure two fields that refer to the link between application and DB APL:

Field	Description
Max. no. of connections	Maximum number of possible connections. The corresponding value may range from 0 to 9000. Default value: 200.
Max. no. of threads	Here you can define the maximum number of threads per connection. The corresponding value may range from 10 to 1000. Default value: 50.

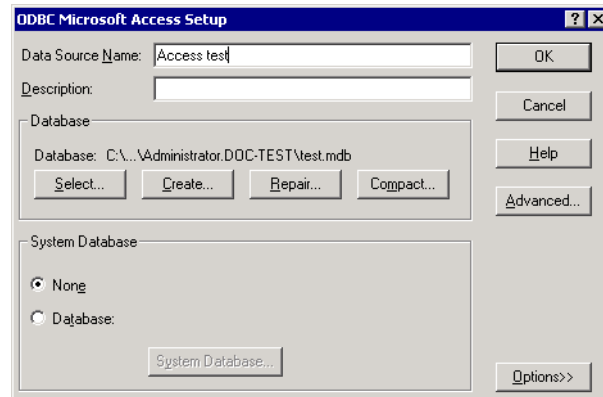
26.4 Configuring a Database for Testing Purposes

For testing the database query by means of the DB APL, you can use the **ODBC Data Source Administrator** to configure data sources of different types. On a 64-bit Windows you need to start the **ODBC Data Source Administrator** in the version for 32-bit applications, because XPR is not a 64-bit application. You do this via **Start > Run > %SystemRoot%\SysWOW64\odbcad32.exe**.

After starting the ODBC Data Source Administrator, select the **User DNS** tab:



Click the **Add...** button and select a driver for a data source in the opening dialog. For example, if you use the driver for a **Microsoft Access Data Source**, the following dialog opens:



Here you can perform various settings and confirm them with the **OK** button. For configuration information please click **Help**.

The configured data source is now listed in the ODBC Data Source Administrator and can be called with SQL commands by different APLs or client applications of the XPR system. For addressing the data source use `NVS : SQL / <data source>`. `<data source>` refers to the defined name of the data source in the ODBC Data Source Administrator. In the **XPR monitor** you can track the single processes of the database connection.

27 Report APL and Report Schedule APL

27.1 Preliminary Remarks

27.1.1 How is this Chapter structured?

The document starts with a general introduction to the reporting principle. After that, a description of how reports are generated follows. Important terms explained in this context are layouts, resource files and jobs.

The reporting feature is performed by two APLs, so that a description of the Report APL (RepAPL) and Report Schedule APL (RepScheduleAPL) configuration dialog follows, before we exemplify the step-by-step generation of a report by an example.

In addition you will be provided with a short introduction to the creation of layouts, which serve as a form of template for creating reports.

Subsequently, the created DBase/SQL databases as well as the XPR database structure will be outlined. Then follows a description of the available layout files for the default and TUI¹ (Telephone User Interface) reports for PhoneMail and VMS. A reference section, in which you can look up the structure of databases for the telephone user interfaces, comes next. In addition, the databases for users, groups and NCO location information will be described.

1. The TUI reports currently support PhoneMail and VMS.

27.1.2 The Databases

The reporting feature uses the information stored as raw data in a database system to create reports.

In case of a XPR system reinstallation only the connection via the **ADO** database interface to an SQL database can be established. An **SQL** database is a relational database, in which the data sets of a file are stored in different tables, which may be interconnected via keys. New entries are assigned to the respective table. The ADO interface, a further development of DAO, manages the connection to an SQL database.

NOTE:

The Microsoft **SQL Server Desktop Engine (MSDE)** for short), which represented a free option to use an SQL server for simple applications, has been replaced by Microsoft with the also free-of-charge **Microsoft SQL Server 2005 Express Edition**. Like *MSDE*, the *Microsoft SQL Server 2005 Express Edition* is a slim version of the *Microsoft SQL server*. With the SQL Server 2005 Express Edition technical options have been increased against MSDE and an administrator tool with graphic user interface (*SQL Server 2005 Management Studio Express Edition*) provided.

Owing to the replacement of MSDE with the SQL Server 2005 Express Edition, MSDE will not be supported on the XPR system any more and the associated setup files no longer supplied. For distribution reasons, the setup files of the SQL Server 2005 Express Edition cannot be shipped but you can download a version from the Microsoft homepage free of charge. The *installation* of or an *upgrade* from MSDE to the SQL Server 2005 Express Edition is described in the manual *OpenScape Xpressions V7 Server Installation*. Switching from MSDE to the SQL Server 2005 Express Edition does not result in any modifications when using the Report and the Report Schedule APL. When registering a database with the Report APL you merely need to note that, contrary to the MSDE installation, no default user and no corresponding default database is automatically provided. After you have installed the SQL Server 2005 Express Edition you need to create an individual user with associated database yourself.

In case of **dBase**, one of the first widespread database systems, each table is stored in a file. Also indices and memos are stored as individual files. New entries are simply attached to a file. In case of dBase databases, **CodeBase** serves as database interface, which enables the creation of compressed databases.

NOTE:

Connecting a **dBase** database using **CodeBase** is only supported in case of an XPR system upgrade with an already existing dBase database connection. When the XPR system is newly set up, a new connection to a dBase database cannot be established any more.

You can obtain continuative information, for example about the databases structure, from [Section 27.10, “Basics on the Raw Data Database Tables”](#).

27.1.3 Backup / Restore

Before you configure a reporting system using the Report APL and the Report Schedule APL, definitely save the log files of the databases via a suitable backup concept! If the created databases of the Report APL should become defect for some reason, they can be completely restored out of the saved log files.

You find introductory information about database systems used in [Section 27.10, "Basics on the Raw Data Database Tables"](#), on page 1365.

You are free to decide which backup concept to use for this purpose.

NOTE:

Please keep in mind that the time taken by the backup respectively restoration process depends on the size of the data amount.

If your created databases should indeed become defect, please proceed as follows to restore your databases:

1. Stop the Report APL. First click on **Start** and then on **Run...** . Enter the command `net stop repapl` there and confirm the entry with **OK**.
2. Depending on the database you use (ADO or CodeBase) you need to continue as follows:

- f) In case of **ADO** with SQL databases:

Delete the two *.dbf files in the directory <XPR Install>\Stat. Delete the tables in the SQL database. To this, you need to manually log on to the database and remove each table individually. This is done easiest with the *Enterprise Manager*, which is a component of the Microsoft SQL server delivery. When using the *SQL Server 2005 Express Edition* the *SQL Server 2005 Management Studio Express Edition* is available as graphic administrator tool. This free tool can be separately downloaded from the Microsoft homepage or is integrated in the *SQL Server 2005 Express Edition with Advanced Services* version.

- g) In case of **CodeBase** with dBase databases:

Delete your created DBase export databases and the `dbstat.ini` file in the `<XPR Install>\Stat` directory.

NOTE:

If a connection between the Report APL and a database is newly established, CodeBase will not be supported any more. You can only revert to connections already configured with CodeBase.

NOTE:

You find an introduction to the differences between CodeBase and ADO in [Section 27.10.1, "Short Introduction to the Databases used", on page 1365](#).

3. Copy the saved log files to the `<XPR Install>\Stat` directory.
4. Start the Report APL so that it can create the DBase of SQL databases again from the existing raw data. First click on **Start** and then on **Run...** . Enter the command `net start repapl` there and confirm the entry with **OK**.

IMPORTANT:

A partial import of secured log files is not supported. With an import the databases must always be completely regenerated. Any other method may lead to inconsistent databases.

In the maintenance script you may adjust the time range the raw data in the log files will be stored in the `<XPR Install>\Log` directory according to your individual needs. Please note however that you will need more disk space if you store the files locally for a longer period of time.

27.2 Introduction: What is Reporting?

The task of reporting is to prepare and visualize statistical data about the proceedings in the XPR system (services, agents, groups, lines, etc.). The reports are a control mechanism aiming to give you an overview about the activities within the XPR system.

These functions are performed by two APLs, the **Report APL** and the **Report Schedule APL**, as well as one **runtime component to create reports**. While the Report APL operates independently from external components, the Report Schedule APL requires the installation of either *Crystal Reports Version XI* or *Crystal Reports 2008* in the Developer Edition in each case. As alternative to a chargeable version by Crystal Reports you can also use the open source project *BIRT*. *BIRT* is shipped on the XPR product data carrier and copied to the `<XPR Install>\ReportEngine` directory upon the installation of the Report Schedule APL. If you have installed both supported report engines (Crystal Reports and BIRT) on one system, only the Crystal Reports engine will be recognized and used by the Report Schedule APL. The setup always includes the installation of the runtime environment for Crystal Reports.

NOTE:

The Report Schedule APL must be explicitly informed about the use of *Crystal Reports 2008*. The registry value `CRDOTNET [REG_DWORD]` needs to be adjusted for this purpose.

The **Report APL** is in charge of writing APL raw data compiled by the `XMRSvc` in log files into a database. The **Report Schedule APL** depends on the Report APL, since in the Report Schedule APL reports are written from the raw data previously written into the database. This is done by means of so-called layouts.

For the Report Schedule APL you need either the *Developer Edition of version XI* or higher by **Business Objects Crystal Reports**, which is subject to license conditions and thus chargeable, or the open source program **Business Intelligence and Reporting Tools (BIRT)** of the Eclipse Foundation from *version 2.1.3*. These programs include a runtime component to create reports used by the Report Schedule APL.

BIRT is an Open Source program and operated within an *Eclipse SDK*. It is included in the scope of delivery and copied into the `<XPR Install>\ReportEngine` directory upon the Report Schedule APL installation. Like Crystal Reports, BIRT contains the basic functionality for designing and creating a report. Creating and designing reports, however, requires the framework eclipse, which can be obtained from the Internet free of charge. Please refer to [Section 27.6, "Creating a Report"](#) for a short introduction

to both programs or editing and designing a report.

IMPORTANT:

If you have installed both supported report engines (Crystal Reports and BIRT) on one system, only the Crystal Reports engine will be recognized and used by the Report Schedule APL. The layout files for BIRT can thus not be used.

For example, you can use the output reports to determine the phone call activities for the entire system respectively for each subscriber. From the number of calls and the duration of incoming, forwarded and outgoing calls you can deduce the load of various resources at specific times. You find further notes for these reports in [Section 27.9, “Available Telephone User Interface Reports \(TUI\) Reports”](#), on page 1350.

27.3 Functionality

Raw data and statistical information stored in SQL databases serve as data base for the Report APL. For upgrades, DBase databases can also be used. Such data and information are provided by the XPR scripts and applications, such as the `IP APL` or the `VOGUE` script. The data of the internal XPR databases (**Journal**, **Correlation**, **Gebühren**) do not deliver any raw data. For using the data of these databases please note [Section 27.6.5, “Creating a Report for the XPR Databases”](#).

NOTE:

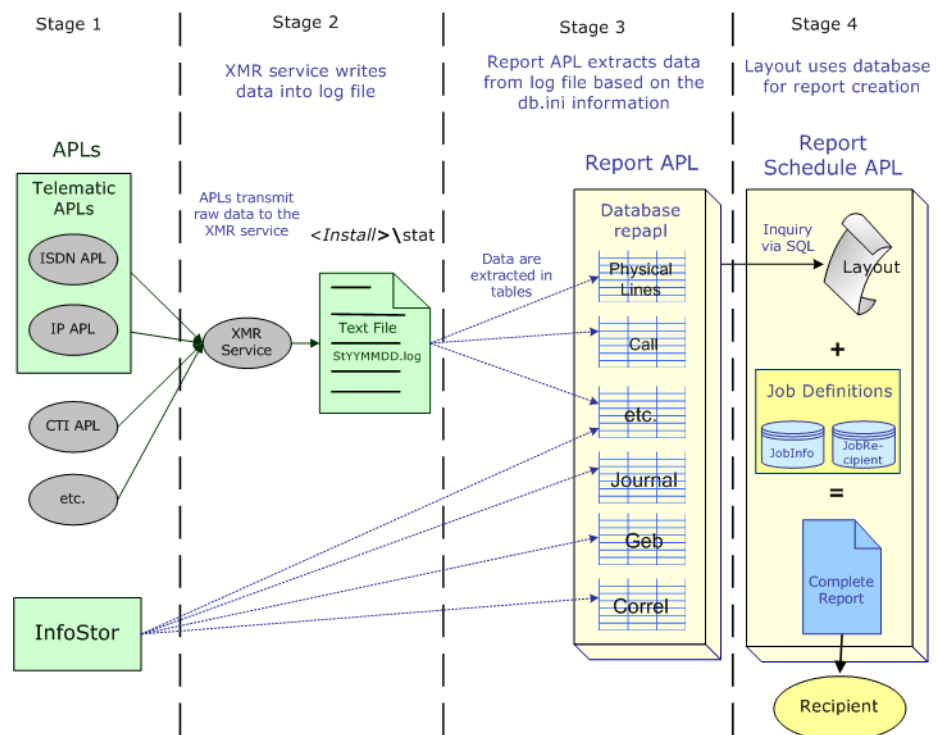
Only the APLs released in the value `StatisticsClasses [REG_MULTI_SZ]` deliver raw data. If value `*` is set, all APLs may generate raw data. We recommend not to set value `*` since the respective log files would become too large.

27.3.1 Report Generation

A report is generated from the **raw data** delivered by the APLs and a **layout**, a kind of formal template for reports. The layout determines which data are used and how they are represented in the report. Via the Report Schedule APL configuration you can define so-called **jobs** to determine which report is created with which layout and when, and who is to receive the result in which format. Reports are created by a so-called Report Engine, a runtime component as contained in Crystal Reports or BIRT. Depending on the selected export format, you can view the thus created report with different external programs such as Microsoft Excel. The Report Schedule APL has thus **three media** to generate a report:

1. The **raw data** delivered by the APLs and scripts in *log files* to the Report APL and stored in a database. The internal XPR databases such as Journal, Geb or Correl do not deliver any raw data stored in log files. For using the data of these databases please note [Section 27.6.5, “Creating a Report for the XPR Databases”](#).
2. The **layouts** that specify how the completed reports will look like.
3. The **jobs** created using the Report Schedule APL and determining at which time a specific report will be generated in the selected format and to which recipient it will be sent.

The following illustration shows the process of generating a report. Generating a report passes several stages. Stage 1 and stage 2 run within the XPR system, Stage 3 eventually assumes the Report APL. The Report Schedule APL is in charge of stage 4.



Stage 1

In stage 1 the XPR services (APLs) transmit raw data to the Extended Message Reporter (XMR) Service. The **InfoStor** manages the XPR databases Journal, Geb, Correl, etc. and maps the data of these databases for the Report APL.

Stage 2

In stage 2 the XMR service writes the raw data it has received in a **log file** of the directory <XPR Install>\stat. <XPR Install> is the directory in which your XPR system has been installed. For information about log file backup and restoration please refer to [Section 27.1.3, “Backup / Restore”, on page 1244](#).

A new log file is created for each day. This log file is a pure text file that is stored in the format `st<YYMMDD>.log`. `<YYMMDD>` represents the date at which the log file was generated, thus year, month and day. Consequently, the file name for Tuesday, September 23 2006 would be `st030923.log`.

As soon as all data has been extracted from the log file, it will be moved into the `<XPR Install>\Log` directory. Here the maintenance mechanism of the XPR server steps in. It will remove these data after a period of 60 days, if the time has not been adjusted. This deletion time can only be set by a manual modification of the maintenance script (see [Section 7.2, "Maintenance Script"](#)).

The internal XPR databases such as **Journal**, **Geb** or **Correl** do not deliver any raw data stored in log files. Such databases are managed by the **Information Store** and merely mapped for usage by the Report APL. You find the data of these databases in the directory `<XPR Install>\Infostor` and they are consequently not written in log files by the XMR service. For using the data of these databases please note [Section 27.6.5, "Creating a Report for the XPR Databases"](#).

Stage 3

In stage 3 the Report APL extracts the data from the log file once or more often a day, if this should be necessary for the creation of the reports. Data are extracted from the log files based on the control information of the `ini` file (Crystal Reports) respectively `properties` file (BIRT), stored in the `<XPR Install>/res/RepApl` directory.

NOTE:

In case of the **ADO** option the `adodb.ini` initialization file is applied. In case of reinstallations, the **CodeBase** option is no longer available. It is merely still supported when the XPR system is upgraded and with a connection to a CodeBase database already established. With a configured database option **CodeBase**, the `db.ini` initialization file is used.

The Report APL then stores such data in tables of an SQL database (ADO option), the format of which can be read by the *Crystal Reports* or *BIRT* program used in the next stage. The database is called **repapl**. This name is used for a connection with Crystal Reports respectively for SQL queries. In case of dBase databases each table is stored in an individual database (CodeBase option).

The XPR databases **Journal**, **Correl**, **Geb** and others are found in the Infostor and are mapped for the Report APL merely as databases; here the path does not lead via the log files. The mapped XPR databases are also stored in the `<XPR Install>/res/RepApl` directory. Such databases have not been conceived for reporting use, though, and can hardly be reasonably linked in a report via key relations. For using the data of these databases please note [Section 27.6.5, "Creating a Report for the XPR Databases"](#).

Stage 4

In stage 4 the actual report is generated.

The Report Schedule APL uses an external runtime module that generates the reports. This module is offered by the reporting systems Crystal Reports or BIRT and requires samples or templates, so-called **layout files**, for its work. These layout files define the format and the contents of the report to be created. You find layout files in the directory `<XPR Install>\res\RepAp1` (see [Section 27.3.2, “Layouts”](#)).

NOTE:

Please note that the runtime components of Crystal Reports respectively BIRT only consider their own layout formats for report creation. I.e. layout files with the extension `rpt` are used by Crystal Reports for report creation, while BIRT only uses layout files with the extension `rptdesign`.

NOTE:

If you have installed both supported report engines (Crystal Reports and BIRT) on one system, only the Crystal Reports engine will be recognized and used by the Report Schedule APL. The layout files for BIRT can thus not be used.

The jobs that determine the report parameters (recipient, format, time range, frequency of execution) are specified by the values in the **JobRecipient** and **JobInfo** databases. You configure these parameters in the configuration dialog of the Report Schedule APL. See [Section 27.5, “Report Schedule APL Configuration”](#) and [Section 27.7, “Structure of the XPR and Reporting Databases”](#).

The layout file is now filled with current data by the runtime component of the reporting system (Crystal Reports or BIRT) used. Afterwards, the created report may be forwarded to several recipients or it may be stored in a directory that has been selected before.

IMPORTANT:

Reports should not be created in peak times as that influences the system performance negatively.

27.3.2 Layouts

A layout is a type of pattern that serves as template for the reports to be generated. It contains the specifications that determine the representation of the database fields. Layouts can be flexibly modified or expanded. For example, you

can add fields that calculate the sum or average of the represented database fields. The formal field representation can also be adjusted to subjective preferences.

A resource file may be assigned to a layout, thus to a layout file. The resource files offer the possibility to influence the layouts without changing them permanently. The resource files contain names in different languages for the layout file text fields used. The corresponding fields are referenced via the same variable names. The following lines show an example of the field definitions of a resource file:

```
[GERMAN]
Caption="Gebührenerfassung pro Teilnehmer"
Head01="Benutzername"
Head02="Kosten in Euro"
Head03="Dienst"
Head04="Empfänger"
Body01="Gesamtsumme:"

[ENGLISH]
Caption="CDR per User"
Head01="User Name"
Head02="Call Charges in Euro"
Head03="Service"
Head04="Recipient"
Body01="Total Amount:"
```

NOTE:

In the `ini` respectively `properties` files you can create resources for several languages. Layout files with the format `rpt` (Crystal Reports) can access the `ini` files. The resource files for the layout files of the format `rptdesign` (BIRT) are subject to the same mechanism, but cannot contain several language resources. I.e. for each language a corresponding resource file with the extension "`properties`" must be created.

When the Report Schedule APL reads the resource file and the system is set to German, the fields of the associated layout file are filled with the field definitions from the `[GERMAN]` section. The contents of the fields that are similar in the resource and layout file are overridden in the layout file. In other words, the field called `Caption` in the layout file contains the content "CDR per User". Depending on the current system language the contents of the text fields are adjusted to the layout file in this way.

Please note that all fields specified in the resource file such as `Caption`, `Head01`, etc. must be available in the layout file. A single field missing in the layout file leads to the report creation being declared as faulty and the creation will be abandoned.

In the `[COMMON]` section global parameters are defined. For example, the name of the server to be used can be specified here via the `Server` parameter.

The assignment resource file and layout is effected via the file name which is the same for both files. It only differs in the ending. The layout file features the extension `rpt` (for Crystal Reports) respectively `rptdesign` (for BIRT), the resource files ends in `ini` (Crystal Reports) respectively `properties` (BIRT).

NOTE:

Please note that the runtime components of Crystal Reports respectively BIRT only consider their own layout formats for report creation. I.e. layout files with the extension `rpt` are used by Crystal Reports for report creation, while BIRT only uses layout files with the extension `rptdesign`.

NOTE:

If you have installed both supported report engines (Crystal Reports and BIRT) on one system, only the Crystal Reports engine will be recognized and used by the Report Schedule APL. The layout files for BIRT can thus not be used.

If you want to change a field label respectively its content in a layout, modify the corresponding field in the `ini` respectively `properties` file. For, modifications to the layout files will be overridden and thus deleted by the resource file in the course of report generation.

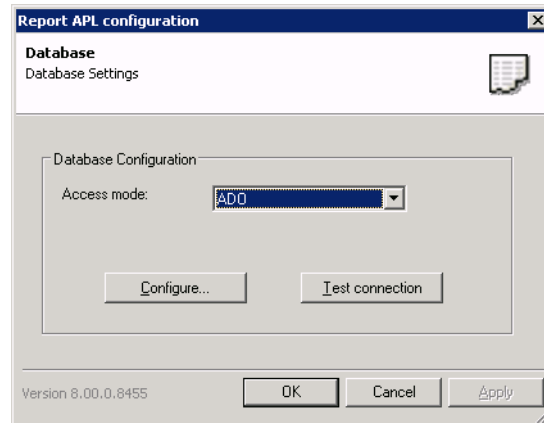
The creation or modification of resource files can be performed in the Report Schedule APL configuration dialog. See [Section 27.5.1.5, "Information Tab"](#).

The default reports, which you can use for report generation, are delivered with the Report Schedule APL setup. You find these layout files and the associated resource files in the `<XPR Install>\res\RepApl` directory. You can create new layouts using Crystal Reports or BIRT. The new reports must also be contained in the mentioned directory. You can obtain a short introduction to Crystal Reports XI and layout creation from [Section 27.6.2, "Creating a Layout with Crystal Reports XI"](#). Analog you receive in [Section 27.6.3, "Creating a Layout with BIRT"](#) a short introduction to working with BIRT.

27.4 Report APL Configuration

Double-click the **RepAPL** module entry in the XPR monitor in the **Modules of** window to open the configuration dialog. Select **Set Options**. The configuration dialog merely consists of an overview.

In the Report APL you perform the configuration for a database connection. Via such a connection the Report APL can export the collected raw data of the system to an external database.



The access modes **ADO** and **CodeBase** are currently available for a database connection.

- **ADO**
In this setting the Report APL cooperates with an external SQL database that supports the ADO database interface.
- **CodeBase**
In this setting the Report APL cooperates with dBase databases (dbf files) of the XPR server.

NOTE:

The **CodeBase** option is only supported for reasons of compatibility to databases already configured. New installations always require the use of the **ADO** option.

An ADO database connection is established via the **Configure...** button. The subsequent function test occurs after a click on **Test connection**.

NOTE:

After you have clicked on the **Test connection** button, a successful connection can only be established if you have saved the specified password on the **Connection** tab with the **Allow saving password** option (see [Section 27.4.2, "Connection Tab"](#)). Since enabling this button does not provide the option to enter

the password, the connection could otherwise not be properly checked. If you do not want to save the password for security reasons, use the **Test connection** button on the **Connection** tab.

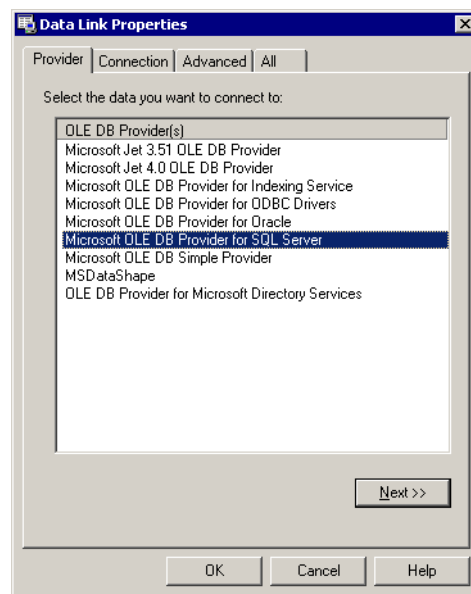
Configuring the database connection via ADO is done with the dialogs of the data linkage properties of Microsoft Windows. The **Help** button in these dialogs opens the data linkage properties of Microsoft Windows.

27.4.1 Provider Tab

On the **Provider** tab you select the OLE database provider used by the Report APL for accessing the management system of the external database.

IMPORTANT:

The Report APL was tested connected to the Microsoft SQL server respectively to the SQL Server 2005 Express Edition. Therefore only the **Microsoft OLE DB Provider for SQL Server** option may be selected in this dialog. All other providers of the list are currently not supported.



The **Next** button leads to the next configuration step – the **Connection** tab.

27.4.2 Connection Tab

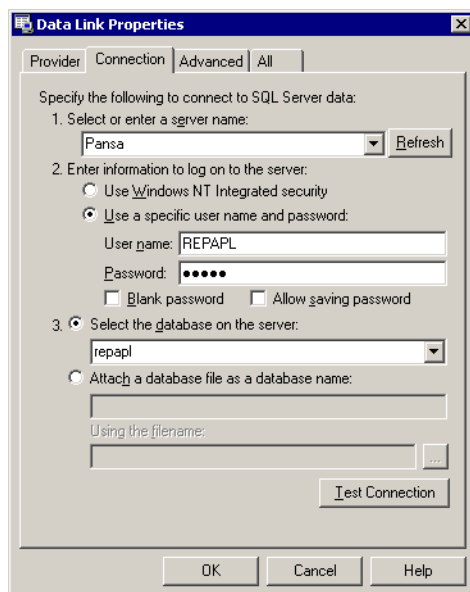
In the **Connection** tab the connection information for the database connection selected in the **Provider** tab is defined.

NOTE:

The settings indicated in the **Connection** tab depend on the provider previously selected.

IMPORTANT:

When registering a database with the Report APL please note for the **Microsoft SQL Server 2005 Express Edition** that, contrary to the **MSDE** installation, no default user and no associated default database is automatically provided. After you have installed the SQL Server 2005 Express Edition you need to create an individual user with associated database yourself.



The connection information is divided into three areas:

1. **Server Name**

Defines the server name on which the external database is configured. The server name may either be entered directly in the text field or selected from the associated suggestion list.

Via the **Refresh** button the suggestion list for server selection can be updated.

2. Logon Information

IMPORTANT:

The **Use Windows NT Integrated security** option is *not* supported and *must not* be used for the Report APL login.

For logging on to the database server you need to enter your **User name** and the associated **Password** in the corresponding fields. Administrator privileges that allow access to the selected database must be assigned to this user name.

If the **Blank password** option is active, logging in at the database server only requires the defined user name but no password. The **Allow saving password** option makes sure the password configured for accessing the database is saved. Therefore this option must always be activated when the **Blank password** option is disabled.

3. Database selection

The exported data of the Report APL can be saved in an existing database on the external database server. Activate the **Select the database on the server** option and enter the name of the desired database in the associating text field. The database to be used can also be selected from the suggestion list in the text field.

NOTE:

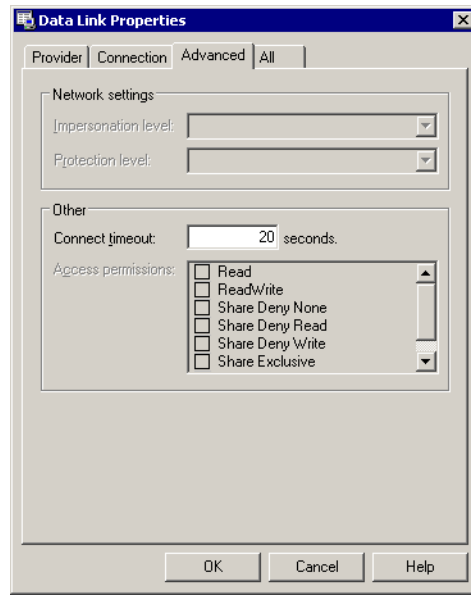
The Microsoft SQL server in version 7 or older will not be supported any more. Compatible to the XPR system is the Microsoft SQL server 2000 (corresponds to version 8) or later versions of the Microsoft SQL server.

The **Attach a database file as a database name** option can be selected for the Microsoft SQL server 2000 or later versions. Enter the database name to be used for the transmitted database file in the **Attach a database file as a database name** field. In addition, you can specify the name of the database file in the **Using the filename** field. Via the  icon you can also look for the database file to be used.

With the **Test Connection** button the attempt is made to establish a connection to the defined database server with the settings performed. If this attempt fails, check the settings for correctness.

27.4.3 Advanced Tab

In the **Advanced** tab additional settings for the Report APL database connection are defined. These settings depend on the selected database provider. With the supported selection of the **Microsoft OLE DB Provider for SQL Server** merely the **Connect timeout** can be defined.



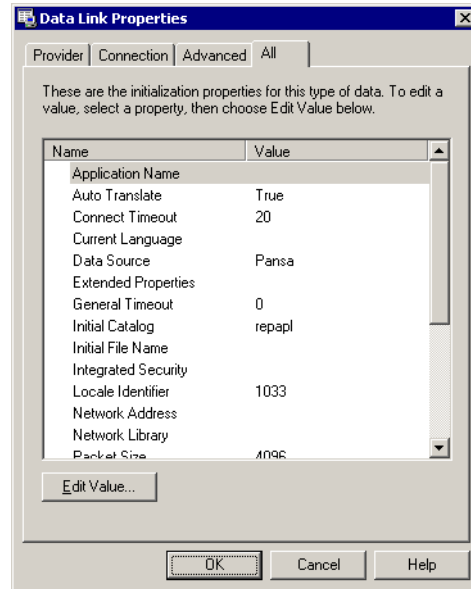
In the **Network settings** section you can perform settings as regards the **Impersonation level** and concerning the **Protection level**. In case of the Microsoft OLE DB Provider for SQL Server these settings cannot be modified.

The **Connect timeout** field is for setting a period after which a connection attempt is terminated if no connection could be established until then. The entry is made in seconds. No timeout is defined by default.

In the **Access permissions** section you can set specific privileges for other users. In case of the Microsoft OLE DB Provider for SQL Server this setting cannot be modified.

27.4.4 All Tab

The **All** summarized all settings of the database connection.



Via the **Edit Value...** button you can edit the selected entry. We recommend not to modify the values.

With a click on the **OK** button you complete the configuration of the database connection.

27.5 Report Schedule APL Configuration

Double-click the **RepScheduleAPL** module entry in the XPR monitor in the **Modules of** window to open the configuration dialog. Select **Set Options**. The configuration dialog is divided into the three tabs **Reports**, **Layouts** and **Parameters**.

NOTE:

The data of the **Times** and **Export** tabs are saved in the **JobInfo** database. See [Section 27.7.5, “JobInfo”, on page 1341](#). The specifications on the **Recipient** tab are saved in the **JobRecipient** database. See [Section 27.7.4, “JobRecipient”, on page 1341](#).

27.5.1 Reports Tab

The **Reports** tab is divided into two work spaces.

In the top section you can decide which report to generate. The window includes information on **Name**, **Status**, **Last Status** and **Layout** of a report. The entries under **Name** are preceded with an icon that indicates the report status.

Icon	Status	Description
	Stopped	This yellow icon indicates a deactivated report job.
	Active	This green icon indicates an activated report job.
	Performance	This icon indicates a report job being executed.
	Done	This icon indicates a report job having been executed.

The status of the reports changes during and after the execution. During the execution the status *Executing* is displayed. After the execution the status changes to *Finished*.

This change of status is not automatically updated. The change becomes only visible if you close the dialog and reopen it.

NOTE:

Please note that the runtime components of Crystal Reports respectively BIRT only consider their own layout formats for report creation. I.e. layout files with the extension `rpt` are used by Crystal Reports for report creation, while BIRT only uses layout files with the extension `rptdesign`. Verify that in the layout column the file name extension corresponds to the reporting system (Crystal Reports or BIRT) you use.

If you have installed both supported report engines (Crystal Reports and BIRT) on one system, only the Crystal Reports engine will be recognized and used by the Report Schedule APL. The layout files for BIRT can thus not be used.

With the help of the three buttons in the top right work space you may **Activate** or **Deactivate**, **Add** and **Remove** the report depending on its current status. You can only add layouts that you have already introduced to the Report Schedule APL. See [Section 27.5.2, “Layouts Tab”, on page 1273](#).

NOTE:

The layout file of the **default charges report** is automatically selected upon the Report Schedule APL installation and displayed on the *Reports* tab with the status *Stopped*. This layout file cannot be removed.

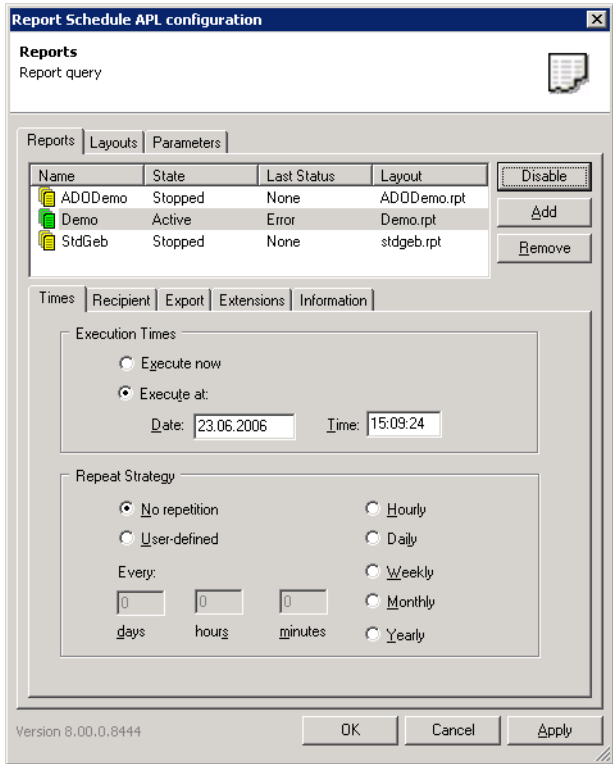
The lower section of the **Reports** tab contains setting options for the reports and consists of the tabs **Times**, **Recipient**, **Export**, **Extensions** and **Information**. The specifications on these tabs always refer to the currently selected report and describe the settings of a job for a report.

NOTE:

The data of the **Times** and **Export** tabs are saved in the **JobInfo** database. See [Section 27.7.5, “JobInfo”, on page 1341](#). The specifications on the **Recipient** tab are saved in the **JobRecipient** database. See [Section 27.7.4, “JobRecipient”, on page 1341](#).

27.5.1.1 Times Tab

In the **Times** tab, within the **Execution Times** section, you can assign either **Execute now** or, via **Execute at**, a fixed time to a report job.



The **Repeat Strategy** section contains options for you to decide whether a job is to be repeated and if so, in which intervals. One of the following three options must be selected: **No repetition**, **User-defined** or a **default interval**.

For a **user-defined** interval between two report creations you can specify **days**, **hours** and **minutes** under **Every**. Entry 1 for days, 2 for hours and 3 for minutes means that after completing a report creation, this report will be recreated after 1 day, 2 hours and 3 minutes.

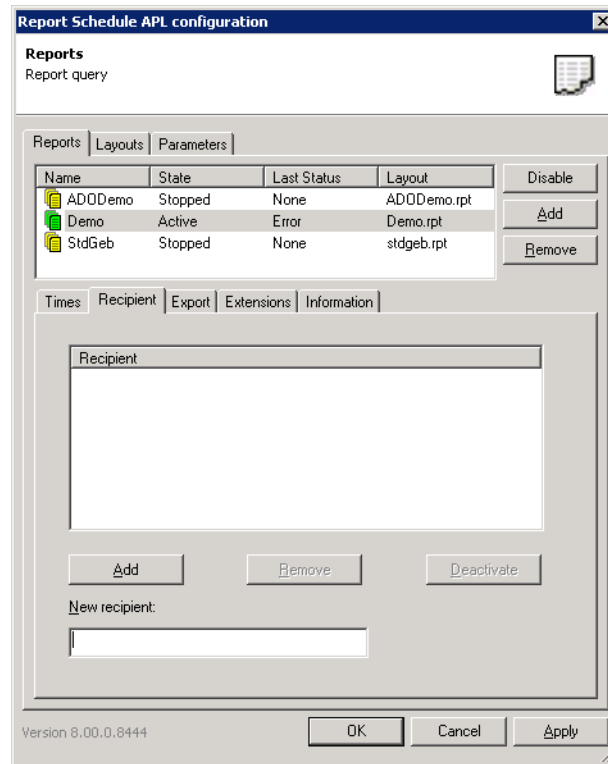
You can also select one of the default intervals **Hourly**, **Daily**, **Weekly**, **Monthly** or **Yearly**. The bench mark is always the completion of a report creation. In other words, after exactly 60 minutes, 24 hours, 7 days, etc. a report is recreated after its previous successful creation.

NOTE:

Make sure that the data are available for the corresponding time periods. In other words, a report generation in an hourly interval is only useful if sufficient data occur in the system within an hour.

27.5.1.2 Recipient Tab

Since the reports are stored on the local hard disc of the XPR server and are overwritten with every report regeneration, they should be sent as message (e.g. via e-mail).



In case of an e-mail address the recipient receives a XPR message after the report generation that contains the generated report as file attachment. The system always inserts the recipient address as NVS address. See also [Section 2.5, “XPR Addressing”, on page 73](#).

You can also specify a printer of the Print APL or a fax calling number (e.g. NVS : FAXG3/1234567890) as recipient.

You add new entries to the recipient list by specifying an address in the **New recipient** field and clicking on **Add**. The entered address will be integrated in the list. You can repeat the procedure to specify several recipients.

Existing entries can be **Removed** or **Deactivated**. With deactivated entries the button changes so that they can be **Activated** again. An activated recipient is indicated with a green tick, a disabled recipient with a red cross. You delete recipient addresses by selecting the relevant address and clicking on **Remove**.

27.5.1.3 Export Tab

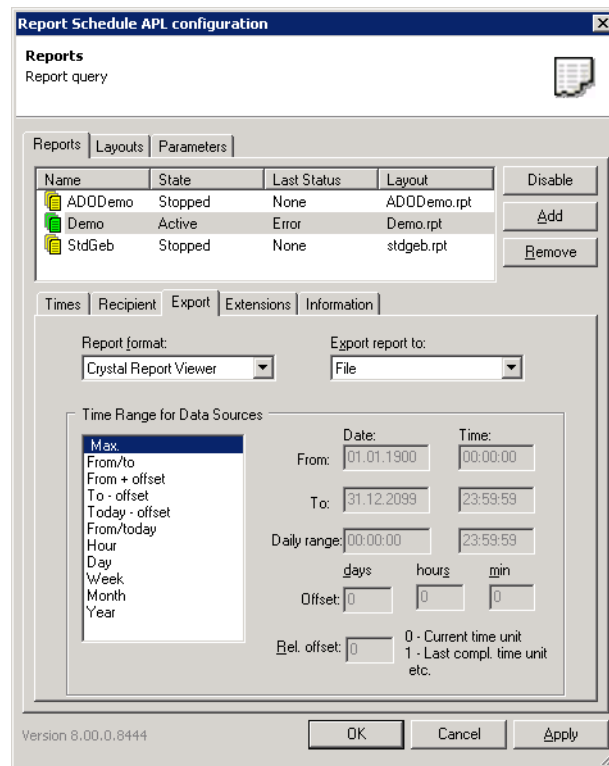
On the **Export** tab you select the **Report format**, the **Time Range for Data Sources** and the destination of the report via the option **Export Report To**.

In most cases, a report is developed for a special export format. For example, the Rich Text Format (RTF) is used for TUI reports. The quality of the output in another export format may then be much worse or specific contents such as diagrams or graphics cannot be displayed. We recommend to use the RTF format for TUI reports and the unformatted text format or the format for Crystal Viewer for other reports. Please use the free of charge *Microsoft Viewer for Word* or *Microsoft Word* for viewing the exported RTF reports. You can download the *Microsoft Viewer for Word* from the download section of the Microsoft homepage. The *WordPad* coming with Microsoft Windows is not able to display the reports correctly.

To view reports in the Crystal Reports format you need the freely available viewer, which, however, is not included in the delivery. You find this viewer under <http://www.sap.com/solutions/sapbusinessobjects/sme/reporting/viewer/index.epx>. As of *Crystal Reports 2008* the file format for the *Crystal Reports Viewer* has changed to `.rpt`. The previous file format (`.rep`) cannot be generated as of *Crystal Reports 2008* anymore. However, you can rename the old reports after `.rpt`. The new viewer is then able to recognize these and displays them as well.

IMPORTANT:

If the Report Schedule APL as well as the Crystal Report Viewer are installed on the XPR server and you uninstall one of these components, files will be deleted that both of the components need. To avoid this, please start the server setup in “repair” mode after a Crystal Report Viewer uninstallation. In this way the missing Report Schedule APL files will be reinstalled.



Under **Report Format** you can determine in which file format the report job is to be put out.

For the layout files with the extension `rpt` supported by *Crystal Reports XI* or *Crystal Reports 2008* the following formats are available for selection:

- Crystal Reports Viewer (*.rep with *Crystal Reports XI* or *.rpt from *Crystal Reports 2008*)
- Rich Text Format (RTF)
- PDF
- Hypertext Markup Language (HTML)
- Comma-separated values
- Text
- Tab Text
- Microsoft Word
- Microsoft Excel
- Fax G3 and Fax G4 in a proprietary format by Cycos as well as in the standard TIFF format.

For the layout files with the extension `rptdesign` supported by **BIRT** the formats *PDF* and *HMTL* are available for selection so far. We recommend the format *PDF*.

The **report destination** is always a **file**. It is not possible to make any changes here.

In the **Time Range for Data Sources** the data used for a report are determined by means of a temporal assignment. On the left hand side you can select different time ranges, which can be configured by means of the settings on the right. Depending on the time range you select, only specific settings can be performed. Settings that cannot be performed are shaded gray.

As time range you specify a start and end time (**from ... to**). Each point in time consists of a date and a time. Such points in time form a framework from which the respective data are used for a report.

The following four basic time ranges are possible:

Time range	Description
All database entries (Max.)	No further settings can be performed, since all available data are used. Consequently, there is no temporal restriction.
Time range with date specification (From/to, From/ today)	For these time ranges you need to specify a start date respectively a start time and • an end date respectively an end time (<i>From/to</i>) or • as end time the current date with the current time (<i>From/ today</i>).
Time range with offset specification (From + offset, To - offset, Today - offset)	When you choose these time ranges, a fixed offset will be considered beside a date. This offset may consist of days, hours and minutes and is either • added to a date respectively a time (<i>From + offset</i>) or • deducted from a date respectively a time (<i>To - offset</i> and <i>Today - offset</i>). For example, setting an offset of 5 days and 12 hours with the <i>Today - offset</i> time range enables using the data of the last 5 days and 12 hours for the report from the point in time when this configuration was selected.

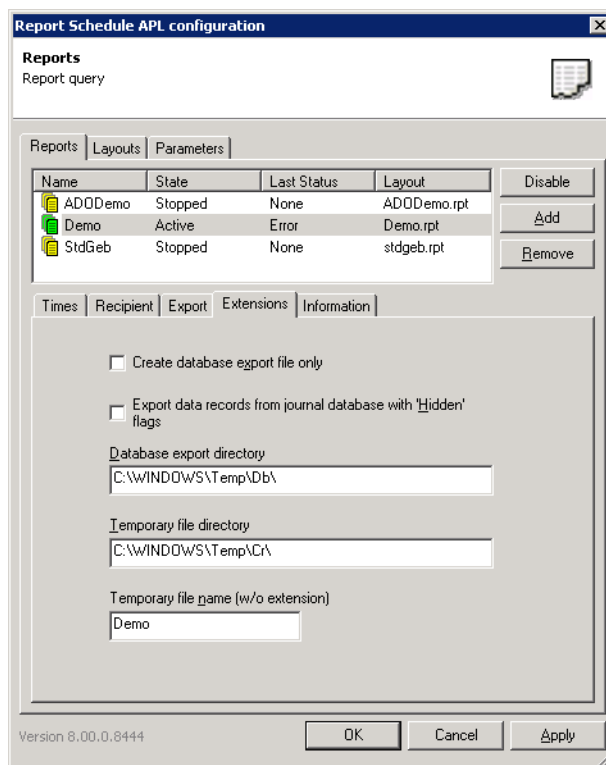
Time range	Description
Time range with specification of a relative offset (Hour, Day, Week, Month, Year)	Besides specifying a fixed offset you can also use a relative one. Each selected option refers to a corresponding time range: • from the 1st to the 60th minute of the same hour (<i>Hour</i>), • from 0:00 to 23:59 of the same day (<i>Day</i>), • from Monday 0:00 to Sunday 23:59 of the same week (<i>Week</i>), • from the first day, 0:00 to the last day, 23:59 of the same month (<i>Month</i>) and • from 1 January, 0:00 to 31 December, 23:59 of the same year (<i>Year</i>). If you select a relative offset of 0, data from the start of the respectively current time range to the current point in time are used for the report. A relative offset of 1 means that the last complete time range is used. The following example clarifies the function of a relative offset for hours: • current time 11:20, offset 0, time range used: 11:00 - 11:20 • current time 11:20, offset 1, time range used: 10:00 - 10:59 • current time 11:20, offset 2, time range used: 09:00 - 09:59 • current time 11:20, offset 3, time range used: 08:00 - 08:59 With the relative offset increasing, the next previous complete time range is thus used. The specification of the relative offset always consists of whole positive numbers and may adopt the maximum value of 9999.

The **Daily range** option can be used to set a day time filter. In other words, the period selected here determines a time span for each day, which is integrated in the entire time range, and when reports are generated, only those data are considered that occurred within this specified time span of a day. A time span of 00:00 to 23:59 is defined by default. The **Daily range** option can only be used for the *ADO* database type and for reports that require this option. Otherwise this option is inactive and shaded gray.

Please remember that not more data can be exported than are available in the database. Thus if you enter the last year as time range, the required data of the last year must still be present in the database.

27.5.1.4 Extensions Tab

In the **Extensions** tab you may set options concerning some database export options. You may also enter the directory where the report files are to be stored and specify a name for the temporary files.



In this configuration tab some database export options can be set. This export is normally only needed if you want to generate a report layout with Crystal Reports or BIRT for the first time. This requires the corresponding database which you can have created with the **Create database export file only** option. In case of ADO, tables are specified in the SQL database, with CodeBase, dBase databases are created. Furthermore, you can use this option to regularly export these data by means of a job if, with extremely short delete times, you still want to generate reports at a later date.

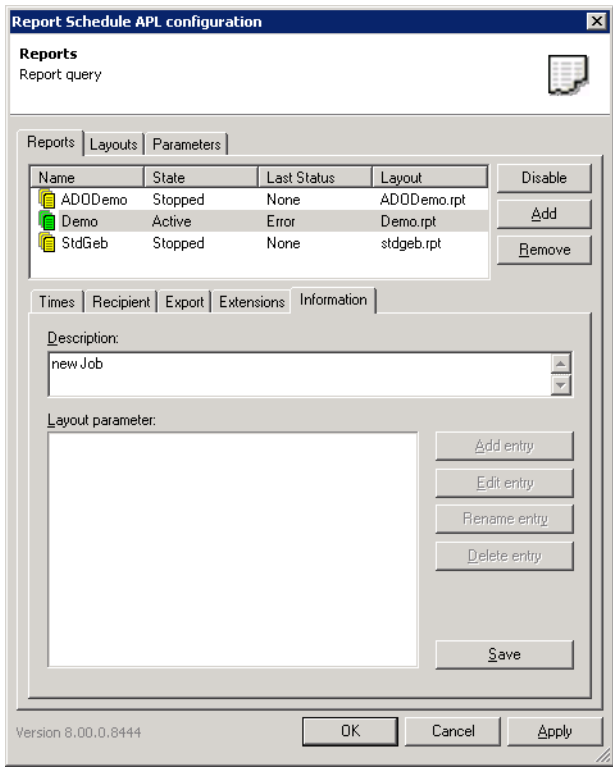
In principle, the SQL database format can be read by any text editor. For viewing an SQL file in a table calculation such as Microsoft Excel the file must first be exported to a file format readable for the program. You will find an overview of these database fields in [Section 27.10, "Basics on the Raw Data Database Tables", on page 1365](#).

Some few fields are flagged "Hidden" in the database. If you need one of these fields to generate a report layout, select the **Export data records from journal incl. HIDDEN flags** option as well. An example are messages generated for MWI notification. These are flagged "Hidden" since they would otherwise be displayed in the users' outbound journal.

Furthermore, you can specify **Files** for saving the DBase database files and for temporal files as well as define a name for the temporal file. Such files and temporal files are only required for Codebase though. In case of ADO, such settings are not needed.

27.5.1.5 Information Tab

The **Information** tab displays the **Description** associated to the selected report layout as well as the **Layout parameters** of the resource file. The function of the resource file of a layout is described in [Section 27.3.2, “Layouts”, on page 1251](#).



The **Description** field displays the text that was created either during the layout generation or by you when selecting the layout in the *Comment* field (see [Section 27.5.2, “Layouts Tab”](#)). The description may be modified at will here.

In the **Layout parameters** field you see the parameter definitions of the layout's resource file contained in the selected report. See [Section 27.3.2, “Layouts”, on page 1251](#). The parameter values correspond to the contents of text fields of a layout as they are displayed in a completely executed report. Information is only displayed if a resource file exists that associates the layout file. The values of these fields are definable here depending on available system languages in which the report can be executed. In other words, using the resource file the text field descriptions of a layout are adjusted to the current system language. If, for example, the system language is set to German, the values of the parameters in the `GERMAN` section are used. Here you can check, for example, whether the respective fields are available in the desired language.

You may modify, rename, remove the parameters or add a new entry via the editor available in this dialog . You should only modify parameter values (right column in the table), though. For, modifications to parameter names (left column in the table) or new parameters are only generated in the resource file and not

automatically adjusted respectively added in the layout file. The parameters in the resource and layout file must match, since otherwise the creation of a report is abandoned with an error message.

If the layout file does not have a resource file, you cannot create it in the configuration dialog of the Report Schedule APL. To create a resource file you need to generate a new file with the name of the associated layout file as well as with the `ini` file extension in the `<XPR Install>\res\RepAPL` directory. You can open the file with any text editor. For each required system language you create now an individual section named [*<language>*], for example [GERMAN] for German, [ENGLISH] for English or [FRENCH] for French. You can enter parameter entries in the Report Schedule APL configuration dialog or in a text editor only. The resource files with the extension `rptconfig` are intended for the layout files by using BIRT. They cannot be imported in the Report Schedule but adjusted by means of an editor. The descriptive language of these resource files is XML.

IMPORTANT:

Please note that each entry in a resource file must have a parameter of the same name in the corresponding layout file, since otherwise no reports can be created.

IMPORTANT:

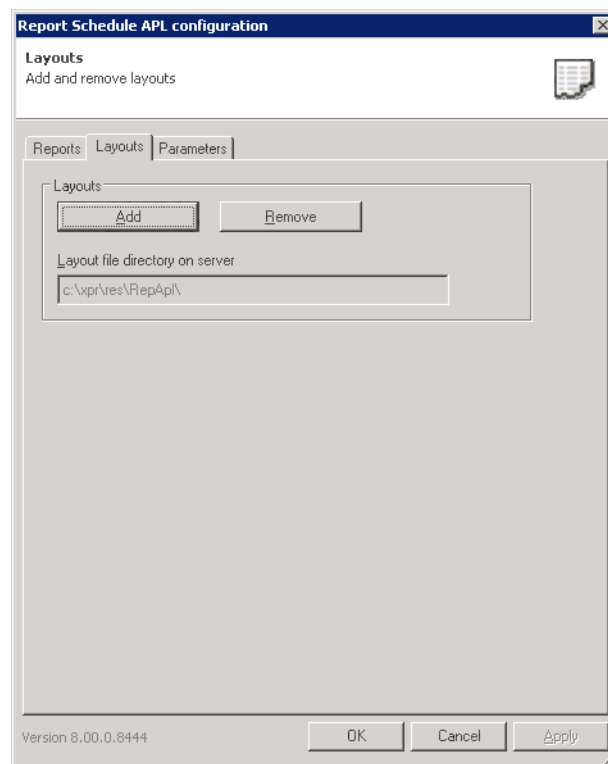
The modifications do not take effect until you have clicked the **Save** button. When you push the **OK** button without having enabled the Save button beforehand, the modifications will be dismissed and reset to the state saved last.

27.5.2 Layouts Tab

On the **Layouts** tab you can add layouts to the Report Schedule APL or remove them again, so that these layouts can be activated and configured on the **Reports** tab. The layouts to be integrated must be in the `<XPR Install>\res\RepApl` folder and have the file extension `rpt`. Removed layouts will not be deleted but merely excluded from use in the Report Schedule APL. You can add each layout to the Report Schedule APL or remove it from there as often as you like.

NOTE:

So that layouts can be used on the Report Schedule APL configuration pages, they must be in the specified directory. This directory cannot be modified on the configuration pages but only in the registry entry **Location** in the `RepApl\Layout` key.



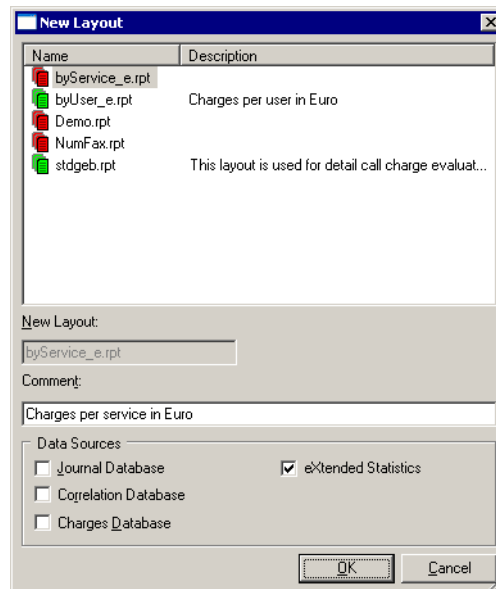
There are buttons that you can use to **Add** or **Remove** layouts for the reports that you want to create. A click on these buttons opens new dialogs. See also the below sections [Adding layouts](#) and [Removing layouts](#). Furthermore, the directory is displayed on the server storing the layout files. The directory path reads `<XPR Install>\res\RepApl` and cannot be modified via the graphic interface. In other words, all layout files to be made accessible for the Report Schedule APL must be in this directory.

NOTE:

The reports to be selected depend on the runtime component they use. *Crystal Reports* can only process layouts with the extension **rpt**, while *BIRT* only considers layout files with the extension **rptdesign**. To improve clarity the names of the layout files supported by *Crystal Reports* begin with **ADO**. Thus verify to select the layout file with corresponding extension supported by the runtime component installed.

Adding layouts

If you click on the **Add** button, the following dialog opens:



In this window all available Report layouts are listed.

New, physically available layouts can be introduced to the Report Schedule APL here. Layouts already known to the Report Schedule APL have a green indication, the others a red one.

NOTE:

Only layouts that have already been introduced to the Report Schedule APL can be used for generating a new report job.

NOTE:

The reports to be selected depend on the runtime component they use. *Crystal Reports* can only process layouts with the extension **rpt**, while *BIRT* only considers layout files with the extension **rptdesign**. To improve clarity the names of the layout files supported by *Crystal Reports* begin with **ADO**.

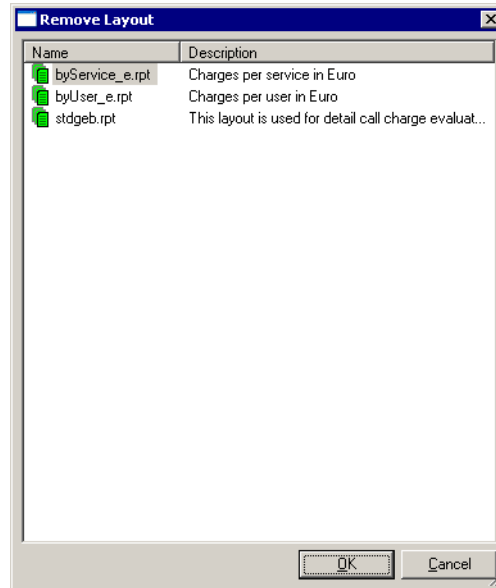
If you select a layout preceded by a red icon, the name will be copied to the **New Layout** field. If a description is available for the report, it is displayed in the **Comment** field. You can change an existing comment or enter one if no description is available.

Furthermore, you select the **Data Sources** used by the layout here. You can choose from the **Journal**, **Correlation** and **Charges databases** as well as **eXtended Statistics**. The latter one is used by all newer layouts and contains the mentioned XPR databases along with statistic information handed over from an

APL to the Report Schedule APL. Such information is, for example, information about contact center operation delivered by the VM APL, or load information about the ISDN APL lines. In case of all newer statistics please always select the **eXtended Statistics** data source in addition.

Removing layouts

A click on the **Remove** button deletes layouts known to the Report APL. If you click on the **Remove** button, the following dialog opens:



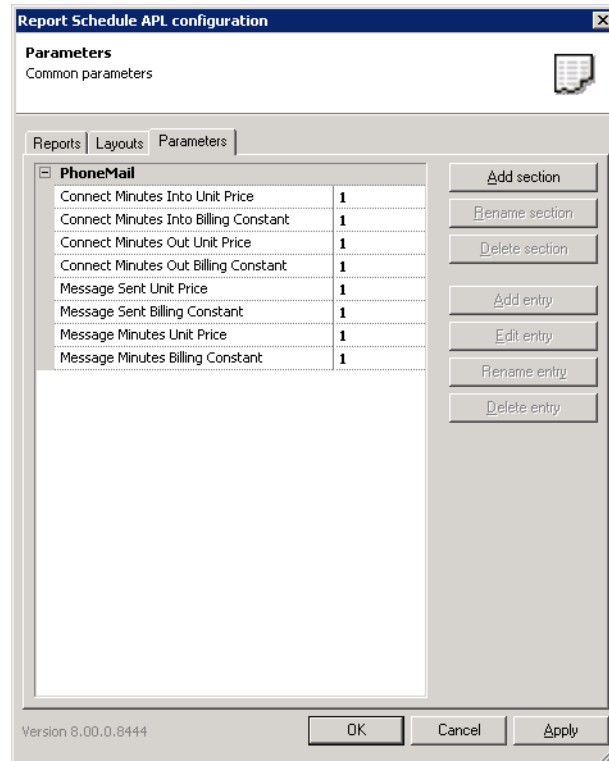
This dialog contains all report layouts known to the Report Schedule APL, i.e. the previously added ones (cf. [Section 27.5.2, “Adding layouts”, on page 1275](#)). Such layouts are indicated by a green icon. To delete a report layout, select it and confirm with **OK**. To remove further layouts, please repeat the described process.

NOTE:

The reports to be selected depend on the runtime component they use. *Crystal Reports* can only process layouts with the extension **rpt**, while *BIRT* only considers layout files with the extension **rptdesign**. To improve clarity the names of the layout files supported by *Crystal Reports* begin with **ADO**.

27.5.3 Parameters Tab

On the **Parameters** tab values are contained the reports use for calculation. These parameters can be created, deleted or modified here. This is done via the editor that is available here.



The parameters can be divided into sections for clarity. You can thus e.g. find the parameters used by the TUI reports for PhoneMail and VMS in the PhoneMail section. Each section contains an arbitrary number of entries so that a folder structure on two levels emerges.

For modifying the paragraphs and entries several buttons are available at the right hand side of the editor window. The upper three buttons serve for adding, renaming and deleting **sections**. The lower four buttons are used for adding, modifying, renaming and deleting **entries**.

All charge information displayed here are filed in the `globals.ini` file which is stored in the `<XPR Install>\res\RepAPL` directory. If you make any changes here, please save this file as it would otherwise be overwritten during the next update.

Up to now, the parameters displayed here have solely been used by one TUI report, the billing report. You will find an explanation of the here adjustable parameters in the description of this report. See [Section 27.9.3.5, "Subscriber Activity: Billing Information"](#).

27.6 Creating a Report

This chapter comprises a sequence of actions you need to take to create a report. This action sequence can be roughly divided into four possible steps:

- So that you can create a report, you need to perform a database connection to an SQL server in the Report APL first ([Section 27.6.1, “Configuring the Report APL for Usage with an SQL Database”](#)).
- Then, you need to activate a layout for the report in the Report Schedule APL. Here you can either create a new layout with Crystal Reports XI or BIRT, or you use an already supplied one.

How to create a new layout with Crystal Reports XI is described in [Section 27.6.2, “Creating a Layout with Crystal Reports XI”](#).

How to create a new layout with eclipse BIRT is described in [Section 27.6.3, “Creating a Layout with BIRT”](#).

- You find an example of an already specified layout in [Section 27.6.2.4, “Example of an available Layout”](#). An overview and explanation of the supplied layout files for default reports is found in [Section 27.8, “Supplied Layout Files for Default Reports”](#). You can compare them to the layout you have created yourself.
- You learn how to select, activate and set the layout you have created yourself or a supplied one in the Report Schedule APL in [Section 27.6.4, “Selecting, activating and setting a Layout”](#).

27.6.1 Configuring the Report APL for Usage with an SQL Database

How to use the database defined during the installation with the Report APL:

1. Open the XPR monitor and log in as administrator.
2. Open the Report APL configuration dialog.
3. Select the **ADO** entry under **Access mode** and click the **Configure...** button.

Another dialog opens.

4. Select the **Microsoft OLE DB Provider for SQL Server** entry in the **Provider** tab and click the **Next>>** button.

The **Connection** tab opens.

5. The **Connection** tab
 - a) Specify the **server name** or select the server on which the above created database is stored from the list.
 - b) Specify the **user name** and the associated **password**.

NOTE:

If the database has been created via the automatic installation, enter **mrs** as user name and **mrspass** as password.

If the Microsoft SQL server has been installed manually, you need to specify as user name and password the data that was defined during the Microsoft SQL installation.

- c) Determine the **database** to be used by the Report APL.
6. Click the **Test Connection** button to test the connection to the SQL server with the settings performed.

A successful connection test is indicated by a corresponding dialog and the Report APL configuration is thus complete.

If the test fails, check the Report APL configuration. For example, the server may have been shut down or the password incorrectly entered.

7. Complete the configurations with the **OK** button.

NOTE:

After you have clicked on the **Test connection** button in the **Report APL configuration** dialog a successful connection can only be established if you have saved the specified password with the **Allow saving password** option. Since enabling this button does not provide the option to enter the password, the connection could otherwise not be properly checked. If you do not want to save the password for security reasons, use the **Test connection** button on the **Connection** tab.

27.6.2 Creating a Layout with Crystal Reports XI

NOTE:

We recommend to contact the Professional Services when creating individual layouts. For, there will be no support for modified or self-created layouts and reports.

Layouts serve as template for reports to be created. You can either revert to layouts already created or generate them using Crystal Reports XI. Crystal Reports XI requires an independent license, thus it is not an XPR system component.

A layout serves to represent the raw data provided by the system coherently and efficiently in the desired manner. The resulting reports are to present the required data and contexts clearly and quickly to the reader. Using the Crystal Reports XI program you can create and edit layouts generated for your requirements.

Besides creating new layouts you can access predefined ones respectively modify them. The XPR system setup provides predefined layout templates. For example, you can use the *ADOFaxReport* layout to display information such as time, number of pages and recipient for all fax messages sent by XPR users. See [Section 27.6.2.4, “Example of an available Layout”, on page 1286](#).

The following sections will briefly introduce you to the operating interface of the Crystal Reports XI program and depict the creation of a simple layout.

NOTE:

This chapter provides only a short introduction to the creation of layouts by means of Crystal Reports XI. For continuative and detailed information please consult the Crystal Reports XI documentation.

27.6.2.1 Layout Structure

Each layout may consist of a large number of different objects and fields. Among the most important objects and fields you find database fields, the text objects, group fields, formulas and special fields. In case of more complex objects and fields, wizards assist you in correctly creating them.

- **Database fields:** These fields are wildcards for the respective data of a database. In the database fields variables are set with which the respective data are referenced. Merely a basic framework of fields for layout creation is deployed and not the actual raw data, which may assume an enormous amount.

- **Text objects:** These fields are freely positionable and contain arbitrary texts. Such texts are not generated from database data but are fixedly defined in the layout. Text objects are used for captions or specifying additional information. Text objects may also contain several fields.
- **Group fields:** Groups are optional objects with which the data represented in the report can be structured as regards contents and form. Each group forms an individual representation as well as editing area. You can specify properties that are only valid for the data of a selected group. We differentiate here between the group head and the group base, which frame the concrete data. Groups may be nested and thus create hierarchies. Group name fields assign a description to the respective group.
- **Formula fields:** This object enables you to apply defined operators and functions to selected database fields. For example, you can perform simple mathematic operations, but also type conversions or document properties modifications. Such fields are also applicable as text fields by assigning them a description and a text string as "formula". The content of a field can be adjusted to the current system language by means of the field's description in a resource file.
- **SQL queries:** With the help of a wizard you can formulate database queries in SQL. You can thus select specific data and display them in the report.
- **Special fields:** These predefined fields provide additional information, which are created during the report generation. Examples of special fields are page numbers as well as date or time specifications.
- **Running total fields:** Such fields enable the most diverse calculations of field values, for example sums and averages. In the process you can determine overall results as well as display intermediate results on any point.

Beyond that, further objects such as graphics, maps, crosstabulations, drawings or OLAP objects and fields for parameters are possible.

The respective objects and fields can either be inserted via the paste menu or by means of the toolbars and explorers.

27.6.2.2 The Workspaces of a Layout

Each layout is divided into a basic framework of specific areas. Each area contains specific objects. The following areas are available:

- **Header area of a layout:** The objects and fields in this area are only output at the beginning of a report. Diagrams and crosstabulations in this area contain data for the entire report. The formulas found in the header area are only evaluated at the beginning of a report.

- **Footer area of a layout:** The objects and fields in this area are only output at the end of a report. Diagrams and crosstabulations in this area contain data for the entire report. The formulas found in the foot area are only evaluated at the end of a report.
- **Page header of a layout:** The objects and fields in this area are output at the beginning of each page. Here you cannot place any diagrams of crosstabulations. A formula found in this area is calculated at the beginning of each new page.
- **Page footer area of a layout:** The objects and fields in this area are output at the beginning of each page. Here you cannot place any diagrams of crosstabulations. A formula found in this area is calculated at the end of each new page.
- **Group header area:** The objects placed in this area are output at the beginning of each new group. The diagrams and crosstabulations positioned in this area refer to the data area of the group. Formulas are evaluated once at the beginning of each new group.
- **Group footer area:** The objects placed in this area are output at the end of each new group. The diagrams and crosstabulations positioned in this area refer to the data area of the group. Formulas are evaluated once at the end of each new group.
- **Detail area:** The data positioned in this area are output once each. Diagrams and crosstabulations are not possible. Each formula is calculated once for each new detail area.

27.6.2.3 The Crystal Reports XI Operating Interface

The Crystal Reports XI operating interface can be divided into the **Design** and the **Preview**. The design contains the single workspaces of a layout into which the desired objects such as database fields, text objects or formulas are inserted and edited. In the preview the concrete data are read out of the connected database and completely displayed in accordance with the settings of the draft. While the design usually comprises only one page, the preview may contain quite a few pages owing to the possible large data amount. The preview roughly corresponds to the report put out by the Report Schedule APL.

Furthermore, the Crystal Reports XI view consists of five auxiliary means **Field Explorer**, **Report Explorer**, **Memory Explorer**, **Workbench** and **Dependency Check**. For the first work steps with Crystal Reports XI only the Field and Report Explorer are of interest.

Using the **Field Explorer** you can add, modify or delete fields. You open the Field Explorer via the **View** menu and the **Field Explorer** option.

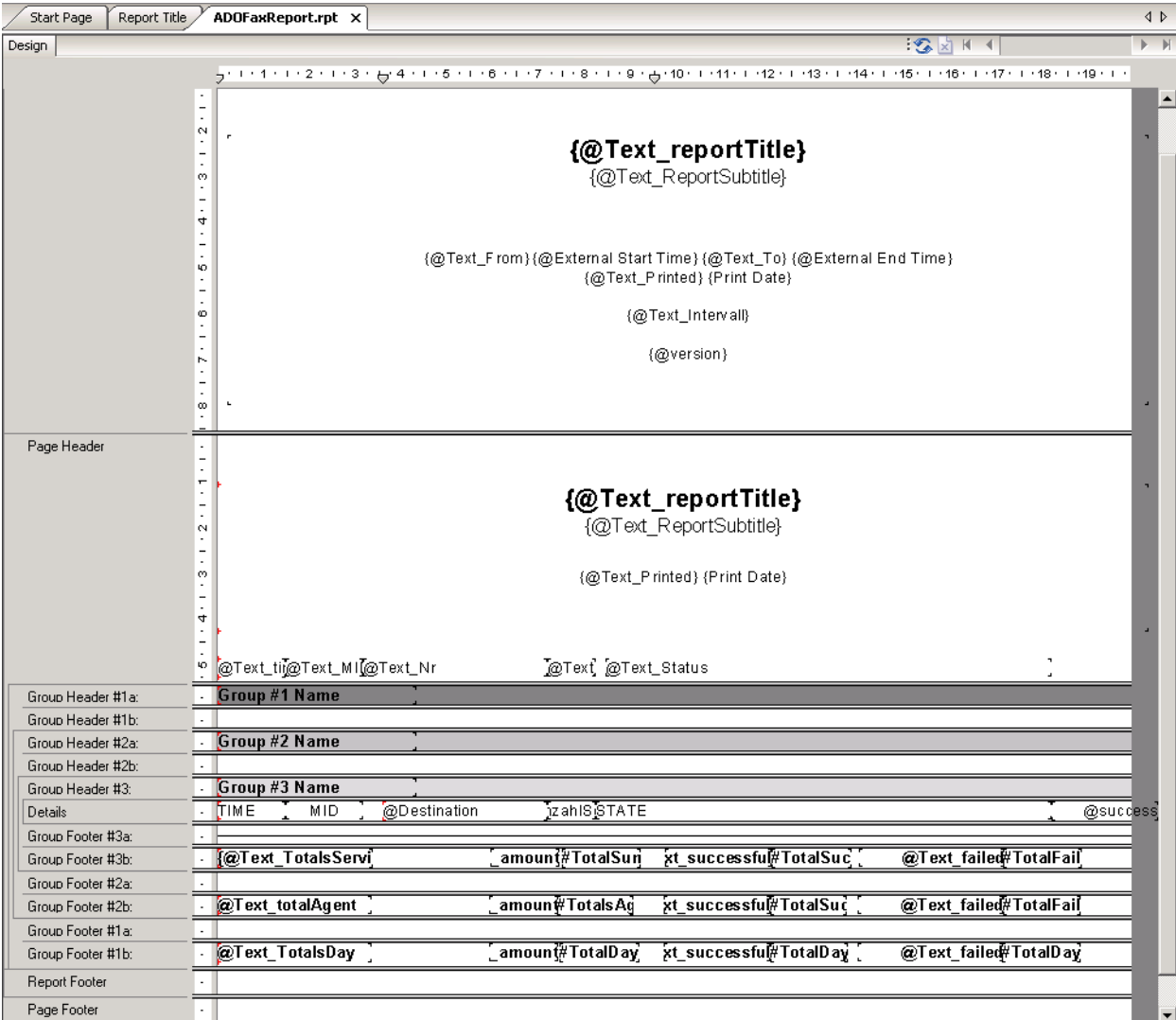
The **Report Explorer** shows the single workspaces of a layout in a structured view. All inserted objects and fields are listed and can be displayed, hidden and modified here.

Beyond that, Crystal Reports has several **toolbars**, which facilitate the operation. For example, you can use the toolbar to open explorers, add fields or edit text objects.

The next section represents a supplied layout. It exemplifies the above Crystal Reports XI components.

27.6.2.4 Example of an available Layout

The below layout is called `ADOFaxReport` and is shipped with an XPR setup by default. This layout serves to arrange the fax messages sent up to now and to perform simple calculations such as summing up specific fax message properties.



You see the typical Design mode operating interface. In the gray column on the left hand side you find a list of workspaces such as Report Header, Page Footer or Details. The layout itself hosts in the single workspaces the corresponding objects and fields. The workspaces are separated by bars.

In the header area of the layout, which serves as title page of the report, you find a large text object. The text object includes references to defined formula fields. Such formula fields either contain strings as descriptions or specific features that are executed during the report creation. Furnishing formula fields with simple

strings has the advantage that only the corresponding formula field needs to be adjusted in case of modifications. The same functionality could also be enabled with the help of text objects. In case of modifications, each text object had to be changed, though.

References to formula fields have automatically the following invocation `{@<field name>}`. The header area of the report respectively the title page looks after the report creation as follows:

Fax Report

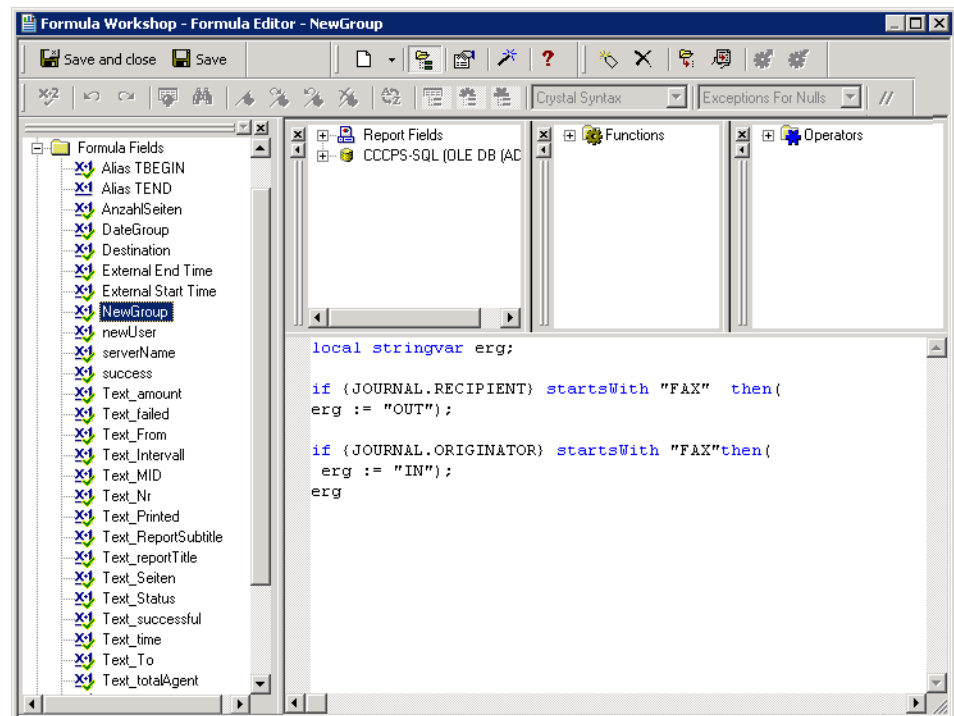
User

From 00:00:00 to 00:00:00
Printed 18/12/2006

Interval of the day

Version: 2.0 / 02.08.05

In the Field Explorer you can access the single formula fields. Select any formula field and click the right mouse button. A context menu opens in which you select the **Edit** command. The so-called **Formula Workshop** opens.



In this **formula editor** you can access all available formula fields and create new ones. Predefined features and operators are already available. The formula editor is described in detail in the Crystal Reports XI user manual.

Besides the layout header area the depicted example also contains a page header with references to formula fields and special fields. Also these fields are found within a text object. References to formula fields are again performed following the scheme {@<field name>} and references to special fields follow the scheme {<special field>}.

Furthermore, the exemplified layout contains different groups and a detail area. There are three groups that sort the data. First, sorting occurs according to the date (group 1), then according to the recipient (group 2) and finally according to in and outgoing fax messages (group 3).

The detail area contains the single database entries sorted according to time (TIME), ID (MID), recipient (@Destination), number of pages (@AnzahlSeiten), status (STATE) and the transmission success (@success).

In the next section you will be shortly introduced to creating an individual layout. It starts with connecting the XPR database to Crystal Reports XI. Subsequently, the fields and objects will be inserted, so that a first complete report can be created.

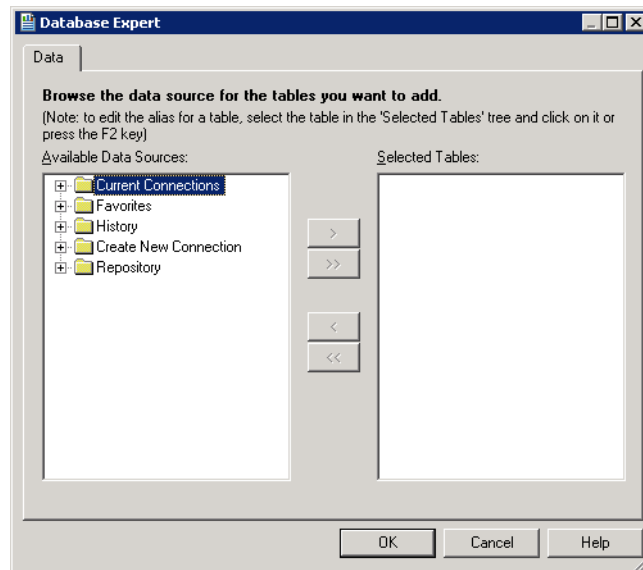
27.6.2.5 Example of a Layout Creation

In the following section we will create a layout step by step as an example. To begin with, click in the Crystal Reports XI **start page** on the **Blank Report** entry.

1. Connecting the Database

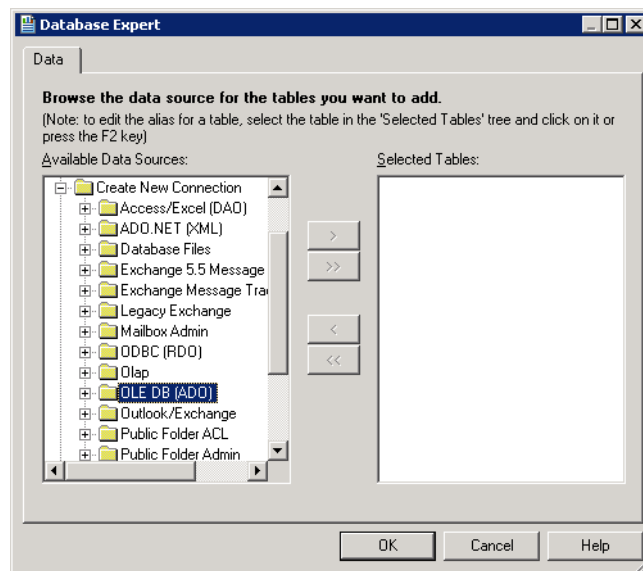
First, you need to connect the XPR database to Crystal Reports XI. Only in this way the single database fields and the values stored therein can be inserted in a layout and be viewed.

- a) Crystal Reports XI opens automatically the **Database Expert** from the **Database** menu.

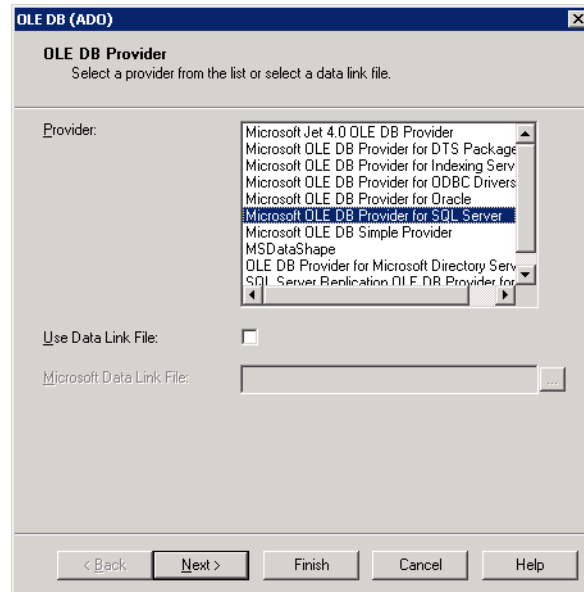


The first tab **Data** is divided into the sections **Available Data Sources** and **Selected Tables**.

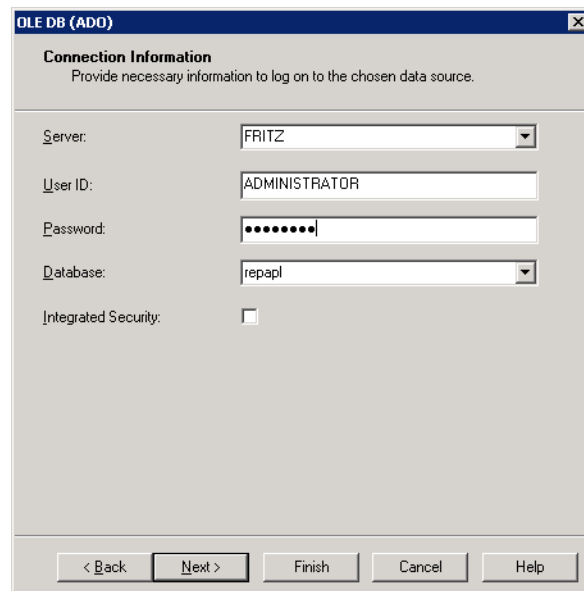
- b) The **Available Data Sources** section shows the possible data sources in the form of a folder structure. Doubleclick the **Create New Connection** folder to make the XPR database available for Crystal Reports XI. Select **DB OLE (ADO)** as database format and doubleclick this folder.



- c) The **OLE DB (ADO)** dialog appears, in which you connect a data source to Crystal Reports XI. In the first step, select **Microsoft OLE DB Provider for SQL Server** as provider. Then click **Next**.



- d) The next step requires the specification of data to access the mentioned data source.

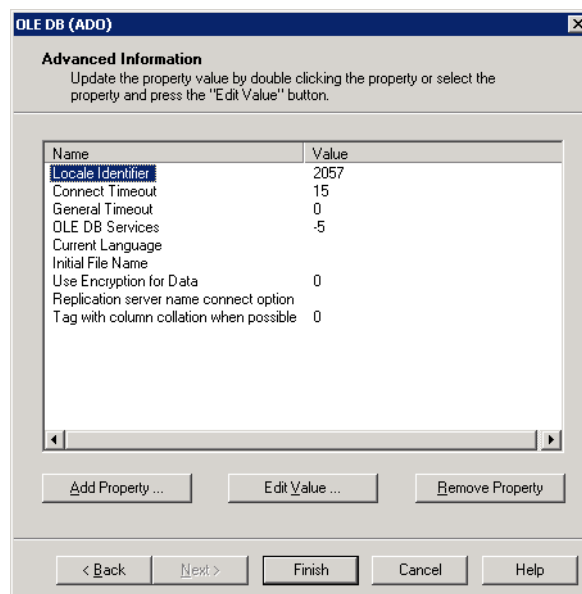


Select the **Server** on which the XPR system is installed. In addition, you need to enter your **User ID** and the associated **Password**. Please note that you need to have administrator privileges to access the XPR database. Finally, select the desired **Database**. This is here the **repapl** list entry. After you have completed your entries, click the **Next >** button.

IMPORTANT:

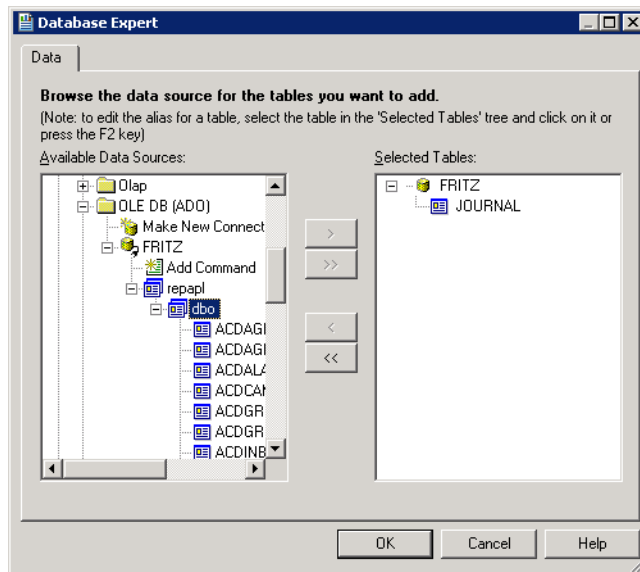
The **Integrated Security** option of Windows NT is *not* supported and *must not* be used for connecting the Report APL to Crystal Reports.

- e) Finally, the dialog provides an overview of the information of the data source you have selected. Confirm the settings with **Finish**.



- f) You are taken back to the **Available Data Sources** tab. The XPR databases are now displayed as **OLE DB (ADO)** subfolders.

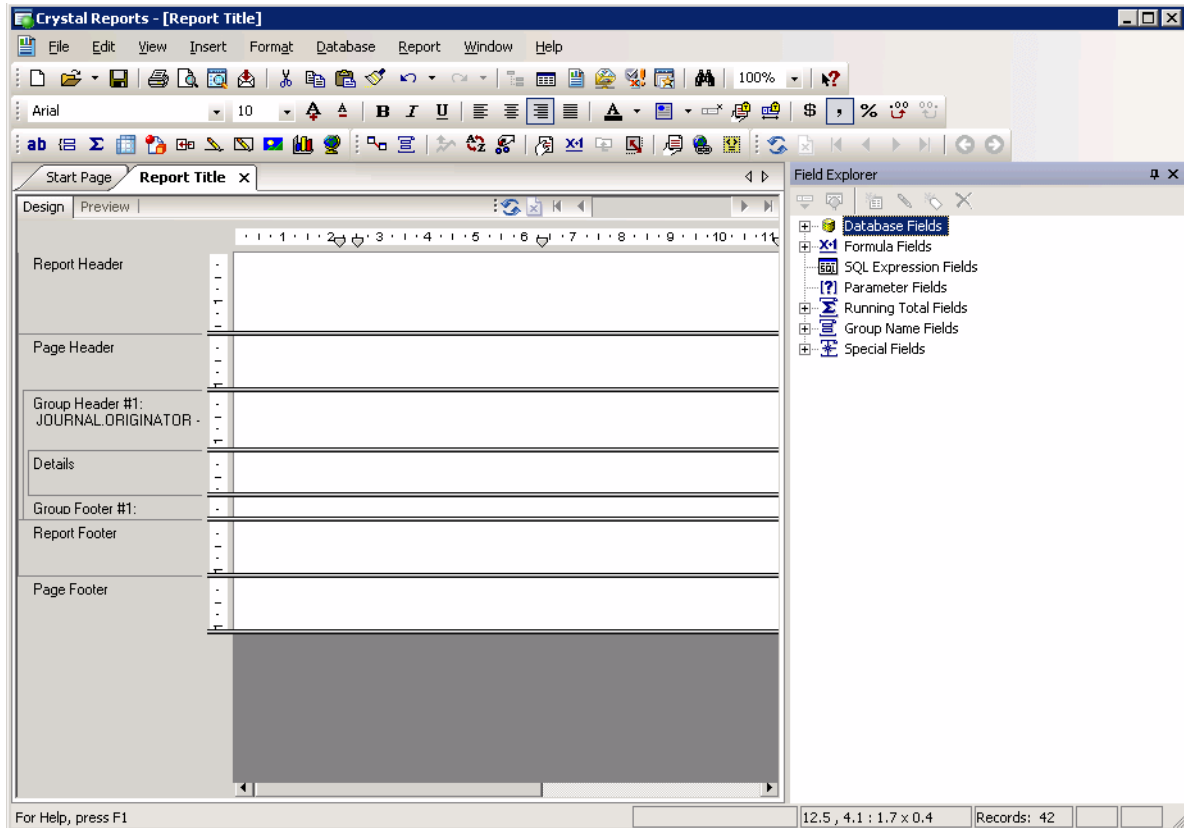
- g) Now select the desired database tables by opening the **repapl** node and moving the single tables into the **Selected Tables** area applying the drag&drop method.



Reversely, you can move tables you do not require back into the **Available Data Sources** area. Please move the **JOURNAL** table into the **Selected Tables** area.

Report APL and Report Schedule APL

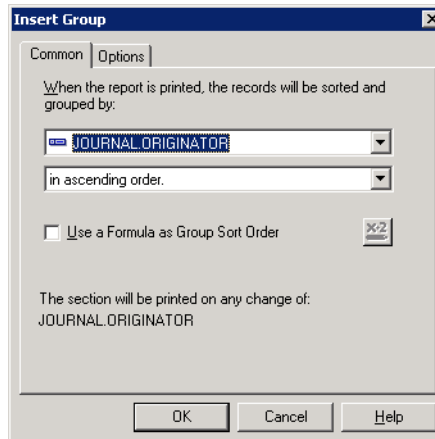
- h) Connecting the database and selecting the associated database fields is now complete. The Crystal Reports XI operating interface appears with a new empty layout.



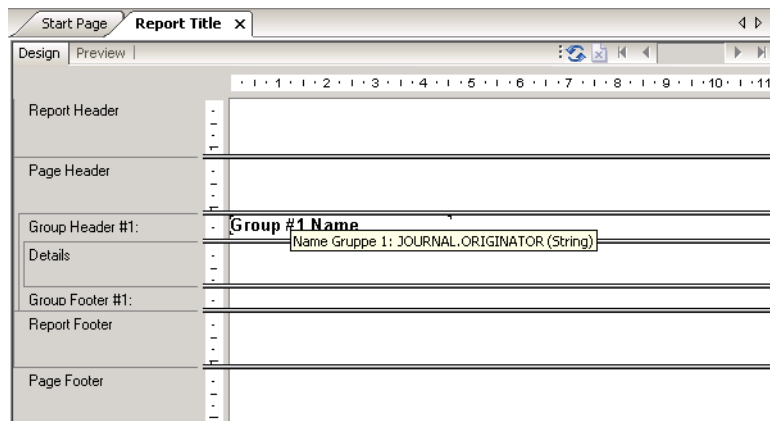
2. Workspaces

In the next step you specify the single layout areas. Header and footer area of the report or pages exist automatically. We now want to define group areas. Verify that you are in the **Design** and not in the **Preview** mode.

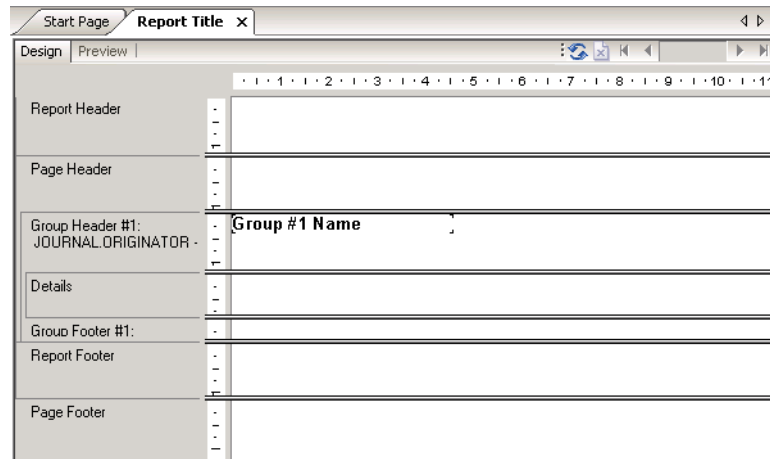
- a) First, you create a group by which means you can sort the represented values. Click on  in the toolbar. The **Insert Group** dialog opens.



Select the `JOURNAL.ORIGINATOR` entry in the top list field and confirm your selection with **OK**. A new group is inserted in your design as workspace, which surrounds a detail area with header and footer area. In addition, a group name field is created that features the value of the `JOURNAL.ORIGINATOR` field.



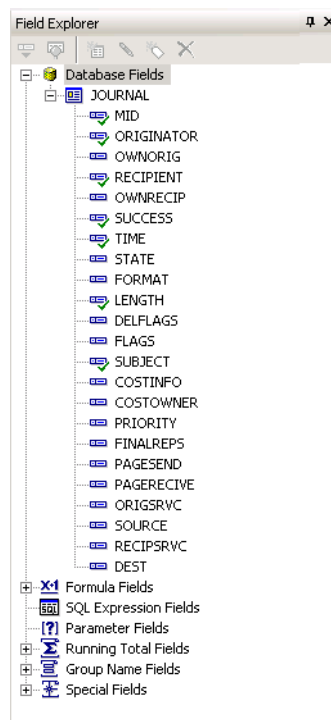
- b) Modify the height of the group header by shifting the dividing line between group header and detail area downward by approximately 1cm. Changing the height is required for inserting column names.



3. Fields

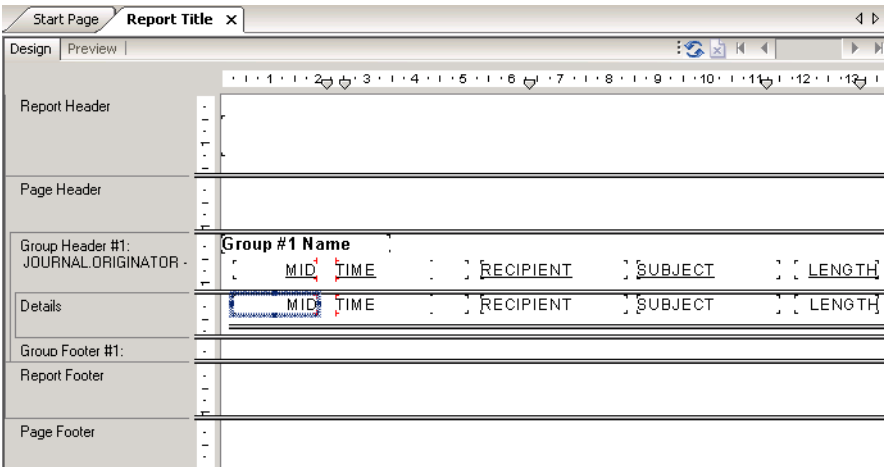
In the next step you will insert single data fields in the layout. Use the Field Explorer for this purpose.

- a) Open the **Database Fields** node in the Field Explorer and then the **JOURNAL** node.

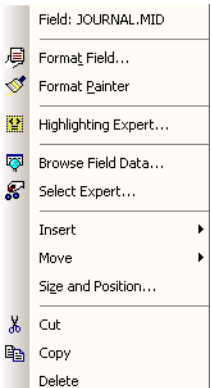


Select the **MID** database field and place it leftmost in the detail area applying the drag&drop method. In addition, a field caption with the name of the database field is automatically created in the page header area. In

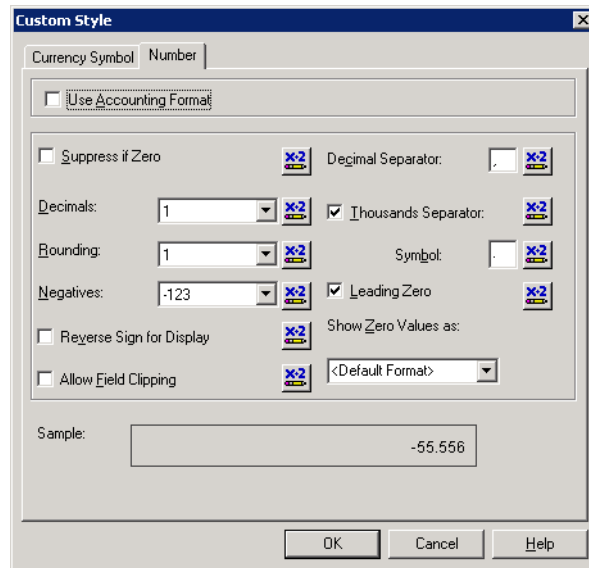
the Field Explorer a correctly used database field is indicated with a green tick. If you remove a database field, the associated field caption is also deleted. Now drag the field caption into the group header area precisely on top of the corresponding database field. Proceed analog with the database fields **TIME**, **RECIPIENT**, **SUBJECT** and **LENGTH**. The database field size automatically adjusts to the greatest value of the respective field. If you thus minimize the field sizes, some values may not be displayed completely.



The ID of the listed messages (MID) is represented as floating point number with two decimal places. Decimal places are not required for the ID, though. So that this ID is listed as whole number without decimal places, click with the right mouse button on the **MID** field in the **detail area**. A context menu opens in which you click on **Format Field**.



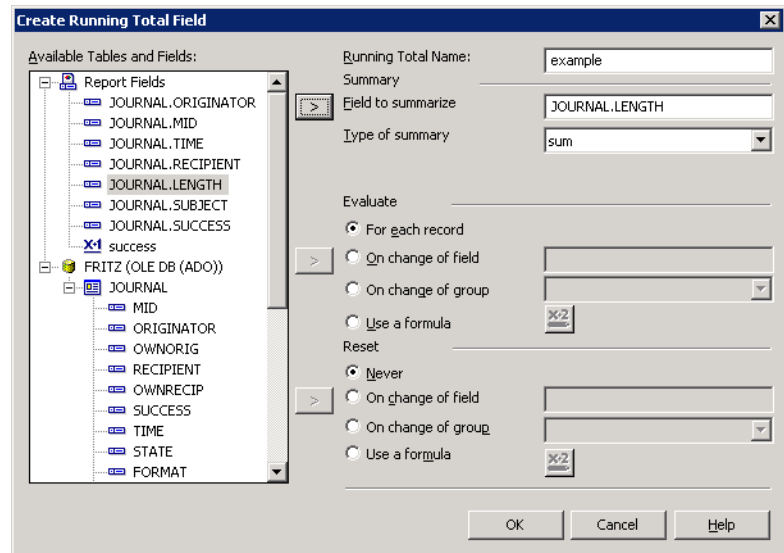
The **Format Editor** opens on the **Number** tab. Click here on the **Customize**. Another dialog named **Custom Style** opens.



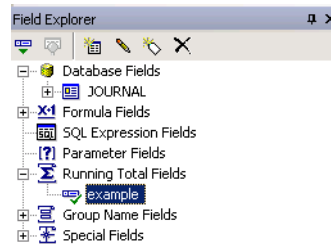
In the **Decimals** field select value **1** and confirm your setting with **OK**. Then close the format editor, again with the **OK** button.

- b) Another important field is the **Running Total field**. With this field you can perform simple mathematic calculations. In the process, the single values are progressionally calculated. An example: The values 1, 2 and 3 exist for a database field. If these values are output as running total field, the values 1, 3 and 6 appear. The values are thus progressionally summed up. Depending on the position of this field, different intermediate results can be put out. If the field is in the detail, group or page area, an intermediate result is put out for the respective value, the respective group or the respective page. In case of the field being located in the report area, only one value is represented once.

You create a new running total field in the **Field Explorer**. Doubleclick the node of the same name. A dialog appears that enables a large number of options upon the creation of a running total field. First, however, you create a simple example by selecting the listed **report field** `JOURNAL.LENGTH` and clicking on the topmost . The entry will then appear in the **Field to summarize**. In the **Running Total Name** field please enter `example` and leave the **Type of summary** on `sum`.



Confirm your specifications with **OK** and the new running total field appears in the Field Explorer.

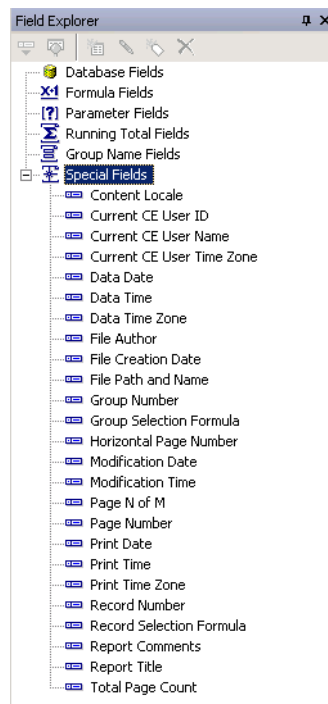


Now drag the running total field `example` next to the `JOURNAL.LENGTH` field in the detail workspace applying the drag&drop method. If you switch from the Design mode to the **Preview** mode you will see that the single values are represented summed up by means of the running total field.

<u>LENGTH</u>	
127,00	127,00
127,00	254,00
127,00	381,00
105,00	486,00
105,00	591,00
127,00	718,00
127,00	845,00
127,00	972,00
127,00	1.099,00
5.165,00	6.264,00

- c) Next, add **special fields** to your layout. You insert special fields either as individual fields or consolidated in a text object. The fields **Report Title** and **Page Number** are inserted as individual fields. The fields **Print Date**, **Print Time**, **Data Date** and **Data Time** are inserted in a text object. The advantage is that the fields can be directly labeled.

Open the Special Fields node in the **Field Explorer**. All special fields will be listed.



Now select the **Page Number** field and drag it into the `Page Footer` workspace with the left mouse button kept pressed.

Add the **Report Title** special field as another field. Select the corresponding field in the **Field Explorer** and place the field in the header area of the report with the left mouse button kept pressed. In this way the report title will only appear at the beginning of the report.

Drag the margins of the field's positioning frame to the margins of the entire report and click in the toolbar on the **center positioned** icon to place the field precisely in the horizontal center of the report.

Using the toolbar you can also edit properties such as font, type, size or color like in other word processing programs. When you modify the font size, you may have to adjust the field frame size.

Report Title					
Group #1 Name					
MID	TIME	RECIPIENT	SUBJECT	LENGTH	Example
MID	TIME	RECIPIENT	SUBJECT	LENGTH	#example
Page Number					

To display a report title you need to specify it first. In the **File** menu access the layout's **Properties**. Here you need to fill in the **Title** field and confirm with **OK**. The same applies for the special fields **File Author** and **Report Comments**. The contents of these fields is also determined in the layout's properties.

Document Properties

Summary | Statistics

Application: Crystal Reports

Author:

Keywords:

Comments:

Title: Report Title

Subject:

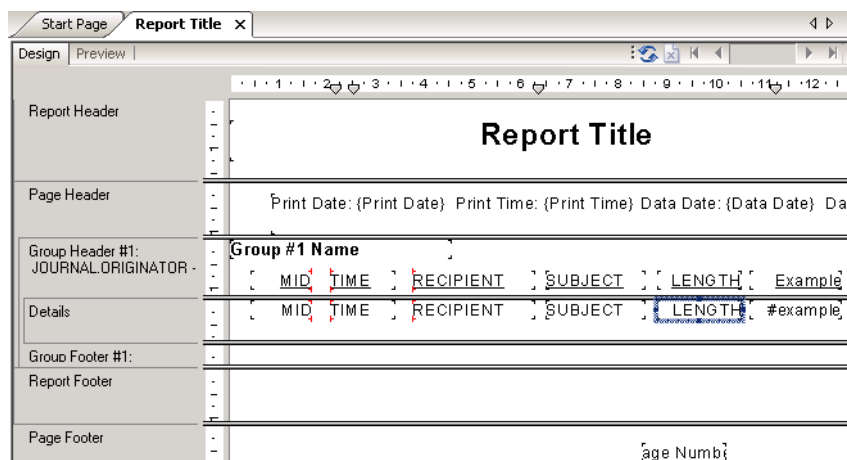
Template:

☒ Save Preview Picture

OK Cancel Help

- d) After you have inserted the two special fields Page Number and Report Title as individual fields, the further special fields are defined within a text object. To create a text object click on **ab** in the toolbar and position the text object in the page header.

Now select the **Print Date** field and drag it into the text object with the left mouse button kept pressed. Proceed analog with the **Print Time**, **Data Date** and **Data Time** fields. The special fields are displayed in the notation `{<special field>}`. Now prefix each special field inserted in the text object with the corresponding field description. For this purpose click on the respective position in the text object and type in the description. Based on these fields you can recognize the up-to-dateness of the report's represented values.

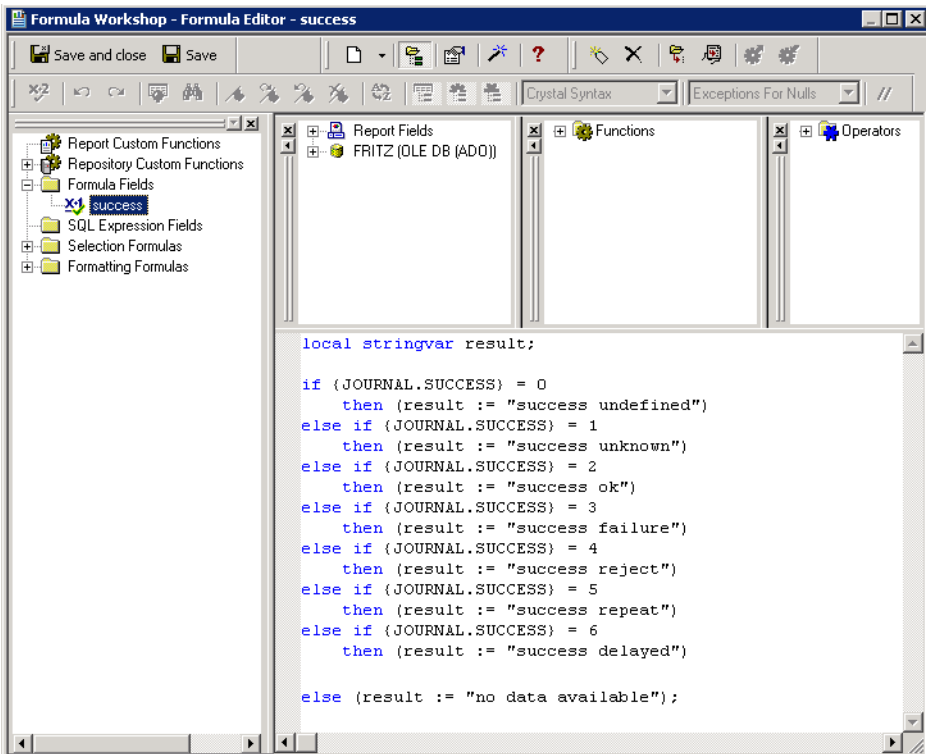


The added fields are in the page header and are thus put out with each new page of the report. Each special field used is indicated in the Field Explorer with a green tick. You can use each special field as often as you like.

- e) Eventually, insert a **Formula Field** in your layout. Formula fields may contain complex features and operators, but also simple strings. Formula fields that exclusively contain strings have basically the same functionality as a text object. Using formula fields several times with drag&drop is much simpler, though. Likewise, modifications to the formula field are adopted by all copies of this field contrary to the tedious modifications to all text objects used.

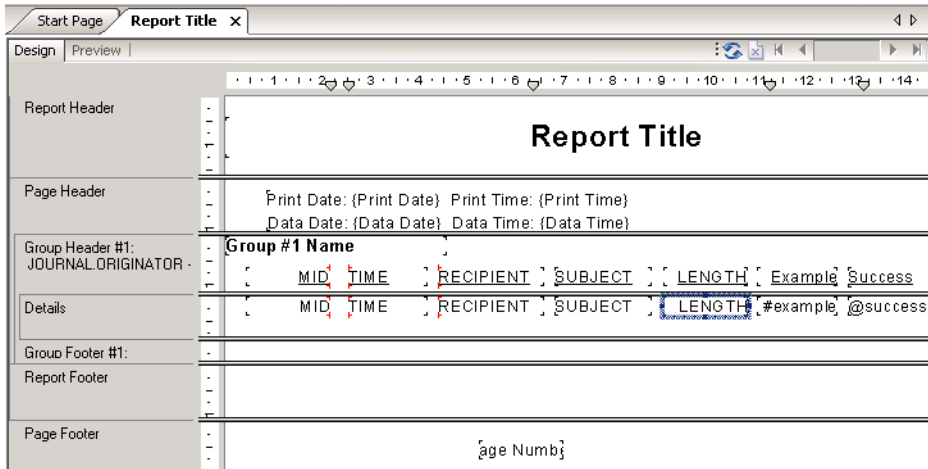
In addition, indirectly specifying texts via a formula field and not directly via a text object enables indicating the formula fields names as parameters in the resource file (see [Section 27.3.2, "Layouts"](#)). In a resource file the parameter values and thus the texts are defined depending on the system language. When changing the system language you can have such texts automatically adjusted to this language. The German description "Benutzername" can be automatically switched to the English "User name" or to the French "Nom utilisateur".

To insert a formula field in your layout, click with the right mousebutton on the field of the same name in the Field Explorer. A context menu opens in which you select the **New...** command. You will be prompted to specify a description for the field. Enter here `success` and click on **OK**. The so-called Formula Workshop opens.



The displayed example creates a query for the `SUCCESS` database field of the `JOURNAL` database. Depending on the field's value, a corresponding text is put out to explain the value. Please obtain the explanation of the `SUCCESS` field from the description in [Section 27.7.3, "The JOURNAL.DBF Database"](#), on page 1335.

A created formula field appears in the Field Explorer with the corresponding description. Now drag the field to the position on the right of the `LENGTH` database field applying the drag&drop method. On top of the formula field position a text object with the content **Success** as caption.



- f) Similar to formula fields, the so-called **Formula Workshop** is used for **SQL fields**. The SQL commands are entered within the Formula Workshop. You find a detailed description of the SQL fields and the Formula Workshop in the Crystal Reports XI user manual.

Switch to the **Preview** tab and all fields will be furnished with values. All database fields used will subsequently be filled with the actual database values and put out. You can thus view and check the actual representation of your report.

Report Title

Print Date: 18/12/2006 Print Time: 12:21:07 Data Date: 11/12/2006 Data Time: 13:51:39

FRITZ/<AUTOREPORTER>

MID	TIME	RECIPIENT	SUBJECT	LENGTH	Beispiel	Success
1	23/06/2006 11:55:18	MAILBOX/ADMI	Autoreport alert CtiA	127	127.00	success delayed
2	23/06/2006 12:07:54	MAILBOX/ADMI	Autoreport alert CtiA	127	254.00	success delayed
3	23/06/2006 12:28:45	MAILBOX/ADMI	Autoreport alert CtiA	127	381.00	success delayed
4	23/06/2006 14:30:34	MAILBOX/ADMI	Autoreport alert mta	105	486.00	success delayed
5	23/06/2006 14:36:16	MAILBOX/ADMI	Autoreport alert mta	105	591.00	success delayed
6	23/06/2006 14:45:53	MAILBOX/ADMI	Autoreport alert CtiA	127	718.00	success delayed
7	23/06/2006 15:01:37	MAILBOX/ADMI	Autoreport alert CtiA	127	845.00	success delayed
8	12/07/2006 12:55:13	MAILBOX/ADMI	Autoreport alert CtiA	127	972.00	success delayed
9	13/07/2006 05:08:40	MAILBOX/ADMI	Autoreport alert CtiA	127	1,099.00	success delayed
10	14/07/2006 05:11:56	MAILBOX/ADMI	Report Server FRITZ	5,165	6,264.00	success delayed
11	15/07/2006 05:15:20	MAILBOX/ADMI	Report Server FRITZ	109	6,373.00	success delayed
12	16/07/2006 05:18:49	MAILBOX/ADMI	Report Server FRITZ	197	6,570.00	success delayed
13	17/07/2006 05:22:07	MAILBOX/ADMI	Report Server FRITZ	109	6,679.00	success delayed
14	18/07/2006 05:25:13	MAILBOX/ADMI	Report Server FRITZ	109	6,788.00	success delayed
15	18/07/2006 05:38:54	MAILBOX/ADMI	Autoreport alert mta	75	6,863.00	success delayed
16	18/07/2006 09:39:01	MAILBOX/ADMI	Autoreport alert mta	75	6,938.00	success delayed
17	18/07/2006 13:39:07	MAILBOX/ADMI	Autoreport alert mta	75	7,013.00	success delayed
18	19/07/2006 05:28:40	MAILBOX/ADMI	Report Server FRITZ	422	7,435.00	success delayed

If you have finished a layout, you need to store it in the path <XPR Install>/res/reap1 to access it in the Report Schedule APL.

On the Reports tab you can then add the layout as current layout and activate it. Please obtain the corresponding setting options from [Section 27.5, "Report Schedule APL Configuration"](#), on page 1261.

27.6.3 Creating a Layout with BIRT

NOTE:

We recommend to contact the Professional Services when creating individual layouts. For, there will be no support for modified or self-created layouts and reports.

BIRT is an open source system of the **eclipse** foundation for **editing** and **generating** reports. Layout files are edited with the `rptdesign` format via the graphic interface of the eclipse framework. You can obtain information about the installation of eclipse and BIRT from the *Server Installation* manual.

NOTE:

Layout files with the format `rpt` can only be edited with Crystal Reports. With BIRT you can neither edit these files nor use them for creating reports.

In the following sections you receive a short introduction to layout editing by means of BIRT. The following aspects will be briefly dealt with:

- [Section 27.6.3.1, “Creating a new Layout”](#)
 - [Section 27.6.3.3, “Connection to the Database Tables”](#)
 - [Section 27.6.3.2, “The graphic Interface”](#)
 - [Section 27.6.3.4, “The Structure of Layout Files in BIRT”](#)
 - [Section 27.6.3.5, “The available Tools and Fields for creating and editing Layouts”](#)
 - [Section 27.6.3.6, “An Example: The Default Billing Report”](#)
-

NOTE:

For a detailed introduction or pointed questions please refer to the corresponding eclipse SDK and BIRT documentation. The ensuing explanations make no claim to be complete but serve a first orientation only.

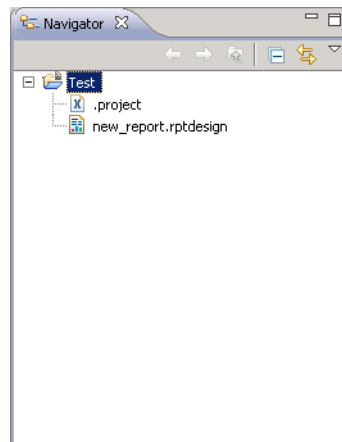
27.6.3.1 Creating a new Layout

When you open a new report project in eclipse, a corresponding **report design** for editing layout files opens. I.e. the graphic interface of the eclipse SDK adjusts to the provided tools and design options. A description of the graphic interface is therefore only useful if a new report project and a new report was opened.

A project serves as container for files of the same type. I.e. you can create as many layout files as you want, which are recorded under a report project.

You create a new report project by clicking the **New** menu option and then on the **Project** sub-item in the **File** menu. A new dialog opens in which you select the **Report Project** entry as project type under **Business Intelligence & Reporting Tools**. Click on **Next** and specify the desired **Project Name** in the next view. Complete your entries with **Finish**.

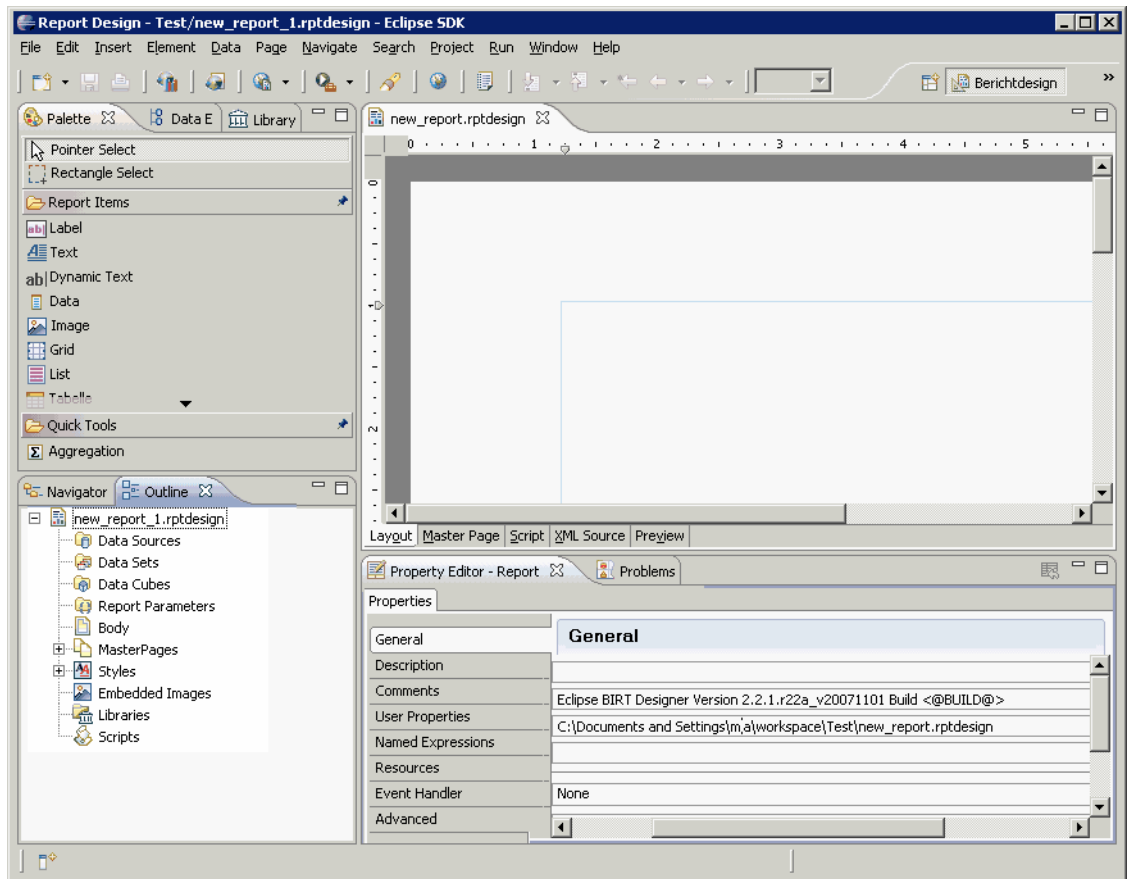
The created project appears in a window in the bottom left portion of the eclipse graphic interface. This window is now called **Navigator**.



To create a new layout click on **File** in the menu bar again. Select the sub-item **New** and then **Report**. A new dialog opens in which you name the new layout. After you have enabled the **Next** button a new view opens in which you select an empty layout from predefined samples. In addition, you can start a tutorial with the **My first report** entry to guide you through the first steps of crating a layout file. Confirm your selection with **Finish**.

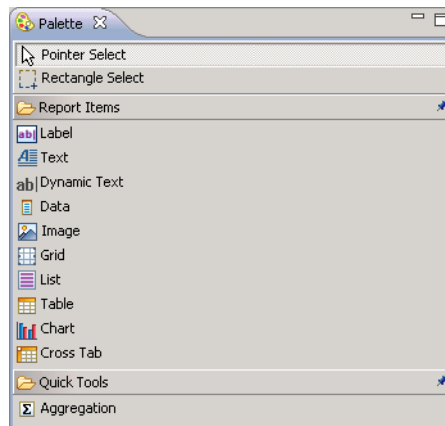
A new layout file as well as the toolbars of the report design open. The graphic interface with the toolbars as well as the functions of the tools and fields contained therein will be explained in the following.

27.6.3.2 The graphic Interface

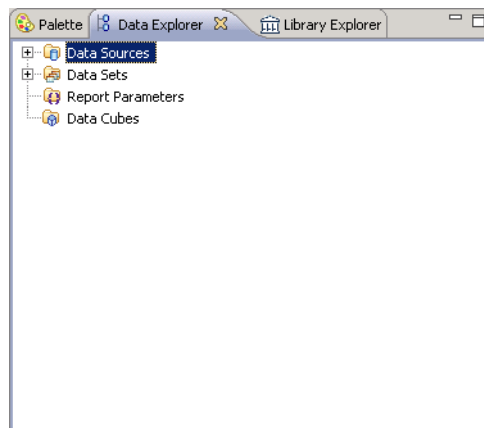


The graphic interface can be roughly divided in five sections:

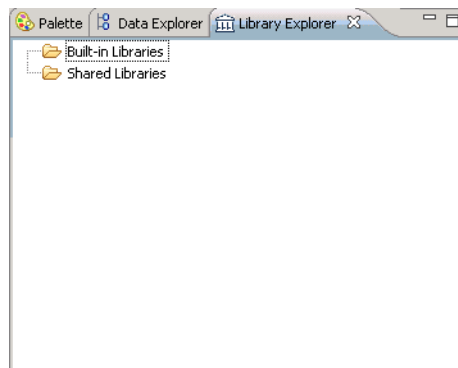
- **The menu and icon bar:** These bars form the upper section of the entire graphic interface. They contain basic administrative and support features by eclipse as well as specific features for editing layouts. Most features contained in the menu and icon bar are also covered by the toolbars. I.e. you can decide whether to use the toolbar and/or the menu/icon bar for editing.
- **Palette, Data Explorer and Library Explorer:** In the middle left section of the entire interface you find the toolbars for editing layouts. The **Palette** contains specific types of fields that can be created by context menu and integrated in a layout by drag&drop. The palette features adjust to the selected layout view (see [Section 27.6.3.5, “The available Tools and Fields for creating and editing Layouts”](#)).



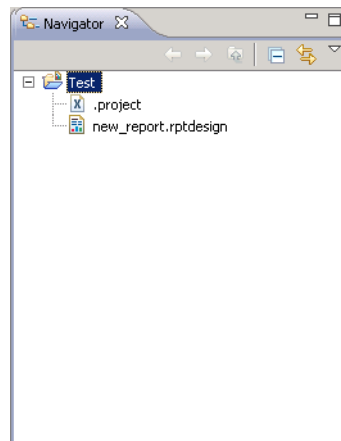
The **Data Explorer** provides an overview of the connected data sources, the variables found there, parameters and aggregated data. Here as well you can move available or created data and fields to a layout by drag&drop.



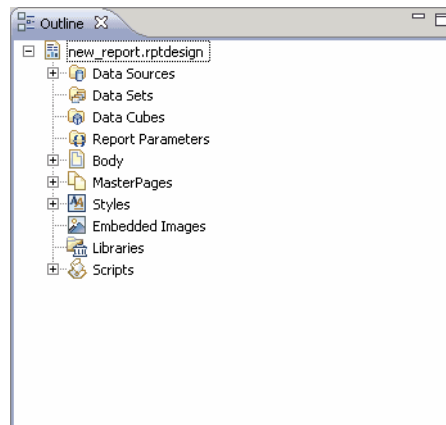
The **Library Explorer** enables you to integrate already existing libraries and invoke them as well as to use features and design options for layout file editing stored there.



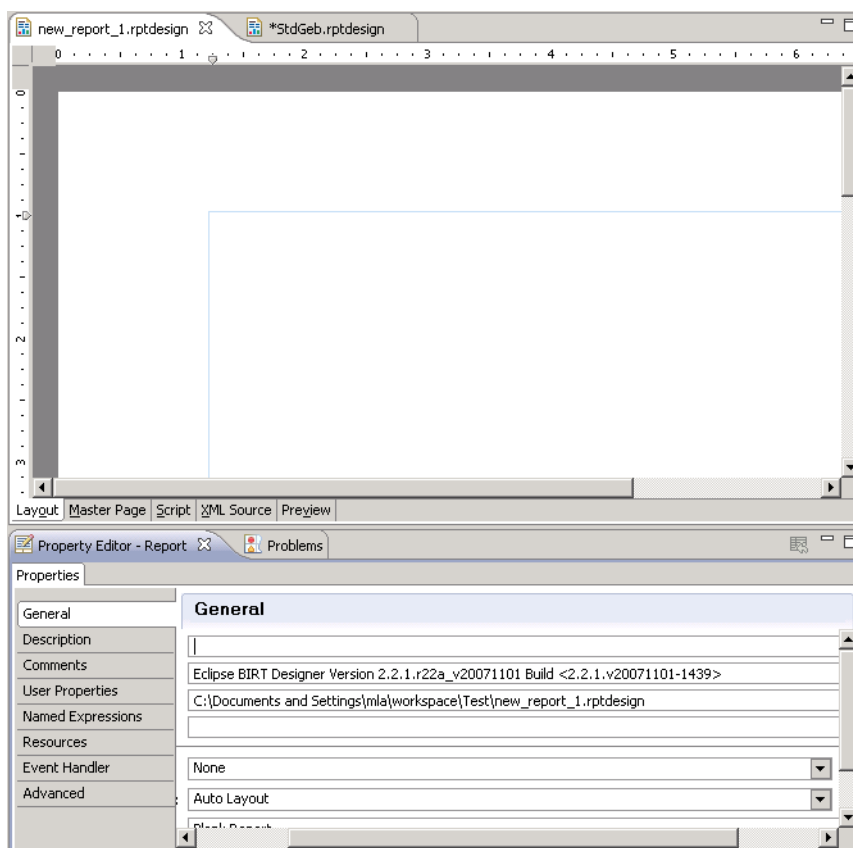
- **Navigator and Outline:** Underneath these toolbars you find the navigator and the outline. The **Navigator** shows an overview of created projects and subordinate files. Here you can open, close, create and delete files.



The **Outline** shows the fields and data used in hierarchical order. You can overview the entire structure of a layout file, and also move or delete single fields.



- **The layout view:** The largest representation portion is occupied by the layout view, which shows the layout you edit in different modes. In **Layout** mode you see the entire layout as workspace, in which you can insert freely definable fields respectively datafields. The single fields are stored and displayed as variables and not filled with concrete data for saving resources. The concrete data will only be loaded from the data source and edited in the **Preview** mode, which, depending on the size and number of data and required calculations, takes some loading time. In the **Master Page** mode you can determine a sample for the layout file by editing the header and footer. This sample is then used as template for each layout page to be created. The **Script** mode enables the implementation of script commands and operators that can be run through at different times of data acquisition respectively layout creation. Finally, the **XML Source** mode enables viewing and editing the properties of the layout file in XML.

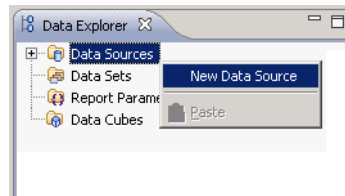


- **Properties and Problems:** Underneath the layout view you find two more windows that display information about the entire layout file or about single, grouped and aggregated fields and data sets. The **Property Editor** provides different information about the properties and settings of the entire file or single fields. Here you cannot only view the properties but also modify them. The **Problems** window lists all stored errors, warnings and information that occurred during the creation of the layout or of the report.

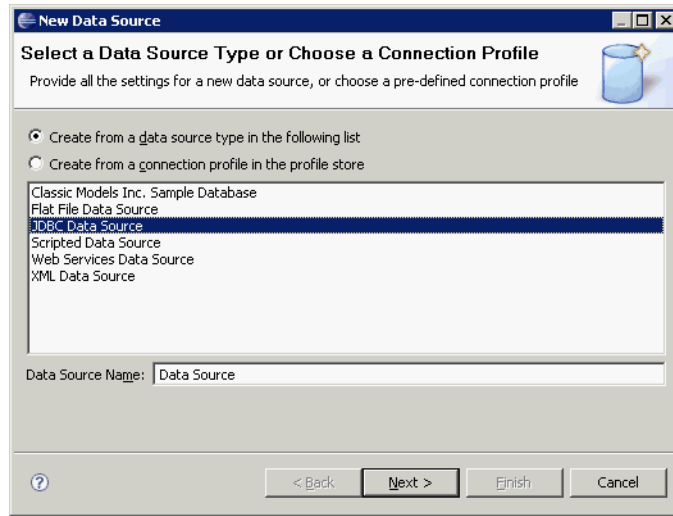
27.6.3.3 Connection to the Database Tables

Before you start editing your layout file you need to introduce the database created by the Report APL as data source to the system. By connecting the BIRT system to the database, the fields used in the database tables can be evaluated and used. In addition, a preview of the layout file can be created by evaluating the concrete data from the data source.

To configure a new data source, switch to the Data Explorer toolbar. There, click the **Data Sources** entry with the right mouse button. A context menu opens in which you click on **New Data Source**.

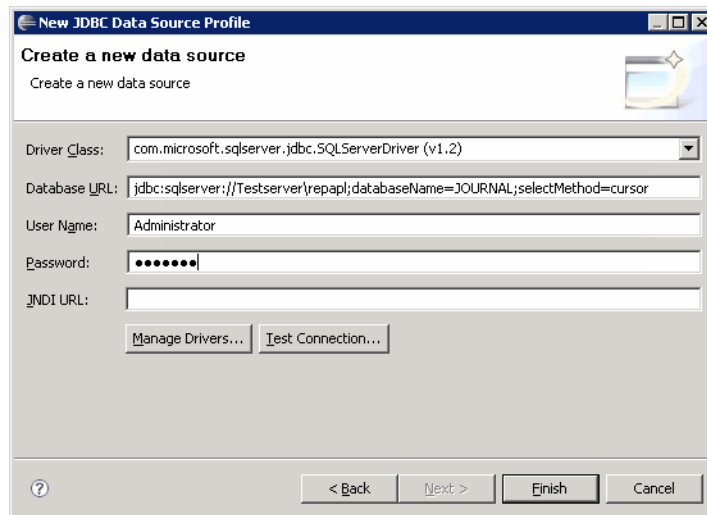


The New Data Source dialog opens. In there select the option **Create from a data source type in the following list** and **JDBC Data Source**.



Click the **Next** button.

Another view opens in which you need to specify the driver class, the database URL, the user name and the password.



As driver class select

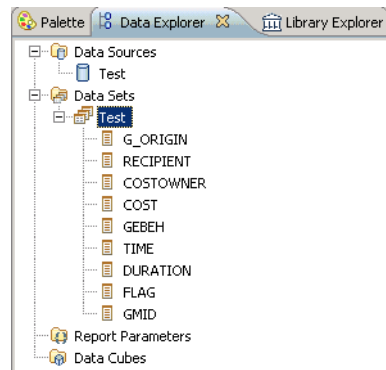
`com.microsoft.sqlserver.jdbc.SQLSERVERDRIVER (v1.2)`. As

database URL you specify as data source server your XPR server and as

database name the desired database tables. With the **Test Connection...** button you can test the correct link between XPR system and BIRT.

Complete your entries with the **OK** button.

The fields of the connected database table are displayed as variables under the item Data Sets in the Data Explorer.



You can edit the settings of your data source by a doubleclick on the corresponding data source in the Data Explorer anytime.

27.6.3.4 The Structure of Layout Files in BIRT

Before we list and shortly describe the single fields and editing options of layout files, we will provide a rough sketch of the general structure of layout files in BIRT.

In the **Master Page** mode you determine the header and footer properties besides the general page settings such as margins and background. These general properties as well as the header and footer are copied and displayed for each created page of the layout file. For example, you can make here specifications for the consecutive pagination, the date of layout creation or insert your company logo on each represented page.

In the **Script** mode you can implement procedures and commands in script language format and have these executed at different times. You can arbitrarily analyze and edit the data from the database to have them represented in the layout in the desired format. As procedures and commands, context parameters, report parameters, native JavaScript features, BIRT features and operators are available for selection. As times you can use the times of preparation (*onPrepare*), of report creation (*onCreate*), of data transfer (*onRender*) or of page break (*onPageBreak*).

In the **Layout** mode you edit the main portion of the layout. Here you can insert different fields and data variables or use tools to have processed data represented as e.g. sum or cross table. The fields are placed in the layout view by wildcard. Not until the Preview mode the exact data from the data source are loaded and the complete report created. In the next section you receive a short introduction to the available tools and fields.

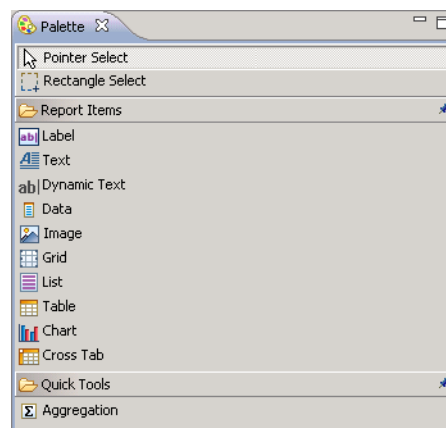
27.6.3.5 The available Tools and Fields for creating and editing Layouts

NOTE:

For a detailed introduction or pointed questions please refer to the corresponding eclipse SDK and BIRT documentation. The ensuing explanations make no claim to be complete but serve a first orientation only.

Palette in the Layout mode

In the **Layout** mode the palette contains the following fields and features:



- **Pointer Select** for pointed selection of fields and areas in the layout file
- **Rectangle Select** for laminar selection of fields and areas in the layout file
- **Label:** Field for specifying information about other fields such as tables or images or for specifying titles and headers
- **Text:** Freely definable text fields
- **Dynamic Text:** Using instructions and functions in script format as well as operators, a text can be dynamically adjusted here
- **Image:** Inserts a graphic in a variety of formats
- **Grid:** Inserts a simple grid with freely selectable columns and lines
- **List:** Adds a list with individual data set and header and footer
- **Table:** Creates a table with freely selectable columns and rows and, contrary to grids, with a definable data set and individual header and footer
- **Chart:** Using a wizard, charts can be crated here
- **Cross Tab:** Using a wizard, a cross table can be created with this tool

- **Aggregation:** This tool simplifies calculating different data sets under consideration of definable conditions

The single fields are implemented in the layout by drag&drop. Either the field is inserted directly or a wizard appears first for creating the field.

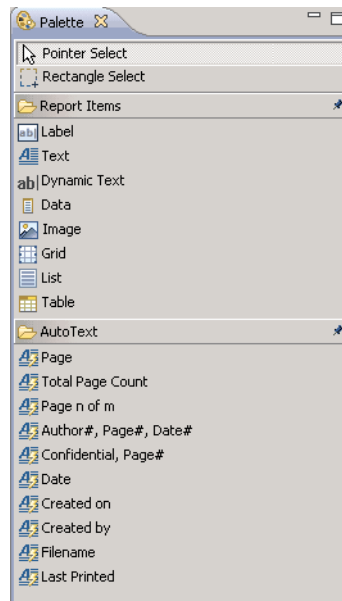
Each field can be implemented in another field and linked in this way. For example, texts, lists or diagrams can be inserted in tables. If the single fields are selected in the layout, you can use the properties editor to view and, if required, modify different settings e.g. for designing, bordering or linking by Hyperlink.

Each implemented field is displayed in the **Outline** view in its respective position and can be invoked and edited there.

Palette in the Master Page mode

In the **Master Page** mode the palette contains mostly the same fields as in the **Layout** mode. Charts, cross tables and aggregations are not possible in master pages, though.

Beyond that, fields are already specified that are often used in headers and footers:



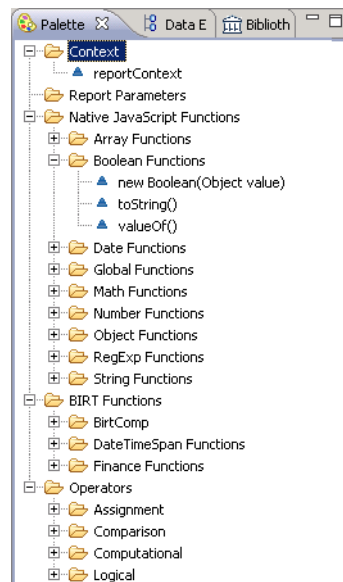
These include the page number (*Page*), the entire page number (*Total Page Count*), the *Page n of m*, the combination of *Author#*, *Page#* and *Date#*, the combination of *Confidential* and *Page#*, the *Date*, the specification *Created on*, the specification *Created by*, the *Filename* and the specification *Last Printed*.

The single fields are implemented in the layout by drag&drop. If the single fields are selected in the layout, you can use the properties editor to view and, if required, modify different settings e.g. for designing, bordering or linking by Hyperlink.

Each implemented field is displayed in the **Outline** view in its respective position and can be invoked and edited there.

Palette in the Layout mode

The view in the **Script** mode does not contain the actual layout file but an editor for creating a script that is added to the layout file. The palette holds predefined procedures, features and operators in the **Script** mode.



Besides context and report parameters, native JavaScript features, BIRT features as well as operators are available. The script can be executed at different times. As times you can use the preparation phase (*onPrepare*), report creation (*onCreate*), data transfer (*onRender*) or the page break (*onPageBreak*).

If you change the view mode, the script is automatically saved. If errors are contained in the script, they are listed in the **Problems** view.

Each created script is displayed in the **Outline** view in its respective position and can be invoked and edited there.

Palette in the XML Source and Preview modes

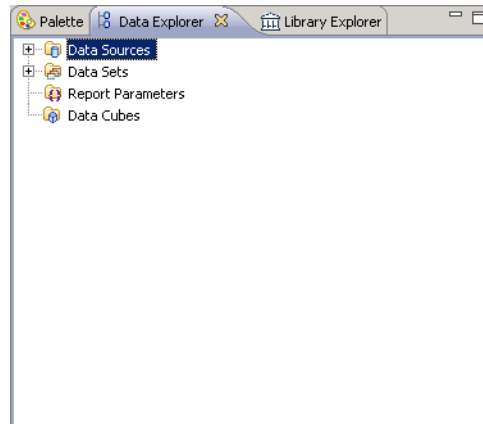
In the modes XML Source and Preview the palette does not contain fields or tools.

The XML Source mode displays the defined properties of the layout file in the XML language. You can perform there any modifications.

Using the Preview mode the concrete data are loaded from the connected database and put out according to the defaults and design of the layout file.

The Data Explorer

The Data Explorer contains the information about the data sources and associated data fields, report parameters and aggregated data.



The **Data Sources** entry contains the linked databases.

The **Data sets** contain the database fields found in the linked data source.

The **Report Parameters** contain data sets formally created but not assigned with a value until their first execution. Typically, you find date or time specifications here.

Data Cubes are grouped or summed-up data sets in a cross table format.

The single fields are implemented in the layout by drag&drop. If the single fields are selected in the layout, you can use the properties editor to perform settings e.g. for designing, bordering or linking by Hyperlink.

Each implemented field is displayed in the **Outline** view in its respective position and can be invoked and edited there.

Groupings

Within the fields Table, List and Grid you can create groupings from the contained data and fields. Groupings serve for sorting and filtering data. Select the corresponding field and click the right mousebutton. A context menu opens in which you click on **Insert Group**. A new dialog opens:

[illegible]

Here you can perform different settings for the group to be created. Besides making specifications as to which data are to be sorted in which format you can use expressions and operators to create filter and sorting rules.

The newly created group is graphically implemented in the layout and contains a line for the group header and group footer. Next to this the group structure is displayed.

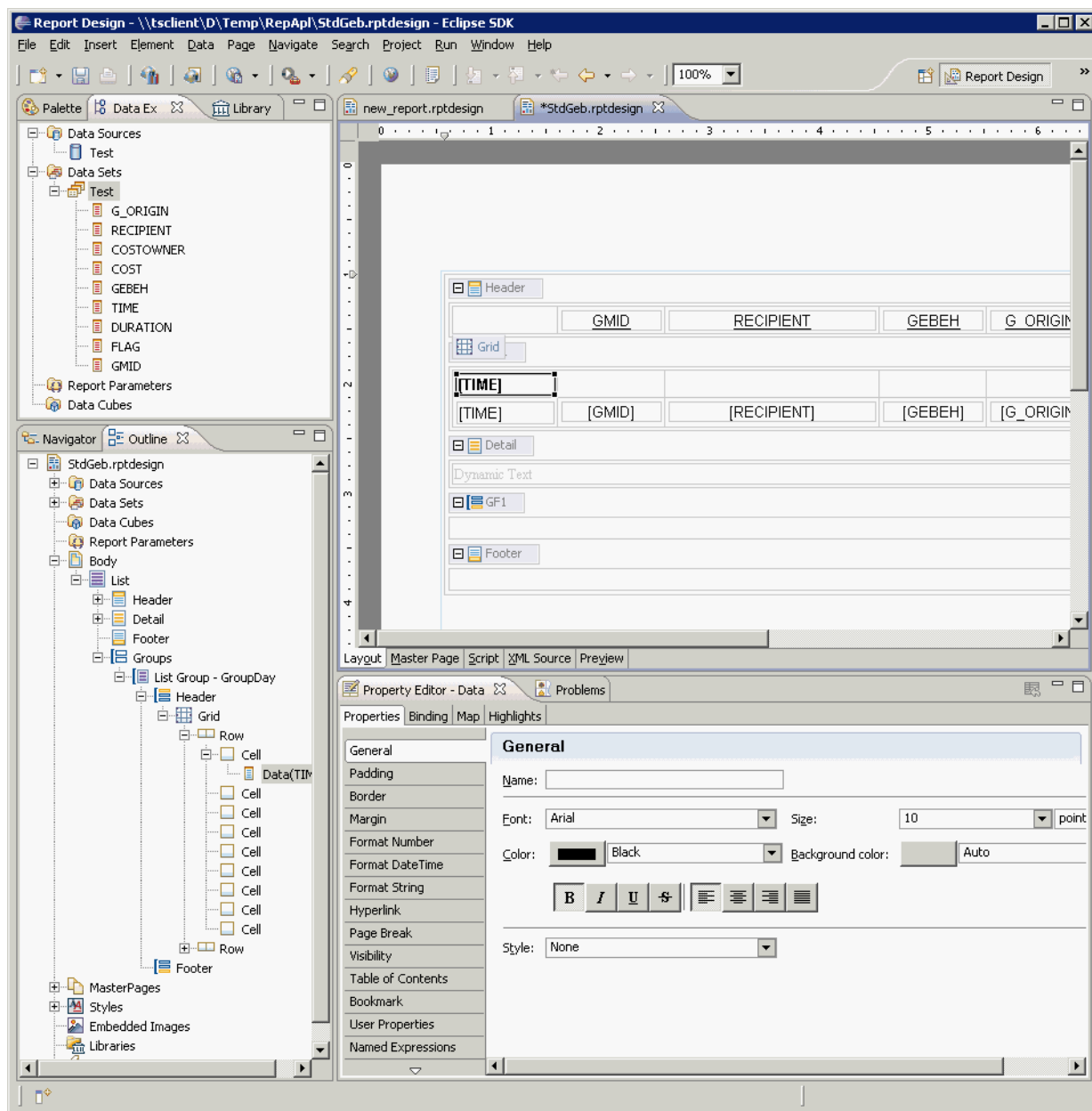
In the next section we will shortly exemplify the default billing report.

27.6.3.6 An Example: The Default Billing Report

The following section summarizes the above design options and operating modes with BIRT. For this purpose we use the default billing report (`StdGeb.rptdesign`) as example.

NOTE:

You find explanations about the function and the single fields of the default billing report in [Section 27.8.2, “Default Billing Report”](#).



In the layout view you see a graphic representation of the fields and data sets used as regards their position and size. The outline contains the same elements of a structured, hierarchical format. For the selected `TIME` data set, the properties editor displays different properties. Besides the connected data source the Data Explorer lists the available data sets. With the execution of the Preview mode the data would be read out of the database and a layout preview created.

27.6.4 Selecting, activating and setting a Layout

To generate a report please proceed as follows:

1. Double-click the **RepScheduleApi** module entry in the **Modules of** window of the XPR monitor.
2. Select **Set Options** with a double-click to open the Report Schedule APL configuration dialog.

Report Schedule APL configuration

Reports
Report query

Reports | Layouts | Parameters

Name	State	Last Status	Layout	Disable
ADDemo	Stopped	None	ADDemo.rpt	
Demo	Active	Error	Demo.rpt	
StdGeb	Stopped	None	stdgeb.rpt	

Add Remove

Times | Recipient | Export | Extensions | Information

Execution Times

☐ Execute now

☒ Execute at:

Date: 23.06.2006 Time: 15:09:24

Repeat Strategy

☒ No repetition

☐ User-defined

Every: days hours minutes

☐ Hourly

☐ Daily

☐ Weekly

☐ Monthly

☐ Yearly

Version 8.00.0.8444

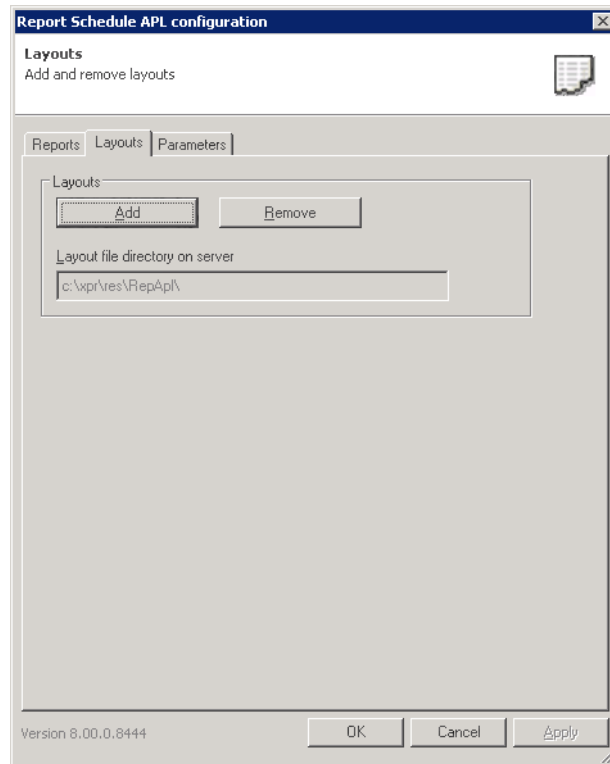
OK Cancel Apply

The following sections describe the procedure of report generation step by step.

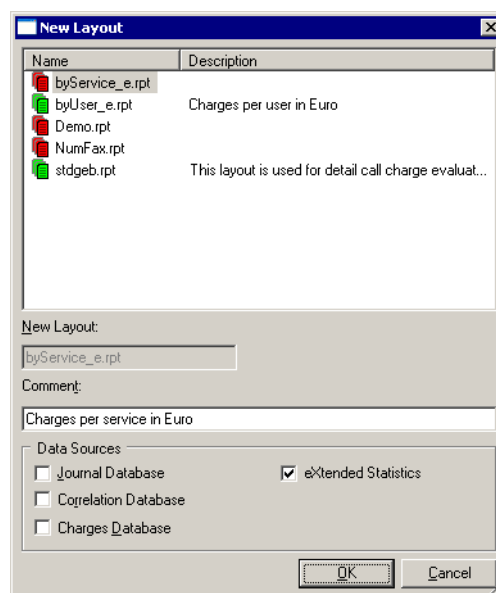
27.6.4.1 Step 1 - Introducing Layouts

To generate the desired report job start as follows:

1. Switch to the **Layouts** tab in the Report APL configuration dialog.
2. Click **Add**.



The following dialog opens:



3. Select the desired report layout.

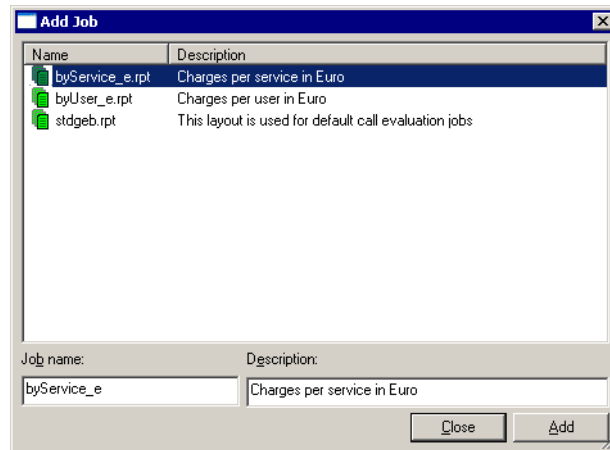
NOTE:

Verify the corresponding layout file extension. Chrystal Reports only supports layouts with the extension `rpt`, while BIRT only considers layout files with the extension `rptdesign` for report creation.

4. Enter a short descriptive text for the report in the **Comment** field.
5. Select the desired data source. In case of all current layouts this is **eXtended Statistics**.
6. Click on **OK** and switch to the **Reports** tab in the Report Schedule APL configuration dialog.

27.6.4.2 Step 2 - Adding a new Layout

1. Click **Add**. A dialog opens that displays all report layouts known to the Report Schedule APL.



2. Select the layout that was introduced to the Report Schedule APL in Step 1 and enable the **Add** button. Repeat this process to add further reports for processing. The dialog remains open until you **close** it with the corresponding button.

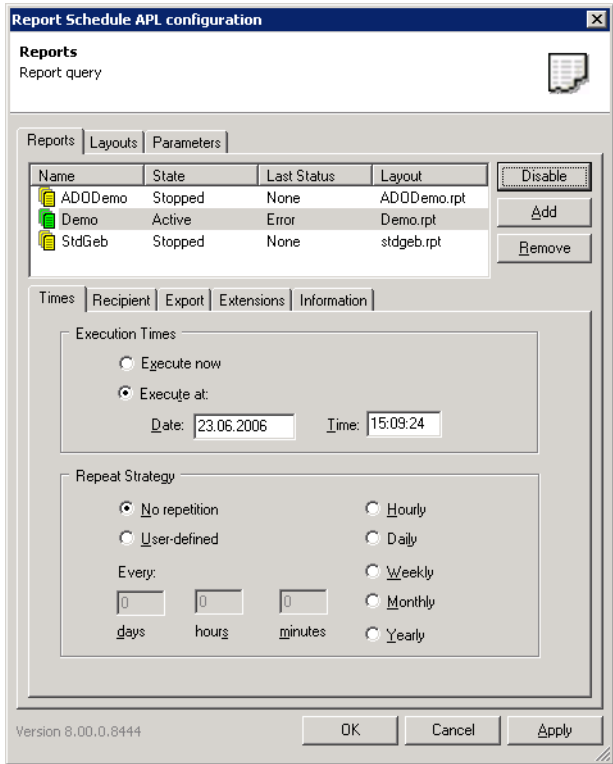
The top section of the configuration dialog displays the report layouts that have been added to the list.

3. Select the report that you want to configure.

In the next steps the parameters for the report setting will be assigned in the configuration dialog under the list display.

27.6.4.3 Step 3 - Setting an Execution Time

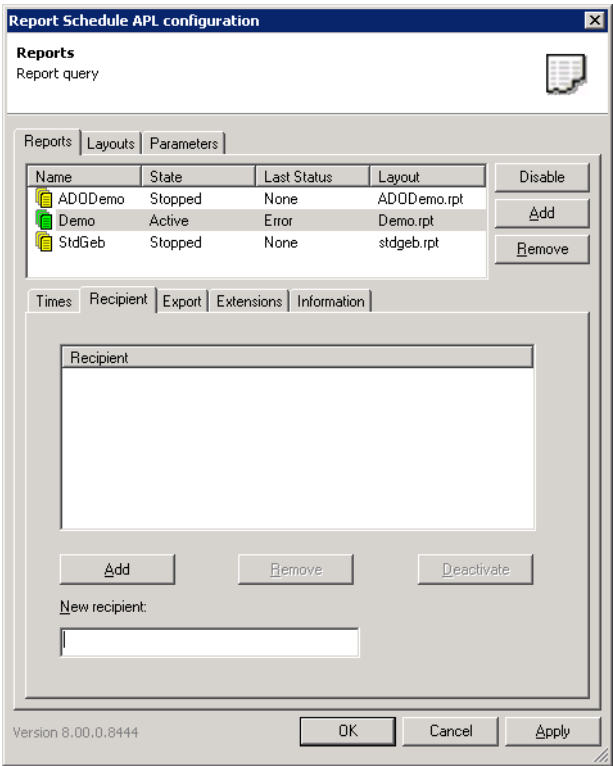
In the **Times** tab, within the **Execution Times** section, you can assign either **Execute now** or, via **Execute at**, a fixed time to a report job.



1. For a test select **Execute now** and **No repetition**. Later, after the activation of the report layout, you can click **Apply** or **OK** and the report job will be immediately executed once.

27.6.4.4 Step 4 - Selecting a Recipient

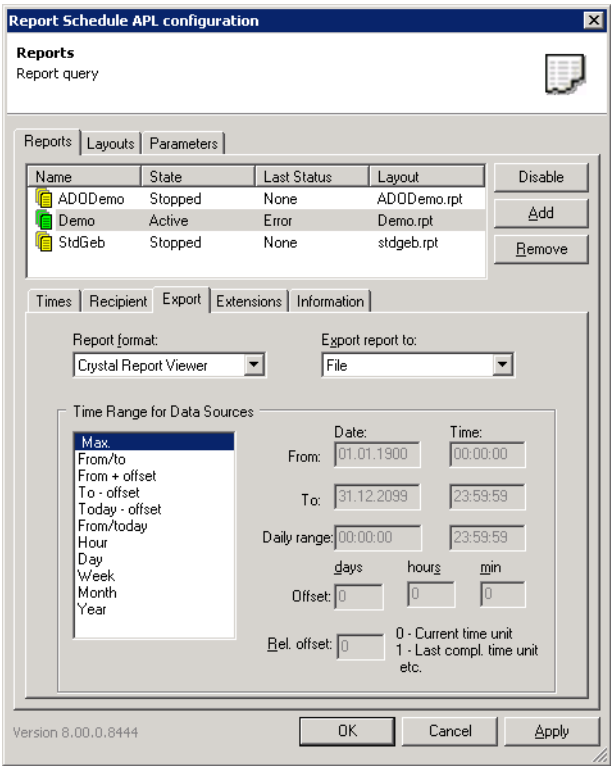
1. Switch to the **Recipient** tab.



2. Enter a XPR user name in the **New recipient** field and press the **Add** button. The system always inserts the recipient address as NVS address (e.g. NVS : <Server name> / <User>).

27.6.4.5 Step 5 - Selecting a Format

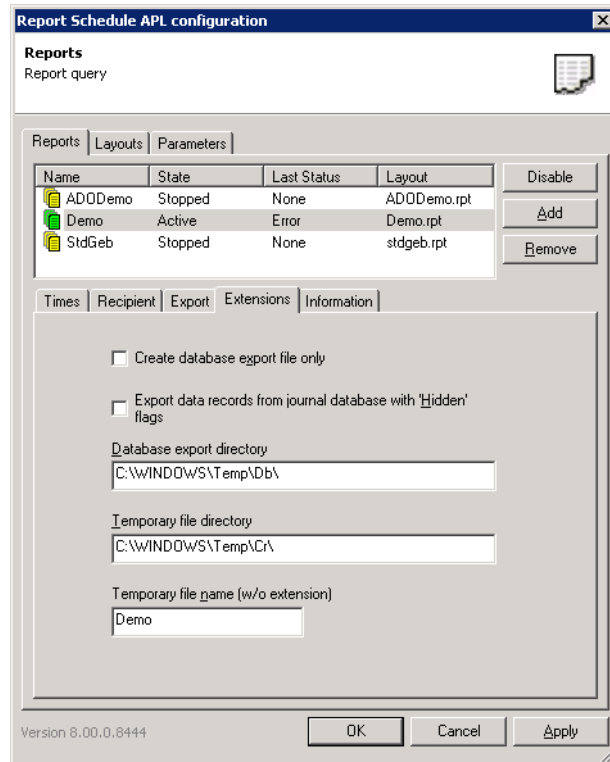
- 1. Switch to the **Export** tab.



- 2. Select the report format for the report job output. In our example select **RTF**.
- 3. Select a **Time Range for Data Sources**. For our example select the setting **Max**.

27.6.4.6 Step 6 - Selecting a Folder

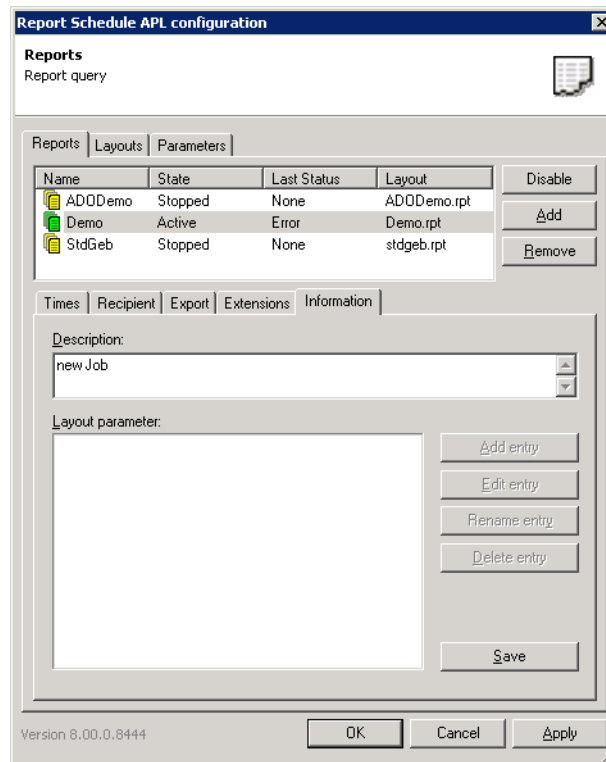
1. Switch to the **Extensions** tab.



2. Enter the path to the folder in which you want to store the data. In our example we store the data in the C : \Temp\Db\ folder.
3. Enter the name for the temporary file in the **filename** field.

27.6.4.7 Step 7 - Describing a Report

1. Switch to the **Information** tab. It displays the **Description** for the report.



2. If no description should be displayed, enter one here.
3. In the **Layout parameter** section you can check for which languages specifications are available in the resource file (see [Section 27.3.2, "Layouts", on page 1251](#)).

27.6.4.8 Step 8 - Activating a Layout

1. After you have selected all parameters, select the configured report layout in the top section of the configuration dialog and click the **Enable** button.
2. Subsequently confirm with **OK**. The report is now created.

27.6.5 Creating a Report for the XPR Databases

When creating reports based on the data of the XPR databases such as Journal, Geb or Correl please note the following:

The data of these databases are administered by the InfoStor and consequently not stored in log files by the XMR service. So that the databases are available for the reporting feature just the same, the data are mapped in the Report APL database. However, report generation by the Report Schedule APL for such databases is restricted.

The time specified in the registry entry **ExportInterval** (see [Appendix E.16.2, “Runtime Engine”](#)) determines after which period the data are exported to the Report APL database and thus updated (default setting: 5 minutes). If, however, a report is activated in the Report Schedule APL, this export for the InfoStor databases will not be executed. Data are only exported to the Report APL if the Report Schedule APL explicitly requests the data, thus creates a report. The raw data of the APLs stored in log files are not affected by this restriction.

If, for example, you have activated a report in the Report Schedule APL that is to create a report every 24 hours, data will also only be exported from the InfoStor every 24 hours. The export interval specified in the registry entry **ExportInterval** will thus *not* be considered.

There are two options for having a report created that has data modifications displayed more precisely. Either you define a short interval, e.g. 5 minutes, for your report on the [Reports Tab](#) of the Report Schedule APL configuration pages, or you define a second report that reads out the InfoStor databases but does not deliver a result. This “empty” report with an also configured short interval sees to the data of the InfoStor databases being exported to the Report APL database at any report execution time. Your actual report can thus access the continuously updated data in the Report APL (according to the specified interval of the report). Since a high resource load is generated by the report creation in short intervals we recommend to create a second empty report.

27.7 Structure of the XPR and Reporting Databases

The XPR databases are the databases:

- **CORREL** ([Section 27.7.1, “The CORREL.DBF Database”, on page 1332](#))
- **GEB** ([Section 27.7.2, “The GEB.DBF Database”, on page 1334](#))
- **JOURNAL** ([Section 27.7.3, “The JOURNAL.DBF Database”, on page 1335](#))

For the reporting feature the

- **JobRecipient** ([Section 27.7.4, “JobRecipient”, on page 1341](#)) and
- **JobInfo** ([Section 27.7.5, “JobInfo”, on page 1341](#)) is used.

A problem with some internal XPR databases is that they have not been designed for the creation of statistics and therefore no common fields exist within the internal XPR databases. This prohibits a useful indexing. Therefore it would be complicated to establish e.g. the number of all fax messages sent from within a XPR user group as a relation between the **Journal** and the **Correl** database would be required.

In the following we will shortly introduce the corresponding databases and their fields.

27.7.1 The CORREL.DBF Database

This database includes Correlation data records from the internal XPR database `CORREL`. This database does not contain time information and is therefore the current export at any given time of the creation of the report.

Each data record defines a field of an address book entry and is used to save the various sorts of correlation information (e.g. address books, user privileges, privilege lists, fax cover page information), that is to say interrelated data.

The actual payload is held in the `KEY` field. That means for each payload a data record is included in the database.

Example

Correlation data records represent several parts of an object. In the address book, the `USER` "MAYER" can be identified via his `NAME` "William Mayer" or his Fax G3 number (`FAXG3`) "4912345678". Two correlation data records would describe this relation:

Field/Column	Data record 1	Data record 2
DOMAIN	<XPR server name>	<XPR server name>
CLASSNAME	USER	USER
CLASS	MAYER	MAYER
KEYNAME	NAME	FAXG3
KEY	William Mayer	4912345678

The following table describes the single fields or respectively the columns separated by tabulators of a correlation data record.

Field/ Column	Description
DOMAIN	The address book context in which this data record is stored. Some current implementations of XPR modules leave this field empty. The XPR Kernel then creates automatically a default <code>DOMAIN</code> entry: data sets with the class name <code>USER</code> , <code>RUND</code> or <code>GLIST</code> receive the <code>DOMAIN</code> <Servername>, all other data sets with an empty <code>DOMAIN</code> field are assigned <Servername>/\$\$SYSTEM.
CLASSNAME	<code>CLASSNAME</code> , <code>CLASS</code> , <code>KEYNAME</code> and <code>KEY</code> define an element of a correlation information object. Examples for <code>CLASSNAME</code> : <code>USER</code> , <code>PRIVILEGES</code> , <code>FAXCOVER</code> .
CLASS	Further subspecification of the information given by <code>CLASSNAME</code> . If e.g. <code>CLASSNAME</code> contains the entry <code>USER</code> , a XPR user name is specified in <code>CLASS</code> , e.g. <code>MAYER</code> .
KEYNAME	Further subspecification of the information given by <code>CLASS</code> . The triple <code>CLASSNAME</code> , <code>CLASS</code> and <code>KEYNAME</code> is unique and defines a unique data set.

Field/ Column	Description
KEY	This field contains the actual payload. <code>KEY</code> is the value belonging to the unique triple <code>CLASSNAME</code> , <code>CLASS</code> and <code>KEYNAME</code> . This value is not unique, so that the same value can come up in several triples containing <code>CLASSNAME</code> , <code>CLASS</code> and <code>KEYNAME</code> .

27.7.2 The GEB.DBF Database

This database contains correlation data records from the internal XPR database Geb. This database stores the charged costs. If the account of charges is active on the XPR server, each send transaction generates a charges data record. The following table describes the fields and columns of such a charges data record:

Field	Description
G-ORIGIN	Trigger of the chargeable transaction (internal: <code>owner_originator</code>). This field contains the originator's NVS address. Example: <code>NVS : SERVER/POSTMASTER</code>
RECIPIENT	<code>owner_recipient</code> of a send process: thus the recipient's NVS address. Example: <code>NVS : FAXG3/+491234567890</code>
COSTOWNER	Cost point to which belongs a fee entry.
COST	The costs summing up during the send job.
GEBEH	Billing units.
TIME	Start of the transmission.
DURATION	Duration of the transmission in seconds.
FLAG	Can be used to flag internal billing states.
GMID	Related Message ID. This field is the basis for the relation to the Journal database (see also <code>MID</code> in <code>JOURNAL.DBF</code>).

27.7.3 The JOURNAL.DBF Database

This database contains the data records of the global server journal, which includes an entry for each send and reception action and the related events. The following table describes the fields and columns of such a `JOURNAL` data set:

Field	Description
MID	Message ID of the data record. These Message IDs are unique for a server and a message. The ID is assigned by the MTA, as soon as he receives a send job and serves as reference for the respective entry in this database. A new send job will be passed to the XPR MTA via the <code>MID 0</code> .
ORIGINATOR	NVS address of the sending service of the message. The static part <code>NVS :</code> of the NVS address is not stored in the journal, thus the address has always the form <code>[Service]/[Address]</code> .
OWNORIG	NVS address of the originator of the sent message.
RECIPIENT	NVS address of the receiving service of the message. This address has always the form <code>[Service]/[Address]</code> . The address is determined by the routing rules of the XPR server. The original address is transferred to <code>org_recipient</code> . This field is not available here.
OWNRECIP	NVS address of the owner of the received message.
SUCCESS	The success status <code>TS_SUCCESS</code> of a send action. The following values are possible:
	0 <code>TS_SUCCESS_UNDEFINED</code> No transaction report has ever been sent.
	1 <code>TS_SUCCESS_UNKNOWN</code> A report has only been sent for information purposes yet, the success of the send process is not clear. A typical example would be a report including "Started sending..."
	2 <code>TS_SUCCESS_OK</code> The document has been successfully sent to the recipient.
	3 <code>TS_SUCCESS_FAILURE</code> The transmission of this document has failed, all repetitions have failed.
	4 <code>TS_SUCCESS_REJECT</code> The XPR service responsible for this transmission is at the moment not able to complete the job for internal reasons. This transaction report causes the XPR MTA to assign the message to the service again for a later delivery. Transmission attempts that have been sent back with such a transaction report are not included in the maximum number of transaction reports. That means that the XPR MTA will assign the job infinite times if it is only answered by such a transaction report. A typical example for the usage of such a report is that the service has not yet finished its initialization.

Field	Description
	5 TS_SUCCESS_REPEAT The transmission of the message has failed because of an external error. This transaction report causes the XPR MTA to reassign the message to the service according to the repeat strategy of this transaction. Only a finite number of these transmission attempts is performed by the XPR MTA. After this limit has been exceeded the message receives the success status TS_SUCCESS_FAILURE . A typical example for the usage of such a report would be that the recipient of the message is temporarily not available.
	6 TS_SUCCESS_DELAYED The XPR server tried to deliver the message directly to a client. The client was not available. Such a state is not considered as a failure (TS_SUCCESS_FAILURE) as the message is already in the user's inbox on the server. Neither is it considered as successful (TS_SUCCESS_OK) since the message has not been delivered physically to the user yet.
TIME	Point of time the message has been sent. The time stamp is set by the sending service.
STATE	Message in clear text about the state of this transaction in the server language.
FORMAT	This field gives the format of the message. You find an overview of the formats in Appendix A, "Document Formats" .
LENGTH	Length of message in bytes.
DELFLAG	The value specifies the different delete states of the entries in the database. The states represent different views of the data records in this database. This value is generally a combination (linked by "or") of some or all of the following values:
	0x0000 This message does not contain a delete flag.
	0x0001 DELETE_ORIGINATOR The originator of a message has deleted the message in his outbox.
	0x0002 DELETE_RECIPIENT The recipient of a message has deleted the message in his inbox.
	0x0004 DELETE_ARCHIVIST The data records flagged like this have been archived.
	0x0008 DELETE_POPPER The data records flagged like this have been retrieved by a POP Mail Client.
FLAGS	This parameter contains a series of the states and properties a message can adopt. A message cannot lose such states and properties. This value is generally a combination (linked by "or") of some of the following values:
	0x00000001 TS_FLAGS_READ Document has been read.
	0x00000002 TS_FLAGS_ARCHIVE Document has been archived.

Field	Description
	0x00000004 TS_FLAGS_PRINTED Document has been printed.
	0x00000008 TS_FLAGS_COST Document costs are charged.
	0x00000010 TS_FLAGS_CARBONCOPY Document is a copy.
	0x00000020 TS_FLAGS_EXLINE Transmission line exact.
	0x00000040 TS_FLAGS_CIT CIT signal has been set.
	0x00000080 TS_FLAGS_EXTERNCOPY Document is a copy, originated by the MTA.
	0x00000100 TS_FLAGS_HIDE Document is hidden.
	0x00000200 TS_FLAGS_DONTFORWARD Document cannot be forwarded.
	0x00000400 TS_FLAGS_NODELMID The Message ID has been chosen by sender.
	0x00000800 TS_FLAGS_NODELDO Document is not deleted during the physical deletion of the journal entry.
	0x00001000 TS_FLAGS_FORM This document has been created as a form.
	0x00002000 TS_FLAGS_MAXREPSFAIL Error because of exceeding the maximum number of repetitions.
	0x00004000 TS_FLAGS_AUTOTIMECPY Automatic copy after a certain time.
	0x00008000 TS_FLAGS_FLAG1 User-defined rule 1.
	0x00010000 TS_FLAGS_FLAG2 User-defined rule 2.
	0x00020000 TS_FLAGS_VFSROUT VFS routing flag.
	0x00040000 TS_FLAGS_XVFS VFS report modifications.
	0x00080000 TS_FLAGS_GATE Document has passed a XPR Gateway (Remote System Link).
	0x00100000 TS_FLAGS_OWNRECNRT Recipient is set by the MTA.
	0x00200000 TS_FLAGS_CONFIDENTIAL This document is confidential.
	0x00400000 TS_FLAGS_ISLOCALUSER The target must be a local user.
	0x00800000 TS_FLAGS_VFSAUTODEL VFS: Automatic deletion after successful sending.

Field	Description
	0x01000000 TS_FLAGS_NOPREFERRED For this recipient address the <i>Preferred</i> rule is not applied.
	0x02000000 TS_FLAGS_ADMINDELETE The document has been deleted by the Admin Task in order to save space on the hard disk.
	0x04000000 TS_FLAGS_PARTIALCONVERSION This document may also be partly converted.
	0x08000000 TS_FLAGS_FLAGGED The inbox entry has been flagged by an IMAP4 user.
	0x10000000 TS_FLAGS_NOTRECENT The inbox entry has been received by an IMAP4 user.
	0x20000000 TS_FLAGS_RESETCIT Reset the CIT signal for 'ps->recipient'.
	0x40000000 TS_FLAGS_MERGED OK and READ report have been merged into one report, no separate receive and read reports exist.
	0x80000000 TS_FLAGS_DONTREPORT No report is sent for this send document.
SUBJECT	Subject field of a message (for e-mails).
COSTINFO	Costs that have been caused by the send transaction.
COSTOWNER	Cost center that has incurred the charges.
PRIORITY	This field describes the send priority. The following values are possible:
	1000 TS_PRIORITY_URGENT Highest default priority.
	4000 TS_PRIORITY_HIGH High default priority.
	5000 TS_PRIORITY_NORMAL Default priority.
	6000 TS_PRIORITY_LOW Low priority.
	10000 TS_PRIORITY_NIGHT Priority that might delay the delivery.
FINALREPS	Number of delivery attempts.
PAGESEND	If the message has been delivered as fax: number of sent fax pages.
PAGERECIVE	If the message has been received as fax: number of received fax pages.
ORIGSRVC	This field includes the service section of the <i>Originator</i> field.
SOURCE	This field includes the address section of the <i>Originator</i> field.
RECIPSRVC	This field includes the service section of the <i>Recipient</i> field.
DEST	This field includes the address section of the <i>Recipient</i> field.
ORIGINAL_RECIPIENT	Original recipient of a message before the first update

Field	Description
TRANSPORT_RECIPIENT	Recipient who serves as intermediate station of the message transport
UPDATE_SEQUENCE	Number of message updates
DELTIME	Time at which a message was deleted
CRTIME	Time at which a message was created
LASTUPDATE	Last message update
ORIG_ORIGINATOR	Original originator of a message before the first update
SERVER_NAME	Server name
ORIG_APL	This field contains the specification of the original APL, which created the transaction
RECIP_APL	This field contains the specification of the APL that received the object of the transaction
DOC_TYPE	Message type, for example Fax3G, SMS, e-mail, etc.
HOPCOUNT	Number of hops, the intermediate stations in the network the message passed through on the way from the originator to the recipient
ORI	Time specification of the APL that sent the message at the time when the same message was transmitted
REC	Time specification of the APL that received the message at the time when the same message was transmitted
RORI	Time specification of the APL that received the message at the time when the same message was received
RREC	Time specification of the APL that sent the message at the time when the same message was received
TEL_COSTUNITS	Number of local billing units
NST	Time at which the message is resent according to schedule
MAXREP	Maximum number of repeated message transmissions
REPT0	Period between the initial message transmission attempt and the first repetition
REPT1	Period between the initial message transmission attempt and the second repetition
REPT2	Period between the initial message transmission attempt and the third repetition
REPT3	Period between the initial message transmission attempt and the fourth repetition
REPT4	Period between the initial message transmission attempt and the fifth repetition
REPT5	Period between the initial message transmission attempt and the last repetition
Filename	Message file name

Field	Description
CONVSRC-FORMAT	Original format of the document at the document's transmission (before a conversion)
CONVDESTFORMAT	Format of the document after the document has been received (after a conversion)
ORG_IDSTRING	Telematic ID of the originator
REC_IDSTRING	Telematic ID of the recipient
FATHERMID	ID of the "father" message (prior message as regards time and content)
SONMID	ID of the "son" message (subordinate message as regards time and content)
BROTHERMID	ID of the "brother" message (commensurate message as regards time and content)
INBOX_STATE	Status of the recipient's inbox
RECIPIENT_INBOX	ID of the recipient's inbox
CONTENT_TYPE	Content format, for example text, HTML, graphic, audio, etc.
PMF_FILENAME	Name of the PMF file of a message

27.7.4 JobRecipient

This database stores the recipients of the current report job for usage in a report.

Field	Description
ACTIVE	This field shows whether the report has been sent to the recipient who will be defined in the following field.
ADDRESS	This field includes the NVS address of the recipient of the current report.

27.7.5 JobInfo

This database lists the parameters of the current report job. These database entries define the name of the completed report, the export format of the report job, the time range of the report and the frequency of the report job's execution.

Field	Description
CREXPDEST	The path and file name of the created report export. The file name extension of the export is determined via the CREXPFMT field. This is the file that is delivered to the recipients of the report.
CREXPFMT	The export format used for this report job. The following values may be used: 0 – Crystal Reports (*.rep) 1 – Rich Text Format (*.rtf) 2 – HTML (*.html) 3 – Tab-separated values (*.tsv) 4 – Comma-separated values (*.csv) 5 – ASCII Text (*.txt) 6 – ASCII Text divided by tabs (*.txt) 7 – Word document (*.doc) 8 – Excel 5 Sheet (*.xls) 9 – Fax G3 Format (*.fg3)
DBTIMESEL	This field contains the type of the used time range. With the old functionality, data of this time range are exported from the PCO-internal databases. With the new functionality, this time range is transmitted as Record Selection Formula to the report layout at runtime. Absolute time ranges: 0 – Complete 1 – From DBTIMEFROM to DBTIMETO 2 – From DBTIMEFROM + DBTIMERNG 3 – From DBTIMETO - DBTIMERNG 4 – From today - DBTIMERNG 5 – From DBTIMEFROM to today Relative time ranges: 6 – A complete hour 7 – A complete day 8 – A complete week 9 – A complete month 10 – A complete year For the relative time ranges the field DBTIMEOFFS gives the relative offset (cf. DBTIMEOFFS).

Field	Description
DBTIMEFROM	The "From-time" in the form YYYY.MM.DD.hh.mm.ss (cf. DBTIMESEL).
DBTIMETO	The "To-time" in the form YYYY.MM.DD.hh.mm.ss (cf. DBTIMESEL).
DBTIMERNG	The time difference in seconds (cf. DBTIMESEL).
DBTIMEOFFS	The relative offset. The meaning is as follows (cf. DBTIMESEL): 0 – The current, generally incomplete time unit. 1 – The last complete time unit. 2 – The penultimate complete time unit. 3 – etc.
JOBID	The unique job ID.
STARTTIME	The time when the job is to be executed.
REPEATMODE	The repeat strategy: 0 – Unique execution 1 – Hourly execution 2 – Daily execution 3 – Weekly execution 4 – Monthly execution 5 – Yearly execution 6 – User-defined repetition
JOBNAME	Name of the report job.

27.8 Supplied Layout Files for Default Reports

Various layout files come with the Report APL, which serve for familiarization with the reporting and for testing the configured connection. Preinstalled are a demo report, a default charges-report, a fax messages report as well as two billing reports, which, on the one hand, refer to the subscribers and, on the other hand, to the services.

Using such provided layout files you can familiarize yourself with the report generation based on simple examples. After you have established a valid ADO database connection in the Report APL (see [Section 27.4, “Report APL Configuration”, on page 1254](#)), you can activate e.g. the demo report in the Report Schedule APL and test the reporting functionality with this report (see [Section 27.5, “Report Schedule APL Configuration”, on page 1261](#)). Furthermore, you can open the existing reports in Crystal Reports and view the existing structure of these reports respectively use them as template for your own reports.

The layout files of the `rpt` format and the file name beginning `ADO` are only considered by Crystal Reports XI, while the files of the format `rptdesign` are supported by BIRT only. Resource files of the same name have for Crystal Reports the format `ini`, while BIRT processes the `properties` format. While an `ini` file may contain all language resources, a `properties` file must be created for each language. `rptconfig` files are assigned to the `rptdesign` layout files of the same name and contain the configured properties of the layout in XML.

NOTE:

If you have installed both supported report engines (Crystal Reports and BIRT) on one system, only the Crystal Reports engine will be recognized and used by the Report Schedule APL. The layout files for BIRT can thus not be used.

NOTE:

As regards usage for BIRT respectively Crystal Reports the layout files only differ in their names and types. The contents of the layout files for BIRT and Crystal Reports are the same.

Furthermore, a consecutively numbered number of SQL files can be assigned to the layout files that allow additional views and data invocations from the database tables. The SQL files are run through according to the sequence of their numbering during the report creation. These SQL files are bound to the layout files of the same name but can be customized, expanded or updated.

Three different types of SQL files can be differentiated:

- SQL files for invoking procedures. These have the format `mrs_SP<name of the layout file without the file format rptdesign><two-digit whole number for numbering>.sql`, e.g.

mrs_SPCallLength01.sql

- SQL files for creating views. These have the format `mrs_<name of the layout file without the file format rptdesign><two-digit whole number for numbering>.sql`, e.g.

mrs_BillingInformation03.sql

- SQL files for creating tables. These have the format `mrs_TbI<name of the layout file without the file format rptdesign><two-digit whole number for numbering>.sql`, e.g.

mrs_TblCallLength01.sql

Like the layout files of the same name the SQL files are found in the directory `<XPR install>\res\RepApl`.

NOTE:

We recommend to contact the Professional Services for creating individual SQL files or modifying existing ones. For, there will be no support for modified or self-created layouts and reports.

27.8.1 Demo Report

The file is called **ADODemo.rpt**.

The Demo report describes how many messages have been transmitted, how long they have been and indicates their success. It is based on the **Journal** database.

NOTE:

This layout file can only be used with the report engine Crystal Reports and not with BIRT.

Column	Description
MID	Unique Message ID.
TIME	Timestamp.
Originator/Recipient	This parameter indicates originator and recipient of the transaction.
SUCCESS	This field describes whether the transaction was successful or not and can contain the following parameters: • OK • delayed • failure
Count of transmitted messages	This field contains the number of the transmitted messages.
Transmitted Bytes	This field contains the sum of the transmitted bytes.
COST INFORMATION	Includes the charges if the billing information has been defined in the respective table.

27.8.2 Default Billing Report

The file is called **ADOSTdGeb.rpt** for using Crystal Reports and **StdGeb.rptdesign** for BIRT.

The default billing report informs about recipients, originators, costs and duration of a transaction. The data for this report is delivered by the database **Geb**. If the billing report is empty, please check if the billing signals needed for this report are transmitted by your phone company.

NOTE:

As regards usage for BIRT respectively Crystal Reports the layout files only differ in their names and types. The contents of the layout files for BIRT and Crystal Reports are the same.

Column	Description
GMID	Message ID of a transaction
RECIPIENT	Recipient of a transaction, represented as NVS address of this document's recipient (inbound journal). This address has the format NVS : <System name> / <User name> (e.g. NVS : SERVER / POSTMASTER) if the recipient is a local user, or the format NVS : <Service> / <Address> all uppercase, if the recipient is no local user, e.g. NVS : FAXG3 / +492130493023.
GEBEH	Charges units
G-ORIGIN	Originator of a transaction, represented as NVS address of this document's originator (outbound journal). This address has the format NVS : <System name> / <User name>, e.g. NVS : SERVER / POSTMASTER if the originator is a local user or the format, NVS : <Service> / <Address> all uppercase, if the originator is no local user, e.g. NVS : FAXG3 / +492130493023.
FLAG	Can indicate internal account status.
DURATION	Duration of transmission in seconds.
COSTOWNER	Cost ID
COST	Number of local currency units accounted for this send transaction.

27.8.3 Fax Message Report

The layout file is called **ADOFaxReport.rpt**.

This report contains the number of the sent or received fax messages divided according to successfully or unsuccessfully transmitted fax messages. The data for this report is delivered by the **Geb** database.

NOTE:

This layout file can only be used with the report engine Crystal Reports and not with BIRT.

The report contains the following parameters:

Column	Description
from	Point in time when a fax message is received
MID	ID of the respective fax message
No.	Fax number of the recipient
Pages	Number of fax pages sent or received with the transaction.
Status	Fax message transmission status.
Success	Successful or failed message transmission status.
Total per:	Total number of sent and received fax messages: division of this specification into total number (number), number of successfully transmitted fax messages (successful) and number of failed fax message transmissions (failed).
Total per Agent:	Total number of sent and received messages (not only fax messages): division of this specification into total number (number), number of successfully transmitted messages (successful) and number of failed message transmissions (failed).
Totals per Day:	Total number of sent and received fax messages on one day: division of this specification into total number (number), number of successfully transmitted fax messages (successful) and number of failed fax message transmissions (failed).

27.8.4 Service-related Billing Report

The layout file is called **ADObyService_e.rpt**.

This report describes the billing per service in euro. This data is delivered by the **Journal** database.

NOTE:

This layout file can only be used with the report engine Crystal Reports and not with BIRT.

The report contains the following parameters:

Column	Description
USER NAME	Name of the originator.
CALL CHARGES IN EURO	Charges for the transaction in Euro.
SERCIVE AND TRUNK	Used service and trunks.
RECIPIENT	Recipient of the transaction.
DATE/TIME	Timestamp.
TOTAL AMOUNT	Total amount of costs for the transactions in Euro.

27.8.5 Subscriber-related Billing Report

The layout file is called **ADObyUser_e.rpt**.

This report describes the billing per user in euro. This data is delivered by the **Journal** database.

NOTE:

This layout file can only be used with the report engine Crystal Reports and not with BIRT.

The report contains the following parameters:

Column	Description
USER NAME	Name of the originator.
CALL CHARGES IN EURO	Charges for the transaction in Euro.
SERVICE	Used service.
RECIPIENT	Recipient of the transaction.
TOTAL AMOUNT	Total amount of costs for the transactions in Euro.

27.9 Available Telephone User Interface Reports (TUI) Reports

The following Telephone User Interface reports are found, like the default reports, in the `<XPR install>res\RepApl` directory. The reports are based on the raw data of the Telephone User Interface databases. You find the description of these databases in [Section 27.12, “Database Tables of the Telephone User Interfaces \(TUI\)”](#). How to integrate the respective reports in the Report Schedule APL and activate them is outlined in [Section 27.5, “Report Schedule APL Configuration”](#).

The TUI reports are split into three groups:

- [Section 27.9.2, “Reports about Systemwide Activity”](#)
- [Section 27.9.3, “Subscriber Activity Reports”](#)
- [Section 27.9.4, “System Security Reports”](#)

27.9.1 Overview

Name	Reference	Content
Systemwide Activity: Call Activity	Calls	Number of direct, forwarded and total calls for every hour
Systemwide Activity: Call Length	Calls	Connect time towards the voice mail system for all calls
Systemwide Activity: Board Load	Calls	Working load of the existing hardware
Systemwide Activity: Number of Accesses	Calls	Number of call processing and voice message calls per hour
Subscriber Activity: Subscriber Message Activity	Subscriber	Number and length of sent and received messages
Subscriber Activity: Subscriber Message Inactivity	Subscriber	Subscriber inactivity based on the last message sent
Subscriber Activity: Subscriber Access Activity	Subscriber	Number and length of direct access to the voice mail system
Subscriber Activity: Subscriber Access Inactivity	Subscriber	Subscriber inactivity based on the last access to their PhoneMail system
Subscriber Activity: Billing Information	Subscriber	Billing information for certain subscribers
Subscriber Activity: Outgoing Calls	Subscriber	Number of subscribers making outbound calls and duration of outbound calls
System Security: Invalid Access Attempts	System	Enumeration of invalid access attempts

27.9.2 Reports about Systemwide Activity

27.9.2.1 Systemwide Activity: Call Activity

The file is called **ADOCallActivity.rpt** for using Crystal Reports and **CallActivity.rptdesign** for BIRT.

The report about call activities registers the number of direct and forwarded calls as well as the total number of calls for each hour. Furthermore, it lists the number of outgoing calls that have been made every hour. Direct calls are calls via the direct or guest access numbers.

An increased number of direct calls (compared to forwarded calls) could suggest that the subscribers often use the transfer extension. Still, it could also indicate that the call answering has been configured falsely or is used incorrectly. Some examples of problems suggest incorrect transfer destinations which prohibit that the subscribers are able to activate the answering of calls at their extensions. Please check if the destinations are correct.

The report is based on the following databases:

- [Section 27.12.3, “Telematic – Call”](#)

The meaning of the column headings in the call activities report is as follows:

Column	Description
Time	The call time is measured hourly. The entry 12:00:00 e.g. applies to the hour from 12:00:00 until 12:59:59.
# Direct	Number of all direct (= not forwarded) calls to PhoneMail or VMS. Here the direct and guest access is counted.
# Forward	Number of all calls towards PhoneMail or VMS via forwarding. In contrast to a direct call in the PhoneMail system, another telephone was called in this case. This telephone has the call then forwarded to (any) PhoneMail or VMS access number. Result: the PhoneMail Forward Access answers.
# Outcall	Number of outgoing calls per hour A notification by User Outcall leads to a login in the TUI.
# Callback	Number of calls to PhoneMail or VMS by Callback Access.
# Transfer	Number of calls to PhoneMail or VMS by Transfer Access.
# Total	Total number of incoming and outgoing calls per hour
% Total	Percentage of PhoneMail or VMS usage at different times of the day.
Peak hour	Hour with the highest number of calls
Total number of calls in PhoneMail/VMS	Total number of calls to the PhoneMail and VMS system
Average calls per day per subscriber	Average number of calls per day per subscriber.

Column	Description
Summary	Summary of all day results in the reports.

The call activity report may provide useful information when you configure your system or check your system load. Please proceed as follows:

- Locate the largest number in the **# Total** column.
- Divide this number through the number of days that are covered by this report (without holidays and weekends).
- Divide this number through the number of system subscribers during the range of time.

The result offers a value for the number of calls per subscriber per hour during the peak time.

This information is useful to judge whether your system meets the requirements of your organization.

27.9.2.2 Systemwide Activity: Call Length

The file is called **ADOCallLength.rpt** for using Crystal Reports and **CallLength.rptdesign** for BIRT.

The Call Length Report includes the connect time to the PhoneMail system for all calls. The average connect time per day per subscriber is also recorded. If subscribers make direct calls, they often listen to several messages at once or use further options of the PhoneMail system. Therefore direct calls are usually longer than forwarded calls. However, long forward calls represent a positive system usage, since this indicates that the callers leave detailed messages. With the help of this report you can control the general system usage.

If the call length values appear too low, you should create reports about subscriber message activities (see [Section 27.9.3.1, “Subscriber Activity: Subscriber Message Activity”, on page 1358](#)) and call activities (see [Section 27.9.2.1, “Systemwide Activity: Call Activity”, on page 1351](#)) to judge on whether further subscriber trainings are necessary.

The report is based on the following databases:

- [Section 27.12.3, “Telematic – Call”](#)

The meaning of the column headings in the call duration report is as follows:

Column	Description
Time	Interval for the evaluation of the length of all calls connected to the PhoneMail of VMS system.
# Direct	Number of all direct (= not forwarded) calls to PhoneMail or VMS. A phone directly addresses PhoneMail/VMS via Direct, Guest, Callback, Transfer or Universal Access. Here the direct and guest access is counted.
# Forward	Number of all calls towards PhoneMail via PhoneMail. In contrast to a direct call in the PhoneMail system, another telephone was called in this case. In contrast to a direct call into the PhoneMail system another device has been called here which will now forward the call to any PhoneMail Access number. Result: the PhoneMail Forward Access answers.
# Outcall	Number of outgoing calls per hour A notification by User Outcall leads to a login in the TUI.
# Callback	Number of calls to PhoneMail or VMS by Callback Access.
# Transfer	Number of calls to PhoneMail or VMS by Transfer Access.
# Total	Total number of calls connected to the PhoneMail or VMS system.
% Total	Percentage of calls connected to the PhoneMail or VMS system.
Time ranges	Call information categorized according to time ranges: 0 to 30 seconds, 30 to 60 seconds, 60 to 90 seconds, 90 to 120 seconds, 120 to 240 seconds and more than 240 seconds.
Most common time range	Time range that contains the most calls of a month

Column	Description
Average duration	Average call duration; specified in seconds
Total connect time	Total duration of all connections of a month; specified in hours:minutes:seconds
Average connect time per day per subscriber	Average connect time per day and per subscriber; specified in hours:minutes:seconds
Summary	Summary of all day results in the reports.

27.9.2.3 Systemwide Activity: Board Load

The file is called **ADOGGeneralUsageByBoard.rpt** for using Crystal Reports and **GeneralUsageByBoard.rptdesign** for BIRT.

The General usage by board report contains information on the usage of the hardware boards. Unfortunately, because of technical restrictions, it is not possible to receive this workload about all available channels. However, with this report it is nevertheless possible to get meaningful information on the system workload by comparing all boards. Thus shortages can be detected and, if necessary, the hardware can be updated.

The report is based on the following databases:

- [Section 27.12.2, “Telematic – Physical Lines”](#)

The meaning of the columns for the General usage by board reports is as follows:

Column	Description
Board number	Number of the considered board.
Time range	Considered time range.
% Busy	Value in percent about the time range, during which all channels of the considered board were busy.
Incoming % Utilization	Value in percent about the time range, during which the board channels were busy with incoming calls.
Outgoing % Utilization	Value in percent about the time range, during which the board channels were busy with outgoing calls.
Total % Utilization	Value in percent about the time range, during which the channels of the board were busy.
Number of Seconds All Channels Were Busy	Total amount of time in seconds all channels of the board were busy.
Number of times all channels were busy	Total amount of time all channels of the board were busy.
Average % Incoming Utilization Per Day	Sum of all values in percent for incoming allocation divided by the number of considered days.
Average % Outgoing Utilization Per Day	Sum of all values in percent for outgoing allocation divided by the number of considered days.
Average % Total Utilization Per Day	Sum of all values in percent the channels of the board were busy divided by the number of considered days.

27.9.2.4 Systemwide Activity: Number of Accesses

The file is called **ADOAccessbyHour.rpt** for using Crystal Reports and **AccessbyHour.rptdesign** for BIRT.

NOTE:

The `AccessbyHour.rpt` report contains the required raw data from the `Call Processing Call` database. With XPR 4.0 this database will not be filled with data anymore, so that this report does not receive any data and remains empty.

This report lists the number of finished call processing and voice notification calls. The calls per day and for the entire selected period are put out. In addition, the hour of day in which the most calls (peak hour) occurred are calculated.

The report is based on the following databases:

- [Section 27.12.1, “Telematic – Call Processing Call”](#)

The meaning of the column headers for the General usage by board report is as follows:

Column	Description
Peak hour	The hour of day with the most calls
#Calls in the peak hour	Number of calls in this hour
Total number of finished call processing calls	Number of calls that have the <code>TYPE=CP</code> value for call processings (see Section 27.12.1, “Telematic – Call Processing Call”)
Total number of finished voice notification calls	Number of calls that have the <code>TYPE=VOICE</code> value for voice notifications (see Section 27.12.1, “Telematic – Call Processing Call”)

27.9.3 Subscriber Activity Reports

The Subscriber Activity Reports may help you to diagnose problems and make your system more efficient. The Subscriber Activity Reports (except the Billing Information Report) are very useful to determine individual subscriber problems.

The Billing Information Report enables you to determine the billing information based on the individual usage. The billing information can be reported with the help of different variables. The billing information may be based on a fixed amount for each usage parameter or on the usage amount for a certain type. The criteria for the billing information is given within the system parameters.

27.9.3.1 Subscriber Activity: Subscriber Message Activity

The file is called **ADOSubscriberMessageActivity.rpt** for using Crystal Reports and **SubscriberMessageActivity.rptdesign** for BIRT.

The Subscriber Message Activity Report shows the number and length of the sent and received messages. With both the Subscriber Message Activity Report and the systemwide report you may determine which subscriber needs more information about the features and the usage of the system. Monitor this report together with the system-wide report.

NOTE:

If the PhoneMail network feature is installed, the network fields appearing in this report specify the number of network messages and the number of the sent and received local messages for each subscriber. Furthermore, the total length of this messages is displayed in minutes. With the help of this report you may find out which subscribers make use of the network feature regularly.

If the value in the **# Messages Sent** column is low, then the subscribers may need training in saving and forwarding messages.

If the value in the **# Messages Received** column is low, then there may be an error in the system forwarding configuration.

The report is based on the following databases:

- [Section 27.12.4, “Telematic – Message”](#)

The meaning of the columns in the subscriber message activities reports is as follows:

Column	Description
Subscriber	Name of the person possessing a mailbox on the PhoneMail system.
Local Messages	Number of sent and received messages in the local PhoneMail system. The data includes the number of messages as well as their length (in minutes). The minimum message length is 1 second. If a message is only 500 or 900 milliseconds long, the value 0 will be displayed for this message length.
Network Messages	Number of sent and received messages from and to external PhoneMail systems in the network. The numbers include the number of messages and their length (in minutes).

27.9.3.2 Subscriber Activity: Subscriber Message Inactivity

The file is called **ADOSubscriberMessageInactivity.rpt** for using Crystal Reports and **SubscriberMessageInactivity.rptdesign** for BIRT.

The subscribers' message activity list itemizes all subscribers who do not meet the criteria contained in the RepScheduleApl in alphabetic order.

It specifies the user and indicates the last time he/she created and sent a message. This enables you to check, for example, which subscribers have a licensed mailbox but have not used it since a specific time anymore.

This list also tells you which subscribers have not sent any messages.

27.9.3.3 Subscriber Activity: Subscriber Access Activity

The file is called **ADOSubscriberAccessActivity.rpt** for using Crystal Reports and **SubscriberAccessActivity.rptdesign** for BIRT.

The Subscriber Access Activity Report shows the number and length of direct accesses to the PhoneMail system. This report helps you to evaluate trainings as well as single subscriber activities.

If the report shows few or short accesses, the subscribers might need further training sessions.

The report is based on the following databases:

- [Section 27.12.3, “Telematic – Call”](#)

The meaning of the columns in the subscriber access activities reports is as follows:

Column	Description
Subscriber/Last access	Shows the subscriber name and the last subscriber access to the PhoneMail system.
# Accesses	Shows the number of direct subscriber accesses to the PhoneMail system.
Access (Minutes)	Shows the total length of direct accesses (in minutes) to the PhoneMail system.

27.9.3.4 Subscriber Activity: Subscriber Access Inactivity

The file is called **ADOSubscriberAccessInactivity.rpt** for using Crystal Reports and **SubscriberAccessInactivity.rptdesign** for BIRT.

Analog to the subscriber activity in the PhoneMail system you can evaluate statistically the subscriber inactivity using this layout file. With reference to a permanent date all subscribers are put out in chronological order who have not accessed their PhoneMail system from this date. In this way you can check, for example, which subscribers have a licensed mailbox but have not used it since a specific time anymore.

27.9.3.5 Subscriber Activity: Billing Information

The file is called **ADOBillingInformation.rpt** for using Crystal Reports and **BillingInformation.rptdesign** for BIRT.

The Billing Information Report provides itemized billing information of the PhoneMail usage for certain subscribers. It is based on the price per unit or the billing constant selected by the system administrator. You may create reports for one subscriber, all subscribers or a group of subscribers.

You will find the parameters of the billing information report on the register card parameters of the user interface of the Report APL. Here, the system administrator may set and modify these parameters with the help of an editor.

The report is based on the following databases:

- [Section 27.12.3, “Telematic – Call”](#)
- [Section 27.12.4, “Telematic – Message”](#)

The meaning of the columns in the call charge reports is as follows:

Column	Description
Connect Time Into PhoneMail – Price per Unit	The calculated amount for each minute the subscriber is connected to their mailbox.
Connect Time Into PhoneMail – Billing constant	The calculated billing constant for each subscriber independent from the time he is connected to his mailbox.
Connect Time Out of PhoneMail – Price per Unit	The calculated sum for each minute a subscriber is connected during an outbound call.
Connect Time Out of PhoneMail – Billing Constant	The billing constant for outgoing calls that has been set on the Parameters tab.
Messages Sent – Price per Unit	The price per unit for each subscriber message sent by PhoneMail.
Messages Sent – Billing Constant	The billing constant for each subscriber that has been set on the Parameters tab - independent from the sum of PhoneMail messages the subscriber has sent.
Message Length (min) – Price per Unit	The price per unit depends on the value that has been set on the Parameters tab and is charged per second referring to the length of the message.
Message Length (min) – Billing Constant	The billing constant for each subscriber that has been set on the Parameters tab independent on the sent message length.
Subscriber Total Price	The price per unit used by every subscriber.
Units	In this column the time is shown the user has been connected to PhoneMail. Syntax: <i>D - hh:mm:ss</i> (e.g. 0 - 03:00:00 means, the user has been connected 0 days and 3 hours to PhoneMail).

Column	Description
Subscriber Total Extended Price	Price for extended costs including the billing constant.

The billing information may be based on one or all of the following variables: connect time, number of sent messages (based on the number of entered destinations), message length and message retention. The price of each billing constant is calculated with the help of the following formula:

$$(\text{Price per Unit} \times \text{Units})$$

Extended prices can be calculated with the help of the following formula:

$$(\text{Price per Unit} \times \text{Units}) + \text{Billing Constant}$$

The network fields in the Billing Information Report are very useful to charge network messages.

27.9.3.6 Subscriber Activity: Outgoing Calls

The file is called **ADOOutcalling.rpt** for using Crystal Reports and **Outcalling.rptdesign** for BIRT.

The Outcalling Report about outbound calls shows the number of subscribers making outbound calls or calling a pager or a telephone. Moreover, it shows the time a subscriber takes for outbound calls during the reporting time interval.

The report is based on the following databases:

- [Section 27.12.3, “Telematic – Call”](#)

The meaning of the columns in the outgoing call reports is as follows:

Column	Description
Name	Name of subscriber making an outbound call.
Extension	Extension of subscriber making an outbound call.
Successful	Number of successful outbound calls to a pager or a telephone.
Unsuccessful	Number of unsuccessful calls to a pager or a telephone.
Connect time towards the	Sum of all outgoing connect times in seconds.
Average	Average length of all outgoing connect times in seconds.

27.9.4 System Security Reports

27.9.4.1 System Security: Invalid Access Attempts

The file is called **ADOInvalidAccessAttempts.rpt** for using Crystal Reports and **InvalidAccessAttempts.rptdesign** for BIRT.

An invalid access attempt occurs in case a wrong subscriber password has been entered. This information may be very useful for you. You may then ask the subscribers to take precautions (e.g. delete messages regularly to grant confidentiality of the mailboxes).

The report lists the extensions for which the number of successive invalid access attempts is equal or greater to the value entered in the property `Number of failed logins before mailbox locks`. The information in the column `Caller` depends on the location of the caller. If the caller and the destination are in the same telephone system, the extension of the caller is displayed in the report. If not, the message `Info. N/A` (information not available) is displayed. For multi-node systems the report always includes subscribers of the local node.

You may use the report to control unauthorized access attempts.

The report is based on the following databases:

- [Section 27.12.5, “Telematic – Invalid Access”](#)

The meaning of the columns in the invalid access attempt reports is as follows:

Column	Description
Name	Subscriber name.
CALLER	Extension of subscriber.
Failed Attempt Time	Date and time of day of failed attempt.
Caller	Extension of the caller who has entered the wrong password.

27.10 Basics on the Raw Data Database Tables

27.10.1 Short Introduction to the Databases used

Since the reporting mechanism is about processing database contents, we begin with a short introduction to the databases used. We do this also with reference to the replacement of **dBase databases** with **SQL databases** and the essential differences between these two database systems.

The database management system **dBase** is one of the first systems of its kind broadly used. Meanwhile, dBase has been replaced with SQL databases to a large extent. With XPR V6, a new installation of a reporting system using a dBase database is not possible anymore. Only an already established dBase database connection with the XPR system is supported.

dBase is not a pure relational database in terms of the definition according to Codd. An architecture with runtime interpreter is used, which executes requests to the database. Each dBase database has a data file with the extension **dbf**. Field definitions are permanent after their creation and cannot be modified anymore. Index and memo fields to support the dBase databases are simple sequential files with fixed data length. Index files have the file extension **ndx**, **mdx**, **idx** or **cdx**. Memo files have the file extension **dbt**. New data records are simply attached to the file. All removed data records are physically deleted only by a specific command. A file thus contains a table.

SQL databases, in contrast, are relational database systems that may have several tables in a file. The tables are related to each other via the unique key fields. Field definitions may be modified.

Accessing the contents of databases requires so-called database interfaces. To connect a dBase database to the Report APL the **CodeBase** database interface is used, while in case of SQL databases the **ADO** interface is used.

NOTE:

The Microsoft **SQL Server Desktop Engine (MSDE)** for short), which represented a free option to use an SQL server for simple applications, has been replaced by Microsoft with the also free-of-charge **Microsoft SQL Server 2005 Express Edition**. Like *MSDE*, the *Microsoft SQL Server 2005 Express Edition* is a slim version of the *Microsoft SQL server*. With the SQL Server 2005 Express Edition technical options have been increased against MSDE and an administrator tool with graphic user interface (*SQL Server 2005 Management Studio Express Edition*) provided.

Owing to the replacement of MSDE with the SQL Server 2005 Express Edition, MSDE will not be supported on the XPR system any more and the associated setup files no longer supplied. For distribution reasons, the setup files of the SQL Server 2005 Express Edition cannot be included in the delivery, but you can download a version from the Microsoft homepage. The installation respectively

an upgrade of MSDE to the SQL Server 2005 Express Edition is described in the *OpenScape Xpressions V7* Server Installation manual. Switching from MSDE to the SQL Server 2005 Express Edition does not result in any modifications when using the Report and the Report Schedule APL. When registering a database with the Report APL you merely need to note that, contrary to the MSDE installation, no default user and no corresponding default database is automatically provided. After you have installed the SQL Server 2005 Express Edition you need to create an individual user with associated database yourself.

27.10.1.1 CodeBase

Compressed Database Tables

CodeBase enables using compressed database tables.

NOTE:

If the ADO option is used, compressed database tables will not be supported.

In the compressed tables raw data are summed up. A compressed table includes a key value for each data record, normally a label (e.g. agent name) and an arbitrary number of numerical values (e.g. call duration) that can be calculated from the raw data by mathematical operations (sum or average).

Each of these data records contains a time range. Start and end time are also contained in the data record (e.g. 1 hour) but no single events. For each different key value coming up in the time range within the raw data its own data record is created in the compressed tables. In other words, only those raw data are included where the key value of the compressed table matches raw data entries. The key value as well as the numerical data can derive from any basis tables, if corresponding relational links are defined and possible.

The basis table the compressed table is derived from is always the basis for the time range. Within this time range the time range for the compressed tables can be selected freely, but should be selected consistently.

A compressed table allows a statistical statement concerning the key value and is therefore called view in the following sections. It is possible to derive as many compressed tables as desired from each basis table in order to enable different views to the raw data.

For each compressed table as many condensed tables as required may be defined. These tables do not change the data structure but condense the compressed database tables into increasingly wider time ranges.

CodeBase and SQL Usage Restriction

If **CodeBase** is used as database for the Report APL, complications may arise owing to combinations of data amount (larger than 500MB), actual data-transfer rate, operating system, service packs and further installed software. One type of error message to indicate this problem may be:

```
CDataBaseTable::Open: could not open or create database  
<[database name]>, CodeBase error <[error number]>.
```

The approach to the solution to be used should be selected according to the current or expected data volume:

- Using the **Microsoft SQL Server 2005 Express Edition**

The *Microsoft SQL Server 2005 Express Edition* is a restricted version of the Microsoft SQL server and replaces the previously used *Microsoft SQL Server Desktop Engine (MSDE)*. MSDE is not supported by the XPR system any more, should therefore not be used any more and be replaced with, for example, the SQL Server 2005 Express Edition. The SQL Server 2005 Express Edition may in the XPR context handle databases of a size up to 4GB. You find more information about the functionality and installation on the Microsoft product homepage and in the *Server Installation* manual.

- Using an **SQL server**

If the data amount exceeds 4GB, using a Microsoft SQL server is an option. This is only realized in the scope of a project including the Professional Services Organization. Over the course of the project the data amount is to be estimated and a corresponding scenario designed. For further information please refer to the *Server Administration* manual.

For information about the configuration of an SQL database and Report APL connection please read [Section 27.4, "Report APL Configuration"](#).

27.10.1.2 ADO

ADO (ActiveX Data Objects) is based on ActiveX and is a further development of DAO (Data Access Objects). Besides databases ADO can also access tabular data sources such as Excel documents. In addition to setting up the connection to the database, objects for returning the data records and to execute commands are created. The database access requires an OLE DB provider. This provider enables the definition of the database and of the corresponding version.

Using compressed tables under CodeBase is inflexible and an effort. By means of SQL Queries under ADO, specific data amounts can be simply stored. Such queries can be easily adjusted and modified, but require sound knowledge of the available database tables.

27.10.2 Database Tables

All tables are provided with a global time range. Data records that are not within this time range are automatically deleted. For the PhoneMail and VMS Telephone User Interfaces so-called **Telephone User Interface databases** exist, which provide raw data for processing in reports.

The basis tables contain the unfiltered and unedited event information (raw data) as they are available in the event files. A separate table is generated for every combination of class and subclass. These tables are not created daily in contrast to the event files, but include the raw data from the global time range. Especially the first column of the table is always the time stamp as it is included in the raw data.

27.10.3 dBase and ADO Database Structure

As a matter of rule, the `adodb.ini` used in case of ADO uses the same syntax and structure as the `db.ini` CodeBase. Both files that serve as structural base for the databases are found in the `<XPR Install>\res\RepAp1` directory.

Please note the following restrictions:

- The maximum length of a column label within a database table is 10 characters.
- In case of Codebase, the database name is the physical file name of the DBase file, with ADO it is the name of the table within the SQL database. This name must be unique.

The modifications to the options in the files `adodb.ini` or `db.ini` can be used for configuring the storage of statistical raw data in the database tables.

TimeStamp

Because of the creation via the XMR service the time stamp is always generated. It must always be the first field in each basis table and each compressed table definition (e.g. 'F01_FI=TSTAMP,C,19,0,1').

Each entry of this file must meet the following rules:

- `<Key> ::= 0|...|9|a|...|z|_` i.e. all digits and letters are possible in lower and upper case. Umlauts and special characters apart from the underscore are not allowed.
- `<KeyValue> ::= <Key>{,<Key>}`
- `<KeyName> ::= a|...|z`
- `<IniEntry> ::= <KeyName>=<KeyValue>`

The following key values must be unique:

- Classes
- Subclasses within a class
- Database names

Each combination of class and the corresponding subclass defines a database basis table and - if defined so - a set of compressed tables. The order of the entries is extremely important.

General structure of statistics databases

Under the [Common] entry, general information is declared. The entry `StartOfWeek` sets the day used as starting day of a week. Value 0 describes Sunday. The weekdays are then consecutively numbered, so that Saturday results in value 6. Monday is defined as start of the week (`StartOfWeek=1`) by default.

Hierarchic database structure

The database features a hierarchic structure. The highest hierarchic level are classes, which may have subclasses. Class and subclass names must be the same as in the protocol files.

Classes are specified in the [Classes] area with the class name. The syntax reads as follows:

```
Classes]
Classes=MTA,<further class names>
```

In the classes the corresponding subclasses are thereupon defined:

```
[MTA]
SubClasses=Accounting,<further subclass names of class 'MTA'>
[<further class names>]
SubClasses=<subclass names>
```

etc.

Database basis class definitions

This section describes the physical structure of the basis table for the subclass "Accounting" of class "MTA". In the [*subclass name*] section the file name of the database table is specified without the *dbf* file extension using the *DbName* variable.

Subsequently, the *Range=<unit, number>* variable defines the time range of the database table, i.e. the maximum time range that a database table may contain. The unit parameter may assume values from 0 to 6 (0=second, 1=minute, 2=hour, 3=day, 4=week, 5=month, 6=year). The number parameter may contain a value of any quantity but should be set with care, since in case of the unit year and a high value for number the data in the time range of the corresponding number of years are stored in a table. This may lead to an unmanageable amount of data in a table. The example *Range=6,1* defines that in the table the data are stored in the time range of one year.

Furthermore, the table contains symbolic field names for the basis table, via which later access is referenced. Declaration of a field name has the following structure: <FieldName>_FI=Name, type, width, decimals, zeros. Name describes here the column name in the database table. Type defines the data type of the field: for example C represents a sequence of characters and N represents a number. Width describes the permissible number of characters respectively digits. Specifying decimals is only possible in case of digits and indicates the possible number of floating points. The zeros parameter sets in case of value 1 the field content to zero, if the field is empty. In the shown example the fields F01 to F10 are defined:

```
[MTA_Accounting]
DbName=GEB
Range=6,1
F01_FI=TSTAMP,C,19,0,1
F02_FI=G_ORIGIN,C,64,0,1
F03_FI=RECIPIENT,C,64,0,1
F04_FI=COSTOWNER,C,64,0,1
F05_FI=COST,N,10,2,1
F06_FI=GEBEH,N,10,0,1
F07_FI=TIME,C,19,0,1
F08_FI=DURATION,N,10,0,1
F09_FI=STATE,N,10,0,1
F10_FI=GMID,N,10,0,1
```

Using the <field name>_T=conversion type, key name command you can specify the conversion type and the key name for a database field. If the first field contains the time stamp (F01_FI=TSTAMP), it must not have a key name. The conversion type may have the values 0=char[], 1=Long and 2=Double. Key names must be specified like in the protocol file.

```
F01_T=0,
F02_T=0,Originator
F03_T=0,Recipient
F04_T=0,CostOwner
F05_T=2,Cost
F06_T=1,Units
F07_T=0,Time
F08_T=1,Duration
F09_T=1,State
F10_T=1,Mid
```

Symbolic index names can be defined in the database table with the command <index name>_TI=name, expression, filter, unique, sort in descending order. Via these names index accesses can later be referenced. The name specifies the index description. The expression determines the corresponding database field. The parameters filter, unique and sort in descending order are not required.

```
T01_TI=_TSTAMP,TSTAMP,0,0,0
T02_TI=_GORIGIN,G_ORIGIN,0,0,0
T03_TI=_RECIPIENT,RECIPIENT,0,0,0
T04_TI=_COSTOWNER,COSTOWNER,0,0,0
T05_TI=_TIME,TIME,0,0,0
T06_TI=_GMID,GMID,0,0,0
```

Definition of the compressed tables

The following section defines the properties of one or several database tables, which contain the compressed information of the basis table.

NOTE:

Compressed tables are only possible with CodeBase and not with ADO!

This paragraph and the following ones define one or several physical database tables, which include the compressed information of the corresponding basis table.

The names of the compressed tables are composed as follows:

```
<Basis table-file name><View number>_<Compressed table
number>
```

The view number starts with 1. The numbering follows the order given in the `CompressedViews` variable. The variable still determines the symbolic names of the compressed views.

```
CompressedViews=V01,V02
```

The values `V01` and `V02` thus specify names for compressed views.

The compressed-table number starts with 0. The numbering follows the order given in `ViewSymbol` (cf. "`VxxTables=`" entries).

Each compressed view is furnished with the parameters `process type` and `basis key origin`: `<compressed view>=process type, basis key origin`.

The `process type` has value 1 to activate the special status handling, i.e. the time the basis key has spent in each status is calculated. To disable this status handling, the parameter has value 0.

The parameter `basis key origin` has value 1, if a basis table different from the direct one is to be used as key. If the direct basis table is used as key, the parameter has value 0.

```
V01=1,0
```

```
V02=0,0
```

If the `process type` is set to value 1, the variables `<compressed view>_BFields` and `<compressed view>_BTags` must be set. The variable mentioned first specifies which field combination describes a unique status. The second variable indicates which index field combination describes a unique status.

```
V01_BFields=V01CF01,V01CF03,V01CF04
```

```
V01_BTags=V01CT01,V01CT03
```

The `CompressedRanges` variable defines the time ranges for compressed tables. The specified values must be determined according to the following structure: `<time range name>=total unit, total number, t-raster unit, t-raster number`. All parameters may possess values from 1 to 6 (0=second, 1=minute, 2=hour, 3=day, 4=week, 5=month, 6=year).

Each of the following compressed tables must at least include the time range of its predecessor. Several t-rasters must fit completely in the t-raster of the successor, otherwise the information of the successor is not correct.

The first example below includes a month divided into hours, the second one includes a year, divided into months.

```
CompressedRanges=C01,C02
```

```
C01=5,1,2,1
```

```
C02=6,1,5,1
```

Definition of the single views of a compressed table

The symbolic name for the compressed tables is defined with the variable `<compressed view>Tables`. The listed tables share the same fields and indices.

```
V01Tables=V01C01
```

The `<compressed views>Fields` variable determines the field names of the compressed table.

```
V01Fields=V01CF01,V01CF02,V01CF03,V01CF04,V01CF05
```

With the command `<view name>_FI=name, type, width, decimals, zeros` field information is assigned to the field names of the compressed table. `Name` describes the column name in the table, `type` the data type, `width` the maximum permissible number of characters and `decimals` the possible decimal places of a number. The `zeros` parameter determines in case of value 1 that the field is allocated with value zero if the field is empty. The start of the time range (`TBEGIN`) must be the first, the end (`TEND`) the second and the index field the third field by definition.

```
V01CF01_FI=TBEGIN,C,19,0,1
```

```
V01CF02_FI=TEND,C,19,0,1
```

```
V01CF03_FI=COSTOWNER,C,64,0,1
```

```
V01CF04_FI=STATE,C,16,0,1
```

```
V01CF05_FI=TIME,N,16,0,1
```

Properties of the compressed table

With the following command you assign properties to the fields of the compressed table:

<View name>_T=Source, Operation, Operation type, Count value, Class, Subclass, Relation key, Relation tag, Value field, Condition field, Condition operator, Condition value, Condition class, Condition subclass, Condition key, Condition relation tag, Condition field

Property	Description
Source	Specifies the original field in the basis table
Operation	The value selected here is used to determine how the values of the basis table field are processed, thus compressed: 0 - Time stamp, 1 - Key value , 2 - Average, 3 - Sum, 4 - Minimum, 5 - Maximum, 6 - Amount, 7 - Time difference, 8 - Count value, 9 - Last value, 10 - First value
Operation type	0 = char[], 1 = long, 2 = double
Count value	If Operation is set to value 8, the value to be counted is specified here.
Class, Subclass, Relation class, Relation key, Relation tag, Value field:	Via these properties, values <i>Value field</i>) can be copied from another basis table. To this, the <i>Relation key</i> of this table must match the <i>Relation tag</i> of the basis table for the <i>Subclass</i> of the <i>Class</i> .
Condition field, Condition operator, Condition value, Condition class, Condition subclass, Condition key, Condition relation tag, Condition field	With the help of these properties a condition may be raised that defines which values of the basis table flow into this field. <i>Condition field</i> refers to the associated basis table, the <i>Condition operator</i> may be '<', '>', '==', '<=', '>=' or '!='. Either the <i>Condition value</i> is used for comparison or, in case of an empty <i>Condition value</i> , another basis table is referenced (cf. <i>Relation class</i>).

Symbolic index names and their parameters for compressed tables

Indices for compressed tables are set with the variable <compressed view>Tags=<index name_1>, <index name_2>, ..., <index name_n>.

```
V01Tags=V01CT01,V01CT02,V01CT03
```

The parameters for each index name are defined with the assignment index name>_TI=name, expression, filter, unique, sort in descending order like before for the basis table.

```
V01CT01_TI=_TBEGIN,TBEGIN,0,0,0
```

```
V01CT02_TI=_TEND,TEND,0,0,0
```

```
V01CT03_TI=_COSTOWNER,COSTOWNER,0,0,0
```

Each further compressed view is defined analog to the depicted procedure.

Setting for storing statistical raw data of the VOGUE script: IVR data retention

This section refers to the configuration for storing data in the tables of the **IVR Application**. Since the tables of the **IVR Box** depend on IVR Application and cannot exist by themselves, the configuration also contains the tables of the **IVR Box**.

With the **IVR data retention** option you define how long the data is stored in the database tables. The command is entered in the format:

RANGE=*unit, number*

The unit specification defines what the number refers to. Unit may have the values 0 (seconds), 1 (minutes), 2 (hours), 3 (days), 4 (weeks), 5 (months) and 6 (years). The **RANGE=5, 6** example thus specifies that the data is stored in the database tables six months. If no specification is made, the data is stored one year.

27.11 Database Tables: CTI Entries

In the following section the following three database entries and their fields are explained:

- CtiCall
- CtiDevEvent
- CtiEvent

Only the fields of these entries are the fields that provide the same information also in different, known environment scenarios, with this information being used for statistics in case of the corresponding correlation. All fields of other CTI entries are not listed, since they may provide different information depending on the scenario. For creating reports we expressly recommend the exclusive use of the fields listed here.

27.11.1 CtiCall

The fields of this entry describe the entire statistical properties of a single call in a connection. The data are saved after the call has been finished to receive all values completely.

Field	Data type	Length/ Values	Description
TSTAMP	Datetime	64	Date and time in the format 'YYYY-MM-DD hh:mm:ss'.
ID	Integer	32	The value describes the unique ID for identifying the call destination.
link	Character	31	Logical name of the CTI connection.
Uid	Integer	32	This call ID is maintained in case of a call rerouting or call forwarding, so that the call flow can be traced.
DEVICE	Character	32	The phone assigned to the call. Specified in the format of a normalized phone number.
COMPTIME	Integer	32	The complete duration of the call in seconds.
RINGTIME	Integer	32	Duration in seconds in which the call was in state <code>ALERTING</code> or <code>DIALING/RINGING</code> . If the call was in these states several times, the times are added.
CONNTIME	Integer	32	Duration in seconds in which the call was connected and not in conference or held. Several connection times are added.
HOLDTIME	Integer	32	Duration in seconds in which the call was held or in state <code>HOLD</code> . If the call was in these states several times, the times are added.

Field	Data type	Length/ Values	Description
CONFTIME	Integer	32	Duration in seconds in which the call was in conference. Several conference times are added.
BUSYTIME	Integer	32	Duration in seconds in which the call was in state <code>BUSY</code> . If the call was in this state several times, the times are added.
STATE	Character	CONN/ TRY	If the call was connected, the field receives value <code>CONN</code> . If only a connecting attempt was performed, value <code>TRY</code> is entered.
DIR	Character	IN/ OUT	The value describes the call direction: <code>IN</code> for incoming calls, <code>OUT</code> for outgoing calls.
CALLER	Character	32	Caller ID in the format of the caller's normalized phone number.
CALLEE	Character	32	Callee ID in the format of the callee's normalized phone number.
REDIR	Character	32	ID of the subscriber who forwards the call in the format of the subscriber's normalized phone number.
CONF	Enum	+4924, +4925, etc.	Contains a list of the participants in a conference in the format of the participants' normalized phone number. In case of two conference sessions the participants in both sessions are listed.
CNTCONSULT	Integer	32	A counter that counts all consultation calls made during the call.
LISTCONSULT	Enum	ID1, ID2, etc.	A list that indicates all IDs of the consultation calls made during the call.

27.11.2 CtiDevEvent

This entry stores information about the events of a phone. An event is defined as a change from the inactive to the active state of the device and analog from the active to the inactive state.

Field	Data type	Length/ Values	Description
TSTAMP	Datetime	64	Date and time in the format 'YYYY-MM-DD hh:mm:ss'.
DEVICE	Character	32	The phone assigned to the call. Specified in the format of a normalized phone number.
link	Character	31	Logical name of the CTI connection.

Field	Data type	Length/ Values	Description
STATE	Character	ALIVE /DEAD	The field describes the call state and may possess the following values: - with value <code>ALIVE</code> the phone has switched to the active state from state <code>DEAD</code>. - with value <code>DEAD</code> the phone has switched from the active state to the inactive state.
LASTEVENT	Datetime	64	Specification of date and time at which the last event was reported. If the created entry <code>CtiDevEvent</code> describes the first event, this field is empty.

27.11.3 CtiEvent

This entry is created each time the call state changes.

Field	Data type	Length/ Values	Description
TSTAMP	Datetime	64	Date and time in the format 'YYYY-MM-DD hh:mm:ss'.
ID	Integer	32	The value describes the unique ID for identifying the call destination.
link	Character	31	Logical name of the CTI connection.
Uid	Integer	32	This call ID is maintained in case of a call rerouting or call forwarding, so that the call flow can be traced.
DEVICE	Character	32	The phone assigned to the call. Specified in the format of a normalized phone number.

Field	Data type	Length/ Values	Description
STATE	Character	see right column	The field describes the call state and may possess the following values: • DIALING: the receiver has been picked up and a number is about to be dialed. The phone of the dialed number rings (outgoing calls only). • RINGING: the receiver has been picked up and a number was dialed (outgoing calls only). • ALERTING: a phone rings (incoming calls only). • CONNECTED: a phone has an active connection (incoming and outgoing calls). • HELD: the call has been held (incoming and outgoing calls). • HOLD: the call is held active (incoming and outgoing calls). • CONFERENCED: the call is in conference with more than two subscribers (incoming and outgoing calls). • BUSY: the called number is either busy or a previously active call was finished (incoming and outgoing calls). • IDLE: the call was finished and the line cleared (incoming and outgoing calls).
DIR	Character	IN/ OUT	The value describes the call direction: IN for incoming calls, OUT for outgoing calls.
CALLER	Character	32	Caller ID in the format of the caller's normalized phone number.
CALLEE	Character	32	Callee ID in the format of the callee's normalized phone number.
REDIR	Character	32	ID of the subscriber who forwards the call in the format of the subscriber's normalized phone number.

27.12 Database Tables of the Telephone User Interfaces (TUI)

NOTE:

The compressed views are only possible in case of the CodeBase database type and are not supported by ADO.

The following databases include the information required for the creation of **Telephone User Interface (= TUI)** reports. The raw data that is processed in the databases is delivered by the Telematic APLs. You find the corresponding files of the databases in the `<XPR install>\res\RepAp1` directory.

Here as well different compressed views for the basic tables are presented. The calculation of the fields of the compressed tables correspond to the source fields in the basic tables.

NOTE:

The listed fields are the fields that provide the same information also in different, known environment scenarios, with this information being used for statistics in case of the corresponding correlation. All fields not listed may provide different information depending on the scenario. For creating reports we expressly recommend the exclusive use of the listed fields.

27.12.1 Telematic – Call Processing Call

From XPR V4.0 this database will not be filled with data any more.

Field	Data type	Width	Description
TSTAMP	Character	19	Timestamp
PROT	Character	64	Protocol name
SOURCE	Character	64	Source
SCRIPTID	Character	10	Script ID
NUMSUB	Number	10	Number of subscribers
SUCCESS	Character	16	Success
TYPE	Character	4	Type (possible values: "CP" for Call Processing, "VOICE" for voice messages)

1st compressed view

Field	Data type	Width	Description
TBEGIN	Character	19	Start time
TEND	Character	19	End time

Field	Data type	Width	Description	
ALL	Character	8	Static text <ALL>	
C_CPOK	Number	8	Based on:	TYPE
			Calculation:	Sum
			Condition:	SUCCESS = COMPLETED
			Condition:	TYPE==CP
C_CPFAIL	Number	8	Based on:	TYPE
			Calculation:	Sum
			Condition:	SUCCESS = BLOCKED
			Condition:	TYPE==CP
C_VOK	Number	8	Based on:	TYPE
			Calculation:	Sum
			Condition:	SUCCESS = COMPLETED
			Condition:	TYPE==VOICE
C_VFAIL	Number	8	Based on:	TYPE
			Calculation:	Sum
			Condition:	SUCCESS = BLOCKED
			Condition:	TYPE==VOICE

27.12.2 Telematic – Physical Lines

This database is needed for the creation of the following reports:

- [Section 27.9.2.3, “Systemwide Activity: Board Load”](#)

Field	Data type	Width	Description
TSTAMP	Character	19	Timestamp
System	Character	2	System
MODE	Character	1	Mode
BOARD	Character	2	Board
CHANNEL	Character	2	Channel
USED	Number	2	Used?
TOTAL	Number	2	Total
BOARDID	Character	5	Board ID
STATUS	Character	4	Status

1st compressed view

Field	Data type	Width	Description
TBEGIN	Character	19	Start time
TEND	Character	19	End time
BRCHANNEL	Character	4	Copy of the key value in the source field BOARD and CHANNEL
STATUS	Character	4	Copy of the source field STATUS (time of the status change)
Time	Number	10	Duration between a STATUS change

2nd compressed view

Field	Data type	Width	Description
TBEGIN	Character	19	Start time
TEND	Character	19	End time
BRCHANNEL	Character	4	Copy of the source fields BOARD and CHANNEL
BOARD	Character	2	Copy of the first value in the source field NODETYPE
TOTAL	Number	2	Copy of the first value in the source field TOTAL
TIMEALLBUS	Number	10	Count in USED how often each value from TOTAL occurs
TEXTTIME	Character	19	Last value of the STATUS that does not correspond to FREE

27.12.3 Telematic – Call

This database is needed for the creation of the following reports:

- [Section 27.9.2.1, “Systemwide Activity: Call Activity”](#)
- [Section 27.9.2.2, “Systemwide Activity: Call Length”](#)
- [Section 27.9.3.3, “Subscriber Activity: Subscriber Access Activity”](#)
- [Section 27.9.3.6, “Subscriber Activity: Outgoing Calls”](#)
- [Section 27.9.3.5, “Subscriber Activity: Billing Information”](#)

Field	Data type	Width	Description
TSTAMP	Character	19	Timestamp
PROT	Character	64	Protocol name
SOURCE	Character	64	Source
SCRIPTID	Character	10	Script ID
NUMSUB	Number	10	Number of subscribers
SUBSCRIB	Character	64	Subscriber
EXTENSION	Character	64	Extension
USERID	Character	64	User ID
CALLER	Character	64	Caller
AMODE	Character	64	Access mode
DURATION	Number	32	The duration of the call.
SUCCESS	Character	64	Success

Table 59 Telematic – Call

1st compressed view

Field	Data type	Width	Description
TBEGIN	Character	19	Start time
TEND	Character	19	End time
ALL	Character	8	Static text <ALL>
C_DIRECT	Number	8	Based on: AMODE
			Calculation: Count
			Condition: AMODE==DIRECT
C_DIRECT3	Number	8	Based on: AMODE
			Calculation: Count
			Condition: DURATION <= 30
			Condition: AMODE==DIRECT

Field	Data type	Width	Description	
C_DIRECT6	Number	8	Based on:	AMODE
			Calculation:	Count
			Condition:	DURATION <= 60
			Condition:	AMODE==DIRECT
C_DIRECT9	Number	8	Based on:	AMODE
			Calculation:	Count
			Condition:	DURATION <= 90
			Condition:	AMODE==DIRECT
C_DIRECT12	Number	8	Based on:	AMODE
			Calculation:	Count
			Condition:	DURATION <= 120
			Condition:	AMODE==DIRECT
C_DIRECT24	Number	8	Based on:	AMODE
			Calculation:	Count
			Condition:	DURATION <= 240
			Condition:	AMODE==DIRECT
C_FWD	Number	8	Based on:	AMODE
			Calculation:	Count
			Condition:	AMODE==FORWARD
C_FWD3	Number	8	Based on:	AMODE
			Calculation:	Count
			Condition:	DURATION <= 30
			Condition:	AMODE==FORWARD
C_FWD6	Number	8	Based on:	AMODE
			Calculation:	Count
			Condition:	DURATION <= 60
			Condition:	AMODE==FORWARD
C_FWD9	Number	8	Based on:	AMODE
			Calculation:	Count
			Condition:	DURATION <= 90
			Condition:	AMODE==FORWARD
C_FWD12	Number	8	Based on:	AMODE
			Calculation:	Count
			Condition:	DURATION <= 120
			Condition:	AMODE==FORWARD

Field	Data type	Width	Description	
C_FWD24	Number	8	Based on:	AMODE
			Calculation:	Count
			Condition:	DURATION <= 240
			Condition:	AMODE==FORWARD
C_OUT	Number	8	Based on:	AMODE
			Calculation:	Count
			Condition:	AMODE==OUTCALL
C_OUT3	Number	8	Based on:	AMODE
			Calculation:	Count
			Condition:	DURATION <= 30
			Condition:	AMODE==OUTCALL
C_OUT6	Number	8	Based on:	AMODE
			Calculation:	Count
			Condition:	DURATION <= 60
			Condition:	AMODE==OUTCALL
C_OUT9	Number	8	Based on:	AMODE
			Calculation:	Count
			Condition:	DURATION <= 90
			Condition:	AMODE==OUTCALL
C_OUT12	Number	8	Based on:	AMODE
			Calculation:	Count
			Condition:	DURATION <= 120
			Condition:	AMODE==OUTCALL
C_OUT24	Number	8	Based on:	AMODE
			Calculation:	Count
			Condition:	DURATION <= 240
			Condition:	AMODE==OUTCALL
C_GUEST	Number	8	Based on:	AMODE
			Calculation:	Count
			Condition:	AMODE==GUEST
C_GUEST3	Number	8	Based on:	AMODE
			Calculation:	Count
			Condition:	DURATION <= 30
			Condition:	AMODE==GUEST
C_GUEST6	Number	8	Based on:	AMODE
			Calculation:	Count
			Condition:	DURATION <= 60
			Condition:	AMODE==GUEST

Field	Data type	Width	Description	
C_GUEST9	Number	8	Based on:	AMODE
			Calculation:	Count
			Condition:	DURATION <= 90
			Condition:	AMODE==GUEST
C_GUEST12	Number	8	Based on:	AMODE
			Calculation:	Count
			Condition:	DURATION <= 120
			Condition:	AMODE==GUEST
C_GUEST24	Number	8	Based on:	AMODE
			Calculation:	Count
			Condition:	DURATION <= 240
			Condition:	AMODE==GUEST
C_CBACK	Number	8	Based on:	AMODE
			Calculation:	Count
			Condition:	AMODE==CALLBACK
C_CBACK3	Number	8	Based on:	AMODE
			Calculation:	Count
			Condition:	DURATION <= 30
			Condition:	AMODE==CALLBACK
C_CBACK6	Number	8	Based on:	AMODE
			Calculation:	Count
			Condition:	DURATION <= 60
			Condition:	AMODE==CALLBACK
C_CBACK9	Number	8	Based on:	AMODE
			Calculation:	Count
			Condition:	DURATION <= 90
			Condition:	AMODE==CALLBACK
C_CBACK12	Number	8	Based on:	AMODE
			Calculation:	Count
			Condition:	DURATION <= 120
			Condition:	AMODE==CALLBACK
C_CBACK24	Number	8	Based on:	AMODE
			Calculation:	Count
			Condition:	DURATION <= 240
			Condition:	AMODE==CALLBACK
C_TRANS	Number	8	Based on:	AMODE
			Calculation:	Count
			Condition:	AMODE==TRANS

Field	Data type	Width	Description	
C_TRANS3	Number	8	Based on:	AMODE
			Calculation:	Count
			Condition:	DURATION <= 30
			Condition:	AMODE==TRANS
C_TRANS6	Number	8	Based on:	AMODE
			Calculation:	Count
			Condition:	DURATION <= 60
			Condition:	AMODE==TRANS
C_TRANS9	Number	8	Based on:	AMODE
			Calculation:	Count
			Condition:	DURATION <= 90
			Condition:	AMODE==TRANS
C_TRANS12	Number	8	Based on:	AMODE
			Calculation:	Count
			Condition:	DURATION <= 120
			Condition:	AMODE==TRANS
C_TRANS24	Number	8	Based on:	AMODE
			Calculation:	Count
			Condition:	DURATION <= 240
			Condition:	AMODE==TRANS
C_ALL	Number	8	Based on:	AMODE
			Calculation:	Count
C_ALL3	Number	8	Based on:	AMODE
			Calculation:	Count
			Condition:	DURATION <= 30
C_ALL6	Number	8	Based on:	AMODE
			Calculation:	Count
			Condition:	DURATION <= 60
C_ALL9	Number	8	Based on:	AMODE
			Calculation:	Count
			Condition:	DURATION <= 90
C_ALL12	Number	8	Based on:	AMODE
			Calculation:	Count
			Condition:	DURATION <= 120
C_ALL24	Number	8	Based on:	AMODE
			Calculation:	Count
			Condition:	DURATION <= 240

Field	Data type	Width	Description	
A_SUBSC	Number	10	Based on:	NUMSUB
			Calculation:	Average
S_DURA	Number	10	Based on:	DURATION
			Calculation:	Sum

2nd compressed view

Field	Data type	Width	Description	
TBEGIN	Character	19	Start time	
TEND	Character	19	End time	
SUBSCRIB	Character	32	Based on:	SUBSCRIB
			Calculation:	<i>Key value</i>
EXTENSION	Character	32	Based on:	EXTENSION
			Copy last value of source field EXTENSION corresponding to subscriber name	
LASTACCESS	Character	32	Based on:	TSTAMP
			Copy last value of source field TSTAMP corresponding to subscriber name	
C_DIRECT	Number	8	Based on:	AMODE
			Calculation:	Count
			Relation:	AMODE==DIRECT
S_DIRECT	Number	8	Based on:	DURATION
			Calculation:	Sum
			Condition:	AMODE==DIRECT
C_OUTOK	Number	8	Based on:	AMODE
			Calculation:	Count
			Condition:	SUCCESS = YES
			Condition:	AMODE==OUTCALL
C_OUTFAIL	Number	8	Based on:	AMODE
			Calculation:	Count
			Condition:	SUCCESS = NO
			Condition:	AMODE==OUTCALL
S_OUTCALL	Number	8	Based on:	DURATION
			Calculation:	Sum
			Condition:	AMODE==OUTCALL
C_OUTCALL	Number	8	Based on:	AMODE
			Calculation:	Count
			Condition:	AMODE==OUTCALL

Field	Data type	Width	Description	
A_OUTCALL	Number	8	Based on:	DURATION
			Calculation:	Average
			Condition:	AMODE==OUTCALL
A_SUBSC	Number	8	Based on:	NUMSUB
			Calculation:	Average
S_DURA	Number	8	Based on:	DURATION
			Calculation:	Sum
S_FWD	Number	8	Based on:	DURATION
			Calculation:	Sum
			Condition:	AMODE==FORWARD
S_GUEST	Number	8	Based on:	DURATION
			Calculation:	Sum
			Condition:	AMODE==GUEST
S_CALLB	Number	8	Based on:	DURATION
			Calculation:	Sum
			Condition:	AMODE==CALLBACK
C_ALL	Number	8	Based on:	AMODE
			Calculation:	Count
C_FWD	Number	8	Based on:	AMODE
			Calculation:	Count
			Condition:	AMODE==FORWARD
C_GUEST	Number	8	Based on:	AMODE
			Calculation:	Count
			Condition:	AMODE==GUEST
C_CALLB	Number	8	Based on:	AMODE
			Calculation:	Count
			Condition:	AMODE==CALLBACK
LASTDIRECT	Character	32	Copy last value of source field TSTAMP corresponding to subscriber name	
			Condition:	AMODE==CALLBACK

27.12.4 Telematic – Message

This database is needed for the creation of the following reports:

- [Section 27.9.3.1, “Subscriber Activity: Subscriber Message Activity”](#)
- [Section 27.9.3.5, “Subscriber Activity: Billing Information”](#)

Field	Data type	Width	Description
TSTAMP	Character	19	Timestamp
PROT	Character	64	Protocol name
SOURCE	Character	64	Source
SCRIPTID	Character	10	Script ID
NUMSUB	Number	10	Number of subscribers
SUBSCRIB	Character	64	Subscriber
EXTENSION	Character	64	Extension
USERID	Character	64	User ID
SCOPE	Character	64	Scope name
MSGLEN	Number	32	Message length

1st compressed view

Field	Data type	Width	Description
TBEGIN	Character	19	Start time
TEND	Character	19	End time
SUBSCRIB	Character	32	Based on: SUBSRIB
			Calculation: <i>Key value</i>
C_LOCSENT	Number	8	Based on: SCOPE
			Calculation: Count
			Condition: SCOPE==LOCALSENT
C_LOCRCV	Number	8	Based on: SCOPE
			Calculation: Count
			Condition: SCOPE==LOCALRECEIVED
C_NETSENT	Number	8	Based on: SCOPE
			Calculation: Count
			Condition: SCOPE==NETSENT
C_NETRCV	Number	8	Based on: SCOPE
			Calculation: Count
			Condition: SCOPE==NETRECEIVED

Field	Data type	Width	Description	
S_LOCSENT	Number	8	Based on:	MSGLEN
			Calculation:	Sum
			Condition:	SCOPE==LOCALSENT
S_LOCRCV	Number	8	Based on:	MSGLEN
			Calculation:	Sum
			Condition:	SCOPE==LOCALRECEIVED
S_NETSENT	Number	8	Based on:	MSGLEN
			Calculation:	Sum
			Condition:	SCOPE==NETSENT
S_NETRCV	Number	8	Based on:	MSGLEN
			Calculation:	Sum
			Condition:	SCOPE==NETRECEIVED
A_SUBSC	Number	8	Based on:	NUMSUB
			Calculation:	Average
C_ALL	Number	10	Based on:	MSGLEN
			Calculation:	Count
S_MSGLEN	Number	10	Based on:	MSGLEN
			Calculation:	Sum

27.12.5 Telematic – Invalid Access

This database is needed for the creation of the following reports:

- [Section 27.9.4.1, “System Security: Invalid Access Attempts”](#)

Field	Data type	Width	Description
TSTAMP	Character	19	Timestamp
PROT	Character	64	Protocol name
SOURCE	Character	64	SOURCE
SCRIPTID	Character	10	Script ID
NUMSUB	Number	10	Number of subscribers
SUBSCRIB	Character	64	Subscriber
EXTENSION	Character	64	Extension
USERID	Character	64	User ID
CALLER	Character	64	Caller

27.12.6 Telematic – Event

This database is needed for the creation of the following reports:

- [Section 27.9.3.5, “Subscriber Activity: Billing Information”](#)

Field	Data type	Width	Description
TSTAMP	Character	19	Timestamp
PROT	Character	64	Protocol name
SOURCE	Character	64	Source
SCRIPTID	Character	10	Script ID
NUMSUB	Number	10	Number of subscribers
C_IN_M	Number	4	Connect time (Login) with price
C_IN_C	Number	4	Connect time (Login) with constant billing
C_OUT_M	Number	4	Disconnect time (Logout) with price
C_OUT_C	Number	4	Disconnect time (Logout) with constant billing
M_MIN	Number	4	Message length with price
M_MIN_C	Number	4	Message length sent with constant billing
M_SNT	Number	4	Message sent with price
M_SNT_C	Number	4	Message sent with constant billing

1st compressed view

Field	Data type	Width	Description
TBEGIN	Character	19	Start time
TEND	Character	19	End time
ALL	Character	8	Static text <ALL>
CNTEVT	Number	8	Based on: TSTAMP
			Calculation: Count
A_SUBSC	Number	10	Based on: NUMSUB
			Calculation: Average
A_C_IN_M	Number	6	Based on: C_IN_M
			Calculation: Average
A_C_IN_C	Number	6	Based on: C_IN_C
			Calculation: Average
A_C_OUT_M	Number	6	Based on: C_OUT_M
			Calculation: Average
A_C_OUT_C	Number	6	Based on: C_OUT_C
			Calculation: Average
A_M_MIN	Number	6	Based on: M_MIN
			Calculation: Average

Report APL and Report Schedule APL

Field	Data type	Width	Description	
A_M_MIN_C	Number	6	Based on:	M_MIN_C
			Calculation:	Average
A_M_SNT	Number	6	Based on:	M_SNT
			Calculation:	Average
A_M_SNT_C	Number	6	Based on:	M_SNT_C
			Calculation:	Average

27.12.7 Telematic – Path Activity

From XPR V4.0 this database will not be filled with data any more.

Field	Data type	Width	Description
TSTAMP	Character	19	Timestamp
PROT	Character	64	Protocol name
SOURCE	Character	64	Source
SCRIPTID	Character	10	Script ID
NUMSUB	Number	10	Number of subscribers
PATHNAME	Character	64	Path name
NODENAME	Character	64	Node name
NODETYPE	Character	4	Node type
NODEEXT	Character	64	Node extension
SUCCESS	Character	16	Success

1st compressed view

Field	Data type	Width	Description
TBEGIN	Character	19	Start time
TEND	Character	19	End time
PATHNODE	Character	128	Copy of source field PATHNAME and of source field NODENAME
PATHNAME	Character	64	Copy first value of source field PATHNAME
NODENAME	Character	64	Copy first value of source field NODENAME
NODETYPE	Character	64	Copy first value of source field NODETYPE
NODEEXT	Character	64	Copy first value of source field NODEEXT
C_USER	Number	8	Based on: SUCCESS
			Calculation: Count
			Condition: SUCCESS==USER
C_DEFAULT	Number	8	Based on: SUCCESS
			Calculation: Count
			Condition: SUCCESS==DEFAULT
C_HANGUP	Number	8	Based on: SUCCESS
			Calculation: Count
			Condition: SUCCESS==HANGUP
C_NONE	Number	8	Based on: SUCCESS
			Calculation: Count
			Condition: SUCCESS==NONE

27.12.8 Telematic – Response Mailbox Activity

From XPR V4.0 this database will not be filled with data any more.

Field	Data type	Width	Description
TSTAMP	Character	19	Timestamp
PROT	Character	64	Protocol name
SOURCE	Character	64	Source
SCRIPTID	Character	10	Script ID
NUMSUB	Number	10	Number of subscribers
PATHNAME	Character	64	Path name
NODENAME	Character	64	Node name
NODETYPE	Character	4	Node type
NODEEXT	Character	64	Node extension
MSGSTATE	Character	16	Message state

1st compressed view

Field	Data type	Width	Description
TBEGIN	Character	19	Start time
TEND	Character	19	End time
PATHNODE	Character	128	Copy of source field PATHNAME and of source field NODENAME
PATHNAME	Character	64	Copy first value of source field PATHNAME
NODENAME	Character	64	Copy first value of source field NODENAME
NODETYPE	Character	64	Copy first value of source field NODETYPE
NODEEXT	Character	64	Copy first value of source field NODEEXT
C_NEW	Number	8	Based on: MSGSTATE
			Calculation: Count
			Condition: MSGSTATE==NEW
C_SAVED	Number	8	Based on: MSGSTATE
			Calculation: Count
			Condition: MSGSTATE==SAVED
C_DELETED	Number	8	Based on: MSGSTATE
			Calculation: Count
			Condition: MSGSTATE==DELETED

27.13 Database Tables: User and Group Data as well as for NCO Location Information

You can share further data for report creation. Such data is contained in database tables for user and group data as well as for NCO locations. This is done creating two new entries in the Report APL registry editor.

The raw data are transmitted even before the log files are processed, thus before the XMR service stores the raw data in the mentioned files in phase 2 (see [Section 27.3.1, "Report Generation"](#)). The Report APL exports the data to database tables, which are then available for report generation in the Report Schedule APL.

The following two registry entries are available:

- **ExportMrsUsers:** With this entry XPR user and group data is exported and stored in database tables.
- **ExportNCOLocation:** This entry has the NCO location information exported to database tables. Besides the locations with name and description, location codes and prefixes are put out.

NOTE:

You receive information about the concept of the *Number Conversion Objects* (NCO) in [Chapter 9, "Number Conversion Object \(NCO\)"](#).

In the following two sections we will introduce the database tables. You will first learn how to activate the data creation. Subsequently, the structure of the respective database tables will be presented. In other words, we show which database tables and associated attributes exist and how the database tables are interlinked. Eventually, there is a description of the database tables and their attributes.

27.13.1 ExportMrsUsers

This feature enables the creation of new database tables, which can be used by the Report APL for report generation. XPR user and group data is exported and stored in database tables.

As precondition for using this feature you need to create the registry entry **ExportMrsUsers**.

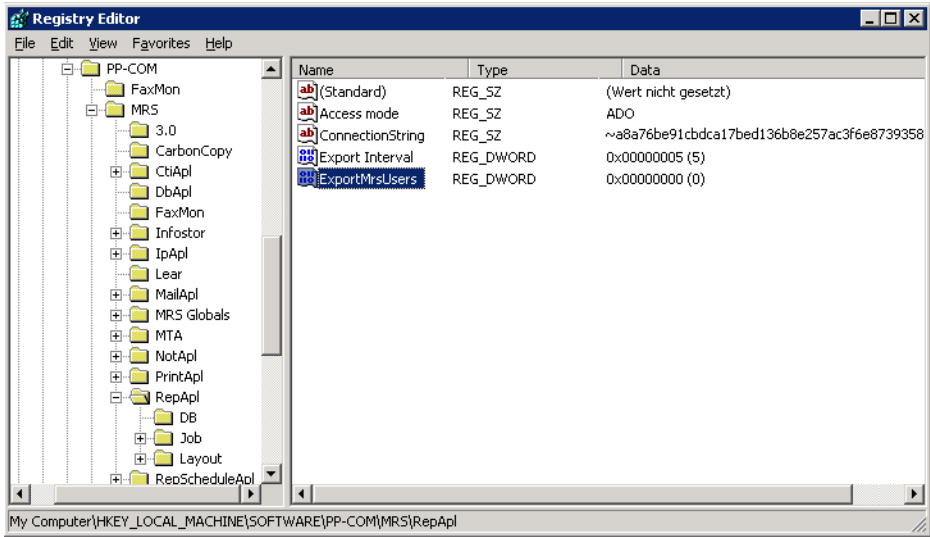
You open the **registry editor** in Windows by clicking on **Start > Run...** and entering the **regedt32** command.

Open the `HKLM\SOFTWARE\Wow6432Node\PP-COM\MRS\RepAp1` folder.

In the **Edit** menu click on **New** and **DWORD Value**.

A new entry is created that you name **ExportMrsUsers**.

Value **0** deactivates the new feature, while value **1** activates it. The report creation is inactive by default.



When you activate the feature, the Report APL creates new database tables, which are then available to the Report Schedule APL for report creation. The new database tables and column names will be described in the following sections.

27.13.1.1 The Structure of the Database Tables

The represented database tables are not defined in the adodb.ini or db.ini files. All shown tables and relations as well as attribute names are permanent. An exception is the `MRSUSERS` table. For this table the SQL command `CREATE TABLE` is executed at runtime for creating the attributes (column names) and the associated data independently from the current data of the **CORREL** database.

The following graphic shows which database tables and associated attributes exist and how these tables are interlinked. The abbreviation *PK* indicates the respective primary key attribute, which uniquely identifies the entries of a table.



The data of each XPR user are read from the `CORREL` database and stored in the `MRSUSERS` table. Each user is assigned a user group (`MRSUSERGROUP`).

In the following section you find a short introduction to the single database tables.

27.13.1.2 The Database Tables

In this section we explain the database tables `MRSUSERGROUP` and `MRSUSERS`.

NOTE:

The listed fields are the fields that provide the same information also in different, known environment scenarios, with this information being used for statistics in case of the corresponding correlation. All fields not listed may provide different information depending on the scenario. For creating reports we expressly recommend the exclusive use of the listed fields.

MRSUSERGROUP

Besides the user group **name** this table contains a unique **ID** for identification and referencing in the database system.

Column name	Data type	Width	Zeros permitted?	Description
UserGroupID	varchar	64	No	Unique ID of the XPR user group, which acts as key attribute.
Name	varchar	64	Yes	Name of the user group of the XPR system

MRSUSERS

This table contains the data for all XPR users. Each user is identified via his/her mailbox.

The table does not have a fixed structure, since the attributes and thus the column names are read from the user data of the `CORREL` database at runtime. The table fields are adjusted to the respective user masks in the system. Only the **MAILBOX** and **GROUP** fields are consistent, since `MAILBOX` is used as primary and `GROUP` as foreign key. The `GROUP` field references the `MRSUSERGROUP` table. A user can only belong to one user group, but a user group may possess any number of users.

Column name	Data type	Width	Zeros permitted?	Description
MAILBOX	varchar	64	No	User mailbox that acts as key attribute.
[GROUP]	varchar	64	Yes	User group that connects the <code>MRSUSERGROUP</code> table as foreign key.

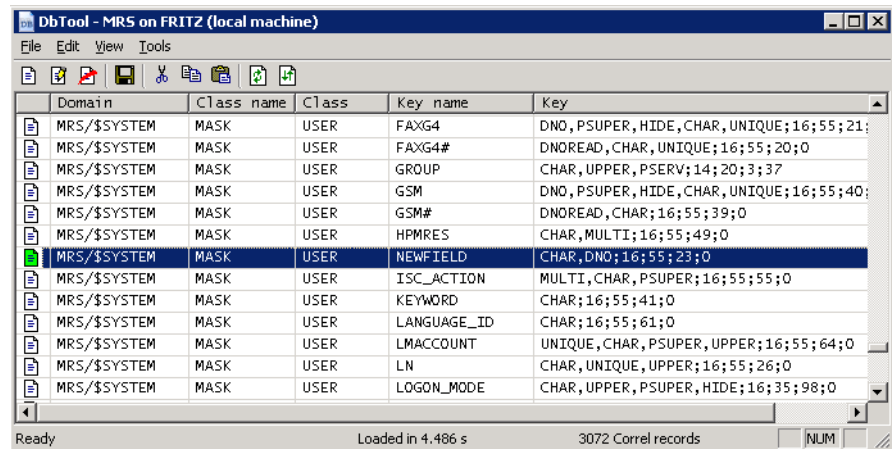
ADDR1, CITY, FAX3G or PHONE are further optional user attributes, which are read from the CORREL database. All these fields are of file type `varchar`, may have a length of 50 and allow zeros.

27.13.1.3 Adding User Attributes manually

You can insert self-created fields for a user in the **MRSUSERS** table. Therefore, the **MRSUSERS** table has dynamic fields. Database fields are created manually via the **DB Tool**.

How create a user field manually and integrate it in the **MRSUSERS** database table:

1. Start the **DB Tool**, which is found in the `<XPR Install>\SDKTools` folder. You find detailed DB Tool instructions in [Section 32.3, “Database-Correl-Tool \(DbTool\)”](#).
2. Create a new field in the class name **MASK** and in the class **USER** of the `<Server name>/$SYSTEM` domain. Enter the desired key name. Furthermore, you need to specify a value in the key, since otherwise the entry will not be stored in the CORREL database. This value will not be used, though, and is merely a wildcard.

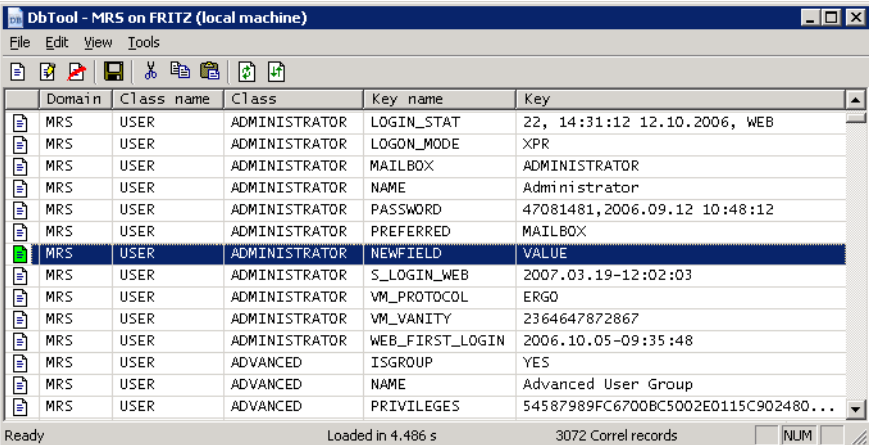


The screenshot shows the DbTool application window titled "DbTool - MRS on FRITZ (local machine)". It contains a table with the following columns: Domain, Class name, Class, Key name, and Key. The table lists various user attributes for the MRS/\$SYSTEM domain, including FAXG4, FAXG4#, GROUP, GSM, GSM#, HPMRES, NEWFIELD, ISC_ACTION, KEYWORD, LANGUAGE_ID, LMACCOUNT, LN, and LOGON_MODE. The NEWFIELD entry is highlighted in blue.

Domain	Class name	Class	Key name	Key
MRS/\$SYSTEM	MASK	USER	FAXG4	DNO, PSUPER, HIDE, CHAR, UNIQUE; 16; 55; 21;
MRS/\$SYSTEM	MASK	USER	FAXG4#	DNOREAD, CHAR, UNIQUE; 16; 55; 20; 0
MRS/\$SYSTEM	MASK	USER	GROUP	CHAR, UPPER, PSERV; 14; 20; 3; 37
MRS/\$SYSTEM	MASK	USER	GSM	DNO, PSUPER, HIDE, CHAR, UNIQUE; 16; 55; 40;
MRS/\$SYSTEM	MASK	USER	GSM#	DNOREAD, CHAR; 16; 55; 39; 0
MRS/\$SYSTEM	MASK	USER	HPMRES	CHAR, MULTI; 16; 55; 49; 0
MRS/\$SYSTEM	MASK	USER	NEWFIELD	CHAR, DNO; 16; 55; 23; 0
MRS/\$SYSTEM	MASK	USER	ISC_ACTION	MULTI, CHAR, PSUPER; 16; 55; 55; 0
MRS/\$SYSTEM	MASK	USER	KEYWORD	CHAR; 16; 55; 41; 0
MRS/\$SYSTEM	MASK	USER	LANGUAGE_ID	CHAR; 16; 55; 61; 0
MRS/\$SYSTEM	MASK	USER	LMACCOUNT	UNIQUE, CHAR, PSUPER, UPPER; 16; 55; 64; 0
MRS/\$SYSTEM	MASK	USER	LN	CHAR, UNIQUE, UPPER; 16; 55; 26; 0
MRS/\$SYSTEM	MASK	USER	LOGON_MODE	CHAR, UPPER, PSUPER, HIDE; 16; 35; 98; 0

Ready Loaded in 4.486 s 3072 Correl records NUM

3. For the desired user (class name **USER** and class user name) now insert a field that carries the name of the field created in step 2 as key name. Enter the desired value of the field as key.



	Domain	Class name	Class	Key name	Key
	MRS	USER	ADMINISTRATOR	LOGIN_STAT	22, 14:31:12 12.10.2006, WEB
	MRS	USER	ADMINISTRATOR	LOGON_MODE	XPR
	MRS	USER	ADMINISTRATOR	MAILBOX	ADMINISTRATOR
	MRS	USER	ADMINISTRATOR	NAME	Administrator
	MRS	USER	ADMINISTRATOR	PASSWORD	47081481,2006.09.12 10:48:12
	MRS	USER	ADMINISTRATOR	PREFERRED	MAILBOX
	MRS	USER	ADMINISTRATOR	NEWFIELD	VALUE
	MRS	USER	ADMINISTRATOR	S_LOGIN_WEB	2007.03.19-12:02:03
	MRS	USER	ADMINISTRATOR	VM_PROTOCOL	ERGO
	MRS	USER	ADMINISTRATOR	VM_VANITY	2364647872867
	MRS	USER	ADMINISTRATOR	WEB_FIRST_LOGIN	2006.10.05-09:35:48
	MRS	USER	ADVANCED	ISGROUP	YES
	MRS	USER	ADVANCED	NAME	Advanced User Group
	MRS	USER	ADVANCED	PRIVILEGES	54587989FC6700BC5002E0115C902480...

4. Save your modifications.

With the next data export to the database tables by the Report APL, the newly created field is integrated in the `MRSUSERS` table. The corresponding user receives in this field the value defined in the `key`. The other users are assigned in this field value `ZERO`.

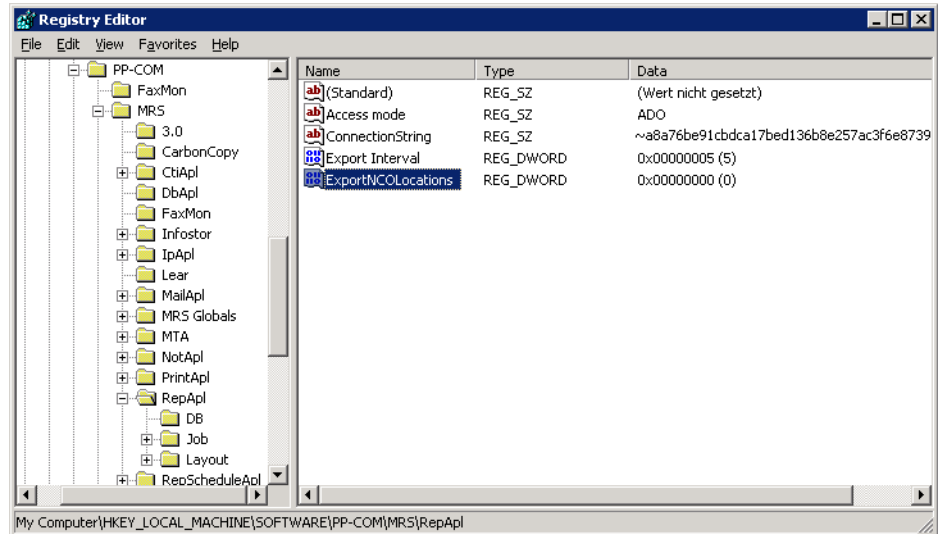
27.13.2 ExportNCOLocation

This feature enables the creation of new database tables containing NCO location information, which can be used for report generation by the Report APL. The location information is a NCO basic information, thus significantly influencing the phone number conversion. It is composed of the location information and prefixes, which are stored in the single database tables. This division of the location information is reflected by the database table structure (see [Section 27.13.2.1, “The Structure of the Database Tables for NCO Location Information”](#)).

NOTE:
You receive information about the concept and handling of *Number Conversion Object (NCO)* in [Chapter 9, “Number Conversion Object \(NCO\)”](#).

- As precondition for using this feature you need to create the registry entry *ExportNCOLocation*.
- You open the **registry editor** in Windows by clicking on **Start > Run...** and entering the **regedt32** command.
- Open the `HKLM\SOFTWARE\Wow6432Node\PP-COM\MRS\RepAp1` folder.
- In the **Edit** menu click on **New** and **DWORD Value**.
- A new entry is created that you name **ExportNCOLocation**.

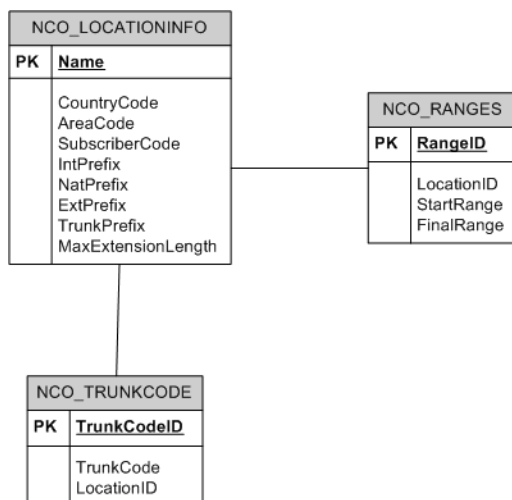
Value **0** deactivates the new feature, while value **1** activates it. The report creation is inactive by default.



When you activate the feature, the Report APL respectively the Report Schedule APL creates new database tables, which are then available for report creation. The new database tables and column names will be described in the following sections.

27.13.2.1 The Structure of the Database Tables for NCO Location Information

The following graphic shows the single database tables, their attributes as well as their interlinking. The connections represent the options to configure NCO locations in the **NCOAdmin**. The abbreviation *PK* indicates the respective primary key attribute, which uniquely identifies the entries of a table.



Besides the mandatory *name*, each NCO location has optional information about location codes and prefixes. By means of the respective attributes in the table `NCO_LOCATIONINFO` such information is assigned to a location. The respective location code or prefix is found in the following attributes:

- Each location may have one `CountryCode`, one `AreaCode` and one `SubscriberCode`.
- Each location may have one `IntPrefix`, one `NatPrefix`, one `ExtPrefix` and one `TrunkPrefix`.
- Each location may have several trunk codes (`NCO_TRUNKCODE`) and range codes (`NCO_RANGES`). Such information is stored in individual, separate tables and assigned to a location with the foreign key `LocationID`.

In the following section you find a short introduction to the single database tables.

27.13.2.2 The Database Tables of the NCO Location Information

In this section we explain the database tables of the NCO location information `NCO_LOCATIONINFO`, `NCO_TRUNKCODE` and `NCO_RANGES`.

NOTE:

The listed fields are the fields that provide the same information also in different, known environment scenarios, with this information being used for statistics in case of the corresponding correlation. All fields not listed may provide different information depending on the scenario. For creating reports we expressly recommend the exclusive use of the listed fields.

NCO_LOCATIONINFO

Each entry in this table corresponds to a location and receives for unique identification the `LocationInfoID` entry. This table is connected to the `NCO_LOCATION` table via the `NCOLocationID` entry. This entry is thus a foreign key. The other fields are optional and are defined in other tables. Such tables are referenced via foreign keys. If the fields do not exist for a location, they contain value `ZERO`.

Column name	Data type	Width	Zeros permitted?	Description
Name	varchar	90	No	The name serves as unique ID for identifying an NCO location.
CountryCode	varchar	50	Yes	Contains the value for the national code of the location.
AreaCode	varchar	50	Yes	Contains the value for the area code of the location.
SubscriberCode	varchar	50	Yes	Contains the value for the subscriber code of the location.
IntPrefix	varchar	50	Yes	Contains the value for the international prefix of the location.
NatPrefix	varchar	50	Yes	Contains the value for the national prefix of the location.
ExtPrefix	varchar	50	Yes	Contains the value for the external prefix of the location.
TrunkPrefix	varchar	50	Yes	Contains the value for the trunk prefix of the location.

Column name	Data type	Width	Zeros permitted?	Description
MaxExtensionLength	numeric	9	Yes	Defines the maximum length of the internal calling numbers. Numbers that exceed this length are not recognized as internal calling numbers.

Each location may only have one entry in the `NCO_LOCATIONINFO` table.

Consequently, a location may only have one entry in the tables `NCO_TRUNKCODE` and `NCO_RANGES`.

NCO_TRUNKCODE

This table contains the trunk code under which the XPR server is connected to a PBX. This code is passed from the PBX to the XPR server with phone number transfers if required.

A location may have several trunk codes. Therefore, the table has the foreign key `LocationID` to reference the `NCO_LOCATION` table.

Column name	Data type	Width	Zeros permitted?	Description
TrunkCodeID	numeric	9	No	Unique ID to identify the trunk code of a location.
TrunkCode	CHAR	10	Yes	Contains the trunk code of a location.
LocationID	varchar	90	Yes	Foreign key to reference the table <code>NCO_LOCATIONINFO</code> .

NCO_RANGES

This table defines range codes under which the telephones of the XPR users in a location can be reached from outside. Numbers that are not contained in a range code upon its definition will be normalized to private phone numbers. If no range code is defined, all phone numbers are accessible from outside.

A location may have several range codes. A range code is assigned to a location via the foreign key `LocationID`.

Column name	Data type	Width	Zeros permitted?	Description
RangeCodeID	numeric	9	No	Unique ID to identify the range code of a location.
LocationID	varchar	90	Yes	Foreign key to reference the table <code>NCO_LOCATIONINFO</code> .
StartRange	varchar	50	Yes	The start number of a range code
FinalRange	varchar	50	Yes	The last number of a range code

27.14 Database Tables of the VOGUE Script

NOTE:

The listed fields are the fields that provide the same information also in different, known environment scenarios, with this information being used for statistics in case of the corresponding correlation. All fields not listed may provide different information depending on the scenario. For creating reports we expressly recommend the exclusive use of the listed fields.

The VOGUE script delivers raw data that serve for statistical evaluation of the properties of applications and controls that were set up using the Application Builder. Each raw data entry has the following structure:

Telematic<tab><Topic><tab><Timestamp>{<tab><Key=Pair of Variates>}+

Like other raw data, the data are written in the log files in the directory <XPR install>\stat.

The single entries have the following significance:

Item	Description
Telematic	The VOGUE script runs on a telematics APL (ISDN APL or IP APL). All raw data of the VOGUE script are prefixed with the Telematic entry.
Topic	As Topic two possible values are defined: • IVR Application: These raw data refer to an application and are created at the end of an application run. • IVR Box: These raw data refer to a control of an application and are created at the end of a control execution.
Timestamp	This point in time represents the end time of an application's or control's execution and thus the point in time of the raw data creation. Start time and duration of an application's or control's execution are available in the key entries.
Key	An amount of different information for each application or control. Such entries will be explained in the upcoming sections.

All entries are written at the end of an application's or control's execution when all information for statistical raw data is available.

The raw data of the VOGUE script are stored in two database tables:

- **IVR Application** to store data for the properties and the run of an entire application. If the data are available and do not contain empty fields, the IVR Application data are continuously written in the log files. In case of a running VOGUE script the creation of such data cannot be stopped.

- **IVR Box** for filing specific information about single controls used. The transmission of these data to the log files can be activated or deactivated in the Application Builder by a selectable option in the configuration of each control used. Each table of the IVR Box is uniquely assigned to a table of the IVR Application.

NOTE:

VOGUE script raw data are created in the log files automatically and continuously. You can export the statistical raw data of the VOGUE script also automatically to the SQL database tables of the SQL server configured in the Report APL using the Report APL (see [Section 27.4, “Report APL Configuration”](#)). This requires checking the settings of the registry entry **ExportIVRStatistics** in the `RepAp1` key. Value 0 is specified by default, so that the export of raw data to the tables of the SQL server is disabled. With value 1 of this entry you activate the transmission of raw data to the database tables of the configured SQL server. You find more information on this in [Appendix E.16.1, “General Entries”](#).

The configuration for creating statistical raw data or, to be more precise, the storage of this data may occur using the `adodb.ini` file (see [Section 27.10.3, “dBase and ADO Database Structure”](#)). You find the file in the `<XPR Install>/res/e/RepAp1` directory.

Within the `adodb.ini` file you find a section indicated with **[IVR Application]**. This section refers to the configuration for storing data in the tables of the **IVR Application**. Since the tables of the **IVR Box** depend on **IVR Application** and cannot exist by themselves, the configuration also contains the tables of the **IVR Box**.

With the **IVR data retention** option you define how long the data is stored in the database tables. The command is entered in the format:

RANGE=unit, number

The unit specification defines what the number refers to. Unit may have the values 0 (seconds), 1 (minutes), 2 (hours), 3 (days), 4 (weeks), 5 (months) and 6 (years). The **RANGE=5, 6** example thus specifies that the data is stored in the database tables six months. If no specification is made, the data is stored one year.

27.14.1 Key Entries of the IVR Application

Each entry is only created if the required information is available. This means that, depending on the execution and the structure of the respective application, specific entries may be missing. Available raw data of the IVR Application are always written in the log files. This writing process cannot be stopped in case of a running VOGUE script.

Key	Meaning	Description
UniqueID	Identifying call ID	The ID consists of 20-character strings. It can only be assigned to one application. All entries for the controls of an application have the same ID. In this way it is possible to track a call.
TelematicApl	Telematics APL	The VOGUE script runs on a telematics APL (ISDN APL or IP APL). The TelematicApl entry thus contains the information on which APL the VOGUE script is configured.
Application Name	Application name	The full application name as described in the Application Builder.
CallerNumber	Phone number of the caller	The phone number of the caller in normalized format, e.g. +492404112233.
CalledNumber	Phone number of the callee	The phone number of the callee in normalized format, e.g. +492404667788. This corresponds in most cases to the phone number assigned to the application.
STARTTIME	Start time of the application	The entry has the following format: yy.mm.dd.hh.mm.ss (for year.month.day.hour.minute.second)
DURATION	Duration of the application's duration	Entire duration of an application's execution in seconds. The execution starts with the first control (see <i>StartBoxName</i>) and ends for a specific reason (see <i>EndCause</i>).
StartBoxName	Name of the start control	Name of the control with which the application starts.
StartBoxType	Type of the start control	Type of the control with which the application starts (e.g. Prompt Control).
EndBoxName	Name of the end control	Name of the control with which the application ends.
EndBoxType	Type of the end control	Type of the control with which the application ends (e.g. End Control).

Key	Meaning	Description
EndCause	Reason for ending the application's execution	Possible values: • CALL FORWARDING: The call was forwarded to a person or to another application. • CALLER HANGUP: The call was ended as the caller hung up. • APPLICATION HANGUP: The call was ended as the application hung up . • SCRIPT CHANGE: The script was changed, for example to Ergo.
ForwardNumber	Phone number to which the call was forwarded	The phone number to which the call was forwarded in normalized format (e.g. +490204400900)
Script	Script to which the call was forwarded	The logical script name to which the call was forwarded (e.g. ERGO).

27.14.2 Key Entries of the IVR Box

Each entry is only created if the required information is available. This means that, depending on the execution, the configuration and the type of the respective control, specific entries may be missing. The creation of these data can be activated or deactivated by a selectable option in the configuration of any control in the Application Builder.

Key	Meaning	Description
UniqueID	Identifying call ID	The ID consists of 20-character strings. It can only be assigned to one application. All entries for the controls of an application have the same ID. In this way it is possible to track a call.
BoxName	Name of the control	Complete control name, which was defined in the Application Builder.
BoxType	Type of control	Possible values: • COMPARE: Compare control • CONNECT: Connect control • DBREAD: DB Read control • DBWRITE: DB Write control • DEFINE: Define control • DOCUMENT: Document control • HANGUP: End control • MENU: DTMF Menu control • INPUT: DTMF Input control • LANGUAGE: Language control • PLAY: Prompt control • QA: Questionnaire control • SCRIPT: Script control • TIME: Time Profile control • VANITY: Contact Dialing control • NAMEDIALING: Name Dialing control • ASRMENU: ASR Menu control • ASREXPRT: ASR Expert control • GREETINGS: Holiday Greetings Control
STARTTIME	Start time for the execution of a box	The value has the format <code>yy.mm.dd.hh.mm.ss</code> (for year.month.day.hour.minute.second)
DURATION	Duration of a box's execution	Total time of a box's execution is seconds. The box starts when the call is forwarded to it and ends when the final result of the execution (see <code>RESULT</code>) is delivered.
NextBox	Name of the next box	Complete name of the box to which the call was forwarded. In this way you can trace the call on its way through the boxes of the application.

The following key entries are not possible for each box, but depend on the box type. Consequently, the keys will be sorted according to box types in the following sections:

27.14.2.1 Holiday Greetings Control

The following specific keys are additionally possible for the Holiday Greetings control:

Key	Meaning	Description
TIMEPROFILE	Time profile name	Name of the time profile selected for the control's execution
Result	Result	Result of the control execution. With this result the control was ended. The following values are possible: • READY: The control was ended in state Ready, thus successfully. • ERROR: The control was ended in state Error. • INTERRUPTED: The control's execution was interrupted by the contact center.

27.14.2.2 ASR Expert Control

The following specific keys are additionally possible for the ASR Expert control:

Key	Meaning	Description
ASRKeyword	Recognized sentence	This key contains the sentence recognized by the speech recognition system.
ASRConfidence	Confidence level	Selected minimum size in percent in which an announcement must be recognized by the speech recognition system so that a valid recognition is produced.
Result	Result	Result of the control execution. With this result the control was ended. The following values are possible: • READY: The control was ended in state Ready, thus successfully. • ERROR: The control was ended in state Error. • TIMEOUT: The control was ended in state Timeout. • RESULT EMPTY: The control was ended in state Empty. • INTERRUPTED: The control's execution was interrupted by the contact center.

27.14.2.3 ASR Menu Control

The following specific keys are additionally possible for the ASR Menu control:

Key	Meaning	Description
ASRKeyword	Recognized keyword	This key contains the keyword recognized by the speech recognition system.
ASRConfidence	Confidence level	Selected minimum size in percent in which an announcement must be recognized by the speech recognition system so that a valid recognition is produced.
Result	Result	Result of the control execution. With this result the control was ended. The following values are possible: • KEYWORD RECEIVED: The speech recognition system has successfully recognized the announced keyword. • ERROR: The control was ended in state Error. • TIMEOUT: The control was ended in state Timeout. • RESULT EMPTY: The control was ended in state Empty. • INTERRUPTED: The control's execution was interrupted by the contact center.

27.14.2.4 End Control

The following specific keys are additionally possible for the End control:

Key	Meaning	Description
Result	Result	Result of the control execution. With this result the control was ended. The following values are possible: • CALL DISCONNECTED: The control has successfully ended the call and thus the connection to the VOGUE script.

27.14.2.5 DB Read Control

The following specific keys are additionally possible for the DB Read control:

Key	Meaning	Description
Result	Result	Result of the control execution. With this result the control was ended. The following values are possible: • READY: The control was ended in state Ready, thus successfully. • ERROR: The control was ended in state Error. • INTERRUPTED: The control's execution was interrupted by the contact center.

27.14.2.6 DB Write Control

The following specific keys are additionally possible for the DB Write control:

Key	Meaning	Description
Result	Result	Result of the control execution. With this result the control was ended. The following values are possible: • READY: The control was ended in state Ready, thus successfully. • ERROR: The control was ended in state Error. • INTERRUPTED: The control's execution was interrupted by the contact center.

27.14.2.7 Definition Control

The following specific keys are additionally possible for the Definition control:

Key	Meaning	Description
Result	Result	Result of the control execution. With this result the control was ended. The following values are possible: • READY: The control was ended in state Ready, thus successfully. • ERROR: The control was ended in state Error. • INTERRUPTED: The control's execution was interrupted by the contact center.

27.14.2.8 Document Control

The following specific keys are additionally possible for the Document control:

Key	Meaning	Description
Result	Result	Result of the control execution. With this result the control was ended. The following values are possible: • READY: The control was ended in state Ready, thus successfully. • ERROR: The control was ended in state Error.

27.14.2.9 DTMF Entry Control

The following specific keys are additionally possible for the DTMF entry control:

Key	Meaning	Description
DTMF	Entered DTMF keys	This key contains the DTMF keys entered via the phone keypad.
Result	Result	Result of the control execution. With this result the control was ended. The following values are possible: • READY: The control was ended in state Ready, thus successfully. • ERROR: The control was ended in state Error. • INTERRUPTED: The control's execution was interrupted by the contact center.

27.14.2.10 Questionnaire Control

The following specific keys are additionally possible for the Questionnaire control:

Key	Meaning	Description
Result	Result	Result of the control execution. With this result the control was ended. The following values are possible: • READY: The control was ended in state Ready, thus successfully. • INTERRUPTED: The control's execution was interrupted by the contact center.

27.14.2.11 Contact Dialing Control

The following specific keys are additionally possible for the Contact Dialing control:

Key	Meaning	Description
Result	Result	Result of the control execution. With this result the control was ended. The following values are possible: • READY: The control was ended in state Ready, thus successfully. • ERROR: The control was ended in state Error. • INTERRUPTED: The control's execution was interrupted by the contact center.

27.14.2.12 DTMF Menu Control

The following specific keys are additionally possible for the DTMF Menu control:

Key	Meaning	Description
DTMF	Entered DTMF key	This key contains the DTMF key entered via the phone keypad.
Result	Result	Result of the control execution. With this result the control was ended. The following values are possible: • DTMF RECEIVED: The entered DTMF key was recognized and is linked to a valid control for forwarding. • ERROR: The control was ended in state Error. • INTERRUPTED: The control's execution was interrupted by the contact center.

27.14.2.13 Name Dialing Control

The following specific keys are additionally possible for the Name Dialing control:

Key	Meaning	Description
Result	Result	Result of the control execution. With this result the control was ended. The following values are possible: • READY: The control was ended in state Ready, thus successfully. • ERROR: The control was ended in state Error.

27.14.2.14 Language Control

The following specific keys are additionally possible for the Language control:

Key	Meaning	Description
Result	Result	Result of the control execution. With this result the control was ended. The following values are possible: • <code>READY</code>: The control was ended in state Ready, thus successfully. • <code>ERROR</code>: The control was ended in state Error. • <code>INTERRUPTED</code>: The control's execution was interrupted by the contact center.

27.14.2.15 Script Control

The following specific keys are additionally possible for the Script control:

Key	Meaning	Description
Script	Script to which the call was forwarded	The key contains the logical name of the script to which the call was forwarded, for example <code>ERGO</code> .
Result	Result	Result of the control execution. With this result the control was ended. The following values are possible: • <code>SCRIPT CHANGED</code>: The call was forwarded to the script selected in the control. • <code>ERROR</code>: The control was ended in state Error.

27.14.2.16 Compare Control

The following specific keys are additionally possible for the Compare control:

Key	Meaning	Description
Result	Result	Result of the control execution. With this result the control was ended. The following values are possible: • <code>CONDITION MET</code>: The condition specified in a rule was met. • <code>ERROR</code>: The control was ended in state Error. • <code>INTERRUPTED</code>: The control's execution was interrupted by the contact center.

27.14.2.17 Connect Control

The following specific keys are additionally possible for the Connect control:

Key	Meaning	Description
ForwardNumber	Phone number to which the call was forwarded	The phone number to which the call was forwarded in normalized format, for example +492404999888
Result	Result	Result of the control execution. With this result the control was ended. The following values are possible: - CALL FORWARDED: The call was forwarded to a phone number specified in the control. - ERROR: The control was ended in state Error.

27.14.2.18 Prompt Control

The following specific keys are additionally possible for the Prompt control:

Key	Meaning	Description
Result	Result	Result of the control execution. With this result the control was ended. The following values are possible: - READY: The greeting was successfully played and the call was forwarded to the control defined in state Ready. - INTERRUPTED: The control's execution was interrupted by the contact center.

27.14.2.19 Time Profile Control

The following specific keys are additionally possible for the Time Profile control:

Key	Meaning	Description
TIMEPROFILE	Time profile name	Name of the time profile selected for the control's execution
Result	Result	Result of the control execution. With this result the control was ended. The following values are possible: • <code>STATE OPEN</code>: The time profile is in state Open at the time of the control's execution. • <code>STATE BREAK</code>: The time profile is in state Break at the time of the control's execution. • <code>STATE CLOSED</code>: The time profile is in state Closed at the time of the control's execution. • <code>INTERRUPTED</code>: The control's execution was interrupted by the contact center.

28 General File Interface (FIAPL)

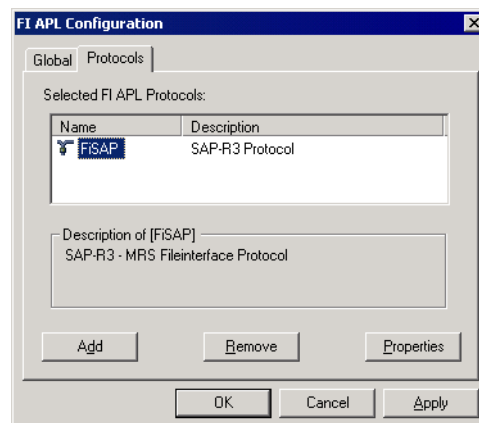
The File Interface APL enables XPR transmission and receipt processes via a file interface. By means of a protocol in script language E, a document header and possibly also reports are written for the documents transmitted from the XPR server to another system. Conversely, for documents sent from this system to the XPR server, an incoming document header is parsed and a send job created for XPR by using this E-script as well.

No predefined protocols are supported. All projects that can be enabled with the FI APL require skills that are normally only available in a professional services organization. If a customer project is to be enabled using the FI APL, the professional service must be involved at any rate.

File Interface protocols installed on the computer can be added through use of the **Add** button, removed with the **Remove** button, and configured using the **Properties** button in the FI APL configuration dialog of the XPR monitor. The number of protocols is restricted to 32.

NOTE:

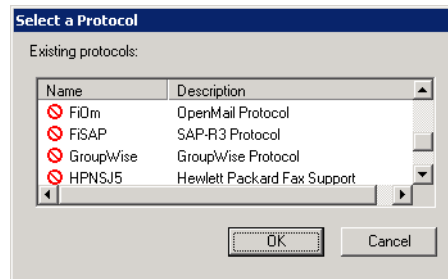
The *supervisor privilege* is required for the configuration.



Please consult the Professional Services for creating individual protocols.

28.1 Adding and removing Protocols

You add protocols on the **Protocols** tab. When you push the **Add** button, a new dialog opens in which you can select existing protocols.



When you confirm your protocol selection, it will be listed on the Protocols tab. If you want to delete a protocol from this list, select it and click the **Remove** button.

28.2 The Protocol Properties

After selecting a protocol you can open its attributes using the **Properties** button. A dialog opens that features two sections: properties for sending documents from a host to the FI APL, and for sending from the FI APL to a host.

28.2.1 Host -> FI APL

The following table describes the fields of the **Host -> FI APL** section:

Field	Description
Poll directory	In the properties dialog the Poll directory : field contains path information for the directory where the host system stores header files which contain the necessary data for transmissions.
Body directory	In the Body directory the host system stores the document bodies that belong to the header.

Field	Description
Edit script	A click on this button opens the FI APL Builtin Editor with the code of the corresponding protocol. Using the editor you can now view and modify the protocol code. Modifications will not be checked for semantically and syntactically correctness, though.
Poll rate	The interval at which the File Interface APL queries for new incoming documents in the poll directory is given in seconds in the Poll rate : field. A maximum of 65535 seconds can be specified. In case of a 0 poll rate, <i>INFINITE</i> is displayed since then no new documents are searched for. This protocol is thus deactivated.
PrivData field size	The PrivData field size: field defines the size of individual data fields set by the various scripts, and which are made available at a later time for reporting purposes. The numbers correspond to the variables %PVD0, %PVD1 and %PVD2, etc. These can be used in the format file. This data is returned in an XPR report and can be written to the report header from the same source. Example: { *, 30 }, { *, 30 }, { DOC, 64 } The first 30 means that %PVD0 is a maximum of 30 bytes long. The same applies analogue for the second 30 and the variables %PVD1. { DOC, 64 } means that a maximum of 64 bytes from the document name (XPR-variable DOC) would be copied to the variable %PVD2. The combined length of all %PVD fields must not exceed 128 bytes. In the example two variables with a length of 30 bytes were used and one with 64 bytes, for a total length of 124 bytes. Alternatively, this global value can be replaced with a definition in the <i><Protocol>.e</i> script. Example: <pre>export const PrivData = "30,*;30,*;64,DOC";</pre> The PrivData field size option is inactive when in the E-script (*.e) this field is already exported or the corresponding functions are already defined.
Maximum per poll	By means of Maximum per poll : you can default set the maximum number of jobs to be read in and processed all at once. This temporarily distributes the load with a very large job. You can specify a maximum number of 32767.
Delete header	In the Poll rate field you can specify the period in which the poll directory is searched for new header files that correspond to the Header pattern . Via the Delete header option, header files that have been processed are removed during this search. This option should only be disabled for testing purposes, when looking for an error.
Check Privileges	The originator's privileges are checked if the Check Privileges option is set. In this way the originator's privileges are checked, e.g. whether he/she is authorized to send a fax document.

28.2.2 File Interface APL to the Host

The following table describes the fields of the **FI APL -> Host** section:

Field	Description
Header directory	In the Header directory the XPR system stores for each send job a header file with the transmission information.
Body directory	In the Body directory the XPR system stores the document bodies that belong to the header.

The **Incoming messages** subdivision contains options for sending fax messages.

The fields of the **Incoming messages** subdivision:

Field	Description
Enable	Receiving fax messages mandatorily requires the activation of the Incoming messages function. Otherwise, only messages by the foreign system would be accepted and reports on the send state would be returned to the foreign system. With activated XPR server to host direction, the event <code>EvIncoming (const t_send *pS)</code> must be defined for incoming messages in the <code><Protocol>.e</code> script.
Suffix	A Suffix is appended to the header files each for messages that arrive at the host system. These files are read by the host system and then accordingly processed.
Fax format	In the Fax format field you need to select a specific file format for incoming fax messages from a list. If you keep the <code><none></code> default entry, no fax messages can be received despite the function being active.
Edit script	This option is not supported any more.

In the **Reports** subdivision you can perform settings for reports that message the successful or unsuccessful transmission status of the fax messages.

The fields of the **Reports** subdivision:

Field	Description
Filter	The Filter for reports to the host system either allows <code>all</code> , <code>final only</code> or <code>none</code> send status messages. The <code>final only filter</code> indicates that only reports are sent that transfer a final send status of a fax message. This allows a rough control of the number of reports. With activated Filter option in the Reports section the <code>EvReport(const t_send *pS)</code> event must be defined for reports in the <code><Protocol>.e</code> script.
Suffix	A Suffix is appended to the header files each for reports that arrive at the host system. These files are read by the host system and then accordingly processed.
Edit script	This option is not supported any more.

28.3 Configuring Sites and Tenants via Import File

You can perform site and tenant settings of the XPR server using the FI APL and a configuration file. For this purpose, the `XprConfig.e` configuration script, which can process the corresponding configuration files, is shipped for the FI APL. These settings apply for an SIP connection.

28.3.1 Configuring the Configuration Script

Before the FI APL can use the `XprConfig.e` configuration script, you need to add and configure it for the FI APL.

Start the configuration

Add the configuration script to the FI APL and configure it by executing the following steps:

1. Open the XPR monitor and log on with an administrator account.
2. Select the FI APL settings in the XPR monitor's modules window.
The FI APL configuration dialog opens.
3. Switch to the **Protocols** tab.
4. Select **Add** and add the `XprConfig.e` script.
The `XprConfig.e` script is now displayed on the **Protocols** tab.
5. Mark the `XprConfig.e` script on the **Protocols** tab and select **Properties**.
6. Specify in the **Poll directory** field a directory the FI APL is to automatically search for new configuration files to read them in.
7. Specify the **Poll rate** field the intervals in which the FI APL is to search the poll directory for new configuration files to read them in.
Setting **0** (INFINITE) deactivates the automatic search.
A reasonable value would be e.g. 10 seconds.
8. Enter `*.xml` in the **Header-Muster** field.
9. Select **OK** to copy the settings for the script.
10. Select **OK** to copy the settings for the FI APL.

The configuration script for the FI APL is now configured. The actual import mechanism is now already functional.

28.3.2 Creating a Configuration File

In the mean time you have configured the import mechanism that adopts the site and tenant settings from a configuration file. For the actual import you now need an appropriate XML-based configuration file that contains the relevant site and tenant settings. The configuration file is e. g. created via the Customer Data Collection (CDC) Tool of the OpenScape Voice. This mechanism allows configuring tenants for SIP protocols only.

NOTE: You find an example configuration file in the following directory of the XPR server:

<XPR Install>\res\FiApl

A configuration file must have the name `ipapl.xml` and the following UTF-8 format and can be created in a text editor.

```
<?xml version="1.0" encoding="UTF-8"?>
<XpressionsConfig>
  <OSVConnection>
    <parameter name="SipProxyIP" value="<IP address>" />
    <parameter name="SipProxyPort" value="<port number>" />
    <parameter name="XpressionsSipServerIP" value="<IP address>" />
    <parameter name="XpressionsSipServerPort" value="<port number>" />
    <parameter name="SipTransportType" value="<TCP|UDP|TLS>" />
    <parameter name="SRTP" value="<disable|MIKEY|SDES>" />
    <parameter name="CodecPrio1" value="<G711A|G711U|G729>" />
    <parameter name="CodecPrio2" value="<G711A|G711U|G729>" />
    <parameter name="CodecPrio3" value="<G711A|G711U|G729>" />
    <parameter name="T38" value="<yes|no>" />
    <parameter name="NumPhysicalChannels" value="<number of channels>" />
    <parameter name="NumFaxChannels" value="<number of channels>"/>
    <parameter name="NumG729Channels" value="<number of channels>"/>
  </OSVConnection>
  <Extensions>
    <Extension>
      <parameter name="ScriptName" value="<PhoneMail entity name>" />
      <parameter name="ExtensionAction" value="add" />
      <parameter name="MSNorRange" value="<extension>--<extension>" />
    </Extension>
    <Extension>
      ...
    </Extension>
    ...
  </Extensions>
```

<Phonemail>

```
<parameter name="ScriptAction" value="<add|modify|delete>" />
<parameter name="ScriptName" value="<protocol entity name>" />
<parameter name="DirectAccess" value="<extension>" />
<parameter name="GuestAccess" value="<extension>" />
<parameter name="CallBackAccess" value="<extension>" />
<parameter name="FaxAccess" value="<extension>" />
<parameter name="TransferAccess" value="<extension>" />
<parameter name="UniversalAccess" value="<extension>" />
<parameter name="TTMEnabled" value="<yes|no>" />
<parameter name="RemTrustedDomainCallNumber" value="<extension>" />
<parameter name="RemTrustedDomainID" value="<domain ID>" />
<parameter name="LocalTrustedDomainID" value="<domain ID>" />
<parameter name="CallingNumSchema" value="<TTM schema>" />
<parameter name="CallingNumMaxLength" value="<phone number length>" />
```

</Phonemail>

<Tenants>

<Tenant>

```
<parameter name="TenantAction" value="<add|modify|delete>" />
<parameter name="TenantName" value="<tenant ID>" />
<parameter name="DirectAccess" value="<extension>" />
<parameter name="GuestAccess" value="<extension>" />
<parameter name="CallBackAccess" value="<extension>" />
<parameter name="FaxAccess" value="<extension>" />
<parameter name="TransferAccess" value="<extension>" />
<parameter name="UniversalAccess" value="<extension>" />
<parameter name="MSNorRange" value="<extension>-<extension>" />
<parameter name="MSNorRange" value="..." />
...
<parameter name="LocationName" value="<location ID>" />
```

</Tenant>

<Tenant>

...

</Tenant>

...

</Tenants>

```

<NCOSites>
  <NCOSite>
    <parameter name="NCOSiteAction" value="<add|modify|delete>" />
    <parameter name="SiteName" value="<location ID>" />
    <parameter name="CountryCode" value="<code>" />
    <parameter name="AreaCode" value="<code>" />
    <parameter name="SubscriberCode" value="<code>" />
    <parameter name="RangeCode" value="<code>" />
    <parameter name="ExtensionCode" value="<code>" />
    <parameter name="TrunkCode" value="<code>" />
    <parameter name="InternationalPrefix" value="<prefix>" />
    <parameter name="NationalPrefix" value="<prefix>" />
    <parameter name="ExternalPrefix" value="<prefix>" />
    <parameter name="TrunkPrefix" value="<prefix>" />
    <parameter name="Var:<variable name>" value="<variable value>" />
    <parameter name="Var: ..." value=" ..." />
    ...
  </NCOSite>
  <NCOSite>
    ...
  </NCOSite>
  ...
</NCOSites>
<NCOConnectPoints>
  NCOConnectPoint>
    <parameter name="CPAction" value="<add|modify|delete>" />
    <parameter name="Name" value="<connection point ID>" />
    <parameter name="Location" value="<location ID>" />
    <parameter name="NCO" value="<NCO ID>" />
    <parameter name="Var:<variable name>" value="<variable value>" />
    <parameter name="Var: ..." value=" ..." />
    ...
  </NCOConnectPoint>
  NCOConnectPoint>
    ...
  </NCOConnectPoint>
  ...
</NCOConnectPoints>
</XpressionsConfig>

```

* **Important:**
 Via the `CallingNumSchema` parameter you can configure the calling number schema more comprehensively than via the TTM settings in the Telematic GUI. Possible further settings, however, are reset to the default values as soon as you invoke the TTM settings in the Telematic GUI.
 See also [Section 28.3.2, "Calling Number Schema", on page 1432](#).

Object sections in the configuration file

The single sections of the configuration file refer to the following settings:

- `<OSVConnection>`
Specifies the most important settings of an SIP device. These are documented in [Section 10.10.4.2, “Properties of SIP-based Devices”, on page 858](#).
-
- NOTE:** Only one single object of type `OSVConnection` can be assigned to each Telematic APL. It cannot be added via a configuration file but only via the configuration GUI of the telematic service.
After the object has been configured via the configuration GUI of the telematic service, you can change its settings using a configuration file.
Objects of type `OSVConnection` cannot be deleted using a configuration file.
-
- `<Extension>`
Specifies the most important settings of an extension. These are documented in [Section 10.9.3, “Extensions”, on page 824](#).
 - `<Phonemail>`
Specifies the most important settings of a PhoneMail entity. These are documented in the following sections:
 - `ScriptName`:
[Section 10.4.3.1, “Configuration Tab General”, on page 639](#)
 - `TTMEnabled` and optional TTM settings:
[Section 10.4.3.12, “Parameter Tab OpenScape”, on page 649](#)
 - All other settings:
[Section 10.4.3.8, “Parameter Tab General”, on page 641](#)
 - `<Tenant>`
Specifies the settings of a tenant. These are documented in the *OpenScape Xpressions V7, Multi Tenancy, Administrator Documentation* manual.
 - `<NCOSite>`
Specifies the settings of an NCO site. These are documented in [Section 9.9.5.1, “Editing Locations”, on page 449](#).
 - `<NCOConnectPoint>`
Specifies the settings of an NCO Connect Point. These are documented in [Section 9.9.4.2, “Editing Connect Points”, on page 446](#).

Action parameters

There are the following `Action` parameters that determine how the relevant object sections are processed during the import.

- CPAction
- NCOSiteAction
- ScriptAction
- ExtensionAction
- TenantAction

You can specify one of the following values for the various `Action` parameters:

- `add`
Adds the relevant object to the XPR server configuration newly.
- `delete`
Removes the relevant object from the XPR server configuration.
- `modify`
Changes the settings of the relevant existing object.

Calling Number Schema

If a call is forwarded from the XPR server to OpenScape UC Application or vice versa as Trusted Transfer Mode, different information must be exchanged between the XPR server and OpenScape UC Application with the forwarding (cf. [Section 10.1.3.1, “How the Trusted Transfer Mode operates”, on page 532](#)). The calling number schema specifies in which format this information is exchanged.

The calling number schema consists of the start character to be used and several consecutive sections in the format:

%<*Argument Index*>\${<*Argument Length*>

The single elements of a section specify:

- **Argument Index**
A running number that serially numbers the different consecutive arguments of the user information.
- **Argument Length**
The permanent data length of the relevant argument.

Example:

Fixed phone number format: <S><TD><ORG><ANI><UID><OTUI><LNG>
Calling number schema: p*%1\$2%2\$1%3\$13%4\$4%5\$2%6\$2 *
Originator number: *90492404000554855486106

* **Important:**
Only the highlighted schema parts can be individually configured via the `CallingNumSchema` parameter. All other settings are reset to the respectively displayed default value as soon as you invoke the TTM settings in the Telematic GUI.

Decoded this results in:

- Start sign (S) : *
- Trusted Domain (TD) : 9
- Original system (ORG) : 0
- ANI : 4924040005548

NOTE:
If the extension features different lengths, dial the longest one.

- User ID (UID) : 5548

NOTE:
The user ID corresponds to the voicebox number entered for the relevant user in the **VOICE#** database field of the XPR Correlation database. In a TTM system environment, the length of this number may vary with the user. In this case the longest of possible user ID lengths must be configured for the user ID argument in the calling number schema.

- Original TUI User Entry Point (OTUI) : 61
- Language (LNG) : 06

NOTE:
If the transferred language is not available for the voice portal, the voice portal TUI is played in the language configured as default language for the relevant voice portal access.

In the example, argument length 13 has been configured for parameter 3 (%3) – the example thus works with 13-digit E.164 numbers.

If you wish to use another length for the extension, you need to configure another argument length for parameters 3 and 4. In doing so please note that the total length of the phone number expression must usually not exceed a maximum length. This length is defaulted by the communications system used.

NOTE:

Maximum lengths for the phone number expression:

- OpenScape Voice: 24 characters
 - HiPath 4000: 22 characters
-

NOTE:

If you change the calling number schema, you need to perform this change for OpenScape UC Application as well as for the XPR server.

28.3.3 Importing the Configuration File

You need to import the site and tenant settings of a configuration file in the XPR server. They are imported automatically after you have stored the configuration file in the FI APL's relevant storage folder.

Start the configuration

How to import the configuration file with the site and tenant settings in the XPR server:

1. Copy the desired configuration file to the storage folder you have configured for the import script (cf. [Section 28.3.1, “Configuring the Configuration Script”, on page 1427](#)).
2. If required, rename the file as `ipapl.xml`.
3. Wait at least as long as you have specified for the import script under **Poll rate** (cf. [Section 28.3.1, “Configuring the Configuration Script”, on page 1427](#)).

The site and tenant settings have now been imported in the XPR server.

28.4 Copying Users from OpenScape UC Application

You can install the supplied FiSym protocol to integrate the XPR server with OpenScape UC Application. This protocol imports user data exported from the Common Management Portal and creates these users on the XPR server.

NOTE: If more than one XPR server or OpenScape UC Application is to be integrated, then you find the corresponding information in the *OpenScape UC Application Configuration and Administration* manual.

28.4.1 Installing the XPR Import Script

All user accounts must be imported from OpenScape UC Application into the XPR user database for the XPR connection to operate smoothly. In particular, the logon data of all users must be transferred to the XPR user database so that users can also log on to the XPR server with their access data.

The user accounts are automatically imported by an import script, which you need to install for the XPR server FI APL.

Start the configuration

How to install the FI APL import script:

1. Access the following directory on the XPR server product data carrier:

```
XpressionsInstall\AddOn\UCApplication\FiSym
```

2. Copy the `FiSym.e` file from this directory to the following directory of the XPR server setup:

```
<XPR Install>\res\FiApl
```

3. Create a new storage directory on the XPR server computer system.

Example: `<XPR Install>\res\FiApl\OscUserImport`

The FI APL shall later search this directory for files that it can read into the XPR server.

NOTE:

The XPR server requires system privileges for reading from the newly created storage directory.

You have now installed the XPR server import script.

28.4.2 Configuring the XPR Import Script

After you have installed the import script for the XPR server FI APL you need to configure this script. Its task is to automatically import files from the storage directory just created into the XPR server.

Start the configuration

How to configure the FI APL import script:

1. Open the XPR monitor and log on with an administrator account.
2. Select the FI APL settings in the XPR monitor's modules window.

The FI APL configuration dialog opens.

3. Switch to the **Protocols** tab.
4. Select **Add** and add the `FiSym.e` script.

The `FiSym.e` script is now displayed on the **Protocols** tab.

5. Mark the `FiSym.e` script on the **Protocols** tab and select **Properties**.
6. Specify the storage directory you have created in [Section 28.4.1, "Installing the XPR Import Script", on page 1435](#) in the **Poll directory** field.
7. In the **Poll rate** field specify the intervals in which the FI APL is to search the poll directory for new files to import them.

Setting **0** (INFINITE) deactivates the automatic search.

A reasonable value would be e.g. 10 seconds.

8. Select **OK** to copy the settings for the script.
9. Select **OK** to copy the settings for the FI APL.

The import script for the FI APL is now configured. The actual import mechanism is now already functional.

28.4.3 Creating an Import File

In the meantime you have configured the import mechanism that will import all user accounts into the XPR user database.

For the actual import you now need an appropriate import file that contains the relevant information of all user accounts.

NOTE:

An import file must always contain all user accounts of OpenScape UC Application that are to access the OpenScape Voice Portal via the PhoneMail script by Trusted Transfer Mode.

For: A user account of the XPR user database is automatically deleted during the import if it was originally imported from the Common Management Portal but is not contained in the current import file any more.

Start the configuration

How to create an import file with all user accounts:

1. Select the domain the user accounts of which are later to be contained in the import file from the **Domain** selection list of the CMP system bar.
2. On the **Operation & Maintenance** navigation tab of the CMP click on **Recovery**.
3. Click on **Import & Export > Export** in the navigation tree.

The configuration export window opens.

4. Select the check box of the **Domain Management** component.
5. Click on **Export**.

The selected data is loaded to the client PC as Zip file.

6. Open or save the file as usual.
7. Click on **Close** to close the export window.

You have now created an import file that contains the relevant user information of all user accounts.

28.4.4 Importing an Import File

The user accounts of the just created import file must now be imported into the XPR user database.

They are imported automatically after you have stored the import file in the APL's storage folder.

NOTE:

An import file must always contain all user accounts of OpenScape UC Application that are to access the OpenScape Voice Portal via the PhoneMail script by Trusted Transfer Mode.

For: A user account of the XPR user database is automatically deleted during the import if it was originally imported from the Common Management Portal but is not contained in the current import file any more.

Start the configuration

How to import the import file with all user accounts into the XPR user database:

1. Copy the just created import file to the storage folder you have configured for the import script (cf. [Section 28.4.2, "Configuring the XPR Import Script", on page 1436](#)).
2. Wait at least as long as you have specified for the import script under **Poll rate** (cf. [Section 28.4.2, "Configuring the XPR Import Script", on page 1436](#)).

The user accounts have now been imported into the XPR user database.

28.4.5 Password and PIN

In case of an import the users are automatically assigned the "password" password and the PIN "1111". If you desire other defaults here, you can achieve this via the registry values **Password** (REG_SZ) and **Pin** (REG_SZ) in key FiAPL\FiSYM. Both keys are unencrypted.

29 Web Services (XML APL)

This chapter provides information on the following topics:

- [Functional Range of the XML APL](#)
- [XML APL Structure](#)
- [Specific Connections via the XML APL](#)
- [XML APL Configuration](#)
- [Standards supported in the XML APL.](#)

29.1 Functional Range of the XML APL

The XML APL serves as an interface via which the XPR server functions are provided as Web service.

Currently, the following features of the XPR server are available via the XML APL web services:

- Messaging
- Computer Telephony Integration (CTI)
- Access to Lotus Notes calendar data
- Access to Lotus Notes task data

29.2 XML APL Structure

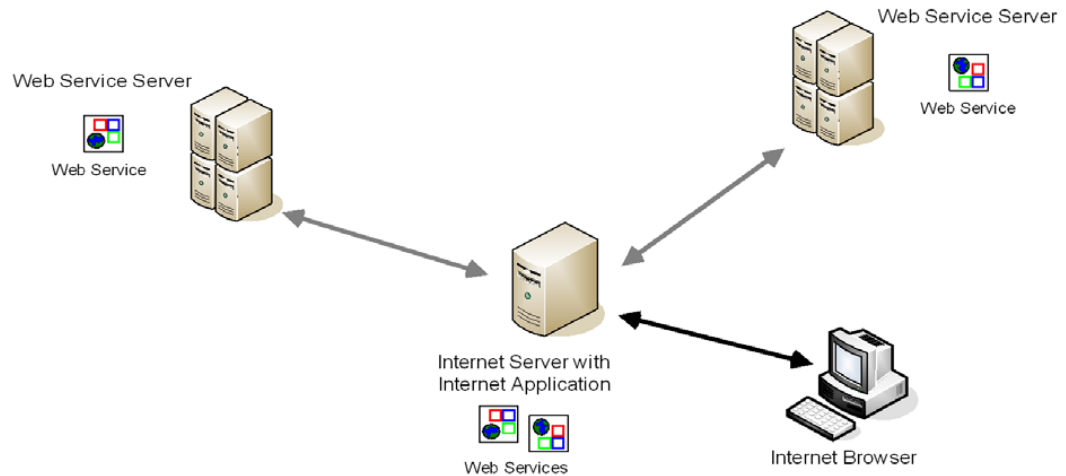
The central component of the XML APL is an integrated web service server. Its task are in particular:

- Announcing the available web services and the description of all provided functions
- Providing the web services

We will have a closer look at these tasks in the next paragraphs. But at first we will discuss what a web service is at all.

29.2.1 What is a Web Service ?

A web service is an internet application that provides services or information for another application. In contrast to a web application a web service does not address the actual internet user. Instead, it makes its web services available for other applications which will then e.g. offer internet users a combination of different web services.



29.2.2 Announcing the Web Services

A web service can only be used by another application after it has been announced as being available as service. This announcement is realized by the web service server that provides the respective service. In our case this is the web service server of the XML APL using the *WebServices Description Language* (WSDL) protocol for the publishing.

During the announcement via the WSDL protocol the following information is e.g. announced via the service:

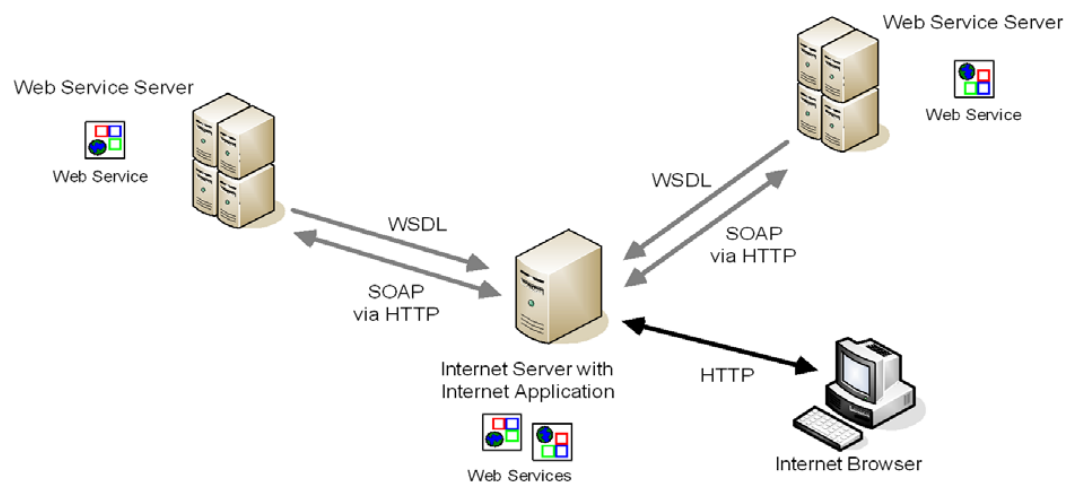
- Internet address of the corresponding web service server
- Used transport protocol
- Interface definition of all provided features

29.2.3 Providing the Web Services

If a web service has been announced by the web service server of the XML APL, other applications can also access this service. For this, they call the desired features of the service that will return all inquired information to the accessing application.

For the communication with another application, the web service server of the XML APL uses the SOAP protocol that again uses HTTP as transport protocol.

The following simplified illustration explains the communication between the web service server of the XML APL, an internet application and internet users.



29.2.4 Web Services of the XML APL

The XML APL currently provides the following interfaces that are based on web services:

- ICI interface (Integrated Communication Interface)
Offers access to TUM messaging and CTI features of the XPR server.

IMPORTANT:

The ICI interface **only** supports messaging via the Mail APL of the XPR server. It only uses TUM basic features for Messaging access to external systems.

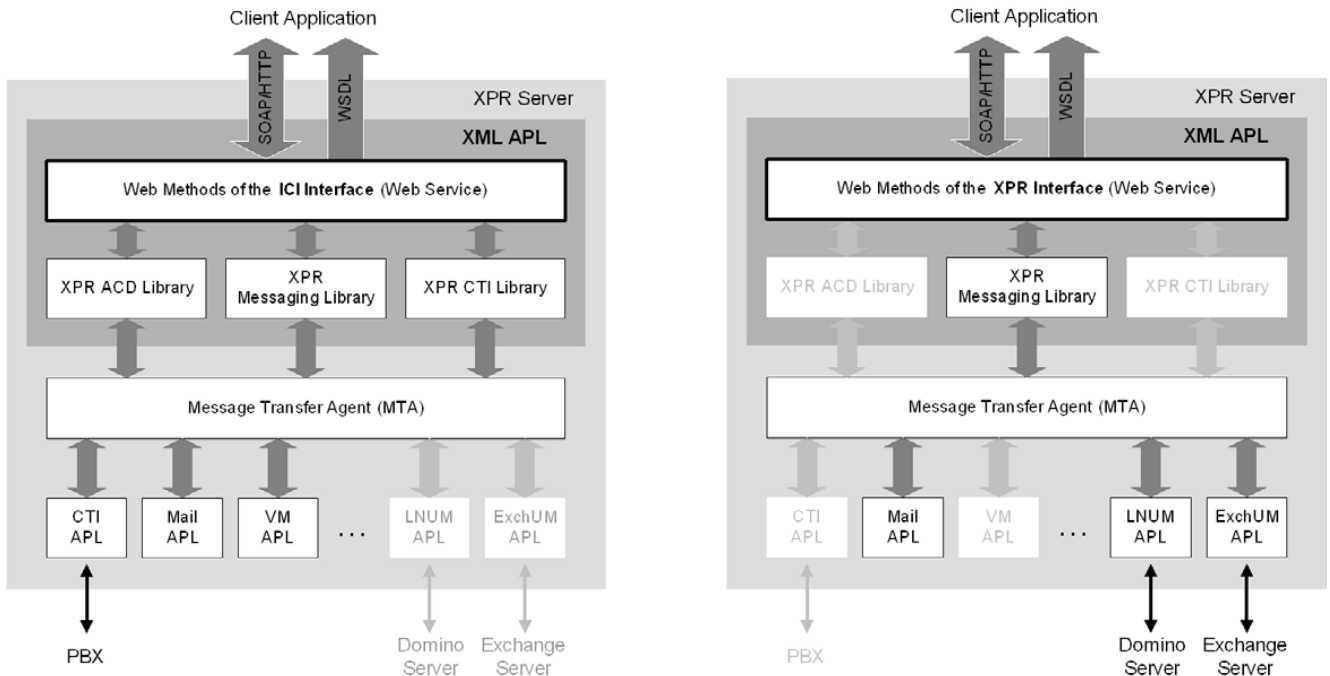
- XPR Interface
Provides access to all TUM Messaging features (basic and advanced features) of the XPR server.

NOTE:

The XPR interface uses different methods (LOGIN, LOGOUT and KEEPALIVE) to administer the connection to an external system. This solution optimizes the ICI interface procedure which realizes login/logoff at the external system for each single TUM message.

- XprCalendar interface
Offers access to the calendar and task data of Lotus Notes users.
Precondition is that the XPR server can access the associated Lotus Notes system via a Unified Messaging interface.

Now, how does a client application communicate with other components in an XPR environment via the interfaces of the XML APL? Let us consider two simple examples: communication via the ICI and XPR interface.



The ICI or XPR interface provides different web methods for external client applications that are announced via WSDL. The complexity of these methods depends on the interfaces that are used.

If a client application uses one of these methods, the XML APL calls the corresponding transaction from one of the XPR libraries. Subsequently, this transaction will be sent to the APL of the XPR server that is required for the execution of the inquired method via the MTA. The result of the enquiry will finally be transmitted to the client application via SOAP/HTTP.

Let's consider this mechanism with the help of a simplified TUM example with the XPR interface: a client application shows which messages are stored in the Lotus Notes inbox for the XPR user *Smith*.

The client application uses the GETMESSAGE web method of the XML APL and transmits the user name – *Smith*. The XML APL will then establish whether the inquired user exists at all and where the content of his inbox is stored. For this, it searches the Correlation database of the XPR server and evaluates the database field PREFERRED for the respective user. That way the XML APL detects for our example that user *Smith* is a TUM user and his inbox is administered by a Domino server.

Subsequently, the XML APL sends the TUM transactions SEARCH and LIST of the TUM Messaging library via the MTA to the LNUM APL. The LNUM APL now accesses the user's Lotus Notes inbox and sends a message about its content to the XML APL. Afterwards, the XML APL transfers this information the client application.

29.3 Specific Connections via the XML APL

This chapter describes the most important system connections via the XML APL interfaces ICI and XPR.

- [Connection of SAP R/3 Systems](#)
- [Connecting OpenScape v2.3 Systems.](#)

29.3.1 Connection of SAP R/3 Systems

SAP R/3 systems can be connected to the XPR server via the ICI interface of the XML APL. In case of this connection the following services that are provided by the XPR server are available for SAP users.

- Messaging
- Computer Telephony Integration (CTI)

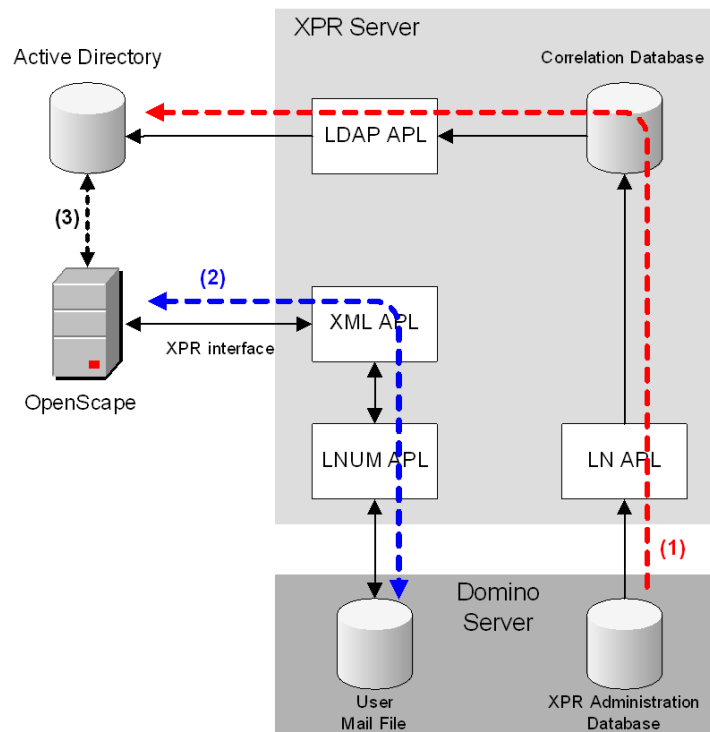
For a detailed description of the connection of an SAP R/3 system via the XML APL and ICI, please refer to the manual *SAP R/3 Gateway*.

29.3.2 Connecting OpenScope v2.3 Systems

NOTE:

This method is used for the HiPath OpenScope v2.3 product only.

An OpenScope system is connected to the XPR server via the XPR interface of the XML APL. The following illustration gives a schematic overview of such a connection.



If an OpenScope system is connected to an XPR server via the XPR interface, it is possible to distinguish between two communication processes.

1. User data replication

The LN APL replicates user data from the XPR administration database of the Domino server to the Correlation database of the XPR server. From here, all user data will be transmitted to an Active Directory via the LDAP APL. There it can be read by the OpenScope system (3).

2. TUM Access

The OpenScope system communicates with the LNUM APL via the XPR interface of the XML APL (see also [Section 29.2.4, “Web Services of the XML APL”, on page 1442](#)). The LNUM APL will then access the user mail database file that is administered on the Domino server as usual.

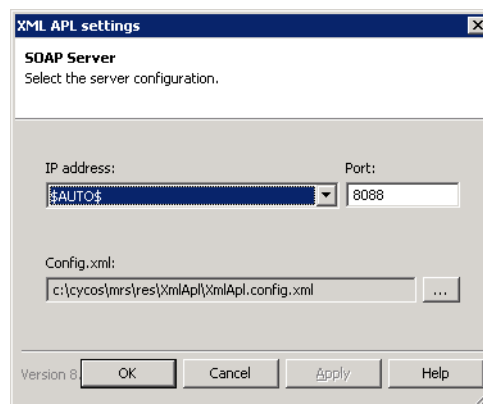
29.4 XML APL Configuration

This chapter provides information on the following topics:

- [Configuration in the XPR Monitor](#)
- [The `Config.xml` configuration file.](#)

29.4.1 Configuration in the XPR Monitor

This chapter describes the XML APL configuration options that are available in the XPR monitor.



You can use the following settings for the XML APL configuration:

IP address

Defines the IP address under which the web service server of the XML APL can be reached.

A selection list is provided for the configuration of this field. This list includes: all IP addresses that exist on the computer system of the XPR server and the **\$Auto\$** setting. If this auto setting is activated, the web service server uses one of the existing IP addresses.

Port

Defines the TCP port via which the web service server of the XML APL can be reached. The default value is **8088**.

Config.xml

Defines the path under which the configuration file `Config.xml` of the XML APL is stored. The default path is `<XPR Install>\res\XmlApl`.

29.4.2 The Config.xml configuration file

IMPORTANT:

Manual modifications of the configuration file `Config.xml` can **restrict** the XML APL features or **make them unusable**.

The `Config.xml` configuration file includes all web service server settings of the XML APL. It saves the settings that are configured in the XPR monitor as well as hidden settings that must not be changed.

The structure and content of the default version of the configuration file are as follows. The settings formatted in bold may be administered in the XPR monitor.

```
<?xml version="1.0" encoding="UTF-8"?>
<waspc-config

  xmlns:waspc="urn:WaspServer"
  xmlns:trans="urn:TransportRepository">

  <!-- HTTP Server transport START -->

  <waspc:import ref="wasp46/conf/serverbase.xml"/>
  <trans:transport trans:class="WASP_HTTPTransportServer"

    trans:scheme="server-http"
    xmlns:hts="urn:HTTPTransportServer"
    hts:reuseCount="15"
    hts:reuseTimeout="30"
    hts:rwTimeout="30"
    hts:acceptTimeout="5"
    hts:chunked="true"
    hts:port="8088"
    hts:hostname="$AUTO$"
    hts:dispatcher="DefaultDispatcher"
    hts:singleThread="0"
    hts:maxSpareThreads="-1"
    hts:maxThreads="-1" />

  <!-- HTTP Server transport END -->

  <waspc:import ref="wasp46/ICI.3.0.serviceendpoints.xml" />
  <!-- waspc:import ref="wasp46/conf/openssl-http-server.xml" /-
  ->

</waspc-config>
```


29.5 Standards supported in the XML APL

The support of the standards SOAP 1.2 and WSDL 1.1 results from the use of the Systinets Web Services server (WASP server 4.6). This version derives from the year 2003 and back then, according to Systinet (<http://www.systinet.com/pr/71>), SOAP 1.2 was fully supported, furthermore, SOAP 1.1 and WSDL 1.1 was mentioned. Possible extensions of the standard after this time are, of course, not supported for the time being.

30 Connection APL

The Connection APL (CONAPL) serves two purposes. On the one hand it is a middleware to enable Remote Procedure Calls (RPC) from Java applications to the XPR server and vice versa. On the other hand it is used for managing external components. These components are server components that are not connected to the kernel as APL.

Fulfilling the middleware task, the Con APL routes function invocations between components, the so-called RPC. RPC describes the invocation of functions between different system components on different computers, which are connected by means of a network. The RPC concept is based on the client-server model, in which the client accesses the server resources, the client invokes a server function and receives a reply from the server. The RPC structure is described in detail in the RFCs 1057 and 1837.

RPC were actually implemented in different concepts. The Connection APL uses **XML-RPC** as RPC mechanism. In case of XML-RPC the sent data is encapsulated in an XML document and transmitted via an HTTP connection. Secure transmission by HTTPS is also possible. But this was not implemented here.

The Connection APL uses the XML-RPC concept to perform function invocations between the XPR server and Java applications in both directions. For using Java applications we recommend the `xmlrpc-Library` version implemented by Apache.

In XPR before version 6, the connection APL was used for connecting the *ComAssistant*. This enables the retrieval of voicemails received via XPR with the *ComAssistant*. Via True Unified Messaging (TUM), such voicemails may also be deposited on *Microsoft Exchange* or *Lotus Notes Domino* servers and played in the *ComAssistant*. This integration of the *ComAssistant* is generally still possible, but the *OpenScape Web Client* cannot be used then.

NOTE:

You can obtain detailed information about the *ComAssistant* functionality and installation from the *ComAssistant* manuals.

As of version 6, *OpenScape Web Client* is an XPR component. This client is based on the *ComAssistant*, so that voicemails can also be retrieved in there via this mechanism.

IMPORTANT:

You cannot use *OpenScape Web Client* and integrate the *ComAssistant* with Xpressions.

Using the Connection APL, any XPR server transactions can be initialized from connected Java client applications and also routed to them.

Port 10000 is used for the RPC mechanism. This port is also used by other applications such as the Network Data Management Protocol. This protocol is used by at least one backup solution. In such a case you can change the port so that the RPC mechanism works again. You need to make changes on three occasions.

1. For the Connection APL, change the registry value [HTTP_Port \[REG_DWORD\]](#).
2. For the *OpenScape Web Client*, change entry `Xpressions.remotePort=10000` in the file [xpressions.cfg](#).
3. For conferences in the JConnector:
In the `<XPR Install>\UCC\common\conf` folder you need to adjust the entry `<Property name="serverPort" value="10000" writable="true"/>` in the following files:
 - `instance_afe199e5-5d77-4342-8a54-ff736a5d0f57-localhost.xml`
 - `instance_9EA1A05C-6853-4629-8516-62CAB112AFDC-localhost.xml`
 - `instance_7e2e07f0-40cb-43bb-a488-d1efbeabdbb8-localhost.xml`

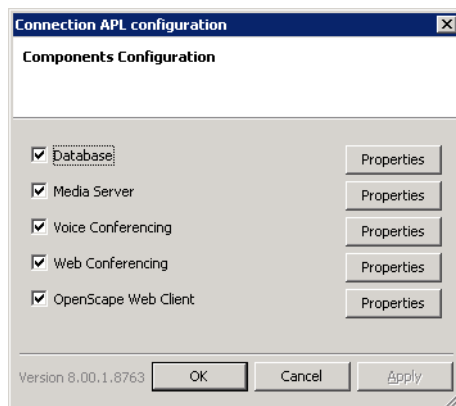
After performing these changes you need to reboot the Connection APL. To be on the safe side, reboot the XPR server.

IMPORTANT:

An upgrade will overwrite these files. Therefore, you need to perform the adjustment after an upgrade once more.

30.1 Configuration

The configuration refers to the external server components to be managed. No settings are necessary for XML-RPC, only the using application may have to be set.



The following components are managed by the Connection APL and can be configured from here:

- [Database](#)
- [Media Server](#)
- [Voice Conferences](#)
- [Web Conferences](#)
- [OpenScape Web Client](#)

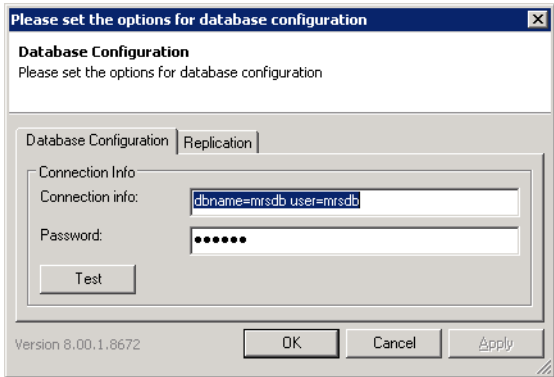
In case of a setup of external server components the Connection APL must be installed on the respective satellite as well. Depending on the components installed on the respective computers you need to activate the corresponding options in the above dialog for the associated Connection APL.

These external components partly write their own log files. All information from these log files is transferred to the XPR monitor and is thus also available in the default log files.

30.1.1 Database

The components Media Server, Voice Conferencing and OpenScape Web Client read their data from an SQL database. For this purpose, the required data is synchronized with the XPR database by replication. PostgreSQL 8.3. is used.

30.1.1.1 Database Configuration

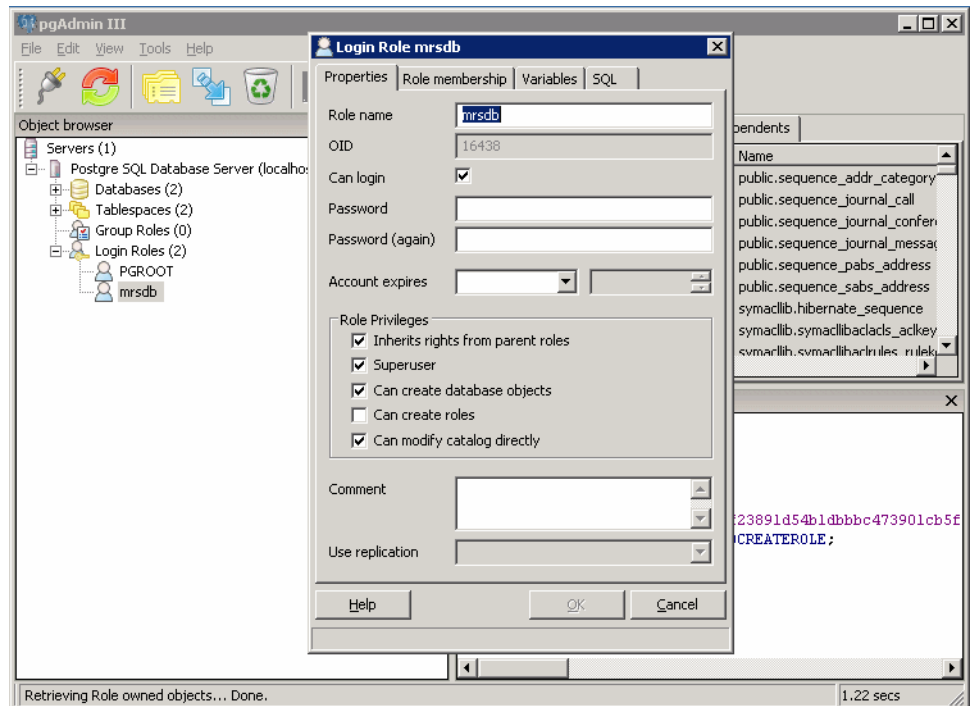


The following parameters can be specified under Connection info:

Parameter	Description
Connection info	
dbname=mrsdb	The database used within the PostgreSQL database. Must not be modified.
user=mrsdb	User for accessing the database. Must not be modified.
hostaddr=	Optional IP address of the database, if it is present on another computer.
port=	Optional port specification for accessing the database.
Password	User password. A modification must also be entered in the configuration for <i>OpenScape Web Client</i> .

Table 60 Parameters for Database Replication of the external Server Components

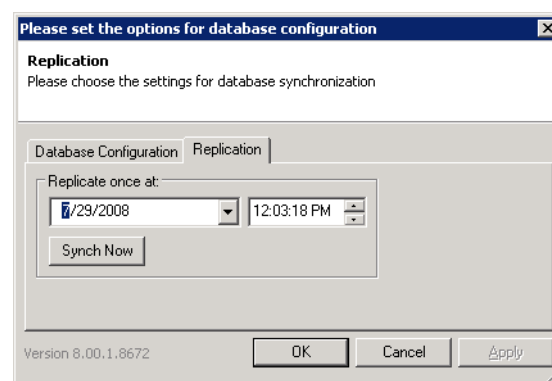
You can use the **Test** button to test the database connection. If an error occurs here, the password is likely to be incorrect. You can change the password via the PostgreSQL administration. Start **pgAdmin III** and open the **Login Roles**. In the context menu for **mrsdb** open the **Properties**. You can then change the password there.



The modified password must then be specified under the **Password** parameter and the function needs to be tested again via the **Test** button.

30.1.1.2 Synchronization

Data is automatically synchronized after each modification. Some minutes after the Connection APL start the first synchronization takes place automatically.



If the data seems to be inconsistent for some reason, you can initiate a complete data synchronization by setting a time and clicking on **Sync Now**. The time specification allows synchronization at a time with low server load.

30.1.2 Media Server

The Media Server serves as substructure of the voice conferencing service. It must be connected to the PBX via SIP. This requires configuring the following Media Server components in the associated Connection APL configuration:

- the SIP provider on the configuration tab [SIP Configuration](#)
- the Streaming provider on the configuration tab [Streaming Protocol \(RTP\)](#)
- the resource bindings on the configuration tab [Managing Resource Bindings](#).

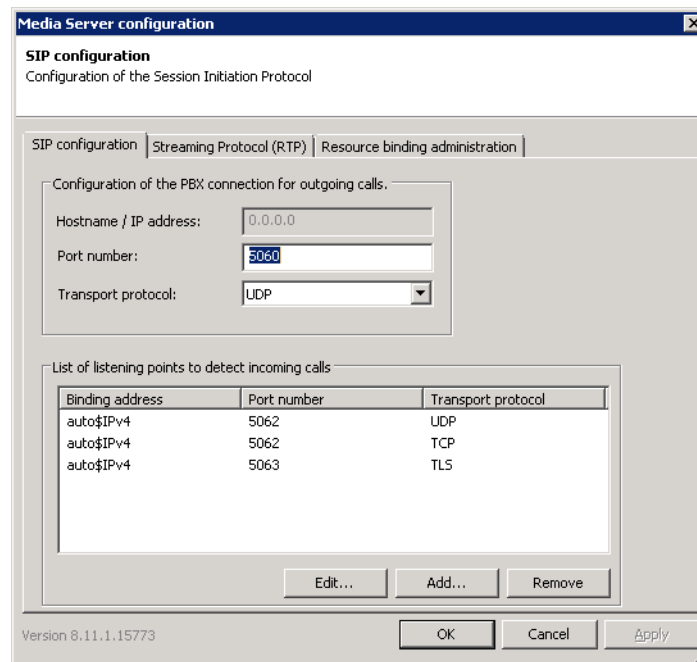
The respective configuration tabs contain the following settings.

30.1.2.1 SIP Configuration

On this tab you specify the communication settings (listening points) that the SIP provider of the Media Server uses for in and outgoing calls.

Each listening point consists of a combination of:

- Host name/IP address
- Port number
- Transport protocol.

**IMPORTANT:**

The Media Server always requires an SIP trunk for the communication. If no SIP trunk is configured in the PBX for the Media Server, the communication between the Media Server and the PBX will fail.

NOTE:

OpenScape Voice end points do not use TLS by default. If you want to use TLS you need to set the transport protocol **MTLS** for the relevant endpoints via the OpenScape Voice Assistant.

Hostname/IP address

Default: 0.0.0.0

Possible values:

- 0.0.0.0
- auto\$ipv4
- <IP address in octet format>
- <host name>

Defines the IP address of the SIP server used by the Media Server for outgoing calls. In case of OpenScape Voice this is the IP address of the SIP service manager (SIP SM).

You can also specify the host name of the associated computer system as alternative.

The default 0.0.0.0 binds to all addresses. auto\$ipv4 binds to the IP4 interface found first.

If SIP is also used on the default port 5060 via the IP APL, two IP addresses are required. Specify in this case explicitly the IP address to be used by the Media Server.

Port number

Default: –

Possible values: <port number>

Note: If a firewall exists between the Media Server and the PBX, you need to activate the port configured here in this firewall.

Defines the port number that the Media Server uses for outbound calls. Port **5060** should be set by default for the transport protocols UDP and TCP and for the transport protocol **TLS** port **5061**. Compare setting [Transport protocol](#).

Transport protocol

Default: –

Possible values:

- UDP
- TCP
- TLS

Defines the transport protocol that the Media Server uses for outbound calls.

<List of listening points for detecting incoming calls>

Displays all listening points configured for incoming calls of the Media Server. When you mark one of the list entries, you can edit the settings of the selected listening point or remove it. See [Edit](#) and [Remove](#).

Edit

Opens a dialog in which you can edit the settings of the selected listening point. See [Section 30.1.2.2, “Editing Listening Points for inbound SIP Communication”](#), on page 1457.

Remove

Deletes the selected listening point from the Media Server configuration.

Add

Opens a configuration dialog in which you can create a new listening point for inbound Media Server calls. See [Section 30.1.2.2, “Editing Listening Points for inbound SIP Communication”](#), on page 1457.

NOTE:

For each available transport protocol you can configure one listening point for incoming calls at the most.

30.1.2.2 Editing Listening Points for inbound SIP Communication

NOTE:

For each available transport protocol you can configure one listening point for incoming calls at the most.

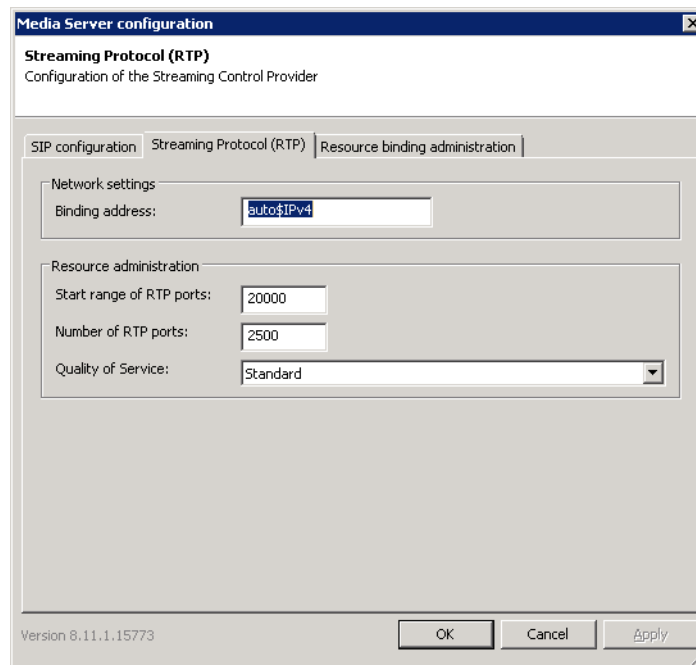
Each listening point for inbound calls contains the following settings:

- Host name/IP address
- Port number
- Transport protocol

These settings correspond to those for outbound calls (cf. [Section 30.1.2.1, “SIP Configuration”, on page 1454](#)).

30.1.2.3 Streaming Protocol (RTP)

On this tab you specify the following RTP settings that the streaming provider of the Media Server uses for the RTP communication with RTP terminal devices.



IMPORTANT:

If there is a firewall between the Media Server and the RTP terminal devices, you need to activate the RTP ports in this firewall that are configured in the Media Server for the streaming.

IMPORTANT:

To use SRTP between telephones and the Media Server, the system times of the telephones and of the Media Server must be synchronized – e.g. via the Network Time Protocol (NTP).

Bind address

Default: <is automatically determined>

Possible values: <IP address in the octet format> or `auto$ipv4`

Specifies the IP address that the Media Server uses for RTP communication on the computer system. `auto$ipv4` binds to the first IP4 interface found.

Start range of RTP ports

Default: –

Permissible values: <even-numbered port number>

Note: If a firewall exists between the Media Server and the RTP terminal devices, you need to activate the port configured here in this firewall.

Specifies the first UDP port of the port range used for the RTP-based transmission of the media streams.

An RTP transmission requires two UDP ports: one for transmitting the actual media stream via the RTP protocol and one for the RTCP protocol that monitors the connection quality. The RTP protocol uses an even-numbered port, and the RTCP protocol of the associated connection uses the next higher odd-numbered port.

Therefore, you need to specify an even number as the starting point for the port range.

Number of RTP ports

Default: –

Possible values: <whole number>

Note: If a firewall exists between the Media Server and the RTP terminal devices, you need to activate the ports configured here in this firewall.

Specifies the maximum number of UDP ports that the Media Server uses for the RTP transmission of media streams.

Since two UDP ports are reserved for one media stream (one port for RTP and RTCP each), the same number of UDP ports set here is once again allocated for the RTCP communication – even if the Media Server does currently not use RTCP.

Example: **Number of RTP ports** = 150

A total of 150 UDP ports is allocated. 75 for the RTP and 75 for the RTCP communication.

Quality of service

Default: Expedited Forwarding (EF)

Possible values: Assured Forwarding Class 1, Low Drop Precedence (AF11)
Assured Forwarding Class 1, Medium Drop Precedence (AF12)
Assured Forwarding Class 1, High Drop Precedence (AF13)
Assured Forwarding Class 2, Low Drop Precedence (AF21)
Assured Forwarding Class 2, Medium Drop Precedence (AF22)
Assured Forwarding Class 2, High Drop Precedence (AF23)
Assured Forwarding Class 3, Low Drop Precedence (AF31)
Assured Forwarding Class 3, Medium Drop Precedence (AF32)
Assured Forwarding Class 3, High Drop Precedence (AF33)
Assured Forwarding Class 4, Low Drop Precedence (AF41)
Assured Forwarding Class 4, Medium Drop Precedence (AF42)
Assured Forwarding Class 4, High Drop Precedence (AF43)
Expedited Forwarding (EF)
Precedence 1 (CS1)
Precedence 2 (CS2)
Precedence 3 (CS3)
Precedence 4 (CS4)
Precedence 5 (CS5)
Precedence 6 (CS6)
Precedence 7 (CS7)
Default

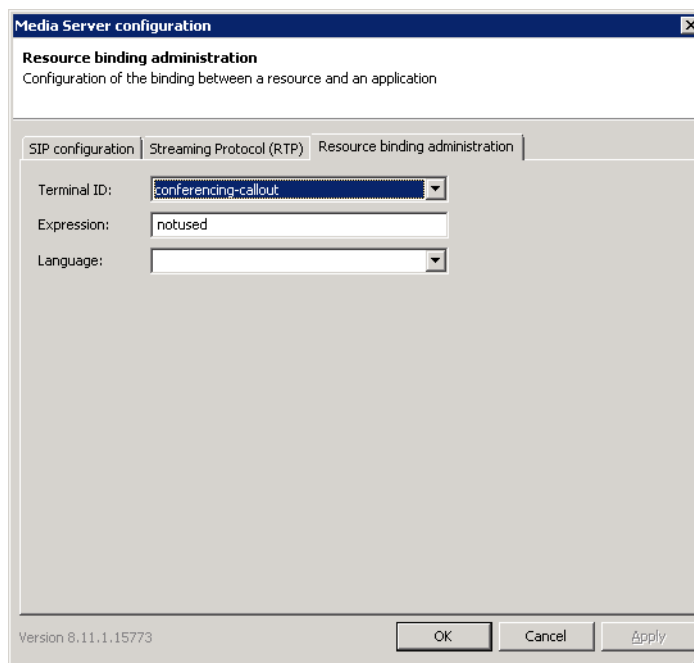
Remark: In case of OpenScape Voice, the DSCP to be used is transferred to the MGCP service of the Media Server by default. The setting performed in this field will not be used until this transfer fails.

Specifies the quality of service (DSCP) used for the RTP communication between Media Server and telephones.

The standardized service qualities can be selected.

30.1.2.4 Managing Resource Bindings

On this tab you specify under which phone numbers a media application of the Media Server is to be reached. For this purpose you use so-called resource bindings of which each represents an assignment of terminal and phone number expression.



Terminal ID

Specifies the terminal of the relevant address binding. A specific media application is bound to each terminal ID in the Media Server.

NOTE:

XPR does not support outbound connections. No number must be configured for the *call-out terminal*. It does not serve for configuring the behavior in case of a possible outbound connection. The bridge number is always used as phone number for an outbound connection.

Expression

Defines the phone number expression of the relevant media application.

The phone number expression appears in the format: complete user portion of a phone number URI consisting of digits and possibly a leading +-sign.

IMPORTANT: The configured number must occur in the format transferred by the PBX. Thus, in case of normalized (E.164) transfer in normalized format here as well.

Language

Defines the language used for the relevant media application of the Media Server. This setting determines the prompt language in the Media Server. If a calling user is known in OpenScape Xpressions V7, he/she will be addressed in his/her language if installed.

30.1.2.5 Configuring the OpenScape Voice Certificate in the Media Server

Creating a certificate for OpenScape Voice also creates in the scope of the proceedings described there a certificate for OpenScape Xpressions V7 used by the IP APL. The new Root certificate of OpenScape Voice is now imported in the keystore used by the Media Server, so that the TLS connection between OpenScape Voice and Media Server is encrypted.

Another requirement is keytool to be installed on the OpenScape Xpressions V7. This program is assumed to be located in the `<XPR Install>\jre\bin` directory.

1. Open a command line in this directory and execute the following command in one line:

```
keytool
  -import
  -trustcacerts
  -alias newRootCA
  -file <XPR Install>\res\certs\newRootCA.pem
  -keystore tls-keystore.jks
  -storepass password
```

2. Check that the new Certificate Authority (CA) has been added. To do this execute the following command in one line:

```
keytool
  -list
  -v
  -keystore tls-keystore.jks
  -storepass password
```

3. Stop and start the Connection APL for the Media Server to use the new certificate.

30.1.3 Voice Conferences

Such conferences are exclusively held via phone. If you configure the conference in *Microsoft Outlook* or *Lotus Notes*, resources are checked for being sufficiently available at the scheduled conference time based on the number of invited participants. Two additional conference ports are on stand-by here to have resources for two unexpected participants.

The conference server configures the conference five minutes before the actual start date. Participants can dial in shortly in advance and hear music until the conference starts. The conference starts with the second participant or, in case of a moderated conference, when a moderator dials in. Five minutes before the conference ends, resources are checked for being available for another 30 minutes. If resources are still available, the conference simply goes on. If other scheduled conferences prevent the active one from being continued, a corresponding message is played to the participants shortly before the conference ends.

You can already start an associated web conference within the entrance grace period of a scheduled conference from the Outlook or Notes plug-in.

Besides the conferences you schedule via calendar you can also start unscheduled ones. XPR checks resources every 30 minutes then and ends an unscheduled conference with a corresponding message if resources are needed for a scheduled conference.

The following components must be configured for the Media Server conference portal in the associated Connection APL configuration:

- the Media Server conference portal on the configuration tab **Conference Applet Configuration**
- the conference server on the configuration tab **Server Settings**

NOTE:

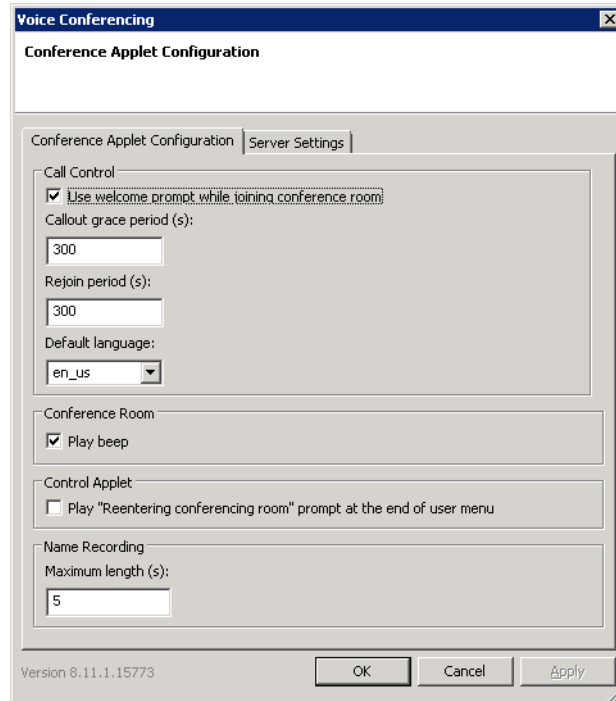
the conference server is also in charge of managing scheduled web conferences.

The conference server requires the further services ActiveMQ and Equinox. ActiveMQ is an event broker. Equinox is an OSGI container in which the conference server operates. You can compare them with an internal DLL. If required, the Connection APL starts or stops these services automatically.

The respective configuration tabs contain the following settings.

30.1.3.1 Conference Applet Configuration

On this tab you define the following individual settings for the Media Server conference portal.



Use welcome prompt while joining conference room

Specifies whether a welcome greeting is played to the conference participant when he/she logs on to the conference.

Callout grace period

Default: 30[s]

Possible values: <time>[s]

The conference portal can call participants at the start of a conference.

Callout grace period specifies how long the conference portal waits for such a call to be answered.

IMPORTANT: XPR does not support the conference portal calling participants.

Rejoin period

Default: 300 [s]

Possible values: <time>[s]

A conference participant may have to leave a conference for technical reasons – e. g. because the telephone connection is cut. If such a conference participant rejoins the conference within a specific period, he/she is automatically assigned to the previous conference without having to make any further entries.

Rejoin period specifies within which period an inadvertently disconnected conference participant is automatically reassigned to the previous conference.

Default language

Default: –

Possible values:

- de_de for German
- en_uk for English (UK)
- en_us for English (US)
- es_es for Spanish
- fr_fr for French
- it_it for Italian

Specifies in which language the conference portal represents the TUI to a caller.

Play beep

With this option being active, a short beep sounds when a participant joins the conference.

Play “Reentering conferencing room” prompt at the end of user menu

With this option being active, the “Reentering conferencing room” option is played at the end of the user menu.

Maximum length (name recording)

Default: 5 [s]

Possible values: <time>[s]

Before entering a conferencing room a user may record his/her name to be announced to the conference participants.

Maximum length (name recording) defines the maximum permissible length of this name recording. When this length is reached, the recording ends automatically.

30.1.3.2 Server Settings

On this tab you determine the following general server settings for the conference portal.

Supported Languages	Bridge Number
de_de	240863
en_us	240863

Termination grace period (s): 600

Web conferencing host address: localhost

Entrance grace period (s): 300

☐ Callout allowed

Version 8.11.1.15773

Supported Languages/Bridge Number

The installed language packages determine which languages are supported. You can enter the bridge number for a configured language here. This number must match the number configured for a language in the Media Server. See [Section 30.1.2.4, “Managing Resource Bindings”, on page 1461](#).

The numbers are listed in the E-mail notification on a conference.

Termination grace period

Default: 600[s]

Possible values: <time>[s]

This is the time at which you are informed about the nearing conference end. The termination grace period is used in different scenarios. This countdown starts, when no conference participant is left. So it gives you some time to re-enter the conference if deserting the conferencing room has occurred inadvertently.

In case of a scheduled conference this is the period in which resources are checked as to whether they are available for another 30 minutes. If they do, the conference is prolonged automatically by this half hour. If they do not, you are informed that the conference will soon come to an end.

Web conferencing host address

Default: <is automatically determined>

Possible values: <IP address in octet format> or <host name> or Fully Qualified Domain Name (FQDN)

Address for XML-RPC of the web conference server.

Entrance grace period

Default: 300[s]

Possible values: <time>[s]

This is the period in which a conference is already accessible prior to the actual (scheduled) start time. Because clocks and watches of conference participants are usually not synchronized, the entrance grace period enables every participant to dial in ahead of schedule.

Callout allowed

Defines whether the conference portal may call conference participants at the conference start. These participants may then join the conference after accepting the call.

IMPORTANT: XPR does not support the conference portal calling participants.

30.1.3.3 Configuring a Notification Text

If you configure a conference via *Lotus Notes* or *Microsoft Outlook*, all participants receive a notification, which resembles the following:

```
-----
Conference data:
-----

Dial the following number to join the conference: +xx xxx xxxxxxxx
Enter the following PIN for identification when requested: xxxxxxxx

Download the conference client under the following URL and start it: http://
xxxxx/

In the conference client, use the following data to join the conference:

Session ID: xxxxxxxx
Password: xxxx
-----
```

The notification language depends on the user language. The administrator can adjust the notification by storing the following three template files in the Conferencing folder in the \\<XPR Install>\MrsUserdata\$ structure for the desired language:

```

HEADER_{LCID}.txt
VOICE_{LCID}.txt
WEB_{LCID}.txt

```

If one of these files is missing, default notifications are sent. <LCID> is the decimal Locale ID. The following values are currently supported:

<LCID>	Language (Country)
1031	German (Germany)
1033	English (USA)
1036	French (France)
1040	Italian (Italy)
1043	Dutch (Netherlands)
1046	Portuguese (Brazil)
1055	Turkish (Turkey)
2057	English (United Kingdom)
2070	Portuguese (Portugal)
3082	Spanish (Spain)

Table 61 Supported LCIDs in Case of Conference Notifications

You may adjust the template files text arbitrarily, with the created notification being composed of all three files. The result is structured as follows:

```

-----
HEADER_{LCID}.txt
-----
VOICE_{LCID}.txt
WEB_{LCID}.txt
-----

```

IMPORTANT: The lines with 28 dashes are used for recognition. If further lines are drawn in the txt files above the dashes, the texts will not be recognized and they may be integrated in the message several times.

You can use the following wildcards in the template files. These wildcards are later replaced with the corresponding conference information:

Wildcard	Meaning
{BridgeNumber}	The voice conference access number. If several numbers have been configured, they are displayed on top of each other.
{PinNumber}	The PIN the conference participants use for logging on to the voice conference.
{WebConfClientUrl}	URL for downloading the web conference client.
{SessionID}	Web conference session ID.

Table 62 Wildcards in Conference Notifications

Wildcard	Meaning
{Password}	Web conference password.

Table 62

Wildcards in Conference Notifications

30.1.3.4 Raw Data for Statistics

The conference service writes raw data for statistic evaluation. This raw data is identical with the raw data described for OpenScape UC Application V6. To obtain details, please refer therefore to section *Structure of the Conference Portal's Statistics Data in the OpenScape UC Application V6 Configuration and Administration*.

Configuration is performed in the `instance_ConferencingStatistics-localhost.xml` file contained in the `<XPR Install>\UCC\common\conf\config-beans` directory.

NOTE:
The file has line end indications like in a Unix system. For a correct representation you can use e. g. WordPad, setting the **Word wrap** option to **No wrap**.

Setting option	Presetting	Description
EnableStatistics	False	Set this value to True to enable raw data writing.
FileName	conferencing-statistics.log	Name of the statistics files. A consecutive number is attached respectively.
FileSize	10MB	The conference portal puts out the collected raw statistics data deploying the Round Robin procedure. In doing so it uses a file system of ten files by default. Each of these files may reach a size of 10MB by default.
NumberOfFiles	10	

Table 63 *Setting Options for configuring Statistics Data of the Conference Portal*

The statistics files are stored in the `<XPR Install>\UCC\equinox\log\traces` directory.

30.1.3.5 Licenses

The available licenses are determined at the server start and then used for resource planning. The following licenses are checked for this purpose:

- Web Conferencing Room (WEBCONFROOM)
- Web Conferencing Participant (WEBCONFPARTICIPANT)
- Audio Conference Room (AUDIOCONFROOM)
- Audio Conference Channel (AUDIOCONFCHANNEL)

Resource planning uses one WEBCONFROOM and $n+2$ WEBCONFPARTICIPANT licenses for each scheduled web conference. Resource planning uses one AUDIOCONFROOM and $n+2$ AUDIOCONFCHANNEL licenses for each scheduled voice conference. n corresponds here to the number of planned conference participants. There is thus always room for two further participants that may join in on short notice. Only the number of participants expected at the start of a scheduled conference is considered. If more external participants are planned for voice conferences than external call channels are available, problems will arise at the conference start. In case of OpenScape Xpressions the room licenses are implicitly contained in the channel licenses.

IMPORTANT: You cannot change the number of conference participants during an ongoing conference. The conference's runtime starts with the first option of dialing in; thus five minutes before the scheduled conference start.

Licenses are not only checked when planning a web conference but also at runtime. A *Web Conferencing Server* (WEBCONFSERVER) license is required for each web conference server. As soon as a web conference starts, one WEBCONFROOM and one WEBCONFPARTICIPANT license is used up per active participant. Participants who have been invited but do not take part in the conference thus do not use up a license at runtime. After the web conference has ended, the allocated licenses are released again.

The available WEBCONFROOM and WEBCONFPARTICIPANT licenses are thus granted dynamically and can be distributed freely via the available web conference servers at runtime.

Voice conference licenses are not checked at runtime.

The behavior may differ subject to the client used. The Outlook as well as the Notes plug-in transfer a media type and can therefore create a pure web conference without licenses for audio conferences. In contrast, the OpenScape Web Client always creates conferences without special media type, so that conferences created via this client always require licenses for audio conferences even if you wish to exclusively use web conferences.

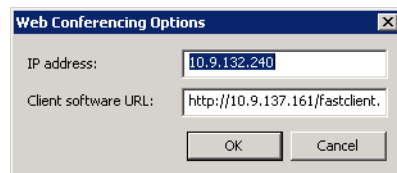
30.1.4 Web Conferences

Web conferences describe the collective use of programs and documents during real-time computer conferences. If allowed by the user, web conferences enable mirroring the desktop. In this way all other conference participants can see the same image, knowing what everybody is on about. Documents and the entire desktop can also be shared for editing. Using the additional features like, for example, chat and whiteboard, issues can be discussed and illustrated. In case of web conferences it is irrelevant where the conference participants are situated. This ensures a high degree of flexibility and saves expenses for long journeys, accommodation etc. Since all session data is transmitted encrypted (256-Bit-AES encryption), sensitive data can be transmitted as well.

The solution used here is based on a web conference server and Windows clients. The client is integrated in optiClient but is also available as independent client. This client need not be installed. It is merely started via a down load link. The client is used in a web conference scheduled in Microsoft Outlook or Lotus Notes.

NOTE:

The client is not available on the product data carrier, because the IP address of the computer that hosts the web conference server must be written on the client. The client is therefore always shipped separately.



Parameter	Description
IP address	The web conference server uses HTTPS as transport protocol for external subscribers. Enter here the IP address of the computer on which the web conference server operates.
Client software URL	Link the conference participants can use for downloading the client. It is, however, only needed if a conference is initiated via Session ID and Password according to the method used before XPR V6R2. This method may still be applied with optiClient, all other clients use the new method, where a link with coded session information is used. The client knows the IP address of the web conference server and connects to it automatically. The client itself must be stored in the setup directory of the web conferencing server. In case of an English Windows server 2008 this is e.g. C:\Program Files (x86)\WebConferenceServer\. The URL to be entered optionally here would then read http://<IP address>/client/FastClient.exe.

Table 64 Configuration Parameters for Web Conferences

NOTE:

Web conference resource planning is taken on by the voice conference server. For this server, the corresponding XML RPC communication must be configured then. See [Section 30.1.3.5, “Licenses”, on page 1471](#) for the required licenses.

NOTE:

If you configure a conference via *Lotus Notes* or *Microsoft Outlook*, all participants receive a notification. You can freely configure the notification text. See [Section 30.1.3.3, “Configuring a Notification Text”, on page 1467](#).

30.1.5 OpenScape Web Client

OpenScape Web Client is a fully developed presence management and communications control tool. With *OpenScape Web Client*, co-workers can extensively handle and monitor your voice communication from your workstation. Co-workers whose job is very much dependent on information can use *OpenScape Web Client* to manage their lines of communication and to access security-relevant company resources in realtime. *OpenScape Web Client* is a centrally configured service the features of which a user can access by web browser.

This service was developed based on the *HiPath ComAssistant*. However, instead of accessing the PBX directly or via *HiPath CAP* it is accessed here via the combination of CSTA and CTI APL. Therefore, some specialties that the *HiPath ComAssistant* used to master with specific PBXs are not possible here. Only the settings listed here were tested and released. You can test continuative configuration options via a project-specific release.

An exception is the *OpenScape Voice* PBX that is directly accessed with the CSTA APL being evaded. If only one *OpenScape Voice* is available, [MultiPBXAutoLearnMode \[REG_DWORD\]](#) must be set to 1. If several *OpenScape Voice* PBXs are available, no special configuration is required, since this configuration is automatically taken on by the corresponding CTI link of the CTI APL. Effects of this specialty:

- No NCO is used for CTI transactions. The *OpenScape Voice* rules are deployed. NCO is used for normalizing numbers that users enter themselves.
- No use of the server-based CTI journal of *XPR*.

NOTE:

The CTI journal is activated as usual. This keeps the server-based CTI Journal, too, since it is still used by e.g. *optiClient*. If the server-based CTI journal is not required, you can deactivate it via [CtiJournal \[REG_DWORD\]](#).

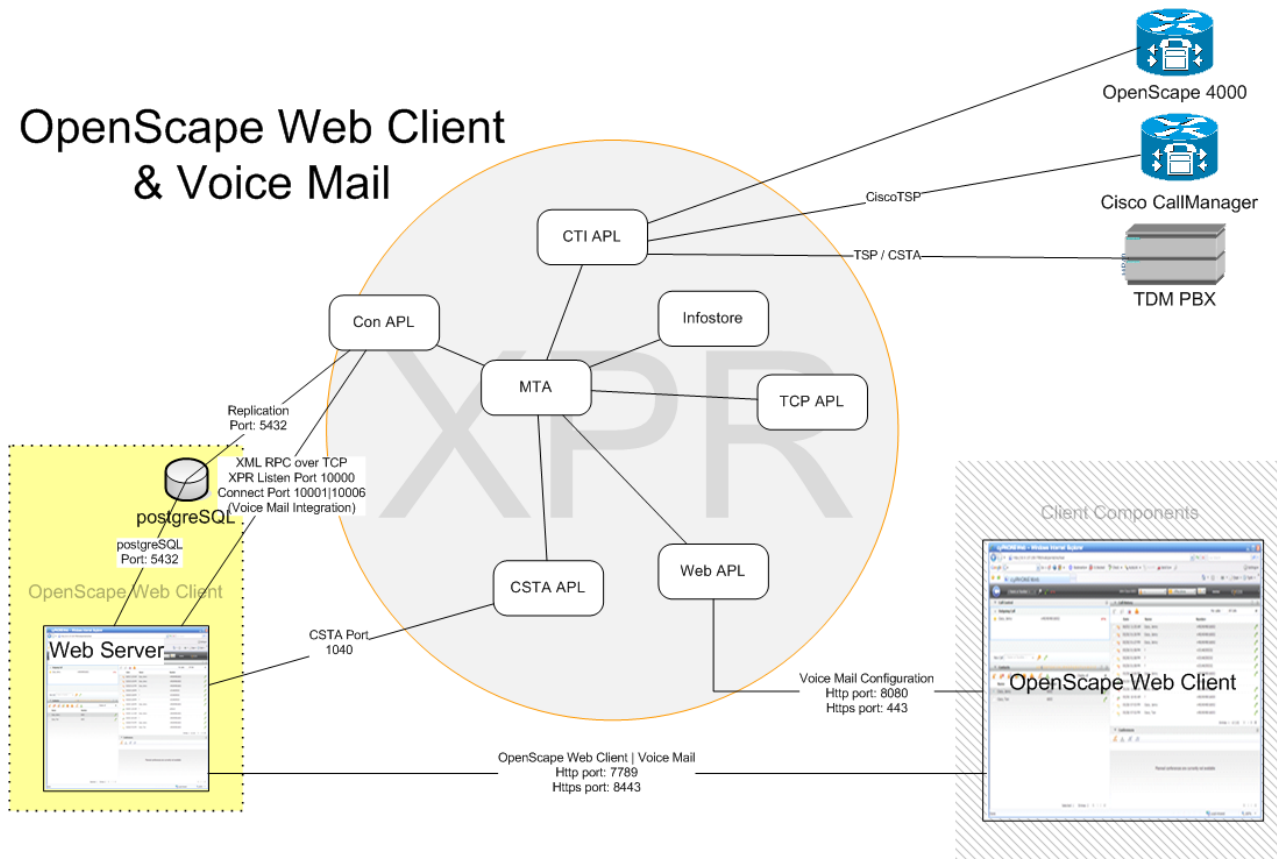
NOTE:

Parallel installation with the *HiPath ComAssistant* is not supported.

NOTE:

OpenScape Web Client writes proprietary log files. Information considered necessary is copied to the default log of the *XPR* server. The *OpenScape Web Client* log files are automatically deleted after 5 days and may occupy up to 60 GB on the harddisk.

OpenScape Web Client & Voice Mail



In this configuration dialog you specify the access data with which *OpenScape Web Client* accesses the PostgreSQL database.

OpenScape Web Client

Web Client Settings

☒ Enable SSL

Hostname: 10.9.30.20

Port: 8443

Database Settings

Hostname: localhost

Port: 5432

Username: mrsdb

Password:

OK Cancel

Parameter	Description
Web Client Settings	
Enable SSL	Access of the clients by HTTP or HTTPS.
Hostname	IP address of the server on which the application for <i>OpenScape Web Client</i> operates.
Port	Port via which the clients access the server. Please note that this setting is only used for enabling correct access to the conference control of the <i>OpenScape Web Client</i> from e.g. Microsoft Outlook. If you actually wish to change the port used for SSL you need to perform this change in the <code>ports.cfg</code> file also. See “Content of the ports.cfg file” on this. Changes made to the <code>ports.cfg</code> file do not take effect until the Connection APL is rebooted.
Database Settings	
Hostname	IP address of the server on which the PostgreSQL database is installed.
Port	Port specification for accessing the database. This port not be modified. If you still need to change it for any reason, please consult the PostgreSQL documentation for performing the corresponding change in the database as well.
Username	User for accessing the database. Must not be modified.
Password	User password. A change must also be entered with the database replication.

Table 65 Configuration parameters of the OpenScape Web Client.

30.1.5.1 Configuring the Voicemail Function

In case of the voicemail function, elements of the Web Assistant are displayed in the *OpenScape Web Client*. These elements are the voicemail inbox and the voicemail settings. Only the voicemails of the 100 messages received last are considered in the voicemail inbox. If you wish to consider more older messages here, you need to adjust the registry value [MaxNumDocsRequest \[REG_DWORD\]](#).

Perform the following adjustments for using these *OpenScape Web Client* functions with direct access to the XPR mailboxes or to mailboxes of a Microsoft Exchange or Lotus Notes environment.

NOTE:

The voicemail function is not supported in combination with VMS or Evo.

PhoneMail

So that PhoneMail can cooperate with the OpenScape Web Client, the **-con** parameter must be added to the script settings.

1. In the XPR monitor open the settings dialog of the telematics APL used.
2. Switch to the **Protocols** tab.
3. Doubleclick the **Xpressions PhoneMail** entry.
The **E-Script Protocol Properties** dialog opens.
4. Switch to the **Script** tab.
5. Click on the **Parameters** button.
The **Xpressions PhoneMail** dialog opens.
6. Switch to the **Customer** tab.
7. Enter **-con** in the entry line under Parameters.
8. Click on **OK** to copy the parameter setting.
9. Close all configuration dialogs for the telematics protocol.

xpressions.cfg

The `xpressions.cfg` file is the central configuration file for connecting *OpenScape Web Client*. After the setup it is found in the `<XPR Install>\xprWebClient\config\common` directory.

In this file the following adjustments are required:

```
Xpressions.ServerAddress=<Web Assistant URL>
```

NOTE:

The same protocol (http or https) should be used as with the *OpenScape Web Client*.

```
Xpressions.remoteIpAddr=<IP address of the computer with Con APL>
```

NOTE:

If this entry is missing, the XprProxy service terminates again immediately after the start.

```
Xpressions.remotePort=10000
Xpressions.localPort=8787
```

param.xml

The `param.xml` file is the Web APL configuration file. After the installation you find it in the `<XPR Install>\res\WebApl\Webadmin` directory. See also [Section 13.6.3, "Changing Web Assistant Default Settings", on page 946](#).

In this file the following adjustments are required:

```
ComAssistantAddress=<OpenScape Web Client URL>  
ComAssistanPort=<OpenScape Web Client port>  
ComAssistantSSLMode=<True|False>  
ComAssistantCert=cacert.pem
```

You find more information about these parameters in [Section 13.6.3.11, “Miscellaneous”](#), on page 961.

JrnService.cfg

After the *OpenScape Web Client* setup you find the `JrnService.cfg` file in the following directory:

```
<XPR Install>\xprWebClient\config\services\default\JrnService
```

So that the journal service can recognize the voicemail journal entries, perform the following setting here:

```
voiceMailDevices=<phone number>[,<phone number>]
```

It is a comma-separated list of phone numbers used by the PBX for call forwarding to XPR. Specify the phone numbers in normalized format without special characters. Example: 4924049011234.

The **Voice-Mail Box** feature can now be displayed in the *OpenScape Web Client* and the Settings menu offers the **Voice-Mail...** feature via which the user can configure his/her private voicemail settings.

Name resolution in the journal

Displaying the user names of internal callers sending voicemails requires the voicemails' subject being set correctly. If the internal mailbox is used, no adjustments need to be performed. In case of Exchange as backend, you need to adjust the display format in the Exchange APL configuration.

1. In the XPR monitor open the settings dialog of the Exchange APL.
2. Open the **Display Formats**.
3. Enter in **Subject (Voice)**:
Voice message {size} seconds <{callername}>

The pointed brackets that enclose the variable {callername} are important here.

30.1.5.2 One-Number Service

The *One-Number Service* feature enables the user to combine mobility, optimal availability and transparency towards third parties.

Via the outbound *One-Number Service* you define the device to be preferred for outgoing calls that you initiate with the help of *OpenScape Web Client*. In case of an *OpenScape Voice* the callee's display then always shows the number of the device configured for the user in the OpenScape Voice. With other PBXs the callee sees the number of the preferred device used.

The inbound *One-Number Service* enables the direct rerouting/forwarding of a call to a definable target. Such a target may be a cell phone or the voicemail box. In case of an *OpenScape Voice* this means that a caller always sees the number he/she has dialed on his/her phone display and not the number of the device on which the call was actually accepted. In case of other PBXs the number of the device actually used is displayed.

How to activate the feature:

1. Set the switch `ONS_ENABLED` in the file
`<XPR Install>\xprWebClient\config\deployment.props`
to YES.
2. Feature activation by the respective user under **menu > General > Common > Forwarding > Preferred device**. There you can configure the *One-Number Service* for **incoming and outgoing calls**.

This feature should basically work with every PBX that enables the CTI transactions Make Call, Consultation Call, Transfer Call and Deflect via the CTI APL. In case of an OpenScape Voice, the service "One-Number Service"/"One Number" must be assigned to the devices for the above specialties to work.

30.1.5.3 Team View

The Team View offers useful features for making calls within the team. You can see the team partners' telephone status and, depending on privileges, you can accept calls, forward them as well as access the team partners' journals (all calls). In addition, the team can share address books. Every user can create shared address books that can be used by a group of selected coworkers. It is then for the group to decide who may use them and which privileges apply.

How to activate the feature:

1. Set the switch `DP.SHOW_TEAMVIEW_PORTLET` in the file
`<XPR Install>\xprWebClient\config\deployment.props`
to TRUE. Add the switch if required.
2. Set the switch `TEAM_FEATURE_SUPPORTED` in the file
`<XPR Install>\xprWebClient\config\deployment.props`
to YES. Add the switch if required.

30.1.5.4 DesktopIntegration

DesktopIntegration is an application program, which can be downloaded via OpenScape Web Client. It enables you to call a subscriber from any application.

How to activate the download feature:

1. Set the switch `DITool_DOWNLOAD_ENABLED` in the file
`<XPR Install>\xprWebClient\config\deployment.props`
 to `YES`. Add the switch if required.

30.1.5.5 Default Display Mode of the Work Area

The OpenScape Web Client has three modes for displaying the work area:

- **Small view**
- **Large view**
- **Compact view**

The compact view is default set. If you want to change the default, execute the following steps:

1. Set the switch `PortalViewModeDefault` in the file
`<XPR Install>\xprWebClient\config\services\default\PortalServlet\portal_gui.cfg`
 as follows:
 - a) 0 for **large view**.
 - b) 1 for **small view**.
 - c) 2 for **compact view**.

30.1.5.6 Providing a Key for SSL Operation

Overview

OpenScape Web Client can be operated in normal or SSL mode. SSL operation requires a key information. Therefore, a demo key is installed during the setup, so that SSL operation can be temporarily used.

When using this demo key, the web browser issues warnings that this key is not a certified one. Normal SSL operation thus requires certified key equipment. You can use the demo key for the initial implementation with SSL and replace it with the official one at a later date.

The entire configuration for the backend server and all frontend servers is stored on the backend server. In case of a default setup the backend server corresponds to the installation computer. The frontend servers collect their configuration data

from there when starting up. This also applies to the SSL proxy configuration. The SSL configuration must therefore occur on the backend server and not on the frontend servers on which the SSL proxy operates.

IMPORTANT:

Even if you do not want to use SSL operation, the configuration steps described in the following sections are required, since the web clients can otherwise not be operated on the frontend servers.

Providing keys

Proceed as follows:

1. Switch to the directory `<XPR Install>\xprWebClient\distribution`. This directory contains the `.keystore_demo` file with the demo key. During the initial setup – when the `.keystore` file does not exist yet – a copy of `.keystore_demo` to `.keystore` is created.
2. Please verify that both files exist. The `.keystore` file is always used as key information for the operation.
3. If you have already acquired officially certified keys, you need to copy this key file into the `<XPR Install>\xprWebClient\distribution` directory and name it `.keystore` as described above.

IMPORTANT:

The key file for operation must always have the file name `.keystore`! The frontend server retrieves only this file when starting up! SSL operation will not work if the file with this name is not available!

30.1.5.7 Secure Sockets Layer Support (SSL)

Operation with and without SSL is standard

OpenScape Web Client can be operated on two security levels by default:

- Operation without SSL (http mode)
All pages are transmitted via the HTTP protocol.
- Operation with SSL (https mode)
The entire session is handled via HTTPS. All pages are transmitted encrypted.

For this purpose, the user may deploy different ports. All ports, the password for the SSL keystore and the name of the keystore file are stored in the `<XPR Install>\xprWebClient\config\common\ports.cfg` file and can be changed there if required by the environment.

You can also completely deactivate operation without SSL.

Deactivating operation without SSL

You may want to completely disallow operation without SSL for security reasons. Proceed as follows:

1. Open the
`<XPR Install>\xprWebClient\config\services\default\Proxy\proxy.cfg` file.
2. Remove the following three lines from the file (or comment them out). You find a corresponding comment directly on top of these lines:

```
serviceCA_HTTP0 = RP_HTTP <?x $SPW_HTTP1_PORT ?> /tweb/psmas 127.0.0.1:<?x $SPW_PSMAPPLHTTP_PORT ?> /  
127.0.0.1:<?x $SPW_WEB_PORT ?>  
  
serviceCA_HTTP1 = RP_HTTP <?x $SPW_HTTP2_PORT ?> /tweb/psmas 127.0.0.1:<?x $SPW_PSMAPPLHTTP_PORT ?> /  
127.0.0.1:<?x $SPW_WEB_PORT ?>  
  
serviceCA_HTTP2 = RP_HTTP <?x $SPW_HTTP3_PORT ?> /tweb/psmas 127.0.0.1:<?x $SPW_PSMAPPLHTTP_PORT ?> /  
127.0.0.1:<?x $SPW_WEB_PORT ?>
```

3. Reboot the Connection APL.

Content of the ports.cfg file

```
#  
# Standard Port Configuration file for ComAssistant  
#  
# Variable settings for ComAssistant port Configuration  
#  
<?x set SPW_STD_PORT = "8180" ?>  
<?x set SPW_MGMT_PORT = "8168" ?>  
<?x set SPW_CAMGMT_PORT = "6468" ?>  
  
<?x set SPW_HTTP1_PORT = "7789" ?>  
<?x set SPW_HTTP2_PORT = "7790" ?>  
<?x set SPW_HTTP3_PORT = "7791" ?>  
  
<?x set SPW_HTTPS1_PORT = "8443" ?>  
<?x set SPW_HTTPS2_PORT = "8444" ?>  
<?x set SPW_HTTPS3_PORT = "8445" ?>  
  
<?x set SPW_XML_PORT = "7778" ?>  
<?x set SPW_XMLS_PORT = "7788" ?>  
  
<?x set SPW_WEB_PORT = "8180" ?>  
<?x set SPW_PSMAPPLHTTP_PORT = "7780" ?>  
<?x set SPW_PSMAPPLXML_PORT = "7778" ?>  
  
<?x set SPW_SSL_PASSWD = "changeit" ?>  
  
#-----  
#DO NOT TOUCH THE FOLLOWING SECTION  
#-----  
  
<?x set SPW_SSL_FILE = ".keystore" ?>
```

Please note that modifications in this file should only be performed if ports conflict with those used on the setup server.

You can also change the password for creating and using the SSL key (file `.keystore`) [here](#).

Please do not change the file name. The name must be `.keystore`!

Generating another keystore file (.keystore)

If the file installed by default is not to be used, you can create a file with another private key as follows. When creating the file please be sure to use the password specified in the `ports.cfg` file identically upon the key generation. The file that contains the key must always be created directly under

`<XPR Install>\xprWebClient\` and carry the name `.keystore`!

1. Stop the Connection APL.
2. If you want to create a keystore called `.keystore` and with different content, you need to delete the existing `.keystore` file first.
3. In a command prompt window, switch to the `<XPR Install>\xprWebClient\` directory and enter the following command **coherently in one line** (you can make this specification also in a batch file):

```
jre/bin/keytool -genkey -keystore ../.keystore -storepass
<password> -keypass <password> -alias tomcat -keyalg RSA
-dname "CN=<Hostname>.<Domain>, OU=<OrgUnit>,
O=<organization>, L=<location>, C=<Country>"
```

e.g.:

```
jre/bin/keytool -genkey -keystore ../.keystore -storepass
myPasswd -keypass myPasswd -alias tomcat -keyalg RSA
-dname "CN=pc1.company.com, OU=CT SE 2, O=Company,
L=Munich, C=DE"
```

4. Thereafter, the `.keystore` file is found in the `<XPR Install>\xprWebClient\` setup directory.
5. Adjust the file content of `ports.cfg` correspondingly.
6. Reboot the Connection APL.
7. Start *OpenScape Web Client*.
The URL for logging on then reads

- for SSL:
`https://<host name>.<domain>:<SPW_HTTPS1_PORT>/`
e.g.: `https://pc1.company.com:8443/`
- without SSL:
`http://<host name>.<domain>:<SPW_HTTPS1_PORT>/`
e.g.: `http://pc1.company.com:7789/`

Keytool key and certificate management tool

With the help of the management tool `keytool.exe` you can manage keystores for private and certified public keys. You find a current description of this management tool on the web pages of the Sun Microsystems Inc. company.

Besides the tool description the path from a private to a certified key is outlined, too. You find this documentation under:

<http://java.sun.com/j2se/1.3/docs/tooldocs/win32/keytool.html>

You find further information in the internet e.g. on the Verisign page.

1. Invoke:
<http://www.verisign.de/support/ssl-certificates-support/index.html>
2. In the "Getting Started" box you find all information you require. Click there on **Generate CSR >>**.
3. In the "Instructions for All Other SSL Certificates" select the **Tomcat** application.

Managing a keystore, step by step

1. Generate a pair of keys for our Tomcat server:

```
<XPR Install>\xprWebClient\jre\bin\keytool
  -genkey -keystore .keystore -storepass changeit
  -keyalg RSA -alias tomcat
```

NOTE:

The tool guides you through entering the name portions of the object for which the key is to be created. Users who have the certificate details displayed in their browser can see this name.

IMPORTANT:

The ensuing steps mandatorily require the availability of the keystore named `".keystore"` and that contains the key you have created here.

2. Create a file with a signing request for this key:

```
<XPR Install>\xprWebClient\jre\bin\keytool
  -certreq -keystore .keystore -storepass changeit
  -alias tomcat -file tomcat.csr
```

3. Send this created file to your Certification Authority (CA).

This authority will return a file with the certificate that represents your public key signed by the CA.

4. For the following steps we assume that the file with the CA certificate is called `tomcat.crt`. If your CA is not listed in the “Cacerts file” of the JAVA runtime environment, you require a “Root Certificate” file by your CA. You need to import this certificate in the “.keystore” keystore as well.

To find out whether your CA is listed in the “Cacerts file”, switch to the setup directory

```
<XPR Install>\xprWebClient\jre\lib\security
```

and execute the following command:

```
<XPR Install>\xprWebClient\jre\bin\keytool
-list -v -keystore cacerts -storepass changeit
```

If your CA is contained in the output list, continue with [step 5 on page 1485](#). Otherwise, import the root certificate of your CA (in this example `ca.crt`) to the keystore “.keystore”. Proceed as follows:

- Import the “Root Certificate” (or all certificates of the certificate chain) by your CA in the keystore:

```
<XPR Install>\xprWebClient\jre\bin\keytool
-import -trustcacerts -alias root
-keystore .keystore -storepass changeit
-file ca.crt
```

- Answer the question whether you trust the certificate with Yes.
- If you have received a certificate chain from your CA, you need to import all certificates with different alias names.

5. Import the certificate `tomcat.crt` in your keystore:

```
<XPR Install>\xprWebClient\jre\bin\keytool
-import -trustcacerts -alias tomcat
-keystore .keystore -storepass changeit
-file tomcat.crt
```

6. Install the generated keystore:

- Copy the keystore file “.keystore” into the directory

```
<XPR Install>\xprWebClient\.keystore
```
- Start the Connection APL.
- Try to connect as follows

```
https://yourserver.yourdomain:8443
```
- If you cannot connect, check in the configuration file

```
<XPR Install>\xprWebClient\config\common\ports.cfg,
```

 which port is defined in the variable `SPW_HTTPS1_PORT`. Use this port if it deviates from the default port 8443.

7. Back up the keystore file. You may have to install it again after a software update of the *OpenScape Web Client*.

30.2 New UC WebClient and Fusion for Office Voice Mail Greeting feature (UCMODE)

A new Voicemail greeting interface has been released for UC WebClient and Fusion for Office which provides the possibility to configure the way users will have access to their VM greetings. The UC users will have the possibility to use the new greetings mode or not depending on the user configuration. It can be set a more user friendly interface for the settings of VM greetings, VM settings with advanced configurations or even disable the user VM access.

For detailed information regarding feature activation, its configuration and usage please check the *OpenScape UC Application, Configuration and Administration, Administrator Documentation*.

30.2.1 Feature prerequisites

This new feature was released starting with the following versions:

- Fusion for Office V1R8.7.0 (Build 111)
- UC V9R4 FR11
 - OpenScape UC Web Client V9.4-0.18.0-1174
- Xpressions Server XPR V7 R1 FR5 HF25 P904 or newer
 - ConApl-811FR5-20099
 - InfoTool-811FR5-20091
 - PlayWave-811FR5-20081

And the following hotfixes:

- Phonemail-811FR5-20108 or newer
- WebAssistant-811FR5-20135 or newer

30.2.2 How to change the Greeting mode using Infotool

This procedure must be done by an OpenScape Xpressions System Administrator.

You can find infotool.exe in the Xpressions server machine in the path:

`C:\OpenScape\xpr\SDKTools`

***InfoTool-811FR5-20091** hotfix or higher installation is mandatory

30.2.2.1 UCMODE parameter

The following Infotool parameters can be used in order to change the user's UC_MODE database entry.

1. UCMODE

This is the new parameter to change the Xpressions correl database entry UC_MODE.

For help please use the parameter:

```
C:\OpenScape\xpr\SDKTools> Infotool.exe help UCMODE
```

2. USER or FILE

The user can specify a single USER or a FILE with a list of users. One user in each line.

The wild card '*' can be used for USER and it will change the UC mode for all voice mail users

3. MODE

The following table describes the 5 possibilities for the administrator to configure the way users will have access to their VM greetings. It is possible to define different settings for each user.

Parameter	Name	Meaning
U	UC mode	Users will be able to record all types of VM greetings defined in UC (Default, Single, Vacation and Business). This is the option recommended for new installations. Compared to Xpressions mode, it provides a more user-friendly UI for the basic settings of VM greetings.
X	Xpressions mode (default)	Users will be able to access the full set of settings for voice mail functionality, including all different VM greetings as defined in Openscape Xpressions. This option is the default option fully compatible with all previous versions. It is the option recommended for existing installations that do not want to have changes in the current VM greetings functionality. Compared to UC mode, it provides advanced configurations.

Parameter	Name	Meaning
O	Xpressions mode with option to UC	Users will remain in Xpressions mode, but they may decide by their own to use the UC mode. This is the option recommended for old installations where the administrator wants to provide a new way for VM greetings configuration without forcing users to use it. Once users decide to use the UC mode, the users are switched to mode N (described below) and a backup of Xpressions configuration is automatically done to allow the rollback.
N	UC mode with option to Xpressions	This option should not be used for the initial configuration of the users. Users will be set automatically to this status as described above (mode O). If the users decide not to use the Xpressions mode anymore, then users are automatically set to mode U, but the administrator may give this option back to the users via using this parameter with Infotool.
D	No access	No access to VM greeting via UC webclient is given for the users. All greetings are defined by the administrator or users will have to access Xpressions Webassistant directly.

4. OPTIONS

If `OPTIONS = batch` is specified, there will be no prompt for changing each user settings. It will run the task without confirmation ('YES' to ALL)

```

Administrator: Command Prompt - infotool.exe UCMODE USER=* MODE=U OPTIONS=batch
C:\Siemens\xpr\SDKTools>infotool.exe help UCMODE
InfoTool v8.11.0(Build 20091)
(c) 1992-2019 Unify GmbH & Co. KG
InfoStor Command Line Utility

USAGE: InfoTool UCMODE USER=<username>!FILE=<user_list.txt> [OPTIONS=[batch]]
Set the user UCMODE to one of the options available.
The default option is X (Xpressions mode).
The options available are: U (UC mode); O (Old mode with shift);
                          N (New mode with shift); X (Xpressions mode);
D (Disable mode)
  if 'file' is specified, the user name must be in a text-file with one use
r in each line
  If 'batch' is not specified and wildcards are specified you are asked
interactively for update of each user.

C:\Siemens\xpr\SDKTools>infotool.exe UCMODE USER=* MODE=U OPTIONS=batch
InfoTool v8.11.0(Build 20091)
(c) 1992-2019 Unify GmbH & Co. KG
InfoStor Command Line Utility

Using namelocator @ pipe://\.\pipe\MrsNameLocatorIPC
Please enter password to continue:
  
```

30.2.2.2 UCMODE parameter usage

Open the command prompt with administrator privileges and use the following syntax:

```
Infotool.exe UCMODE USER=<username> | FILE=<user_list.txt>
MODE=[UC MODE] [OPTIONS=[batch]]
```

Set the user UCMODE to one of the options available:

The options available are U, X, O, N or D (See table above).

- If `file` is specified, the user name must be in a text file with one user in each line.
- If `batch` is not specified and wildcards are specified you are asked interactively for an update of each user.

NOTE: In this option, the wild card '*' will change the user profile for all voice mail users. And the `OPTIONS=batch` parameter will run the task without confirmation (YES to ALL)

NOTE: DBtool administrator password must be entered to proceed with the task.

Wildcards '*' and '?' can be used:

```
Infotool UCMODE USER=UserT* MODE=U
Infotool UCMODE USER=UserTest_10?? MODE=O
```

Examples:

- Change user CELTA to the UCMODE=O (OpenScape Xpressions mode with shift to the UC mode):

```
C:\OpenScape\xpr\SDKTools>Infotool.exe UCMODE USER=CELTA
MODE=O
```
- Change all users listed in the file `user_list.txt` to the UCMODE=U (UC mode):

```
C:\OpenScape\xpr\SDKTools>Infotool.exe UCMODE
FILE=user_list.txt MODE=U OPTIONS=batch
```
- Change all voice mail users in the Xpressions system to the UCMODE=X (Xpressions mode):

```
C:\OpenScape\xpr\SDKTools>Infotool.exe UCMODE USER=* MODE=X
OPTIONS=batch
```

30.2.2.3 How to change the user profile to 'Default system settings' for all mailbox users using SETVMSET parameter

This command is also added in the infotool in order to change the user configuration to the option 'Use default system settings'. Although this is not mandatory, it is highly recommended to perform this action in order to make users to start using UC greetings mode.

Example of use case:

Open the command prompt with administrator privileges and use the following syntax:

```
Infotool.exe SETVMSET USER=<username> | FILE=<user_list.txt>
```

NOTE: If 'file' is specified, the user name must be in a text file with one user in each line

In order to evict being prompted for each user change, the batch mode can be used:

```
infotool setvmset user=* OPTIONS=batch
```

NOTE: In this option, the wild card '*' will change the user profile for all voice mail users. And the 'OPTIONS=batch' parameter will run the task without confirmation ('YES' to ALL) .

NOTE: DBtool administrator password must be entered to proceed with the task.

Wildcards '*' and '?' can be used:

```
infotool setvmset user=UserT*
infotool setvmset user=UserTest_10??
```

```
Administrator: C:\Windows\System32\cmd.exe - infotool setvmset user=* OPTIONS=batch
InfoStor Command Line Utility
USAGE: InfoTool [node=<server name or address>] <cmd> [<params>]

cmd=[export|import|fulllexport|fullimport|maskexport|maskimport|
classimport|delete|rm|purge|verify|addressbook|casecheck|
quota|killuser|cleanuser|genalias|deleteold|deleteolddeleted|
resend|enumcorrel|setvmset]

Type 'InfoTool help <cmd>' to get more help about
a specific command.

Most functionality is also available from MTAs maintenance scripts,
however, the syntax of some options differs a little.
Please consult the documentation for maintenance scripts.

C:\Windows\system32>infotool setvmset user=* OPTIONS=batch
InfoTool v8.11.0 (Build 19913)
© 1992-2018 Unify GmbH & Co. KG
InfoStor Command Line Utility

Using namelocator @ pipe://\.\pipe\MrsNameLocatorIPC
Please enter password to continue:
```

30.2.3 UC_MODE database entry using CMP and HpmApl

The UC_MODE user entry can be set on Xpressions users directly via Openscape CMP User template sync with HpmApl.

For more detailed information regarding CMP usage and user sync using Xpressions Template please refer to *OpenScape Common Management Platform, Administrator Documentation*.

30.2.4 Loop detection on IpApl

IMPORTANT: LOOPDETECTION must be enable in the Xpressions IpApl protocol and must never be set to 0.

To avoid unintentional loops in SIP connection, when recording a greeting on phone and call is redirected to the Voice mail for example. It is strongly recommended to activate the SIP loop detection in the OpenScape Xpressions IpApl.

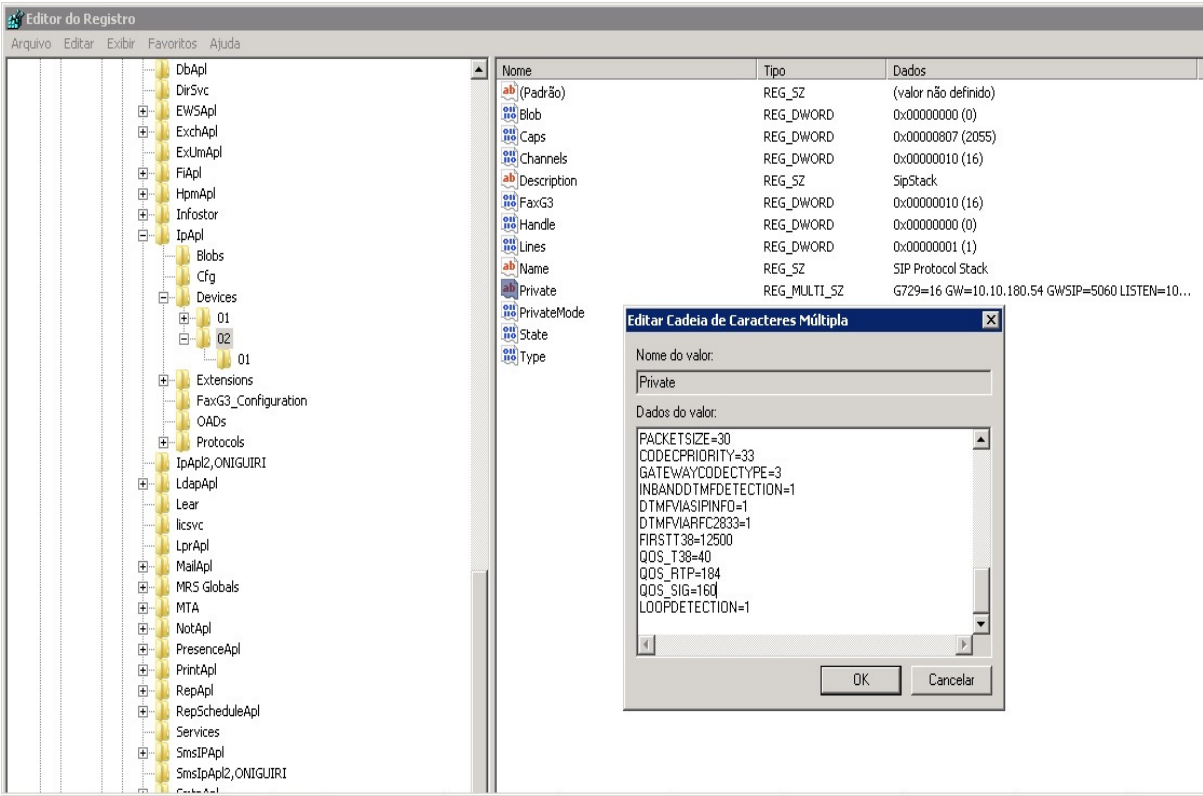
The following registry key must be verified:

HKLM\Software\Wow6432Node\PP-COM\MRS\IpApl\Devices\02\Private

Please check IpApl registry settings

LOOPDETECTION parameter inside SIP Protocol cannot be present in the 'Private' registry entry or must be set to 1.

(e.g. LOOPDETECTION=1)



31 Converting Voicemail into Text (VM2TXT APL)

This APL allows converting received voicemails into text via an external service provider. Both, this text and the voicemail are then available in parallel. The voicemail contents is therefore already accessible as e-mail and need not be completely played. Another advantage is the option to look for text passages in voicemails.

Technical conversion procedure:

1. The caller leaves a voicemail.
2. XPR checks whether the recipient has the *Voicemail transcript* privilege. If so, the voicemail is handed over to the VM2TXT APL.
3. XPR requests a conversion from the external service provider (Nuance) by HTTP request. In this process, the language set for the user is deployed. If the caller spoke in another language, conversion will fail.
4. Nuance performs the conversion and stores it on its own server.
5. XPR prompts Nuance for the conversion in regular intervals and retrieves it when available.
6. The text conversion is attached to the voicemail and sent to the recipient.

NOTE: Only this last step concludes the process and the voicemail is delivered to the recipient. Voicemail delivery will thus be delayed by the conversion process.

You need to conclude a contract with the service provider (Nuance) and, in turn, you receive a URL for the conversion process and two SSL certificates. The first one is a client certificate, which secures the VM2TXT APL connection to Nuance. The second one is a root certificate, which prevents connecting the wrong server.

The server of the service provider converts the voicemail only up to the length the service provider has specified. Consequently, only part of the voicemails longer than that will be returned as text. The contract with Nuance e.g. includes an expiration date and a time contingent the customer has purchased. The converted voicemails are deducted from this time contingent. As soon as it is used up, the Nuance server will not perform any conversions anymore.

If conversion errors occur, they are put out in the default log file of the XPR server and attached as text to the voicemail instead of the converted text.

31.1 Proceedings

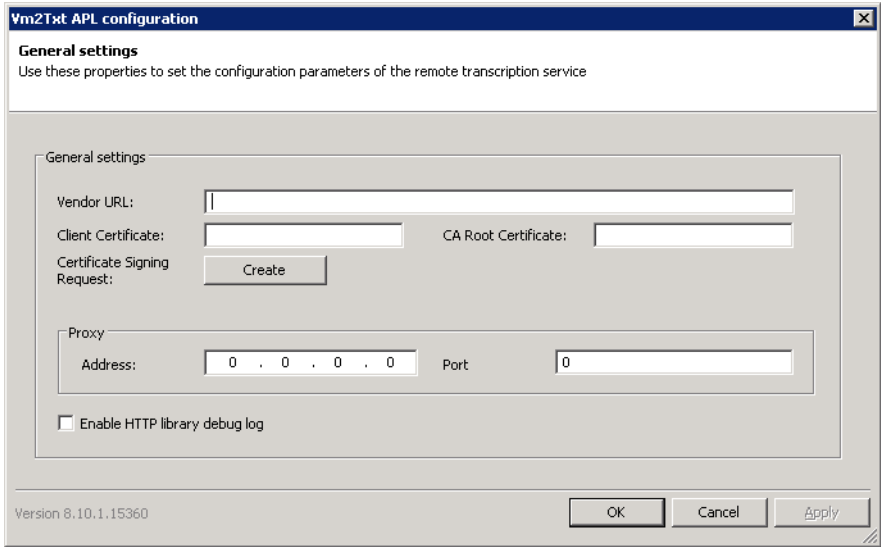
- 1. Create a **certificate signing request**.
- 2. Go to the Nuance web portal and create an account.
- 3. Send the **certificate signing request** (`NuanceCSR.pem`) to Nuance via the web portal.
- 4. Purchase the capacity you require.
- 5. Download the signed client certificate and save it under `<XPR Install>\res\certs.`
- 6. Specify the name of the client certificate in the configuration.
- 7. The Certificate Authority Root Certificate (CA Root Certificate) received from Nuance must also be saved under `<XPR Install>\res\certs` and specified in the configuration.

31.2 Configuring the VM2TXT APL

You configure the VM2TXT APL from the XPR monitor:

- 1. Open the entry **Vm2TxtApl** in the modules window under **Settings**.
- 2. Double-click on the option **Edit Settings** and enter your administrator password.

The VM2TXT APL configuration dialog is displayed.



Option	Description
Vendor URL	Conversion server URL delivered by the vendor.

Option	Description
Client certificate	File name of the client certificate delivered by the vendor. The path is always <XPR Install>\res\certs.
Certificate authority root certificate	File name of the CA root certificate delivered by the vendor. The path is always <XPR Install>\res\certs.
Certificate signing request	If you do not have received a client certificate yet, you can create a corresponding request here via Create. In addition to the request a private key is created. Both files are created in path <XPR Install>\res\certs. The name of the request is NuanceCSR.pem. The request must be sent to the vendor (Nuance). The name of the private key is NuancePrivateKey.pem.. The private key must remain in the certificate directory but should be backed up as usual. If a private key is available, creating is impossible.
Proxy	
Address	If you need a proxy server for connecting the XPR server to the internet, enter here the IP address of the proxy server.
Port	Port of the optional proxy server.
Enable HTTP library debug log	Log you can activate optionally. This log is created under the name vm2txt_curl_debug.txt in the <XPR Install>\log directory.

32 Tools

The following tools are not necessary for the regular XPR server operation, but can be perfectly used for maintenance and analyzing purposes. After the installation they are stored in the `<XPR Install>\SDKTools` folder.

NOTE:

The server and tools require administrative privileges. Therefore, select *Run as administrator* in the context menu.

CompactDB

You can use CompactDB to downsize the XPR server databases by removing data records labeled as deleted. See [Section 32.1, “CompactDB”, on page 1501](#).

CtiTest

With CtiTest you can test CTI features of the XPR server. See [Section 32.2, “CtiTest”, on page 1503](#).

DbTool

DBTool is a graphical tool for editing the entries in the Correlation Database of the XPR system for the advanced administrator. See [Section 32.3, “Database-Correl-Tool \(DbTool\)”, on page 1510](#).

ExchFailSafe

Privileges check before the installation of an Exchange connection. See the *Microsoft Exchange Gateway* manual.

InfoTool

With InfoTool you can apply various operations to the XPR databases via the command line. See [Section 32.4, “InfoTool”, on page 1529](#).

LogTool

With LogTool you can display the files of the Audit Logging. See [Section 32.5, “LogTool”, on page 1532](#).

MsgSize

This tool delivers specifications about the number and size of messages for single users and user groups. See [Section 32.6, “MsgSize Tool”, on page 1539](#).

Octel Migrator

With the Octel Migrator you can transfer Octel user data records to the XPR database. See [Section 32.7, “Octel Migrator Tool”, on page 1540](#).

OpenSSL

See [Section 12.1.5, “Secure Sockets”, on page 909](#).

RangesNCO

This command line program reads the extension ranges from the Correlation and creates an import file for the NCO Admin from this. See [Section 32.8, “RangesNCO”, on page 1550](#).

Rename Server

With this command line you can change the Windows server name or the IP address of the Windows server on which the XPR server operates. See [Section 32.11, “Rename Server”, on page 1552](#).

SystemInfo

The SystemInfo tool is not required for normal XPR server operation, but can be used for maintenance and analysis purposes very well. The SystemInfo tool is web-based and therefore requires an operating Web APL. You invoke the tool via the icon placed on the desktop.

SystemInfo offers a comprehensive overview of all relevant information and system messages. See [Section 32.16, “SystemInfo”, on page 1561](#).

SystemVersionInfo

System information output. See [Section 32.12, “SystemVersionInfo”, on page 1555](#).

Time zone support

Activates the time zone support. See [Section 32.13, “Time Zone Support”, on page 1556](#).

UnifiedLogTool

If required, you can activate logging for all clients of the XPR server. See [Section 32.14, “Logging Tool for Clients”, on page 1558](#).

XPRHFPackInstaller

This tool has the goal to automate the installing process of the Xpressions Hotfix Packages (HF). See [Section 32.17, “XPRHFPackInstaller”, on page 1561](#).

ZombiDetect

Using ZombiDetect the administrator can check the XPR Message Store integrity. See [Section 32.15, “ZombiDetect”, on page 1560](#).

32.1 CompactDB

CompactDB is used to compress the database files `correl.dat`, `distrib.dat`, `geb.dat`, `journal.dat`, and `rech.dat`, thus downsizing them. You find it in the `<XPR Install>\SDKtools` directory. Compression means that deleted entries which would otherwise only be labeled with an appropriate marker are actually removed. The maximum size of a database file is 2 GB, so that you should use CompactDB before this limit is reached.

IMPORTANT: CompactDB does not work in combination with extended database files (`correlx.dat`, `distribx.dat`, `gebx.dat`, `journal.xdat`, and `rechx.dat`), which OpenScape Xpressions V7 uses with fresh installations as of V7R1. These files are not limited to 2 GB per file, so that they need not be compressed.

IMPORTANT: The operation requires three times the size of the database files to be compressed. Make sure that at least this space is available.

IMPORTANT: CompactDB may take some time after its invocation. Schedule the invocation bearing in mind that the server must be shut down for this purpose. After the server shutdown, the following services must be rebooted manually: `licsvc`, `nameloc`, `cfgsvc`, and `xmrsvc`.

IMPORTANT: CompactDB must be invoked in the `<XPR Install>\Infostor` directory.

Invocation:

```
compactdb [correl|distrib|geb|journal|rech]
```

Without specifying a parameter, all databases are compressed; otherwise only the database specified by the parameter.

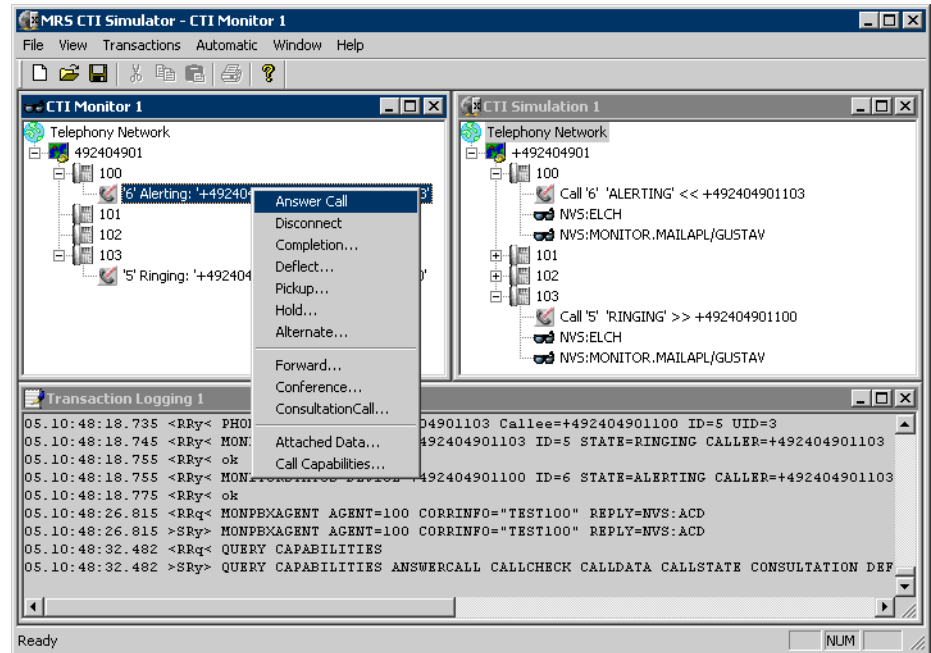
The steps you need to execute:

1. Stop OpenScape Xpressions V7.
2. Back up all database files (*.dat) in the `<XPR Install>\Infostor` directory.
3. If required, start the XPR License Server (`licsvc`) service.
4. Start the XPR Name Locator (`nameloc`) service.
5. Start the XPR Configuration Service (`cfgsvc`) service.

6. Start the XPR Status Dispatcher (xmrsvc) service.
7. Open a command line and switch to the `<XPR Install>\Infostor` directory in there.
8. Invoke `compactdb`.
9. Start OpenScape Xpressions V7.

32.2 CtiTest

CtiTest is a tool for testing the CTI features of the XPR server. It is programmed as APL for the XPR server and can therefore only be executed on a computer system on which the XPR server is installed and booted.



32.2.1 Starting the Program

IMPORTANT:

CtiTest can only be executed on a computer system on which an XPR server is installed and booted.

After the XPR server setup you find the CtiTest program in the `<XPR Install>\SDKTools` directory. Start it there with a doubleclick.

As soon as the program has been started, you see in the modules window of the XPR monitor the new entry *CtiTestApl* under *Topics*. Furthermore, the XPR server establishes the new logical line with the address *NVS:ELCH* and activates it.

32.2.2 CtiTest User Interface

CtiTest provides the following windows for testing the CTI features of the XPR server.

- CTI Monitor
- Transaction Logging
- [CTI Simulation](#)

Of these windows you will definitely need the **CTI Monitor** and **Transaction Logging** window for your work. Which other windows may be required depends on the type of test you want to perform with CtiTest.

IMPORTANT:

You may open only one window of each window type at a time.

The following sections describe the basic features of the different windows.

32.2.2.1 CTI Monitor

The **CTI Monitor** window replaces the function of a CTI client at the XPR server for testing purposes. In this window you can define terminal devices to test the CTI monitoring and CTI control of the XPR server. If you use a PBX in this process that is connected to the XPR server via the CTI APL, the terminal devices must be available at the PBX used.

CTI Monitor displays by default only the XPR server NCO location that you have configured as master location. How to display other NCO locations of the XPR server is explained in [Section 32.2.4.1, “Displaying additional Locations in the CTI Monitor Window”](#), on page 1508.

32.2.2.2 Transaction Logging

In the **Transaction Logging** window you can monitor all transactions

- that CtiTest sends to the MTA of the XPR server

Example of a sent request:

```
15.14:06:55.284 >SRq> MONITORSTATUS
DEVICE=+492404901101...
```

Example of a sent reply:

```
15.14:06:55.291 >SRy> QUERY CAPABILITIES ANSWERCALL ...
```

- that the MTA of the XPR server sends to CtiTest.

Example of a received request:

```
15.14:06:55.301 <RRq< QUERY CAPABILITIES
```

Example of a received reply:

```
15.14:06:55.330 <RRy< MONITOR Device=+492404901102 ...
```

32.2.2.3 CTI Simulation

IMPORTANT:

If you want to use the **CTI Simulation** window, you need to deactivate all CTI links of the CTI APL that may be installed in the XPR server. This ensures the sending of the CTI transactions from the MTA to the CtiTest APL.

The **CTI Simulation** window simulates a PBX connected to the XPR server. In this way you can test CTI features without actually having to connect a PBX to the XPR server.

If, for example, you establish in the **CTI Monitor** window a connection between two monitored terminal devices, you can see in the **CTI Simulation** window how a PBX with its terminal devices would react.

The **CTI Simulation** window always displays the terminal devices that are monitored by the XPR server components. This also includes the **CTI Monitor** window. Under the terminal devices the logical lines of the components that monitor the respective terminal device are displayed.

Furthermore, **CTI Simulation** always displays only the XPR server NCO location that you have configured as master location. How to display other NCO locations of the XPR server is explained in [Section 32.2.4.2, “Displaying additional Locations in the CTI Simulation Window”](#), on page 1509.

32.2.3 Working with CtiTest

The following sections will familiarize you with the most important CtiTest features.

32.2.3.1 Testing CTI Monitoring and CTI Control

This section describes the following actions for testing CTI features:

- [Configuring a terminal device for CTI monitoring and CTI control](#)
- [Testing CTI monitoring and CTI control of a configured terminal device](#)
- [Testing CTI monitoring and CTI control of a phone connection.](#)

Configuring a terminal device for CTI monitoring and CTI control

How to configure a terminal device for CTI monitoring and CTI control in CtiTest:

1. In the **CTI Monitor** window open the context menu for the location in which you want to test the CTI control and CTI monitoring of terminal devices.
2. Select **New Monitors...**
3. Enter the phone numbers of the terminal devices the CTI monitoring and CTI control of which you want to test.

NOTE:

If you use a PBX for the test that is connected to the XPR server via the CTI APL, the terminal devices must be configured and available at the PBX used.

4. Confirm your entries with **OK**.

Subsequently, the specified terminal devices with their respective stati are displayed under the relevant location.

Testing CTI monitoring and CTI control of a configured terminal device

How to test the CTI monitoring and CTI control of a configured terminal device:

1. In the **CTI Monitor** window open the context menu for the terminal device the monitoring and control of which you want to test.
2. From the context menu select the feature that you want to test for the selected terminal device.

In the **Transaction Logging** window you now see all transactions exchanged between CtiTest and the XPR server. At the same time, you can trace in the **CTI Monitor** window how the concerned terminal device status change. These status changes should also be visible in parallel at the associated terminal devices of the PBX used.

Testing CTI monitoring and CTI control of a phone connection

How to test the CTI monitoring and CTI control of a phone connection:

1. Establish a phone connection between monitored terminal devices.
This phone connection will be displayed in the **CTI Monitor** window under the involved terminal devices.
2. Open the context menu for the phone connection.
3. From the context menu select the feature that you want to test for the selected phone connection.

In the **Transaction Logging** window you now see all transactions exchanged between CtiTest and the XPR server. At the same time, you can trace in the **CTI Monitor** window how the concerned connection status change. These status changes should also be visible in parallel at the associated terminal devices of the PBX used.

32.2.3.2 Testing without available PBX

With CtiTest you can perform tests without actually having to connect a PBX to the XPR server.

To activate a PBX simulation in CtiTest, open the **CTI Simulation** window.

32.2.4 Tips and Tricks

This section provides tips and tricks on the following topics:

- [Displaying additional Locations in the CTI Monitor Window](#)
- [Displaying additional Locations in the CTI Simulation Window](#)
- [Database-Correl-Tool \(DbTool\)](#)
- [Database-Correl-Tool \(DbTool\)](#).

32.2.4.1 Displaying additional Locations in the CTI Monitor Window

NOTE:

To display another NCO location in the **CTI Monitor** window, you need to know the NCO administrator password for configuring NCO clients.

The **CTI Monitor** window displays by default the XPR server NCO location that you have configured as master location. How to display another NCO location in the **CTI Monitor** window:

1. Open the NCO-Admin.
Start the `NumberConversionAdmin.exe` program in the `<XPR Install>\bin` directory for this purpose.
2. In the NCO Admin switch to the **Clients** tab.
3. Select the **CtiTestApl** entry from the NCO clients list.
4. Create a new Connect Point and assign it the location that you want to additionally display in the **CTI Monitor** window.
5. Close the **CTI Monitor** window in CtiTest.
6. Open a new **CTI Monitor** window via **File > New > Monitor Window**.

The new **CTI Monitor** window now displays the new location besides the NCO master location.

32.2.4.2 Displaying additional Locations in the CTI Simulation Window

NOTE:

To display another NCO location in the **CTI Simulation** window, you need to know the NCO administrator password for configuring NCO clients.

The **CTI Simulation** window displays by default the XPR server NCO location that you have configured as master location. How to display another NCO location in the **CTI Simulation** window:

1. Open the NCO-Admin.
Start the `NumberConversionAdmin.exe` program in the `<XPR Install>\bin` directory for this purpose.
2. In the NCO Admin switch to the **Clients** tab.
3. Select the **CtiTestApl** entry from the NCO clients list.
4. Create a new Connect Point and assign it the location that you want to additionally display in the **CTI Simulation** window.

IMPORTANT:

The name of the new Connect Point must start with *Simulation*. Otherwise it will be displayed as new location in the **CTI Monitor** window.

5. Close the **CTI Simulation** window in CtiTest.
6. Open a **CTI Simulation** window via **File > New > CTI Simulation**.

The new **CTI Simulation** window now displays the new location besides the NCO master location.

32.3 Database-Correl-Tool (DbTool)

NOTE:

Since DbTool accesses the server via Named Pipes you have to be local administrator on the computer the XPR server is running on for each call.

NOTE:

Writing operations on the database require a password. Only the service personnel know this password.

32.3.1 Introduction

DbTool is a tool for editing the entries in the **Correlation Database** of the XPR system for the advanced administrator. It requires complete understanding of the database entries and the XPR server functionality. The Correlation Database is a user and system database that is administered by **Infostor** such as all other XPR databases.

The DB Tool is an alternative to the above **Infotool** for performing operations in the Correlation Database. When using the infotool, the respective commands must be entered in command line format. The DB Tool however provides a graphic tool for editing. Commands do not need to be entered manually any more, so that the knowledge about their syntax and semantics is not required. The commands are executed via a toolbar and various menus, which saves time.

IMPORTANT:

DbTool works online on the database. Each modification immediately takes effect on the XPR server.

32.3.1.1 Function

The DbTool is first of all in charge of representing the user and contact data from the Correlation Database in a clear and structured way.

The loaded Correlation data records can be modified and deleted. In addition, new data records can be generated and data records searched for and replaced. The tool can thus be used for maintaining and organizing Correlation database entries.

Furthermore, the DB Tool can be used to test an existing XPR system and to check it for errors. An arbitrary number of test users can be generated in one step and also be removed again.

The DB Tool is not recommendable for generating many users with specific defined variables. We recommend the creation of a table with the help of a spreadsheet application such as Microsoft Excel that can be imported via InfoTool with the help of the `IMPORT rec=user` option.

32.3.1.2 Start Requirements

To start the DB Tool the XPR server must have been booted. Only an operational XPR server enables the DB Tool to establish a connection to the database.

Modifications to data records and saving them takes immediate effect in the Correlation Database and lead to alterations in the system configuration. For example, modifying the group membership of users immediately leads to a changed privileges status of the respective users.

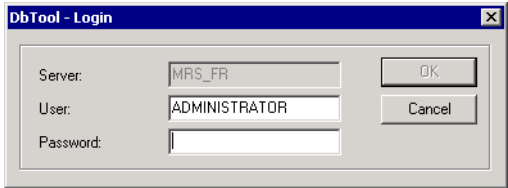
32.3.2 Start

After the installation the DbTool is stored in the <XPR Install>\SDKTools folder.

When you start the DbTool for the first time, you are prompted to specify an XPR server name. You can either select the local computer under **Local Computer** or under **Computer Name** enter the corresponding name of the XPR server. Confirm your entry with **OK**.

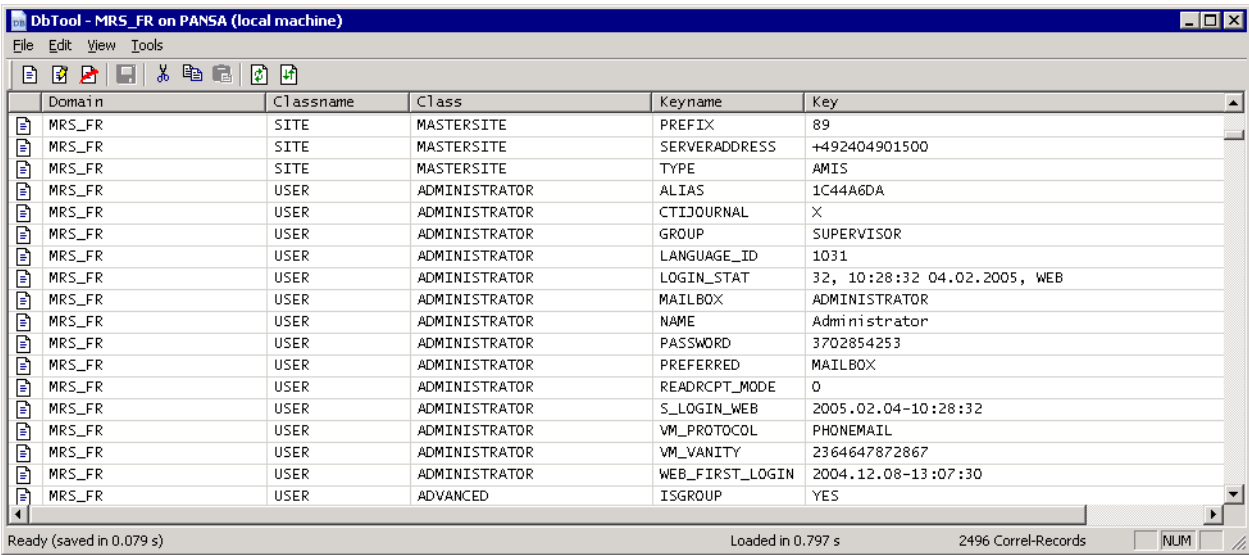
You can login at another XPR server via the DbTool at all times. In the **View** menu click the **Change Server...** option and modify the specifications.

You will then be prompted for your user account and password as with any start of the DbTool.



NOTE:
You have to login with an XPR user account which provides administrative privileges in order to be allowed to use the DbTool.

Confirm your entries with **OK** and the DbTool starts after a successful log-in. The database opens and the data are listed sorted according to the format DOMAIN<tab>CLASSNAME<tab>CLASS<tab>KEYNAME<tab>KEY. In addition, some internal fields such as ID, Update ID, Creation Time and Update Time are displayed.



If the login is incorrect, the DbTool will be started, but the database connection will not be established. You can try again to login via **Tools > Login**.

32.3.3 The Data Record Operations

There are several options available to perform the operations for data record administration. The instructions here stick to the operation by means of the toolbar. Operations that cannot be accomplished via the toolbar will be explained using the menu bar.

32.3.3.1 Operations by Means of the Toolbar

The following description refers to the sequence of the toolbar icons from left to right.

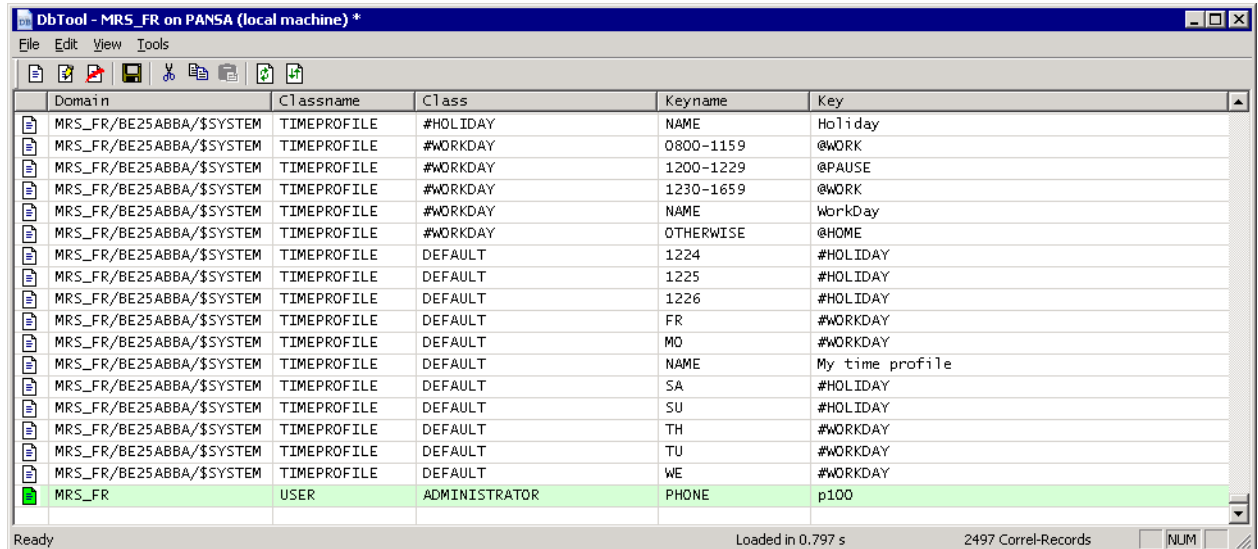
Icon	Description
	Defining a new Data Record
	Editing a Data Record
	Deleting a Data Record
	Saving a data record
	Cutting a data record
	Copying a data record
	Inserting a data record
	Updating data records
	Sorting data records

Defining a new Data Record

To insert a **new data record** proceed as follows:

1. Enable the  icon and a new, empty data record will be created at the end of the list.
2. Click on a field to release it for making entries.
3. When you have finished your entry for the respective field, click another one and the previous field closes.
4. Proceed as described in steps 2 and 3 to fill in further fields.
5. A new data record features a **green** background after the fields having been filled in.
6. Click the  icon to save the new data record. Saving the data record transforms the green background into a white one to signify that the new specifications have now been copied to the database.
7. Enable the  icon and the list is sorted. The newly inserted data record is set to its corresponding position.

8. Click the  icon to check whether the new data record has been copied to the database.



Domain	Classname	Class	Keyname	Key
MRS_FR/BE25ABBA/\$SYSTEM	TIMEPROFILE	#HOLIDAY	NAME	Holiday
MRS_FR/BE25ABBA/\$SYSTEM	TIMEPROFILE	#WORKDAY	0800-1159	@WORK
MRS_FR/BE25ABBA/\$SYSTEM	TIMEPROFILE	#WORKDAY	1200-1229	@PAUSE
MRS_FR/BE25ABBA/\$SYSTEM	TIMEPROFILE	#WORKDAY	1230-1659	@WORK
MRS_FR/BE25ABBA/\$SYSTEM	TIMEPROFILE	#WORKDAY	NAME	WorkDay
MRS_FR/BE25ABBA/\$SYSTEM	TIMEPROFILE	#WORKDAY	OTHERWISE	@HOME
MRS_FR/BE25ABBA/\$SYSTEM	TIMEPROFILE	DEFAULT	1224	#HOLIDAY
MRS_FR/BE25ABBA/\$SYSTEM	TIMEPROFILE	DEFAULT	1225	#HOLIDAY
MRS_FR/BE25ABBA/\$SYSTEM	TIMEPROFILE	DEFAULT	1226	#HOLIDAY
MRS_FR/BE25ABBA/\$SYSTEM	TIMEPROFILE	DEFAULT	FR	#WORKDAY
MRS_FR/BE25ABBA/\$SYSTEM	TIMEPROFILE	DEFAULT	MO	#WORKDAY
MRS_FR/BE25ABBA/\$SYSTEM	TIMEPROFILE	DEFAULT	NAME	My time profile
MRS_FR/BE25ABBA/\$SYSTEM	TIMEPROFILE	DEFAULT	SA	#HOLIDAY
MRS_FR/BE25ABBA/\$SYSTEM	TIMEPROFILE	DEFAULT	SU	#HOLIDAY
MRS_FR/BE25ABBA/\$SYSTEM	TIMEPROFILE	DEFAULT	TH	#WORKDAY
MRS_FR/BE25ABBA/\$SYSTEM	TIMEPROFILE	DEFAULT	TU	#WORKDAY
MRS_FR/BE25ABBA/\$SYSTEM	TIMEPROFILE	DEFAULT	WE	#WORKDAY
MRS_FR	USER	ADMINISTRATOR	PHONE	p100

You can also **cut**, **copy** data records and **paste** them in another position. These operations can be compared with those that you perform for example in the Windows Explorer or with texts in word processing systems.

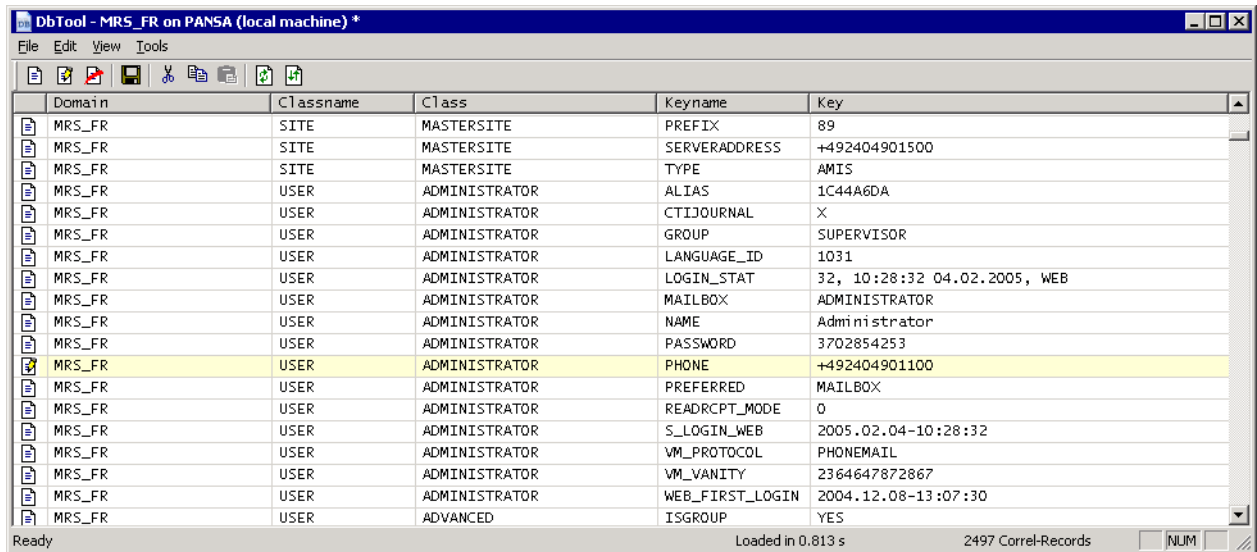
Operation	Description
Cut	To cut a data record, select it first and click the  icon. When you paste this data record in another position, it disappears in its original position.
Copy	If you want to keep the data record in its original position, you may only copy it. Select the data record and click the  icon.
Paste	To paste a data record again, select the desired position and click the  icon. Pasted data records change their background color from white to green .

Like new data record entries, pasted ones can be edited in all columns. Proceed as described under the **steps 2 to 8** for defining a new data record.

Editing a Data Record

With the **Edit Correl-Record** operation you can change the **key** of data records. How to edit data records:

1. Select the data record you want to edit.
2. Click the  icon in the toolbar.
3. The key field of the selected data record is released of modifications. Click on this field and perform your alterations.
4. When you have finished your entry, click another field and the previous one closes.
5. The edited data record changes its white background to a **yellow** one.
6. Click on the  icon for data saving. Saving the data lets the modifications take effect, so that the data record background is white again.
7. Click the  icon to check whether the modifications have been copied to the database.



Domain	Classname	Class	Keyname	Key
MRS_FR	SITE	MASTERSITE	PREFIX	89
MRS_FR	SITE	MASTERSITE	SERVERADDRESS	+492404901500
MRS_FR	SITE	MASTERSITE	TYPE	AMIS
MRS_FR	USER	ADMINISTRATOR	ALIAS	1C44A6DA
MRS_FR	USER	ADMINISTRATOR	CTIJOURNAL	X
MRS_FR	USER	ADMINISTRATOR	GROUP	SUPERVISOR
MRS_FR	USER	ADMINISTRATOR	LANGUAGE_ID	1031
MRS_FR	USER	ADMINISTRATOR	LOGIN_STAT	32, 10:28:32 04.02.2005, WEB
MRS_FR	USER	ADMINISTRATOR	MAILBOX	ADMINISTRATOR
MRS_FR	USER	ADMINISTRATOR	NAME	Administrator
MRS_FR	USER	ADMINISTRATOR	PASSWORD	3702854253
MRS_FR	USER	ADMINISTRATOR	PHONE	+492404901100
MRS_FR	USER	ADMINISTRATOR	PREFERRED	MAILBOX
MRS_FR	USER	ADMINISTRATOR	READRCPT_MODE	0
MRS_FR	USER	ADMINISTRATOR	S_LOGIN_WEB	2005.02.04-10:28:32
MRS_FR	USER	ADMINISTRATOR	VM_PROTOCOL	PHONEMAIL
MRS_FR	USER	ADMINISTRATOR	VM_VANITY	2364647872867
MRS_FR	USER	ADMINISTRATOR	WEB_FIRST_LOGIN	2004.12.08-13:07:30
MRS_FR	USER	ADVANCED	ISGROUP	YES

Ready Loaded in 0.813 s 2497 Correl-Records NUM

Deleting a Data Record

How to delete existing data records:

1. Select the data record you want to remove.
2. Click the  icon in the toolbar.
3. The data record to be deleted appears in **red**. You can remove the data record deletion indication by repeating the steps 1 and 2 with the same data record.
4. Enable the  icon for saving. Only after saving the data record deletion takes effect and the data record is removed from the database.
5. Click the  icon to check whether the data record has been removed from the database.

Restoring the old State

You can restore the state after the last saving process with a click on the  icon. A query makes sure whether or not you want to save the modifications performed. To save the modifications click **OK**, if you want to restore the state after the last saving process, click **No**. Corresponding to your selection the data are updated and put out assorted.

32.3.3.2 Operations via the Edit Menu

Selecting, finding and replacing Data Records

Besides the common operations to be simply performed via toolbar, there are further options to **Select, Find and Replace** data records.

Selecting all Data-Records

With the **Select all Correl-Records** command all database data records are selected and receive a gray background.

Selecting special Data Records

Under the **Select special...** menu option you can select the **Next changed Correl-Record**, the **Previous changed Correl-Record**, the **First Correl-Record of next User** or the **First Correl-Record of previous User**. The name of a user is in the "Class" column.

If you select the **Next changed Correl-Record** option, the marking jumps from the current position in the database list downward to the next data record that has been changed.

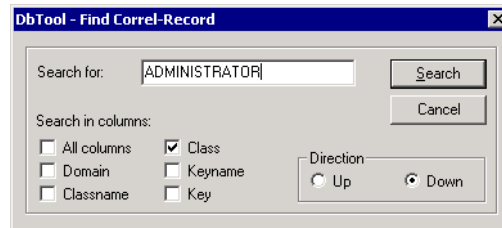
If you select the **Previous changed Correl-Record** option, the marking jumps from the current position in the database list upward to the next data record that has been changed.

The **Class** column displays the respective user with the corresponding data. With the commands **First Correl Record of next User** or **First Correl-Record of previous User** you can jump to the first data record of the user that is below or above the position of the current marking.

Finding a Data Record

How to find a data record based on specific criteria:

1. Call the **Find Correll-Record** to open a dialog.

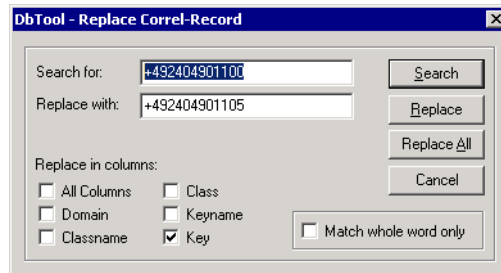


2. In the **Search for:** field enter the desired search item.
3. Of the check boxes in the **Search in columns:** portion either select **All columns** or only specific ones. To look for a search item in a specific column, remove the **All columns** indication beforehand.
4. In the **Direction** field set the search sequence to **Up** or **Down** from the currently selected position in the database list.
5. Click the **Search** button to start the process. After a successful search, the data record found is indicated in the database.
6. To find further data records that fulfill the same search criteria, restart the search via **Find Correll-Record**. Your search criteria have been saved so that you only need to enable the **Search** button to look for a data record that corresponds to your search criteria.
7. If the entire database has been searched and no further data records found that match the search criteria, the search function jumps back to the beginning of the database list. Thus the first data record found is indicated again. You **do not** receive a report when the entire list was searched.

Replacing Data Records

How to look for items in the **Key** column and replace them with other items:

1. Call the **Replace Correl-Records** command and the corresponding dialog opens.



2. In the **Search for:** field enter the search item and in the **Replace with:** field specify the desired item for the replacement.

NOTE:

The **Replace in columns:** field is without function up to now, since only items in the **Key** column can be searched for and replaced. Leave the default setting **All Columns** selected.

3. With the **Match whole word only** option you can choose whether to use the search item as independent word or as part of other items.
4. Start the search process with a click on the **Search** button. The search results are indicated in the database list. If no items are found according to the search criteria, an error report is issued.
5. A click on the **Replace** button replaces the item previously found with the search function that has been selected automatically.
6. Repeat steps 4 and 5 to have further items individually searched for and replaced.
7. The **Replace All** button replaces all items that correspond to the search criteria. After the replacement process you are informed about the number or replaced items. The modified data records appear in **yellow**.
8. Click on the  icon for data saving. Saving the data lets the modifications take effect, so that the data record background is white again.
9. Click on the  icon to check whether the modifications have been copied to the database.

32.3.4 Importing and Exporting Data

32.3.4.1 Import

You can import data from other sources. The file to be imported should contain the format string

DOMAIN<tab>CLASSNAME<tab>CLASS<tab>KEYNAME<tab>KEY in the first line . The DOMAIN specification is optional, since this column contains the server name and is automatically adapted to the current server. We recommend the file extensions **txt** or **idx**. Other file formats may not be recognized.

NOTE:

Please note that imported data records overwrite existing data records with the same class name, class and key name when they are saved in the database list.

How to import data records:

1. In the **File** menu select the **Import...** option.
2. If required, look for the file to be imported and confirm your selection with **Open**.
3. A message informs you about the successful file import. All data records that were imported appear with a **blue-green** background color.
4. If you have not imported the domain as described above, the domain column remains empty. Not until the data are saved the domain entry is automatically generated. Data records with the class names `USER`, `RUND` or `GLIST` contain `<Server>` and all other entries `<server>/$System` as domain entry.
5. A click on the  icon adds the imported data records to the database.

32.3.4.2 Export

If you want to copy data for specific purposes to another storage location, you can export them. In the **File** menu select the **Export...** option.

A window appears in which you specify the file name and the target path for the file to be exported. We recommend the file extensions **txt** or **idx**.

Example:

You can export data to view them with other programs. You can open and edit the exported file with Microsoft Excel. Numbers should be entered as strings, since Excel removes leading zeroes as with telephone numbers. In addition you should save the file in txt format again, so that it can be reimported in the DbTool.

32.3.5 Tools

In the Tools menu you can set the **user options**. By means of the user options it is possible to change **settings** for users, to **create** new users and to **delete** users. Furthermore it is possible to configure **Options...** for the DbTool and to change the **server language**.

32.3.5.1 Changing the Server Language

You can change the default language for voice mail and the Web Assistant in the menu item **Change server language**.



To select another language, mark the desired language in the default list and click **Save**.

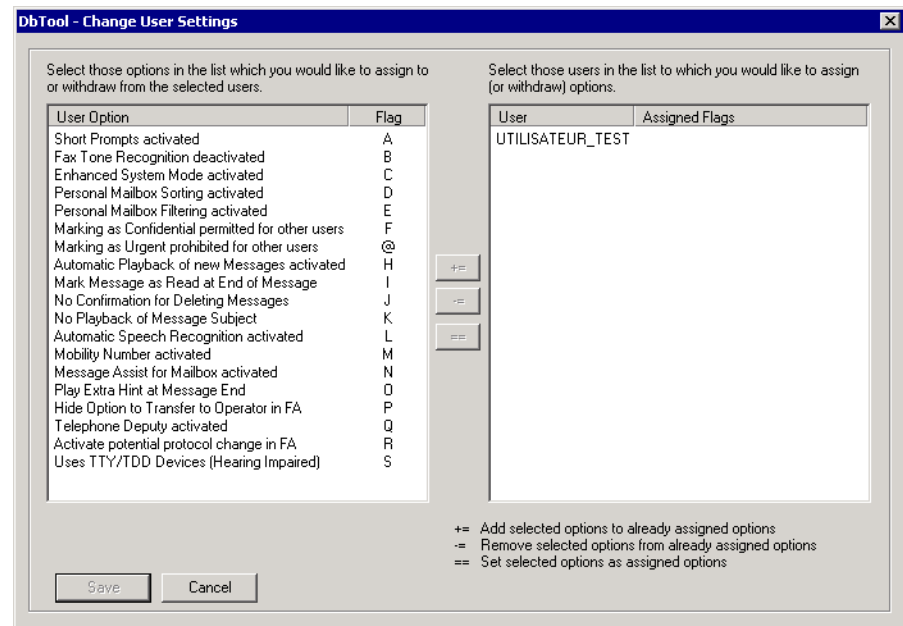
With the **Up** and **Down** buttons you can move the marking from one entry to the next on top or below. The topmost entry in the list corresponds to the language default set for new users.

The setting modifications take effect with the **Save** button.

32.3.5.2 Change User Settings

The **user settings** relate to the user voice mail settings listed in [Section 4.3.9, “User Options”, on page 106](#). The dialog for user settings alteration is divided into two sections.

The left portion shows a list with preset user options and associating flags for indication. The right portion lists the users for whom a voice entry is defined. A user will not be listed in the user list without a voice entry. The options assigned are indicated by the associating flag.



By selecting a desired user option and a user, the following operations can be performed:

Icon	Description
+=	You can assign the selected user options to the selected user with this icon.
-=	If the selected user options have already been assigned to the selected user, you can remove these user options with this icon again.
==	This icon sets the selected options as the only new option for the user and removes all previously added ones.

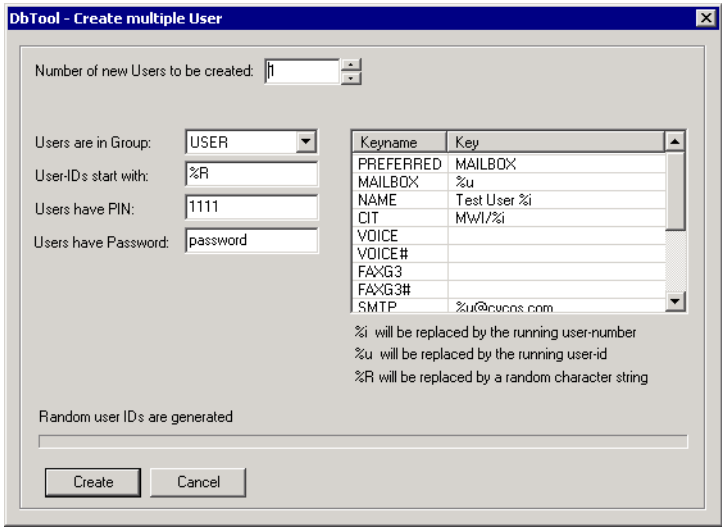
The modifications take effect with the **Save** button.

In the database list the modified entries thus appear in **yellow** and the newly generated entries are **green** highlighted.

32.3.5.3 Creating new Users

With the **Create new Users...** option you can generate as many new users as you want. This function is solely suitable for generating an arbitrary number of test users to test the system. This feature is not suitable for the creation of real user accounts.

NOTE:
In [Chapter 4, “User Data Administration”](#) of this manual, the single database fields and key names are explained in detail. To create a new user you should be familiar with the significance of the database fields.



The following table contains a description of the fields that you find in the **Create multiple User** dialog.

Field	Description
Number of new Users to be created	Enter the desired number of new users in this field.
Group	In this field you can select one of the different available user groups. The various groups have different privileges.
User-IDs start with	The %R value in this field generates an arbitrary user ID. If you want to enter a user ID, delete the %R value and make the corresponding entry. A number is automatically added to the user name as further indication. Several users defined will thus only be distinguishable by the automatically generated number at the end of the user name. The status bar in the bottom portion of the dialog displays the IDs generated for the new users.
Users have PIN	Predefined setting for the PIN number. This is the same for all users to be created.

Field	Description
Users have Password	Predefined setting for the user password. This is the same for all users to be created.
Key name/ Key	In this field you can enter the corresponding keys for specific, predefined key names. Some fields such as NAME and SMTP have predefined settings that automatically generate distinguishable keys. • %i generates the matching user number, • %u generates the corresponding user ID. You can still change these settings for a value. Double-click the corresponding field, enter the value and close the field with a click. Empty key fields as well as empty key names can also be furnished with a value. Follow the steps required for changing a value. The significance of the key names and key is explained in detail in this manual's Chapter 4, "User Data Administration".

With a click on the **Create** button the new users are added to the end of the list and green highlighted.

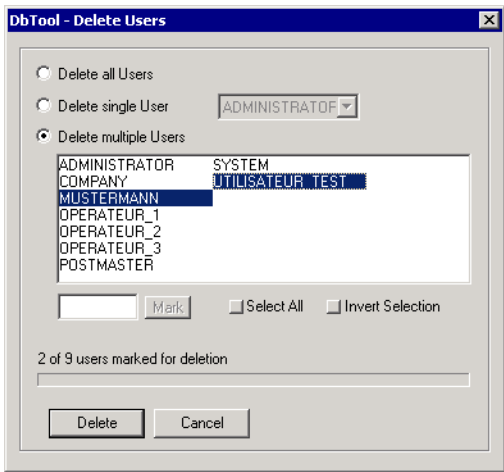
Just as with **creating new data records** you need to **save** the alterations in the list with a click on .

Then click  to **sort** the list.

Enabling the  icon you can **check** whether the new users have been integrated in the list.

32.3.5.4 Deleting Users

The **Delete Users...** option enables you to remove users. By means of check boxes you can decide whether to **Delete all Users**, **Delete single User** or **Delete multiple Users**.



Option	Description
Delete all Users	When you choose this option, all users in the database will be selected for deletion. A click on the Delete button removes the users.
Delete single User	Selecting this option activates the associating field where you can pick an arbitrary user for deletion. A click on the Delete button removes the user.
Delete multiple Users	Via this option you can in the window thereunder select as many users as you want for deletion. • Mark: With the Mark button you can select users whose names begin with specific letters in addition to the users you have selected for deletion. For example, entering an "E" marks all users beginning with E. For this selection enter the required letter sequence and click the Mark button. • Select All: With the Select All button you can mark all users for deletion. • Invert Selection: With the Invert Selection button you can remove the indication for all users selected for deletion. The users that have not been selected for deletion are simultaneously selected for deletion. This function is useful if e.g. 98 users are to be removed from a list of 100. Select the two users that are to remain in the list for deletion and click Invert Selection. 98 will be selected for deletion while the two previously selected ones remain in the list.

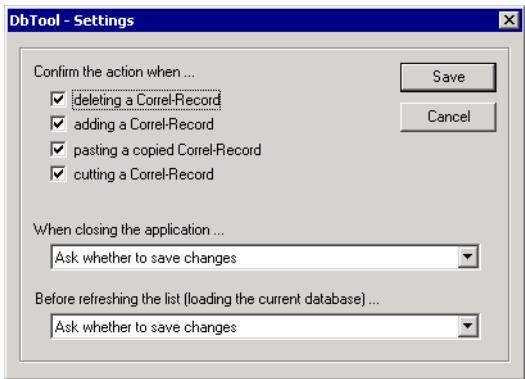
With a click on the **Delete** button the selected users are at first red highlighted.

Proceed as with **deleting data records**, by clicking the  icon to remove the selected data records from the list for good.

Enable the  icon to **check** whether the modifications have been copied to the database list.

32.3.5.5 Further Options

Via the **Options...** menu item you can perform settings for the DB Tool. With these options, queries for performing operations and queries for saving modifications are basically set.



The following table describes the options available:

Option	Description
Confirm the action when...	With this option you can determine whether to receive a query before performing specific operations. This query is to make sure that the performance of an operation is really wanted or rather abandoned. A confirmation request can be activated for the following actions : • deleting a Correl-Record • adding a Correl-Record • pasting a copied Correl-Record • cutting a Correl-Record
When closing the application...	You can choose between the following options before you stop the program: • a query for saving data, • automatic saving of the modifications in the database, • automatic dismissal of the modifications in the database
Before refreshing the list (loading the current database)...	You can choose between the following options before you update the database list: • a query for saving data, • automatic saving of the modifications in the database, • automatic dismissal of the modifications in the database

The setting modifications take effect with the **Save** button.

32.4 InfoTool

NOTE:

Since InfoTool accesses the server via Named Pipes you have to be local administrator on the computer the XPR server is running on for each call.

NOTE:

Writing operations on the database require a password. Only the service personnel know this password.

Call (Local): `INFOTOOL <Task>`

Call (Remote): `INFOTOOL node=\\<Windows Server name> <Task>`

Possible commands for `<Task>` are described in [Section 7.2, “Maintenance Script”, on page 214](#). Exception: the parameter `record=` is abbreviated as `rec=` in the command line Utility InfoTool.

Example: Remote Correlation Import

To import a Correlation database remotely to the Remote Windows Server \\BIG, the following string would have to be entered:

```
INFOTOOL node=\\BIG IMPORT REC=CORREL FILE=CORREL.TXT
```

Generate a user list who has used the system last time

There is the parameter `EXPORT REC`

```
Infotool.exe EXPORT REC=USAGE file=<output.file> [all=TRUE]
```

it generates a list of users with the last time the user have used the system.

Each time the user access the Xpressions backend, the `LAST_ACCESS` database field is updated.

NOTE: MailApl and ExUmApl from XPR V7R1FR5 HF18 hotfixes are required since those apIs updates the Xpressions database.

32.4.1 Deleting Correlation Data Records

Correlation data records can be deleted with the InfoTool by importing a file with the special KEY `<<<DELETE>>>`. E.g. the import of the file

DOMAIN	CLASSNAME	CLASS	KEYNAME	KEY
SERVER	USER	TEST	FAXG3	<<<DELETE>>>

could delete the Fax G3 addresses of the user `TEST` on the XPR server `SERVER`.
The single entries are separated by a `<TAB>`.

32.4.2 Deleting User Accounts

Through use of the command `InfoTool KillUser User=<User ID>` a user and all data belonging to that user, address book entries, entries in distribution lists, and all documents owned by the user would be deleted. This operation is similar to that of the Maintenance Task `OldUserCleanup`.

It is also possible to use a `*` as wildcard so that with the `InfoTool KillUser User=abc*` command all user accounts starting with `abc` can be deleted. In this case a security prompt appears for each user account to be deleted. This query can be switched off with the optional `batch` parameter.

32.5 LogTool

32.5.1 Definition and Function

The **LogTool** is designed to display the Audit Logging files. These encrypted files are stored in the <XPR Install>\Log directory. All modifications of the configuration are logged here.

32.5.2 Working with the LogTool

32.5.2.1 The Toolbar

The functions used most often can be executed via the toolbar.



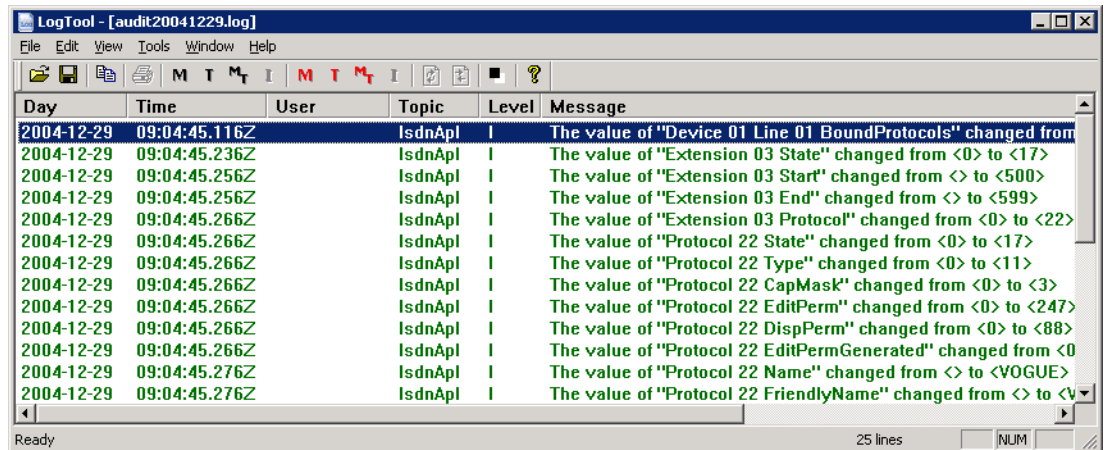
The single symbols will be explained in the following table. A detailed explanation of the executing steps will follow.

Icon	Meaning
	Opens an Audit Logging file.
	Saves the modifications of an Audit Logging file.
	Copies single selected lines.
	Filters for the user of a selected log entry, so that only the entries with this user are displayed in the list.
	Filters for the topic of a selected log entry, so that only the entries with this topic are displayed in the list.
	Filters for the user and the topic of a selected log entry, so that only the entries with this user and topic are displayed in the list.
	Without function
	The entries resembling the user of the selected entry are deleted from the list like the selected entry itself.
	The entries resembling the topic of the selected entry are deleted from the list like the selected entry itself.
	The entries resembling the user and the topic of the selected entry are deleted from the list like the selected entry itself.
	Without function
	The confirmation of this icon shows or hides the filter that has been last used.
	Without function
	Changes the background color of this view.
	Indicates the LogTool version.

32.5.2.2 Open Audit Logging Files

Audit Logging files are opened via the icon . A window opens where you can select the file to be opened. The Audit Logging files are stored in the `<XPR Install>\Log` directory and contain the prefix audit in the file name.

When you open an AuditLog file, the following window will be displayed.



All other files cannot be opened with the LogTool. Other log files are automatically displayed with a text editor when you attempt to open them.

32.5.2.3 Filtering Entries

With the help of the LogTool filtering possibilities you can select entries and have them displayed separately. The entries that have not been selected are removed and only the respectively selected entries will remain in the list. Anyhow, it is possible to effect filtering with the help of **Modules (User)**, **Topics** or with a user-defined entry.

In the toolbar it is possible to filter for **Modules** or the **Topic**.

The Modules (User) Filter

If you filter for **Modules**, the entries are selected that comply with the selected field in the User column.

To execute this filtering operation, select the desired entry and click on **M**. Only one entry can be selected. It is not possible to select several entries.

To execute this filtering action you can also use the menu bar. The term User is used instead of Modules. Select the desired entry and click the subentry **Filter current User** under **Tools**.

You can show or hide the filter via the icon .

You can reestablish the old state and delete the filter by clicking **Reset Filter** under **Tools**.

The Topic Filter

If you filter the **Topic**, the entries are hidden that do not comply with the selected entry concerning the table entry Topic. For instance, a file includes entries for the topic WebApl and the topic SmtmApl. If an entry containing the topic WebApl is filtered for its topic, all entries with SmtmApl are hidden in the topic field. The list only displays the entries including WebApl in the topic field.

To execute this filtering operation, select the desired entry and click on **T**. Only one entry can be selected. It is not possible to select several entries.

You can show or hide the filter by clicking the  icon.

You can reestablish the old state and delete the filter by clicking **Reset Filter** under **Tools**.

The Modules and Topic Filter

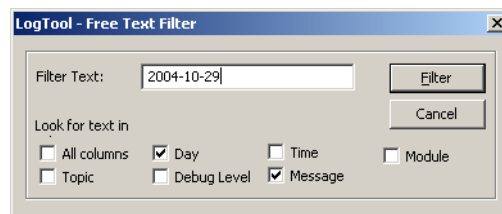
Additionally, you can filter for the user and the topic at the same time. Therefore click the icon  or go to **Tools** to the subentry **Filter current User and Topic**.

You can show or hide the filter by clicking the icon .

You can reestablish the old state and delete the filter by clicking **Reset Filter** under **Tools**.

Free Text Filter

In addition to the predefined **filters** you can select entries according your requirements with the help of a **Free Text Filter**. You call this filter via the **Tools** menu and the sub entry **Free Text Filter**.



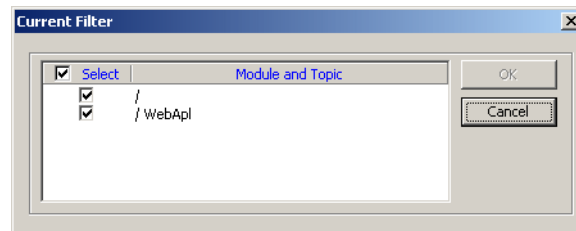
In the **Filter Text** field you enter the text string that will be searched and filtered for in the entries of the file.

You can select the columns in which the text for the filtering will be searched in the check boxes of the **Look for text in** section. You can select several or all columns. To search in all columns select the check box **All columns**.

Click the **Filter** button to perform the search and filtering operation.

Filter Settings

In this window the currently set filter is displayed and ameliorations can be effected. For this, open the **Current Filter** window via **Tools > Current Filter Settings** .



You can select the respective filters by ticking them. Ticking the check box **Select** selects all filters. Your selection becomes effective with **OK**.

32.5.2.4 Hiding Entries

You can differentiate in showing and hiding entries according to the topic, the module (user) or modules and topic.

Exclude Module (User)

This feature hides the entries that correspond to the selected entry in the **User** field. The selected entry is also hidden.

To execute this function select the respective entry and click on the **M** icon.

You can show or hide the filter by clicking the  icon.

You can reestablish the old state and delete the filter by clicking **Reset Filter** under **Tools**.

Exclude Topic

This feature hides the entries that correspond to the selected entry in the **Topic** field. The selected entry is also hidden.

To execute this function select the respective entry and click on the **T** icon.

You can show or hide the filter by clicking the  icon.

You can reestablish the old state and delete the filter by clicking **Reset Filter** under **Tools**.

Exclude Module and Topic

This feature hides the entries that correspond to the selected entry in the **User** and **Topic** fields. The selected entry is also hidden.

To execute this function select the respective entry and click on the **MT** icon.

You can show or hide the filter by clicking the  icon.

You can reestablish the old state and delete the filter by clicking **Reset Filter** under **Tools**.

32.5.3 Additional Editing Possibilities

Additional possibilities to edit the Audit Logging file are exporting the data, setting bookmarks, showing and hiding bookmarks, searching entries, joining several opened files as well as detecting time differences. Furthermore, you can copy entries to paste them afterwards e.g. to a text file.

Export

you can convert the entries of an Audit Logging file into the CSV format. CSV means **Comma Separated Value** and has been designed for saving database data. It is e.g. compatible with Microsoft Excel.

You can either select all entries of a file or only select a certain number. Therefore open the subentry **Export** in the **File** menu and then **All** for all entries or **Selection** for the selected entries in the dialog window. In this window you can enter the name of the target file and the target destination of this file.

Bookmarks

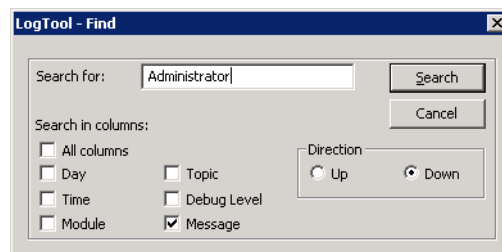
Within the entry list you can set bookmarks. These are colored and serve as markers that you can always go to.

Select a line that you would select as bookmark and go to **Toggle Bookmark** in the **Edit** menu. The entry is selected in terms of color and can now be used as entry point. Therefore click **Step Bookmark** in the **Edit** menu and the selection will move down to the next bookmark. If there is no bookmark further down, the selection moves back to the first bookmark in the list.

You can remove bookmarks by selecting the respective bookmark and by then clicking **Toggle Bookmark** in the **Edit** menu.

Search

You can also search for corresponding entries in the AuditLog-File. Click **Find** in the **Edit** menu. A dialog window opens for the search.



Enter the term you want to **Search for** in the respective field.

Select the columns in which you want to search in the check box in the **Search columns** section. The check box **All columns** selects all columns. The **Direction** field defines the search direction.

Clicking **Search** starts the search and selects the first search result in the list. For a new search the search window must be reopened and the search must be initiated again.

You will be notified if no accordance could be found.

Joining open files

You can join two or more open Audit Logging files with the currently displayed file.

Therefore click the  icon and a window opens for file selection. Only the files opened in the LogTool are displayed. You can select the respective file by ticking it. Ticking the check box **Select** selects all files.

Your selection becomes effective by clicking **OK** and the result will be displayed in a new file.

Detecting time differences

All entries of the Audit Logging files include time data. You can now have the time difference between two entries calculated. Select the corresponding entries and click the right mouse button. A context menu opens. Click **Show Time difference**. The result will be displayed in a window that pops up.

If you select several entries, the difference will also be calculated for the entries with the greatest time difference. This means that the time difference between the top and bottom entry is calculated, since the list is in chronological order.

Copy

You can copy entries and paste to another program. Therefore select an entry and click .

32.5.4 Display Settings

As to the LogTools representation, you can modify the font and the background color.

Font type

In the **View** menu and the sub entry **Font...** you can define type, size and form of the applied font.

Background colors

In the **View** menu and the sub entry **Background Color** you can show or hide the background color or modify it.

Via **Toggle Background color** you can show or hide the background colors. This feature can also be effected by clicking the  item.

The commands **Modify Color 1** and **Modify Color 2** both applied background colors are modified.

The **Reset Color** command resets the modifications to the basic settings.

32.6 MsgSize Tool

This tool delivers specifications about the number and size of messages for single users and user groups.

```
msgsize node=<Node> uid=<User ID> pwd=<Password>
      [group=<Group list>] [user=<User List>] [file=<Output file>]
<Group list>=<Group ID 1>[,<Group ID 2>,...<Group ID n>]
<User List>=<User ID 1>[,<User ID 2>,...<User ID n>]
```

node=<Node> is the name of the XPR server that is queried.

uid=<User ID> pwd=<Password> are a combination of user ID with associated XPR password of a user with *supervisor privilege*.

Reports are either put out via [group=<Group list>] for one or several user groups and all users contained therein, or the users to be queried are directly specified via [user=<User List>]. If neither a group nor a user is specified, a report is put out for all users.

[file=<Output file>] is the path and file name in the which specifications are written. If no file is specified, the output occurs on *standard output*, thus normally in the console window.

Example: Group SUPERVISOR

```
msgsize node=XPRDOC uid=administrator pwd=tom123
group=SUPERVISOR
file=sv.txt
```

This command writes the data in the `sv.txt` file for the SUPERVISOR user group and all users contained therein. This output occurs itemized according to voicemails and other messages as well as old and new messages.

```
Start Time: 2008-01-11 12:04:51
End Time: 2008-01-11 12:04:51
/-----
| Voice
| Group                |New Count |Minutes   |Old Count |Minutes   |
| SUPERVISOR           |          0|          0|          3|          0|
|-----
| Non-Voice
| Group                |New Count |KBytes    |Old Count |KBytes    |
| SUPERVISOR           |          7|          1|          3|        3656|
|-----
| Voice
| User                |New Count |Minutes   |Old Count |Minutes   |
| NVS:XPRDOC/ADMINISTRATOR |          0|          0|          3|          0|
|-----
| Non-Voice
| Group                |New Count |KBytes    |Old Count |KBytes    |
| NVS:XPRDOC/ADMINISTRATOR |          7|          1|          3|        3656|
|-----
```

32.7 Octel Migrator Tool

32.7.1 Function

The Octel Migrator Tool enables you to transfer Octel user data records to the XPR database in a simple manner. In this process, the user data records are divided into single user data, distribution lists and user groups.

Before the Octel data records are transferred to the XPR system, you are provided with different setting options. Besides general transfer configuration settings, you can also assign specific default properties to users as well as user groups. You can thus partly control the data record import and save work.

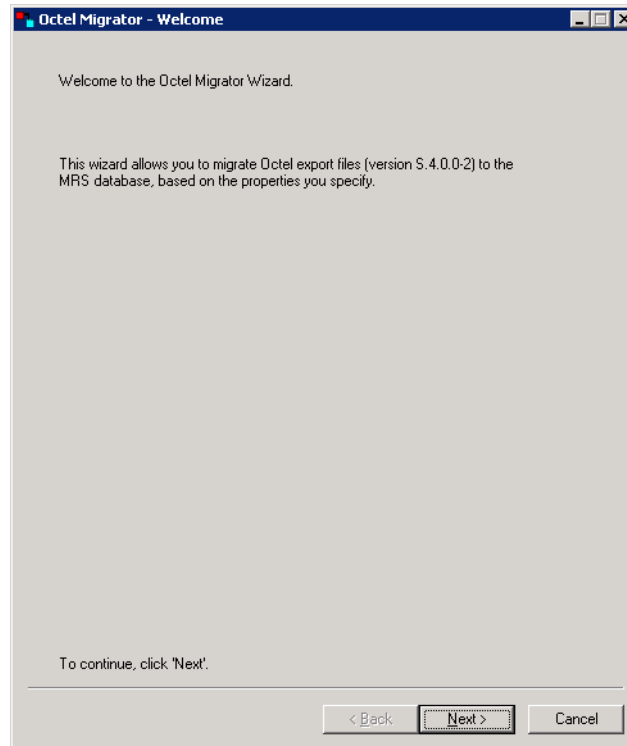
NOTE:

Please note that only Octel user data of **version S.4.0.0-2** can be transferred to the XPR database.

32.7.2 Performance

The Octel Migrator Tool `OctelMigrator.exe` is found in the `<XPR Install>\SDKTools` folder after the XPR server installation.

The tool starts with a welcome dialog and guides you like a wizard through several dialogs step by step, as you need to make various settings there.



You reach the respectively next dialog with the **Next** button. If you have not made required settings, a warning will draw your attention to this. With the **Back** button you can return to the previous dialogs to check and change settings if required. With the **Cancel** button you can terminate the process anytime.

32.7.2.1 Step 1: General

The first dialog displays basic settings for the transfer of Octel user data to the XPR database system.

Octel Migrator - General

Octel file
Enter the Octel file to migrate:
[ettings\mk\Desktop\kpmg-bf_config_short.cap] [Browse ...]

Output file
Select "Save invalid entries" to save invalid Octel data for rework:
☒ Save invalid entries
Enter the file to save invalid octel data to:
[C:\Documents and Settings\mk\My Documents] [Browse ...]

Logging
Select the logging level :
[WARN] [v]
Enter the name of the log file:
[C:\DOCUME~1\mk\LOCALS~1\Temp\1\Octel] [Browse ...]

MRS backup
Select "Back up MRS" to back up the MRS database before migration:
☒ Back up MRS
Enter the name of the backup file:
[C:\DOCUME~1\mk\LOCALS~1\Temp\1\mrs-c] [Browse ...]

To continue, click 'Next'.

[< Back] [Next >] [Cancel]

The dialog is divided into the four sections **Octel file**, **Output file**, **Logging** and **MRS backup**.

Octel file

In this section you select the file with the Octel user data. After a click on the **Open** button you can look for the corresponding file and select it with a mouseclick. The selected file then appears with storage path in the text field.

NOTE:

Please note that only Octel user data of **version S.4.0.0-2** can be transferred to the XPR database. The file must feature the entry `SYSTEM SOFTWARE RELEASE S.4.0.0-2` as header.

Output file

Invalid Octel user data entries can be optionally saved for processing at a later date. To activate this feature, select the **Save invalid entries** option first. You then need to select a file in which the invalid entries are stored. With the **Open** button you can look for an appropriate file and select it. This selected file appears in the text field inclusive storage path. Use **Text** as file type.

After the transfer of the Octel user data to the XPR system you can manually process invalid entries that may have come up, so that these can be integrated in the XPR system. Using the InfoTool (see [Section 32.4, “InfoTool”](#)) or the DBTool (see [Section 32.3, “Database-Correl-Tool \(DbTool\)”](#)) you can import such processed user data in the XPR database system.

Logging

While the Octel data records are transferred to the XPR system, a logging file is created.

Via the **logging level** drop-down menu you can choose from five different levels to determine the level up to which logging information is written. The following five options are available:

Logging level	Description
Debugging	The logging file integrates error, warning, debug and information messages.
Information	In the logging file, error, warning and information messages are stored.
Warning	In logging file, error and warning messages are listed. This level is the default setting.
Error	In the logging file only error messages are put out.
None	The logging file does not integrate any messages.

In the **Enter the name of the log file** field preset the `OctelMigrator.log` file in the temporary directory of the logged in user. You can also use the **Browse** button to select an individual file as storage location for the logging. The file used appears in the text field inclusive storage path.

MRS backup

For security reasons you can create a copy of the XPR user database before the Octel user data are imported.

To activate this option, place a check mark next to **Back up MRS**.

Subsequently, you can either use an automatically created or an individual file for the backup. An automatically created file is used by default, and this file carries the description `mrs-correl-<DDMMYYYY>.txt` for the current date and is stored in your temporary file. You can select an individual file using the **Browse** button.

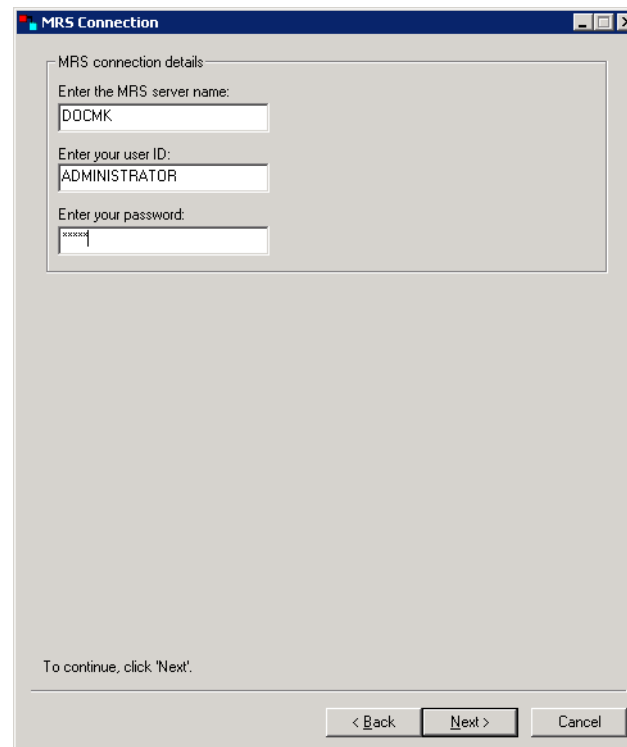
The file used appears in the text field inclusive storage path.

32.7.2.2 Step 2: Connection

In the next step you need to specify the **MRS server** and authenticate yourself with **ID** and **password**. For the **MRS server**, enter the name of your XPR server.

IMPORTANT:

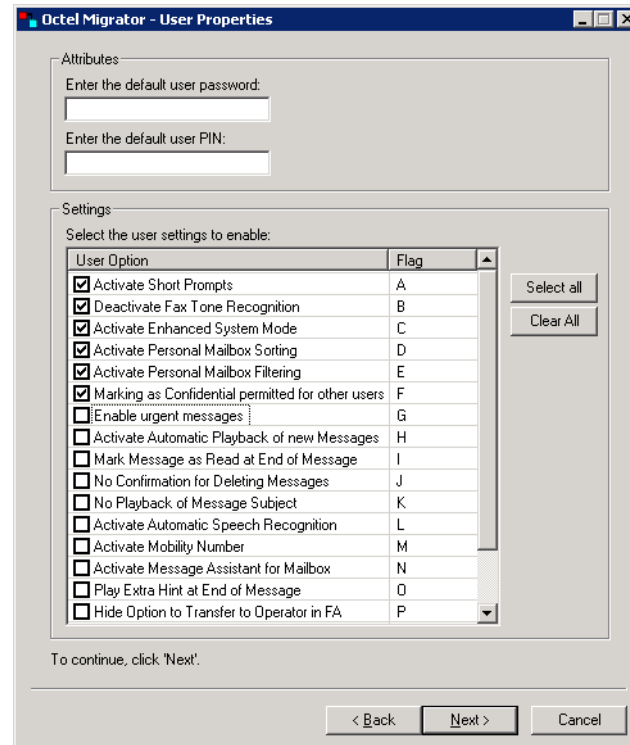
Please note that the user ID must have the *Supervisor privilege* so that Octel data records may be transferred to the XPR system.



The screenshot shows a Windows-style dialog box titled "MRS Connection". Inside the dialog, there is a section labeled "MRS connection details" which contains three input fields: "Enter the MRS server name:" with the text "DOCMK", "Enter your user ID:" with the text "ADMINISTRATOR", and "Enter your password:" with a masked password "password". At the bottom of the dialog, there is a message "To continue, click 'Next'." and three buttons: "< Back", "Next >", and "Cancel". The "Next >" button is highlighted with a black border.

32.7.2.3 Step 3: User Properties

In the third step you can define specific default values for all users of the Octel data records to be transferred.



Octel Migrator - User Properties

Attributes

Enter the default user password:

Enter the default user PIN:

Settings

Select the user settings to enable:

User Option	Flag
☒ Activate Short Prompts	A
☒ Deactivate Fax Tone Recognition	B
☒ Activate Enhanced System Mode	C
☒ Activate Personal Mailbox Sorting	D
☒ Activate Personal Mailbox Filtering	E
☒ Marking as Confidential permitted for other users	F
☐ Enable urgent messages	G
☐ Activate Automatic Playback of new Messages	H
☐ Mark Message as Read at End of Message	I
☐ No Confirmation for Deleting Messages	J
☐ No Playback of Message Subject	K
☐ Activate Automatic Speech Recognition	L
☐ Activate Mobility Number	M
☐ Activate Message Assistant for Mailbox	N
☐ Play Extra Hint at End of Message	O
☐ Hide Option to Transfer to Operator in FA	P

Select all

Clear All

To continue, click 'Next!'

< Back Next > Cancel

First you can specify the **password** and the **PIN** for each user. Each user who is transferred from the Octel data records to the XPR system receives then the same password and PIN. The user should change such values as quickly as possible.

Next, you can assign all users to be transferred specific **user settings**. You can select the following settings, which are later mostly required for using the PhoneMail TUI:

- Abbreviate prompts
- Deactivate fax tone recognition
- Activate enhanced system mode
- Activate personal mailbox sorting
- Activate personal mailbox filtering
- Marking as confidential permitted for other users
- Enable urgent messages
- Automatic playback of new messages activated

- Mark message as read at the end of message
- No confirmation for deleting messages
- No playback of message subject
- Automatic speech recognition activated
- Mobility number activated
- Message assist for mailbox activated
- Play extra hint at message end
- Hide option to transfer to operator in FA
- Activate referral extension
- Activate potential protocol change in FA
- Uses TTY/TDD Devices (Hearing Impaired)

Using the **Select All** button you can mark all options

By means of the **Clear All** button, all markings are removed.

32.7.2.4 Step 4: MRS Group Properties

In this dialog you can specify the user group and thus the privileges and default values inherited from this group as user group **attributes**.

Octel Migrator - MRS Group Properties

Privileges
Select the the MRS group to use when defaulting privileges:
USER

Attributes
Enter the maximum company greeting duration in seconds (0 means infinite):
0
Enter the maximum greeting duration in seconds (0 means infinite):
0
Enter the maximum message duration in seconds (0 means infinite):
0
Enter the maximum name recording duration in seconds (0 means infinite):
0
Enter the minimum number of digits allowed for PINs:
6
Enter the Lifetime of PINs in days (0 means infinite):
0
Enter the number of failed logon attempts before the mailbox is locked:
3
Enter the number of warning days before PINs expire (0 means infinite):
0
Enter the maximum number of private distribution lists (0 means infinite):
0
Enter the postmaster ID:
POSTMASTER

To import users to the MRS, click 'Next'.

< Back Next > Cancel

In the **Privileges** section you find a list of the user groups that exist in the XPR system. All imported Octel users are assigned the group you select and inherit the group's privileges. So, if you select the administrators group, each user group imported from the Octel data records receive the administrator privileges.

In the **Attributes** section you enter specific values for the attributes of the Octel users to be transferred. You can specify the values for the following attributes:

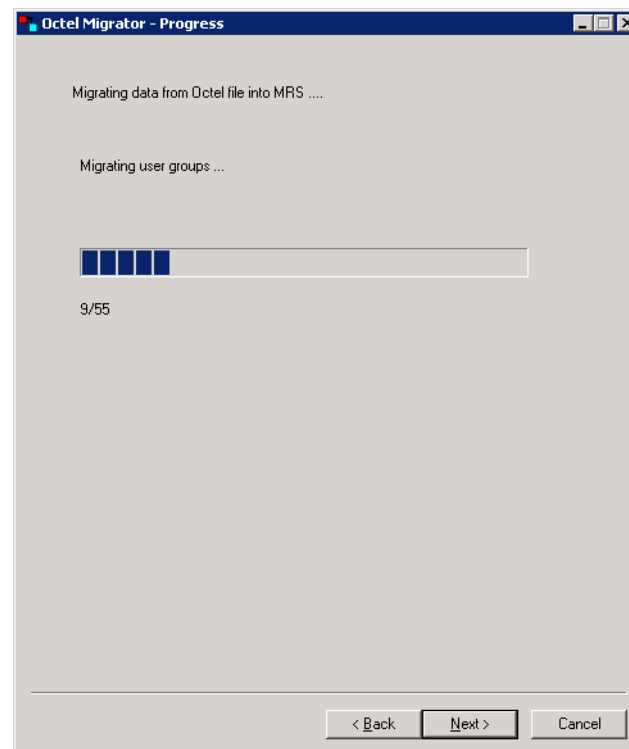
- The maximum company greeting duration in seconds
- The maximum greeting duration in seconds
- The maximum message duration in seconds
- The maximum name recording duration in seconds
- The minimum number of digits allowed for PINs
- The lifetime of PINs in days
- The number of failed logon attempts before the mailbox is locked
- The number of warning days before the PIN expires
- The maximum number of private distribution lists

In case of attributes specified in seconds or days, value 0 deactivates a temporal limit.

In addition, you can define the user ID of the PhoneMail postmaster.

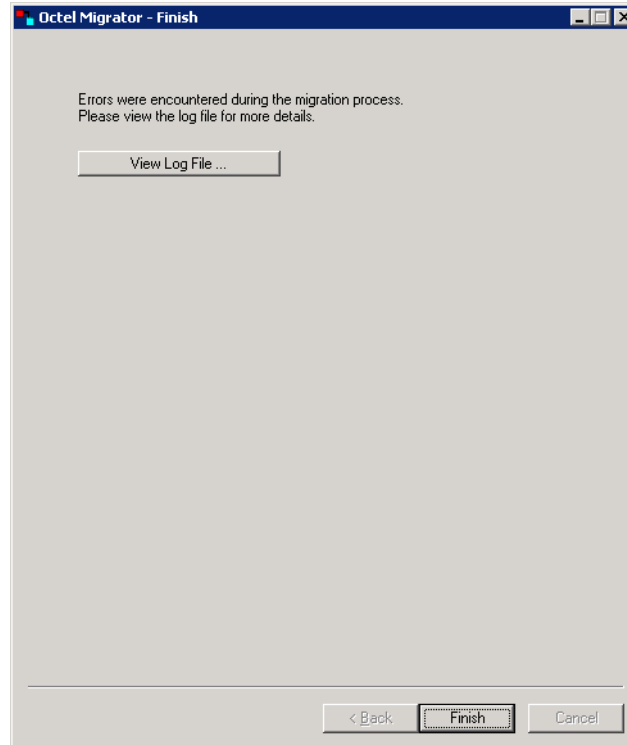
32.7.2.5 Step 5: Progress

This dialog displays the current work step of the transfer process and its progress anytime.



32.7.2.6 Step 6: Summary and Completion

When the Octel data records transfer is complete, you are informed in the last step about possible errors that occurred during the transfer.



With a click on the **View Log File** button you can view the log file and evaluate the corresponding report details.

The new users can finally be viewed and edited with the Web Assistant.

32.8 RangesNCO

Background: We assume an XPR installation at a PBX that supplies several locations or "location codes" but works with a closed numbering plan. In case of a closed numbering plan, each extension has a unique number and can be reached via this number independently from the location, assigned "location code", or private/E.164 property. XPR must now be able to determine the complete number (private or E.164) from an extension number. The required information can be manually deposited in the NCO configuration, which is rather complex. This tool serves for simplification.

32.9 Syntax

For the application North America, RangesNCO runs without parameters with the preset default values. In other cases you can control the behavior via the parameters.

```
RangesNCO.exe -p <Pattern> -s <Size> -x <Filename> -h
```

IMPORTANT:

The parameters `-p` and `-s` must always be stated in combination, even if only one of them deviates from the default value. All other parameters are optional.

Parameter `-p <Pattern>`:

Via `<Pattern>` you specify the schema of the phone numbers in the database. It is defined via letters C, A and S. C represents the country code, A stands for the area code and S for the subscriber code.

Default: `-p CAAASS`

Example: `+1555456` with `-p CAAASSS`

1 is thus the country code (USA/Canada), 555 the area code and 456 the subscriber code.

Parameter `-s <Size>`:

`<Size>` specifies the length of the extension number.

Default: `-s 5`

Example: Extensions be 2304, 5122 and 3122

Consequently, you needed to specify `"-s 4"` as parameter.

Parameter `-x <Filename>`:

File name of the created XML import file for the NCOAdmin.

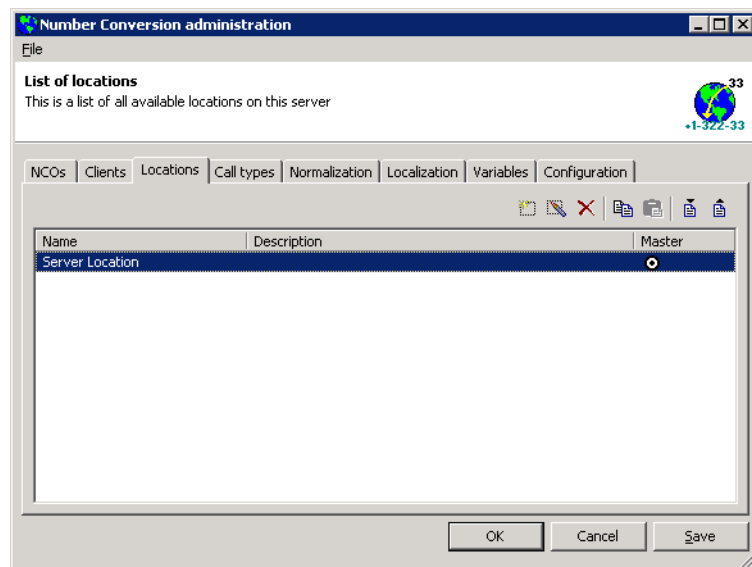
Default: `-x nco_autogen.xml`

Parameter -h:

Issues a brief help on the program's options.

32.10 Proceedings

1. Import the data determined by CDC in the Correlation database.
2. Create the import file for the NCO Admin by means of RangesNCO.
3. Start `<XPR Install>\bin\NumberConversionAdmin.exe`.



4. Click on .
5. Select the import file `nco_autogen.xml`.
6. Activate the imported configuration with a click on the radio button in the **Master** column.
7. Accept the security prompt for the configuration modification.
8. Save the changed NCO configuration.

32.11 Rename Server

This command line program allows changing the Windows server name or the IP address of the Windows server on which the XPR server operates. The corresponding references in the Correlation database, the Journal database, Windows registry, the Media Server, OpenSOA configuration files and third-party configuration files are adjusted.

IMPORTANT: `renservr` must be invoked from the directory `<XPR Install>`.

NOTE:

Rename Server prompts for a password when being executed. Only the service personnel know this password.

NOTE: If there are any error information after stopping the ConApl service, it can be ignored.

NOTE: After the process has finished please check also the procedures described in 'E.1.5.1 CCF File' for changing the License Service IP address.

Proceed as follows:

1. Invoke `renservr` to change the IP address or name of the Window server.
2. After you have been prompted by the `renservr`, stop the Connection APL (CONAPL).
3. Change the IP address or name of the Windows server via the Windows configuration.
4. If the IP address was changed, stop the XPR server and reboot it.
If the name of the Windows server was changed, the computer needs to be rebooted.

Syntax: `RenServr [-h] [-i] [-r] [-d] [-s] [-o | -x] <old name> <new name>`

Parameter `-h` [`--help`]:

help message

Parameter `-i` [`--ignore-journal`]:

DO NOT change data in journal

Parameter `-r [ --ignore-registry ]:`

DO NOT change data in registry

Parameter `-d [ --database-only ]:`

change ONLY data in correl and journal

Option `--journal-other EXPERIMENTAL:`

replace other journal fields (with system-only option)

Option `--journal-nolock EXPERIMENTAL:`

disable the journal locking. Use only if no other Xpressions component is running

Parameter `-s [ --simulation ]:`

No action; perform a simulation of changes

Parameter `-o [ --host ]:`

Replace only host name occurrences

Parameter `-x [ --system ]:`

Replace only system name occurrences

Parameter `-p [ --password ]:`

arg Password needed for RenServer.

<old name>:

The old Windows server name or the old IP address.

<new name>:

The new Windows server name or the new IP address.

Host is the machine name, like: `\\HOST\Folders$`

System is the Xpressions name, like: `NVS : SYSTEM/ADMINISTRATOR`

Example:

```
renservr.exe XPROLD XPRNEW
```

32.11.1 Satellite-inherent Specials

When changing the IP address, the following manual change must be performed on a satellite in addition:

In the registry key

HKLM\SYSTEM\CurrentControlSet\Services\namoloc

the IP address of the parameter `nameloc=\\<IP address>` must be adjusted to the new IP address of the kernel computer in the **ImagePath** registry value.

32.11.2 Particularities of Systems with Connection APL and OpenScape Web Client

When the name is changed, the local user account must be adjusted for the PostgreSQL database in the registry, because an update of the XPR server at a later date will otherwise fail. The name of the Windows server must be manually changed to the new name.

To do this, change in the registry key

HKLM\Software\Wow6432Node\PostgreSQL\Services\pgsql-8.4

the registry value **serviceAccount** from the old to the new name of the Windows server accordingly.

32.12 SystemVersionInfo

This program issues the installation history and the version state of all installed XPR system components. The version information of components on the satellite system cannot be displayed, though. The implemented hotfix versions can be optionally displayed. More items of displayed information are the version numbers of the installed E scripts, NCO rules, drivers and operating system information. Using the **File > Save** option you can write all this information as several text files into a zip archive. If you invoke SystemVersionInfo from the command line and specify a file with the ZIP suffix as parameter, the export file is immediately created without any further interaction.

NOTE:

This zip archive with all optional information should always be part of an error report. For this purpose, check mark all options in the **Export** menu.

32.13 Time Zone Support

The Time Zone Support Tool controls the usage of time zones in the XPR server.

By default, the time zone of the server location is valid for all XPR server users. This can be confusing if the users of a distributed server are spread among several time zones.

If the time zone support of the XPR server is activated via the Time Zone Support Tool, an individual time zone can be assigned to each user. This is evaluated for the time zone specific display of time information in the XPR clients and in the delivered messages. The assignment of time zones to users is performed via the Web Assistant. For further information please refer to the *Web Assistant* manual.

32.13.1 Important Notes for the Usage of Time Zone Support

The time zone support requires certain conditions for the correct time zone display in the applied XPR clients. Therefore, after the activation of the time zone support, only those client versions are applied that are delivered with XPR version 4 or later.

IMPORTANT:

During the activation and deactivation of the time zone support via the Time Zone Support Tool the XPR server database is modified. Therefore the XPR server is automatically stopped after the Time Zone Support Tool has been called. This interrupts the server services.

32.13.2 Calling the Time Zone Support Tools

The Time Zone Support Tool is a program for the command line and is executed via the `TimeZoneSupport.exe` file. This file is stored in the `<XPR Install>\bin` directory after the XPR server installation.

The `TimeZoneSupport.exe` file can be called with two alternative parameters.

- `TimeZoneSupport on`
Enables the usage of time zones in the XPR server.
- `TimeZoneSupport off`
Disables the usage of time zones in the XPR server.

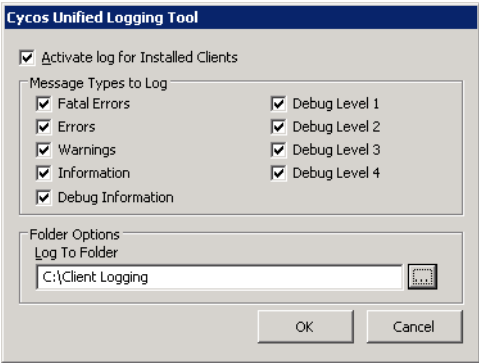
If the Time Zone Support Tool is called without any parameter, a short note indicates the supported parameters.

32.13.3 Cluster with Microsoft Windows Server

In case of an installation on a cluster, stopping the services by TimeZoneSupport is considered a crash and the services are automatically rebooted. Therefore, you cannot activate the timezone support.

32.14 Logging Tool for Clients

If required, you can activate logging for all clients of the XPR server. For this purpose you need to execute the `UnifiedLogTool.exe` program on the client after previously copying it to the client from the `<XPR Install>\SDKTools` folder. Beyond that, an XPR client application should be installed on the client computer.



The configurable options correspond to those that are also available for the log filter of the server components in the XPR monitor. In case of errors the support would issue the corresponding instructions for setting the filters.

IMPORTANT:

The folder to host the log file should be writeable by the local user SYSTEM. The MSPSVC runs as service under this account and is otherwise unable to write its log data.

IMPORTANT: Under Windows Vista and Windows 7, `UnifiedLogTool.exe` must explicitly be started via the context menu option Run as Administrator. This is also the case if the executing user belongs to the group of local administrators himself/herself.

The log filters are stored on the client computer in the registry key `Software\Cycos AG\UnifiedLog`. After the invocation of the Unified Logging Tool the key is available in `HKEY_LOCAL_MACHINE` as well as in `HKEY_CURRENT_USER`. The following values are created at this:

LogActive [REG_DWORD]

Default:	<No default>
Possible values:	0 – Logging deactivated 1 – Logging activated for all installed clients

Switch client logging on or off.

LogFilter [REG_DWORD]

Default:	<No default>
Possible values:	Bitmask: 0x001 – Fatal errors 0x002 – Errors 0x004 – Warnings 0x008 – Information 0x010 – Debug information 0x020 – Debug level 1 0x040 – Debug level 2 0x080 – Debug level 3 0x100 – Debug level 4

Bitmask with the log filter settings.

LogPath [REG_SZ]

Default:	<No default>
Possible values:	<Path>

Path into which the single log files of the installed clients are written.

32.15 ZombiDetect

NOTE:

For the ZombiDetect invocation a special password is queried. Only the service personnel know this password.

Using ZombiDetect the administrator can check the XPR Message Store integrity. This check includes the search for non-referenced documents in the XPR message store. Such documents are either not referenced to from the journal database anymore, or they are data records the referenced documents of which is no longer available on the harddisk. The first category is called “Zombi”, the second one is named “Lost”.

If ZombiDetect finds corresponding errors, it can repair the respective entries.

This utility can be used on a running server. If this is not desired, the XPR server can be shut-down and restarted in the following order:

```
LICSVC start
NAMELOC start
CFG SVC start
XMRSVC start
INFOSTOR start
```

ZombiDetect can now be started. The following command line parameters are supported at this:

Option	Meaning
-h	Display help. The possible command line parameters are displayed.
-l <arg>	Minimum age in hours that a Lost document must have.
-z <arg>	Minimum age in days that a Zombi file must have.
--ignore-lost	Edit Zombi documents only.
--ignore-zombies	Edit Lost documents only.
-r	Repair the found consistency errors automatically.
--version	Display version information.

Table 66 ZombiDetect command line parameters

An invocation without command line parameter corresponds to the following invocation:

32.16 SystemInfo

NOTE: You need to activate the **SystemInfo** script in the Web APL for this tool to work.

After the installation you can invoke SystemInfo from the desktop via the **SystemInfo** icon.



This program contains all information about the system, the APLs, the physical computer-performance and harddisk capacities.

A message overview (Rapid State) is integrated in the SystemInfo. The messages contain the connection status of the APLs, show blocked services and error reports.

32.17 XPRHFPPackInstaller

NOTE: This tool can only be used on Failover Cluster environments with all Xpressions services offline including license service.

This tool has the goal to automate the installing process of the Xpressions Hotfix Packages (HF).

The HF package hotfixes must be inside a zipped file. The tool extracts in a temporary folder all the Hotfixes of the HF package and starts a sequential installation.

The hotfixes are classified in two kind: hotfixinstaller hotfixes and Msi hotfixes. Beyond that, the hotfixinstaller hotfixes are categorized in: Services, Kernel and Others.

- Services:
all the hotfixes that are installed as services (Apls) in the Xpressions server.
i.e.: MTA, IpApl...
- Kernel:
special type of services that belongs to the Xpressions kernel:
"LicenseServer", "Mrs", "Mta", "cfgsvc", "nameloc", "Infostor", "XmrSvc" and "CycosOpenSSL".
- Others:
hotfixes that do not belong to the Services neither to the Kernel category.

Options available:

- --all: 'Install all Hotfixes, services, others and MSI'
- --services: 'Install only the hotfixes that are services'
- --kernel: 'Install only the kernel services'
- --msi: 'Install only the hotfixes that are MSI'
- --others: 'Install the hotfixes that are not services nor MSI'
- --logfull: 'Enable the full log'
- --file: 'Specify the package file to be used: must be a compressed file(zip)'
- --extractonly: 'Only extract the package file, without performing installation'
- --silent: 'Install hotfixes in silent mode'
- --forceInstall: 'Install all the hotfixes skipping the installation checks'
- --skipXprCheck: 'Skip the Xpressions installation check'

Basic usage:

- a) XPRHFPackInstaller.exe --file HotFixPack.zip --all
(Install all hotfixes, including Msi files)
- b) XPRHFPackInstaller.exe --file HotFixPack.zip --kernel
(Install only the hotfixes that are from kernel category: "CycosOpenSSL", "LicenseServer", "Mrs", "Mta", "cfgsvc", "nameloc", "Infostor", "XmrSvc")
- c) XPRHFPackInstaller.exe --file HotFixPack.zip --msi
(Install only the hotfix that are msi files)
- d) XPRHFPackInstaller.exe --file HotFixPack.zip --other
(Install all the hotfixes that are not Msi and not belong to the kernel category)
- e) XPRHFPackInstaller.exe --file HotFixPack.zip --forceInstall
(Attempt to install all the hotfixes, not performing installation checks)
- f) XPRHFPackInstaller.exe --file HotFixPack.zip --extractonly
(Performs the extraction of all the hotfixes of the compressed file to the OUTPUT folder. Do not install anything)

32.18 Xpressions Toolkit

With this tool you can have quick access to the main Xpressions administrative tools and shortcuts to useful Microsoft Windows tools for analysis and troubleshooting. This tool also provides easy access to important Xpressions folders and Xpressions registry settings.

32.18.1 Installation

The installation folder of the Xpressions Toolkit is located at:

`<Xpressions installation folder>\SDKTools`

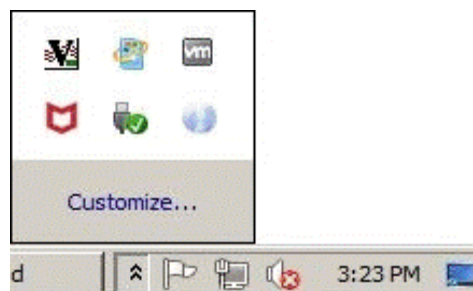
and

`<Xpressions installation folder>\SDKTools\XprToolkit` directory.

During the hotfix installation a shortcut of the Xpressions Toolkit is created in the desktop area:



A system tray icon is created to allow access to the Xpressions Toolkit features:

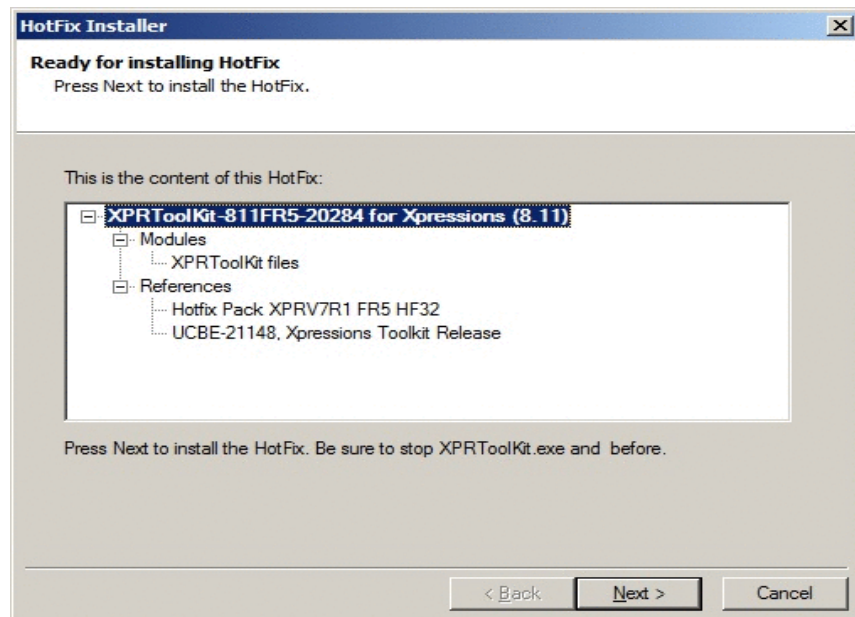


The Xpressions Toolkit is configured to start automatically during the system startup.

The XPRToolkit can be installed via XPRToolkit hotfix available on latest XPR V7R1FR5 Hotfix package.

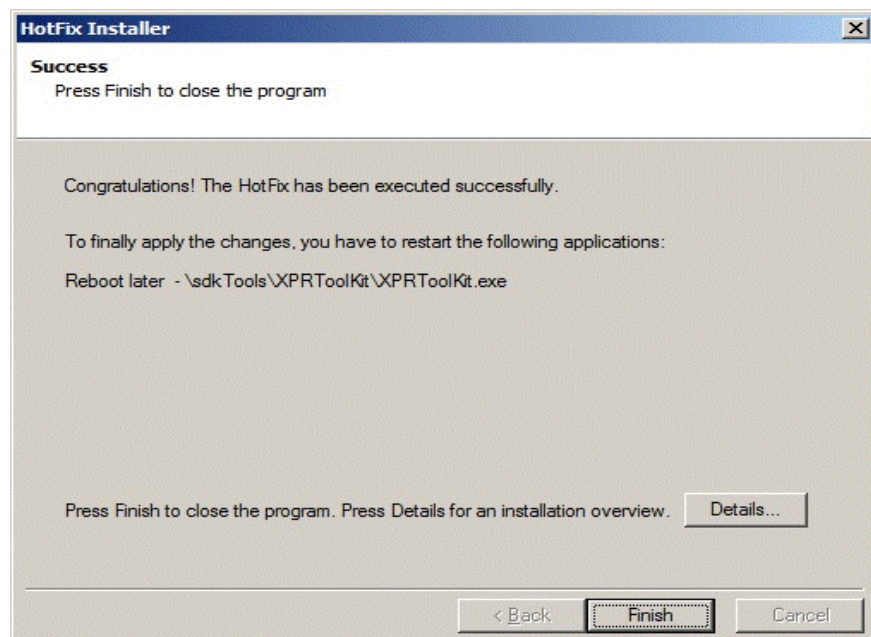
Follow the steps below:

1. Run the **XPRToolKit hotfix**.
2. Click **Next**



Wait until the installation process finishes.

3. Click **Finish**

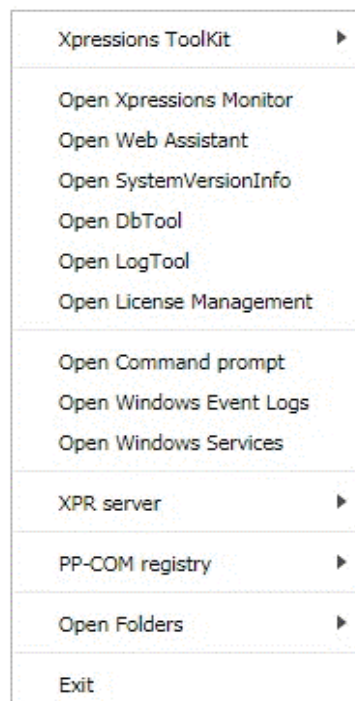


32.18.2 Tool information

- **XML configuration file:**
 - The XprToolkit installation folder contains a **.xml** file that enables you to customize some XprToolkit settings.
 - The configuration file name is `xprToolkitConfig.xml`
- **Traces:**
 - The XprToolkit creates a file called `XprToolKit.log` in the folder where the executable of the XprToolkit is located.

32.18.3 XprToolkit features menu and usage

By clicking the XpressionsToolkit icon in the systray the following menu opens::



32.18.3.1 Xpressions Toolkit' section

From this section you can:

- access information about the XprToolkit version,
- export the log of the XprToolkit
- open the folder where the program is installed.

- About

This option shows XPRToolkit version information.

- Export Log

This option opens the XPRToolkit log file.

- Installation folder

This option opens the XPRToolkit installation folder in Windows Explorer

e.g. `<xpr install directory>\SDKTools\XPRToolKit`

32.18.3.2 Main Xpressions tools section

From this section you can have quick access to the main Xpressions administrative tools.

- Open Xpressions Monitor

This option launches XPR Monitor.

- Open Web Assistant

This option launches WebAssistant in default browser.

- Open SystemVersionInfo

This option launches Xpressions system version tool.

- Open DbTool

This option launches Xpressions database tool.

- Open LogTool

This option launches Xpressions Log tool.

- Open License Management

This option launches License Management in default browser (when available in the current server).

e.g. `https://127.0.0.1:8859/`

In order to customize this address the following part of the **xprToolkitConfig.xml** file should be changed:

```
<clm>
    <protocol> https </protocol>
    <ip>127.0.0.1</ip>
    <port>8859</port>
</clm>
```

32.18.3.3 Windows tools section

From this section you can have quick access to the most common Microsoft Windows administrative tools.

- Open Command prompt

This option open a command prompt in the location which the Xpressions server is installed.

- Open Windows Event Logs

This option opens Windows Event Log.

- Open Windows Services

This option opens Windows Services Management Console.

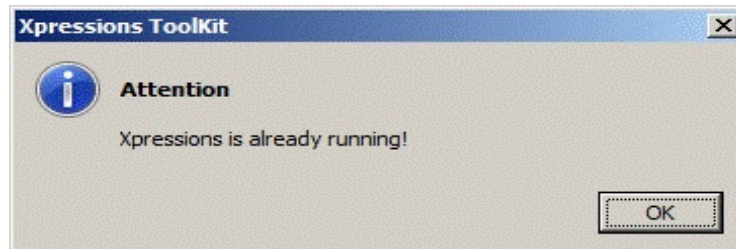
32.18.3.4 'Xpr Server' menu

From this section you can start and/or stop the Xpressions server.

- Start

This option starts the Xpressions services.

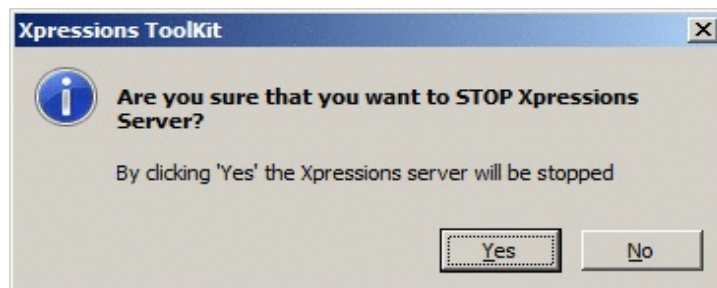
If Xpressions is already running, the following warning message pops-up:



- Stop

This option stops all Xpressions services.

A dialog box opens asking you to confirm that the Xpressions server will be stopped.



- Update

Feature currently not available.

32.18.3.5 'PP-COM registry' section

From this section you can perform operations (open and/or export) in the Xpressions server Windows registry.

- Open

This option opens Windows registry at:

HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\PP-COM\MRS\MRS Globals

- Export

This option exports the Xpression PP-COM registry folder to a file.

32.18.3.6 'Open Folders' section

From this section you can open the 'Windows Explorer' with the location of important Xpressions folders.

- XPR Master logs

This option opens the XPR Master logs folder in Windows Explorer.

e.g. `<xpr install directory>\log\`

- SDKTools

This option opens the XPR SDKTools folder in Windows Explorer.

e.g. `<xpr install directory>\SDKTools\`

- Installation

This option opens the XPR installation folder in Windows Explorer.

e.g. `C:\OpenScape\xpr\`

32.18.3.7 e) 'Exit' command

This option stops the XprToolkit application by exiting it.

33 Component-spanning Features

The XPR architecture and the flexible use of all components allow new features to be created for the system simply via administration. Several examples of this are given in the following so that you can understand the mechanism and create your own applications.

33.1 Fax Buffering When Busy

A familiar feature from the Hicom TeleCommunicationsServer (TCS) is “Buffering when busy” for the Fax service. However, the feature there was very tightly integrated into the Hicom, which means that it cannot be identically simulated by XPR.

The following prerequisites must be created for each physical fax device that should be able to use this feature:

- `call forwarding on busy` must be activated in the PBX for the fax device (Hicom 300: AMO COSSU, Parameter FWDBSY).
- in the PBX, a destination must be configured for the fax device to a number for call forwarding on busy (for Hicom 300: fixed call forwarding); this number must either be configured as fax access for the PhoneMail script (if the redirected number is supplied when setting up the connection, which is the case for Hicom 300 and CorNet-N) or it must lie in the number range of the FAXG3 protocol or the PhoneMail script with activated fax tone recognition (Hicom 300: AMO ZIEL).
- the fax device must be configured as user in XPR with the following user data:
 - in `FAXG3#`: the call number of the fax device
 - in `PREFERRED`: `FAXG3`

Now, to implement buffering for a fax device that has been configured in this way, the following rule must be added to the user-defined routing rules (see [Section 7.4, “XPR Server Rules”, on page 234](#)):

```
NVS:FAXG3.*/*[ORG=NVS:FAXG3.*/*;RECDB(PREFERRED)=FAXG3;FLAG!=FLAG2]=
NVS:FAXG3.*/*[DEFER=120;FLAG=FLAG2]
```

The `DEFER` parameter can be used to set the time (in seconds) after which a fax received via call forwarding on busy should be redirected to the originally selected fax device.

There are two different ways of processing the job further, depending on the PBX settings.

If the fax device is still busy or busy again when this new delivery is attempted,

- either call forwarding on busy is repeated, so that the 1st delivery attempt by XPR is successfully processed; a new buffering job is generated. This loop does not end until the fax device is really free one time (default setting for Hicom 300: AMO COT without the parameters LWNC and DFNN but with NLCH)
- or call forwarding on busy is rejected and sent back to the caller by the PBX. In this case, the current delivery attempt is terminated and the redialing strategy of the FAXG3 protocol is used for sending the job again with the repeat cycles defined there.

Because XPR processes all fax jobs to the same destination phone number sequentially, a fax device cannot be addressed simultaneously more than once, even by the server.

If, however, another fax device is used as the output device after buffering, then

- the user data for the fax device configured as user in XPR should be extended to include a new data field `FAX2ND` (see [Section 34.2, “Adding a New User Data Field”, on page 1575](#)) and the call number of the deputy fax device should be entered here.
- the above routing rules should be changed to

```
NVS:FAXG3.*/*[ORG=NVS:FAXG3.*/*;RECDB(PREFERRED)=FAXG3;  
FLAG!=FLAG2]=NVS:FAX2ND/<DB>[FLAG=FLAG2]  
NVS:FAX2ND.*/*=NVS:FAXG3/*[FLAG=NOPREFERRED;ABORT=1]
```

Alternatively, a LAN printer can also be used as the output device. In this case,

- the user data for the fax device configured as user in XPR should be extended to include an entry in the `HOME-PRINTER` data field, which must contain a name of the printer configured in XPR and
- the routing rules must be correspondingly changed to

```
NVS:FAXG3.*/*[ORG=NVS:FAXG3.*/*;RECDB(PREFERRED)=FAXG3;  
FLAG!=FLAG2]=NVS:VM_PRINTER/<DB>[FLAG=FLAG2]  
NVS:VM_PRINTER.*/*=NVS:PRINTER/*[FLAG=NOPREFERRED;ABORT=1]
```

For greater control over busy problems in general, you should consider whether it would not make more sense to work more intensively with fax mailboxes. If XPR has the appropriate line equipment, there should then be no more busy states at all and all users can access their fax documents via the PC or telephone.

Another idea is to refrain from assigning the public fax number to a fax device, but rather follow the procedure described above and route all incoming fax documents for this fax number to XPR directly via activated fixed call forwarding and to output them using the routing rules mentioned at a printer or fax device whose call number is not made public. This allows parallel fax input to be serialized to a single terminal, thus reducing the number of required fax devices.

33.2 Event Signaling

The event signaling feature, familiar from Hicom 300 VMS, can also be provided in a similar form by XPR. Any event, even an external one, that, on a Windows computer that is networked with XPR, is able

- to activate a command line prompt,
- to start a batch file or
- to write an entry to the Windows Event Viewer

can be used to inform any group of receivers via

- call by telephone,
- FAX,
- SMS,
- Email and / or
- mailbox entry

of the existence of this event. In this way, service centers can easily be informed of the existence of particular events, even if the appropriate contact person is out of house.

Event signaling is achieved by using the components LogServ (this tool can be downloaded from the ftp server) along with the intelligent use of the Active Alert mechanism's filter functionality ([Section 7.1.1.3, "Active Alerts", on page 193](#)) in combination with different protocols, separate addresses or distribution lists.

When this feature is used in combination with SMS, please note that no GSM provider guarantees the delivery of SMS messages.

Priority transmission may also be necessary for this type of signaling. For more information refer to [Section 34.5, "Priority Control", on page 1577](#).

34 Tips and Tricks

34.1 Defining a proprietary TEMP Variable

Normally, XPR uses for temporary files the directories set for the system or the logged-in user in the environment variables TEMP or TMP.

To restrict the XPR use of directories, you can create the new environment variable XPRTEMP. You should create this variable as system variable as well as for the user account under which the XPR server services operate. It is used for example by Playwave and other TUI protocols.

NOTE: The XPRTEMP variable is not used by the Smart Backup. You can use [MaintenanceBackupTemp \[REG_SZ\]](#) instead.

You can then create this directory as exception in the antivirus software used. This prevents “Race Conditions”, under which XPR as well as the antivirus software want to simultaneously access the same file.

Proceedings:

1. Log on with the XPR service account under which the XPR server services operate also.
2. Create the new folder for temporary files on the drive with the most free memory. Example: D:\XPRTEMP
3. Open the **Properties** via the computer's context menu (rightclick on **Start > Computer**).
4. Click on **Change settings** to open the **System Properties**.
5. Go to **Advanced > Environment Variables....**
6. Create a new variable named **XPRTEMP** under both the user variables and system variables. This variable should contain the entire path of the above created new folder for temporary files as value.
7. The new temporary directory is active after an XPR server reboot.

34.2 Adding a New User Data Field

Special routing rules frequently require that you add an additional data field to the user data. This is done as follows:

1. Export the current user profile with a command line call:

```
infotool maskexport file=<path information>\schema.txt
```

2. Save the existing structure by copying the file just created:

```
copy <path information>\schema.txt <path information>\schema-  
new.txt
```

3. Editing the new schema:

The mask export creates a text file that can be edited with any text editor. To add a new user data field, the area `$mask USER` must be expanded. The database field is marked with upper-case letters and the input field is marked with a sequence of # characters. A single # character represents a check box. No tabs may be used in this area.

The `$attrib` field, which comes after the `$mask` part, must describe the new database field with its properties. It is important here that the data field name is separated from its properties by a tab and that all properties are separated from one another by commas. Examples of permitted properties are:

CHAR	character string
UNIQUE	unique
UPPER	only upper-case letters
LOWER	only lower-case letters

4. Save under the new structure name
5. Import the new user profile with a call from the command line

```
infotool maskimport file=<path information>\xprschema-neu.txt
```

Note that such a change to the Communications client will not be visible until the Communications client is restarted.

34.3 Copies of Received Messages

For specific mailboxes, copies of received messages shall be created, which are either placed in another mailbox, put out on a printer or forwarded. To this you define a new user data field named `COPY` and expand the rules for automatic routing copies (see [Section 7.4, “XPR Server Rules”, on page 234](#)) by one rule of the type:

```
NVS:*/*[FLAG!=CARBONCOPY]=NVS:COPY/<DB>
```

You can then enter an NVS address as alternative recipient for each mailbox.

Examples:

- `NVS:XPRSRV/HM` as alternative mailbox entry for the user `HM` on the server `XPRSRV`.
- `NVS:SMTP/hm@sample.de` as SMTP redirection destination.

34.4 Fax Delivery at favorable Tariffs

The users can assign priorities to the fax jobs. These priorities must be converted into system-specific delivery times if tariffs that are actually more favorable should be used. This is achieved by extending the user-specific routing rules by

```
NVS:FAXG3.*/*[PRIO>=LOW;FLAG!=FLAG1]=NVS:FAXG3.*/*[DEFER=21:00;FLAG=FLAG1]
```

This causes the transmission of all fax jobs with low (`LOW`) or very low (`NIGHT`) priorities to be delayed. The time of day at which the cost-effective transmissions should take place must be given as the value for `DEFER` (e.g. when there is a cheap or night tariff). Of course, other combinations of priority and transmission times are conceivable. Remember then the priority values that led to the greater or equal condition in the above rule:

```
URGENT (1000)
HIGH (4000)
NORMAL (5000)
LOW (6000)
NIGHT (10000)
```

34.5 Priority Control

A central fax or SMS server based on XPR is to preferably process the transmissions of a specific circle of subscribers. In this way send jobs of this circle of subscribers will not be delivered delayed if the send jobs by all users should accumulate. If the server applies originator checks to send jobs, you can make for all preferred subscribers an entry in a new user data field, which you query in the user-defined routing rules (see [Section 7.4, “XPR Server Rules”, on page](#)

234). Depending on this user data field you can then set the job priorities.

If the administration effort is too big or originator checks are not performed, it is advisable to define a new logical protocol. The privileged subscribers need to enter the name of this protocol as destination protocol. Via the user-defined routing rules a conversion into the correct physical protocol is then performed and also the desired priority assigned upon this conversion.

Example: a selected subscriber group should be allowed preferred SMS transmission. The protocol SMSS is defined and communicated to just this group of subscribers. All other subscribers continue to use the SMS protocol. The user-defined routing rules should be extended in this case, as an example, by:

```
NVS:SMS.*/*[PRIO!=LOW]=NVS:SMS.*/*[PRIO=LOW]
NVS:SMSS.*/*[PRIO!=HIGH]=NVS:SMS.*/*[PRIO=HIGH]
```

34.6 Line Control

When several GSM transmission boxes are used, it is particularly useful, depending on the destination phone number, to select the correct transmission box so that the least expensive provider is used for the transmission. This is achieved via routing rules (see [Section 7.4, "XPR Server Rules", on page 234](#)), which use a particular physical line, depending on the destination phone numbers.

Here is an example based on a possible configuration for Germany in which

- All SMS transmission jobs to D1 phone numbers (160, 170, 171, 172) to the first transmission box (lines 2-5)
- all calls to Eplus phone numbers (163, 177, 178) are to be transferred to the second transmission box (lines 6-8)
- all calls to Viag Interkom O-2 (176, 179) are to be transferred to the second box (lines 9-10),
- all other domestic calls should be transferred to the first box (line 11),
- calls to Austria are to be transferred to the first box (line 12) and
- remaining jobs are to be transferred to the second box (line 13):

```
NVS:SMS.*/*[ABORT=0]=NVS:MSGSM.*/*
NVS:MSGSM.*/+49160*[ABORT=0]=NVS:MSGSM.A0101/+49160*[ABORT=1]
NVS:MSGSM.*/+49170*[ABORT=0]=NVS:MSGSM.A0101/+49170*[ABORT=1]
NVS:MSGSM.*/+49171*[ABORT=0]=NVS:MSGSM.A0101/+49171*[ABORT=1]
NVS:MSGSM.*/+49172*[ABORT=0]=NVS:MSGSM.A0101/+49172*[ABORT=1]
NVS:MSGSM.*/+49163*[ABORT=0]=NVS:MSGSM.A0102/+49163*[ABORT=1]
NVS:MSGSM.*/+49177*[ABORT=0]=NVS:MSGSM.A0102/+49177*[ABORT=1]
NVS:MSGSM.*/+49178*[ABORT=0]=NVS:MSGSM.A0102/+49178*[ABORT=1]
NVS:MSGSM.*/+49176*[ABORT=0]=NVS:MSGSM.A0102/+49176*[ABORT=1]
NVS:MSGSM.*/+49179*[ABORT=0]=NVS:MSGSM.A0102/+49179*[ABORT=1]
```

```
NVS:SMMSGSM.*/+49*[ABORT=0]=NVS:SMMSGSM.A0101/+49*[ABORT=1]  
NVS:SMMSGSM.*/+43*[ABORT=0]=NVS:SMMSGSM.A0101/+43*[ABORT=1]  
NVS:SMMSGSM.*/*[ABORT=0]=NVS:SMMSGSM.A0102/*[ABORT=1]
```

Please note that these phone numbers cannot be unambiguously assigned to a provider anymore, since it is possible to keep one's phone number in case of a provider change.

35 Behavior in Case of an Error (Trouble Shooting)

When an error occurs, it will normally be reported to the Support. So that the Support can quickly start solving the problem with all information at hand as far as possible, we provide here some tips for compiling the information to be delivered.

35.1 Event Viewer

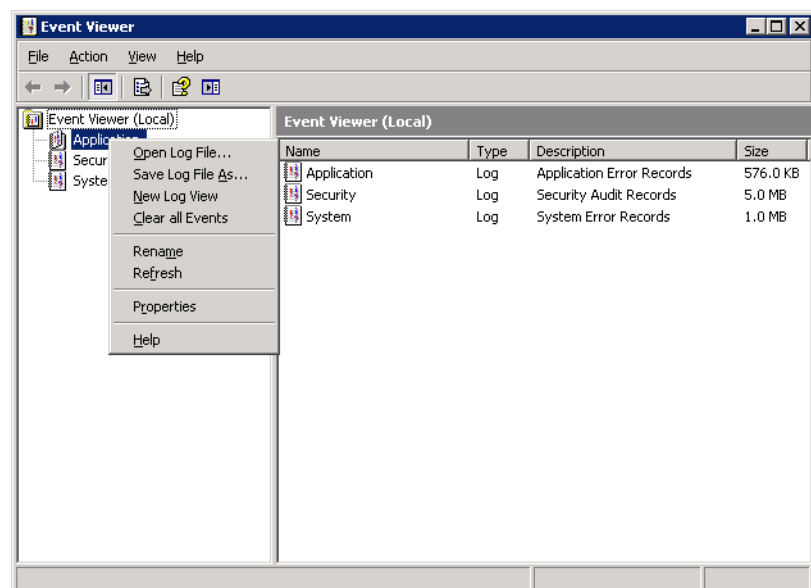
The Windows Event Viewer is a program which you can use to monitor all events in the system. In the Windows operating system, an event is any significant occurrence in the system or in an application that requires users to be notified. For critical events such as a full server or an interrupted power supply, a warning message may be seen on the screen. For many other events that do not require immediate attention, the Windows NT operating system adds information to an event-log file to provide information without disturbing the workload of the user. Windows adds event information to an event log file without interrupting your work at the computer.

The Event Viewer can be used to display and manage logs for system, security, and application events. Event logs can also be stored as an archive.

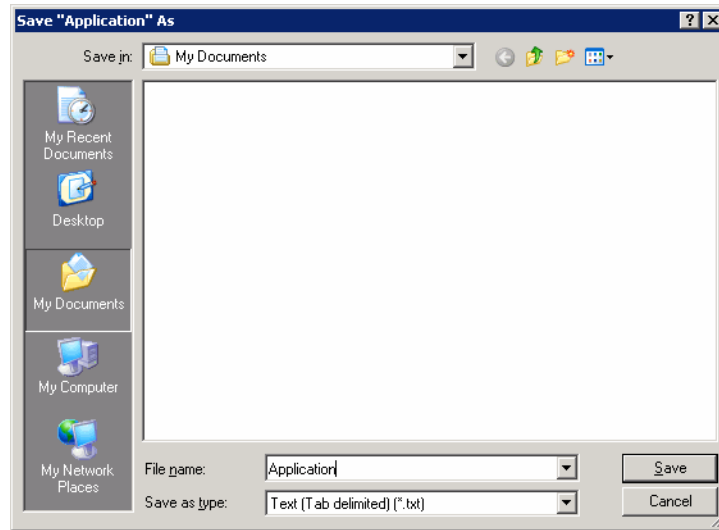
NOTE:

License violations are displayed in the event bar as error with the source MTA.

To find an error the Support coworkers usually need these precise archived event logs. To save a log, open its context menu with a rightclick:



Select the **Save Log File As...** option.



Set the **file type** to **Text (Tab delimited)**. Then specify a name for this log and save it.

NOTE:

Never use the other possible file types, since this will make the log evaluation difficult or even impossible.

Repeat this procedure for the other logs of the event display, always assigning a different name.

35.2 XPR Monitor

The log that contains the error case should be created in a single file. Several log files that cover single APLs each complicate the time flow overview. The argument that a separate log file for each APL improves clarity is also not really a valid one here since filter and search functions in a suitable editor serve clarity purposes at least just as good.

Please note that the system performance may be affected by the log creation. Especially in case of the MTA the system behavior should be watched and, if required, the respectively highest log level (debug 4, debug 3, ...) not be logged. Though this will aggravate the error search at a later date it is possibly the only way to receive a usable error log at all.

35.3 Overview of the installed Components

Via [SystemVersionInfo](#) you can write the installation history and the version level of all installed XPR system components in a file. See also [Section 32.12](#), “[SystemVersionInfo](#)”, on page 1555.

35.4 Client Protocol

To obtain an error log in case of client applications, use the [UnifiedLogTool](#) program on the client concerned. See also [Section 32.14](#), “[Logging Tool for Clients](#)”, on page 1558.

A Document Formats

XPR supports diverse document formats. In most cases they are given in the form of a token when necessary. We differentiate between master formats that can include any other formats, so that an upper class is formed from text, graphic and audio formats. In addition, there are also printer formats which appear only in connection with a Print APL line exported by an NVS server. The NVS server was an early predecessor of the XPR server and ran on the real-time operating system QNX.

A.1 Master Formats

Token	Format Description
BIN	All file formats not recognized by XPR. They comprise especially binary formats like Word files, Excel Sheets, ... The formats can only be converted into the fax format by the applications converter of the XPR server.
EML	Internet MIME standard electronic mail format.
PMF	Cycos multi-document format.

A.2 Text Formats

Token	Format Description
AS7	Text in 7-bit ASCII font.
ASC	Text in ASCII font (codepage 437, standard DOS font with IBM symbols).
MIT	7-Bit ASCII coded 8-bit MIME text. Display is as TXT.
TLX	Telex ITA2 font.
TTX	Teletex T.61 font.
TXT	Text in ANSI font (codepage 850, standard Windows font).

A.3 Graphic Formats

Token	Format Description
BMP	Windows bitmap. Result of fax conversion.
DCX	Multi-page PCX format (default fax format from Microsoft)
FG3	Cycos Fax G3 format. This format is replaced with the new default fax format TG3.
FG4	Cycos Fax G4 format. This format is replaced with the new default fax format TG4.
BMP_COL	Fax data in bitmap converted into Windows BMP standard. A trilinear gray scale interpolation is performed.
JPG	This format usually occurs if fax data were converted into a JPEG format with 9 gray scales.
PS	Adobe PostScript format.
TG3	Compressed multi-page TIFF Fax G3 format
TG4	Compressed multi-page TIFF Fax G4 format
TIF	Compressed single page TIFF fax format.
TIF_BMP	This compressed TIFF fax format is not supported anymore. When you select this format, a program configurable via TiffToExternalConverter [REG_SZ] is invoked instead, which converts TIFF into an arbitrary format. In the <code>XpressionsInstall\AddOn\Fax-to-Pdf</code> directory of the product data carrier you find, for example, a converter for delivering fax messages as PDF. When you activate this external conversion, you should not have selected any further graphics formats beforehand. In the GUI this format is selected via the External Converter setting.
TIF_MUL	Compressed multi-page TIFF fax format. This format is obsolete and should not be used anymore.

NOTE:

Ever so often a TIFF is not consistent with the specification. You can view this specification, for example, under <http://www.dcs.ed.ac.uk/home/mxr/gfx/2d/TIFF-f.txt>. According to this, only TIFFs with the pixel width 1728, 2048 or 2482 are allowed. We recommend the pixel width 1728. Documents deviating from the specification cannot be converted by the MTA and sent as fax. In this case you may try to link the TIFF mechanism described in [Section E.1.4, “Application Converter”, on page 1648](#) to another application. One option would be, for example, the Microsoft Office Document Imaging. The supplied program `imgprint.exe` is used by default setting.

IMPORTANT:

The fax standard defaults 1728 pixels with 204 dpi. This standard matches exactly a US Letter page, but is a bit wider than A4. XPR saves the inbound fax without any loss of information. But when printed out on A4, a received fax must

be downscaled or its margins cut to some degree. Most printers leave a blank margin on the document anyway, which aggravates this problem. XPR adjusts the printout to A4, so that a fax page is printed out as an A4 page.

NOTE: In case Imgprint is not able to convert scanned TIFF documents correctly and the conversion result is rotated and compressed,

In Windows 2008 The Desktop Experience feature can be used

- Activate Desktop Experience feature in Windows 2008 Server Manager
- Remove, or rename ...\\xpr\\bin\\imgprint.exe file
- Restart Xpressions
- Now Xpressions use the print / printto information from HKEY_Classes_Root "rundll32.exe"(Windows 2008 Desktop Experience).

Or Irfanview can be used as image printer, following the steps below.

- Install IrfanView for all users.
- Remove or rename ...\\xpr\\bin\\imgprint.exe file

If you associate the image extensions with IrfanView then the
HKEY_CLASSES_ROOT\\IrfanView.jpg
and
HKEY_CLASSES_ROOT\\IrfanView.png
will be used in place of
HKEY_CLASSES_ROOT\\.jpg
and
HKEY_CLASSES_ROOT\\.png

the same is valid for fax extensions:
HKEY_CLASSES_ROOT\\IrfanView.tif
will be used in place of
HKEY_CLASSES_ROOT\\.tif

The configuration has to be done in
HKEY_CLASSES_ROOT\\Irfanview.jpg\\shell\\printto\\command
HKEY_CLASSES_ROOT\\Irfanview.png\\shell\\printto\\command
HKEY_CLASSES_ROOT\\Irfanview.tif\\shell\\printto\\command

If you do not associate the image extensions with Irfanview then
HKEY_CLASSES_ROOT\\.jpg
will continue as jpegfile
and the configuration has to be done in
HKEY_CLASSES_ROOT\\jpegfile\\shell\\printto\\command
(same for TIFImage.Document, pngfile)

In both cases (image/fax files associated with IrfanView or not)

...\printto\command has to be

```
"c:\Program Files (x86)\IrfanView\i_view32.exe" "%1" /
print="%2"
```

or if IrfanView 64-bit was installed:

```
"c:\Program Files\IrfanView\i_view64.exe" "%1" /print="%2"
```

This has to be done for jpegfile (or Irfanview.jpg), TIFImage.Document (or IrfanView.tif), pngfile (or IrfanView.png).

Xpressions restart is required.

A.4 Audio Formats

Token	Format Description
AIFF	Audio format
AU	Audio format, found mostly in Unix environments.
PCM	Cycos ISDN Voice PCM coding.
WAV	Windows Wave RIFF Audio Format (uncompressed, 8 bit linear). As a matter of principle, this format has difficulties with quiet passages and should not be used anymore.
WAV_A	Windows Wave RIFF Audio Format (compressed, A-Law encoded, 8 KHz Mono).
WAV_MU	Windows Wave RIFF Audio Format (compressed, μ -Law encoded, 8 KHz Mono).
WAV_C	Windows Wave RIFF Audio Format (compressed, non-WAV_A or WAV_MU).
WAV_16	Windows Wave RIFF Audio Format (uncompressed, 16 bit linear). This is the recommended standard format.

A.5 NVS Printer Formats

The formats are only required by the Print APL of the NVS server on QNX. In other words, only when a remote system link to an NVS server exists.

Token	Format Description
PCL	HP-PCL -4 printer language with additional Cycos information for the Print APL of the NVS server.
PPS	Adobe Postscript Format with additional Cycos information for the Print APL of the NVS server.

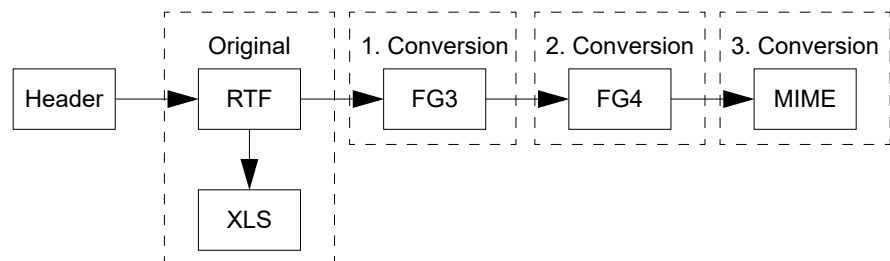
A.6 Multi Document Format (PMF)

The PMF format was developed for the implementation of e-mails with attachments within XPR. Formats from foreign mail systems can also be stored within the PMF format.

A PMF file always consists of a header and one or more representations of a document. The first representation is always the original format, which can also consist of numerous files. The following representations are made through conversions as required for display on the client or for transmission.

Example

Schematic structure of a document created in Microsoft Exchange (RTF with an Excel table) which is to be sent through a distribution list. Since the various database recipients have different preferences, the document is converted into a fax G3, G4, and a MIME document format. Please note that the MIME message contains the single files of the document created by Microsoft Exchange again, since MIME is also a format that can handle e-mails with attachments.



A.7 Format Conversions

To ⇨ From ↓	TLX	ASC	ANS	TTX	FG3	FG4	WAV	PCM	AS7	DCX	PS	DIB	DIBC	TIF DIBM	TIF FAX	BIN	JPG	AIFF	AU	TG3	TG4	WAV A	WAV U	WAV C
TLX		X	X	X	X	X	TTS	TTS	X	X	0	0	0	0	0	0	0	0	0	X	X	TTS	TTS	0
ASC	X		X	X	X	X	TTS	TTS	X	X	0	0	0	0	0	0	0	0	0	X	X	TTS	TTS	0
ANS	X	X		X	X	X	TTS	TTS	X	X	0	0	0	0	0	0	0	0	0	X	X	TTS	TTS	0
TTX	X	X	0		X	X	TTS	TTS	X	X	0	0	0	0	0	0	0	0	0	X	X	TTS	TTS	0
FG3	0	OCR	OCR	0		X	OCR +TTS	OCR +TTS	OCR	X	0	X	X	X	X	OCR	X	0	0	X	X	OCR +TTS	OCR +TTS	0
FG4	0	OCR	OCR	0	X		OCR +TTS	OCR +TTS	OCR	X	0	X	X	X	X	OCR	X	0	0	X	X	OCR +TTS	OCR +TTS	0
WAV	0	ASR	ASR	0	ASR	ASR		X	0	0	0	0	0	0	0	0	0	X	X	ASR	ASR	X	X	X
PCM	0	ASR	ASR	0	ASR	ASR	X		0	0	0	0	0	0	0	0	0	0	0	ASR	ASR	X	X	X
AS7	X	X	X	X	X	X	TTS	TTS		X	0	0	0	0	0	0	0	0	0	X	X	TTS	TTS	0
DCX	0	0	0	0	X	X	0	0	0		0	0	0	0	0	0	0	0	0	X	X	0	0	0
PS	0	0	0	0	PS	PS	0	0	0	0		0	0	0	0	0	0	0	0	PS	PS	0	0	0
DIB	0	0	0	0	X	X	0	0	0	0	0		0	0	0	0	0	0	0	X	X	0	0	0
DIBC	0	0	0	0	0	0	0	0	0	0	0	0		0	0	0	0	0	0	0	0	0	0	0
TIF DIBM	0	0	0	0	0	0	0	0	0	0	0	0	0		0	0	0	0	0	0	0	0	0	0
TIF FAX	0	0	0	0	X	X	0	0	0	0	0	0	0	0		0	0	0	0	0	0	0	0	0
BIN	0	0	0	0	BIN	BIN	0	0	0	0	0	0	0	0	0	0	0	0	0	BIN	BIN	0	0	0
JPG	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
AIFF	0	0	0	0	0	0	X	0	0	0	0	0	0	0	0	0	0	0	X	0	0	0	0	0
AU	0	0	0	0	0	0	X	0	0	0	0	0	0	0	0	0	0	X	0	0	0	0	0	0
TG3	0	OCR	OCR	0	X	X	0	0	OCR	X	0	X	X	X	X	OCR	X	0	0	0	X	0	0	0
TG4	0	OCR	OCR	0	X	X	0	0	OCR	X	0	X	X	X	X	OCR	X	0	0	X	0	0	0	0
WAV A	0	ASR	ASR	0	ASR	ASR	X	X	0	0	0	0	0	0	0	0	0	X	X	ASR	ASR		X	X
WAV U	0	ASR	ASR	0	ASR	ASR	X	X	0	0	0	0	0	0	0	0	0	0	0	ASR	ASR	X		X
WAV C	0	ASR	ASR	0	ASR	ASR	X	X	0	0	0	0	0	0	0	0	0	0	0	ASR	ASR	X	X	

Legend:

X	Conversion always possible
TTS	Conversion possible if text-to-speech software is installed and licensed.
ASR	Conversion possible if automatic voice recognition software is installed and licensed (not supported at present).
PS	Conversion possible if MgoSoft library is installed (default). IMPORTANT: Ghostscript must not be used anymore In order to avoid any vulnerabilities or any conversion issues using Ghostscript, please delete the contents from <code>res\convert\ghostscript</code> folder and Disable Ghostscript, see DisableGS [REG_DWORD] .
OCR	Conversion possible if OCR software is installed and licensed.
BIN	Conversion possible if fax service software is installed and licensed.
0	One-step conversion not possible (in general, conversion is not possible on white background).
BLUE	Audio formats
GREEN	Text formats
YELLOW	Two-step conversion possible.
PINK	One-step conversion.

A.7.1 Multi-format Documents

Conversion between PMF and E-MAIL is possible.

PMF

A PMF file contains multiple conversions or representations of one and the same document. All simple document formats can be added to a PMF file.

PMF can create new representations of a document contained or extract it as a document type, if permitted by the above matrix.

Two-step conversions are also possible:

- e.g. FG3 to WAV: can be performed via FG3 > TXT > WAV (fax reader)
- e.g. PS to DCX: can be performed via PS > FG4 > DCX

E-mail

An e-mail file contains a body text and no, one or multiple attachments.

Every document format can be converted into e-mail.

One-step conversions make working with a built-in viewer convenient.

Original format is FG3

- E-mail can contain an FG3 attachment (no one-step conversion)
- E-mail can contain a TIFF attachment (one-step conversion)
- E-mail can contain a JPEG attachment (one-step conversion)

Original format is PCM

- E-mail can contain an AU attachment (no one-step conversion, no playback software available)
- E-mail can contain a WAV attachment (one-step conversion, playback software available)

A.8 Application Conversions

The MTA can convert specific application formats into a fax format by invoking an associated application. Application converters are available with the following programs for the formats:

Microsoft Office 2016/2021/2024/365 Apps

Microsoft Word	doc, rtf, html
Microsoft Excel	xls
Microsoft PowerPoint	ppt, pps
MgoSoft Library*	pdf

* **MgoSoft Library** has already been installed as part of the kernel setup. If problems occur, you can disable this conversion by means of DisableMgo [REG_DWORD] and try other applications.

IMPORTANT:

The customer needs to ensure that the Microsoft licensing conditions are observed also for the client licenses required when using the OpenScape Xpressions server conversion for Office documents. The required Microsoft licenses are not included in the scope of delivery and must be provided by the customer.

Other application conversions are not approved, but you can use them project-specifically without producer support. You find more information about project-specific use in [Section E.1.4, “Application Converter”](#), on page 1648.

IMPORTANT:

To enable the MTA performing an application conversion under Windows Server 2008 or higher, it must run under a user account. Application Conversion requires a default printer that, however, is not offered for the local system. As a result, the Application does not start and no conversion can be performed.

NOTE:

The application conversion for fax messages sent via the XPR occurs using third-party applications such as the Microsoft Office package. Some foreign applications under heavy load may cause problems that prevent the conversion of further fax messages after some time. The interfaces of the foreign applications are in this case in an undefined state. This problem cannot

be solved by the XPR. If a customer system encounters such a problem, we recommend a regular operating system reboot. This will prevent uncontrolled interruptions of the XPR system operation.

IMPORTANT:

When using fax stationery created with Communications you need to take special care. In case of an application conversion a graphics page is created from the document, which is then covered with the fax stationery. As a result, the company logo on the fax stationery may hide text.

NOTE: Due to security methods, the actions that can be performed on PDF documents are limited. For this reason, documents may not be convertible with Xpressions embedded MGOSoft library. External tools should be used in such cases. For more information, please refer to [Section E.1.4, “Application Converter”, on page 1648](#).

In the following you find some common problems and solutions.

A.8.1 Wrong Directory for temporary Files

The application conversion fails if the directory for temporary files points to a user directory. To examine this, check the registry value `DefaultDir (REG_SZ)` in the `HKLM\Software\Wow6432Node\PP-COM\FaxMon` key. The system directory for temporary files should be referenced there. This directory is normally `C:\Windows\temp`.

A.8.2 Windows Spooler Service

Microsoft is currently recommending the following two options for the mitigation of the following vulnerability:

<https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-34527>

Options:

- **Option 1** - Disable the Print Spooler service
- **Option 2** - Disable inbound remote printing through Group Policy

Option 2 is the one recommend when Xpressions is in use.

Important: Please do not use Option 1 since this would affect Xpressions functionality (usage of printapl and Office document conversions when sending faxes and any other applications configured as PSR using section Sect. E.14 from Server Administration manual will not work)

Using Microsoft remediation Option 2 will prevent the remote code execution, local code execution with privilege escalation will still be possible.

A.8.3 Conversion Error in Case of MS Office

As remedy do not operate the MTA service under the *System* user account but under a normal user account. Please assign the account the **Log on as a service** privilege under **Local Security Policy > Local Policies > User Rights Assignment**.

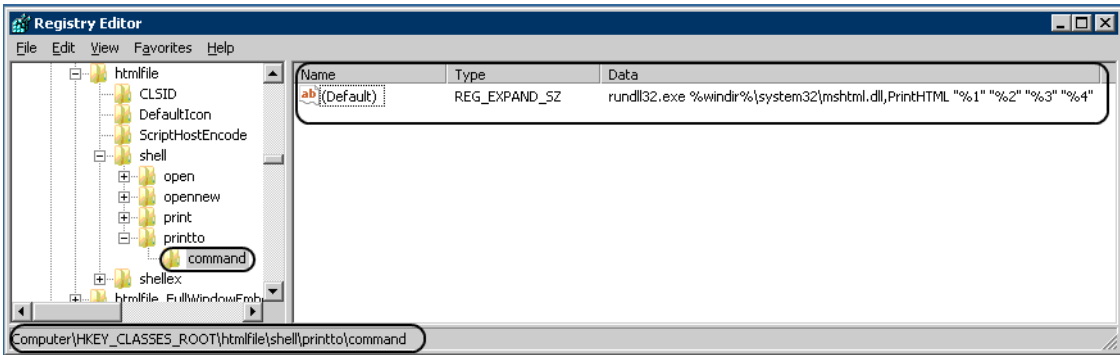
Start the Office applications under this user account once to avoid entering the user name and its initials.

A.8.4 Switching the HTML Conversion to Microsoft Word

HTML conversion has been released for Microsoft Word. Ever so often it is not correctly linked to Microsoft Word, though. To determine the currently active link you can reboot the SMTP APL. At the start it displays the linked applications for various file extensions. In case of HTML this information would be something like:

02.10:17:03.054 SmtplApl | BinToFax: Documents with extension .htm are fax printable (Key: htmlfile)
02.10:17:03.054 SmtplApl | BinToFax: Documents with extension .html are fax printable (Key: htmlfile)

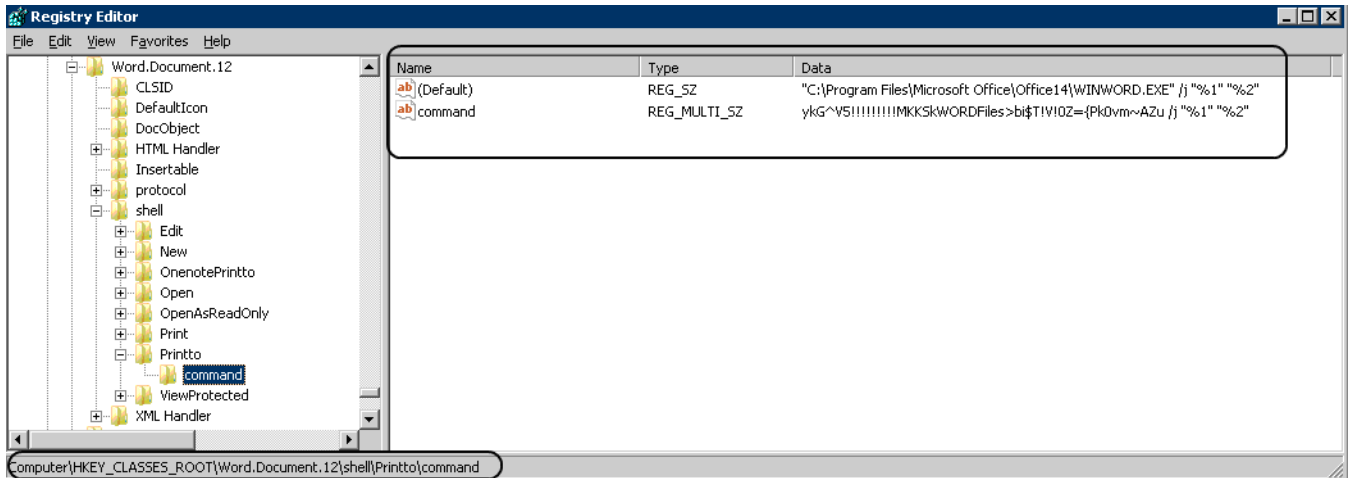
The application results from the specification Key: `htmlfile`. You can now see the application used with files ending on `HTM` or `HTML` for printing in the registry under `HKEY_CLASSES_ROOT\htmlfile\shell\printto\command`.



Just like for HTML we now determine the key of the installed Microsoft Word version:

02.10:17:03.053 SmtplApl | BinToFax: Documents with extension .docx are fax printable (Key: Word.Document.12)

Here too we find the corresponding entry under `HKEY_CLASSES_ROOT`. In our example this would be for `Word.Document.12`:



Both these entries must now be entered under `HKEY_CLASSES_ROOT\htmlfile\shell\printto\command`. The simplest way is here to export this key. You receive a *.reg file. You can edit this file using e. g. Notepad, changing the line `[HKEY_CLASSES_ROOT\Word.Document.12\shell\printto\command]` to `[HKEY_CLASSES_ROOT\htmlfile\shell\printto\command]` in there. You can run the changed *.reg file as administrator, thus importing the desired information to the right position in the registry.

NOTE: In Office 2021/2024 and 365 Apps the printto command path is different, as follows:

`HKEY_CLASSES_ROOT\Word.Document.12\shell\Printto\command`
 (Default) = "C:\Program Files\Microsoft Office\Root\Office16\WINWORD.EXE" /j "%1" "%2"

A.8.5 Word and temporal Files

In case of a conversion, Microsoft Word leaves files in the directory for temporary files. Since such files are not automatically deleted by these programs and, consequently, we do not have an XPR problem here, we cannot offer a real solution but at least an evasion of this problem.

You should regularly delete all temporary files using a maintenance job. This maintenance job should be carried out in the TEMP directory as well as in the TEMP directory of the user under whose account the MTA runs.

Example of a batch invocation for deleting the temporary files of the user account:

```
@echo off  
del %TEMP%
```

To delete the temporary system files, another line must analog be implemented in the batch. In doing so, it is not possible to specify this directory via an environment variable, though. If required, please check the access privileges for the system's TEMP directory.

A.8.6 Microsoft Error Reporting

Problems may occur, if an application such as Microsoft Word wants to send error reports to Microsoft. This is, for example, the case, when a document cannot be opened properly. If the XPR server does not have an Internet access, this error report cannot be sent to Microsoft.

For each attempt to send an error report, a Windows Task dw20.exe is generated, which stays permanently active. At the same time, the faulty documents are deactivated by the respective office application and are then found under "deactivated elements". Such elements seem to block the XPR after a while.

The remedy is to deactivate the Microsoft error reporting. To this, open the **Advanced** tab and click on **Error Reporting** under **Start>Control Panel>System**. A dialog opens, in which you select **Disable error reporting** and remove the tick set for the **But notify me when critical errors occur** option. A click on **OK** makes the error reporting feature disappear.

The Windows service for the reporting is still active though. To disable this service as well, click on **Administrative Tools** and open the **Services** there. Doubleclick **Error Reporting Service** and set the Startup type to **Disabled**. Confirm with **OK** and the Windows error reporting is entirely disabled.

A.8.7 Switching the HTML conversion to Bersoft HTMLPrint

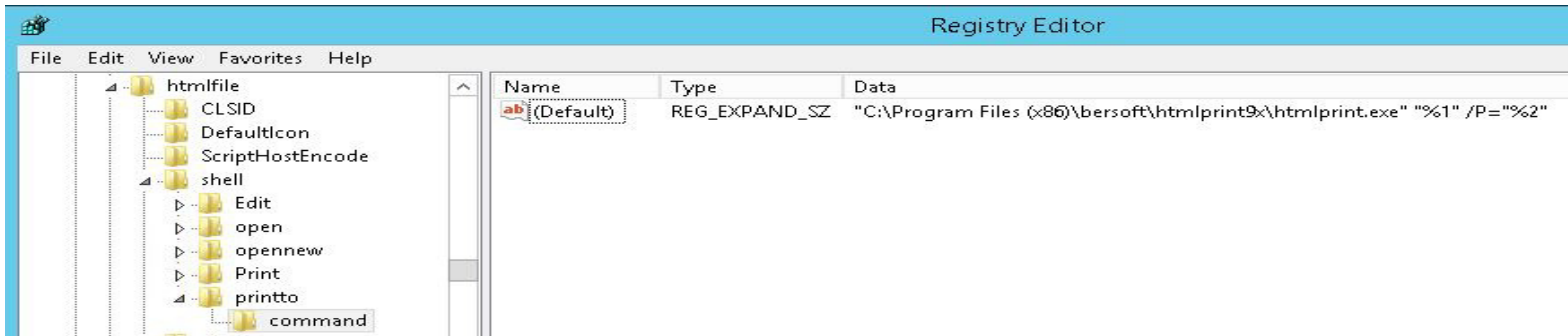
HTML Conversion has been released for Bersoft HTMLPrint.
Version 9.06 from Bersoft (<http://berswoft.com>)

To determine the currently active link you can reboot the SMTP APL. At the start it displays the linked applications for the various file extensions. In case of HTML this information would be something like:

02.10:17:03.054 SmtplApl | BinToFax: Documenst with extension .htm are fax printable (Key: htmlfile)

02.10:17:03.054 SmtplApl | BinToFax: Documenst with extension .html are fax printable (Key: htmlfile)

The application results from the specification Key: htmlfile. You can now see the application used with files ending HTM or HTML for printing in the registry under HKEY_CLASSES_ROOT\htmlfile\shell\printto\command.



the default registry key content need to be changed as follows:

[HKEY_CLASSES_ROOT\htmlfile\shell\printto\command]
"C:\Program Files (x86)\bersoft\htmlprint9x\htmlprint.exe" "%1" /P="%2"

NOTE:

Please, be aware that this path may change depending on the Bersoft HTMLPrint installation. Please, adjust it if necessary.

You can run the changed *.reg file as administrator, thus importing the desired information to the right position in the registry.

B Xpressions Forms SMTP for Outlook 2007

NOTE:

The Outlook Forms are elements of the optiClient Extensions. The standard installation is described in the *Server Installation* manual. The normal procedure is the invocation of `Setup.exe`, which installs the required `vcredist_x86.exe` and subsequently starts the setup of the MSI packet as well as in the `Setup.ini` configuration file. In case of an installation via the `Setup.exe` the configuration set in `Setup.ini` overrides the one of the MSI packet.

IMPORTANT:

With XPR 5 the installation was adapted to Microsoft Installer (MSI). A side effect of this adaption is that an upgrade from the old versions is no longer possible. The Outlook forms previously installed with another setup program must first be uninstalled. Subsequently, the current Outlook forms can be installed via MSI.

B.1 General Information about the Xpressions Forms SMTP for Outlook 2007

Depending on the system environment two methods of implementing local Outlook forms SMTP for Outlook 2007:

1. For systems based on Microsoft Exchange Server in conjunction with Outlook 2007.
This version is used if you operate Microsoft Outlook natively at a Microsoft Exchange server. For this purpose, the components *Server Based Forms* are used in combination with the *Server Based Forms Client Components*. This version is comprehensively described in the *Microsoft Exchange Gateway* manual.
2. For systems based on XPR Server
In this case Microsoft Outlook is directly connected to the XPR server by IMAP or POP3 protocol. New messages are sent to the XPR server by SMTP via the SMTP APL . In this case the Outlook forms are used as "local forms for SMTP". This version's configuration options are described in the following.

NOTE:

The local forms for SMTP cannot be installed in a terminal server environment.

The operation of the local Outlook forms for SMTP is identical with the forms Outlook uses for the connection to a Microsoft Exchange server. Only the toolbar contains additionally the  button. Via this button the message icons in the Outlook inbox journals can be refreshed. This is necessary when the message icons are no longer set correctly after a specific period because of an error in Outlook.

For the description of the local forms for SMTP operation please refer to the *Outlook Extensions* manual.

You can use the local forms for SMTP in parallel with the *OpenScape Xpressions optiClient 130*. They thus form a part of the *optiClient Extensions*. For the installation please refer to the *Server Administration* manual. How to operate the *OpenScape Xpressions V7 optiClient* is described in the *optiClient* manual.

B.2 Silent Setup

When you invoke the MSI installation packet for the local forms via the command line using `msiexec`, you can run the installation via the `/quiet` parameter without user interaction.

At the same time, two so-called public properties must be transferred to the MSI installation packet, which would otherwise be queried interactively. These properties are the Web Assistant URL (`PWEBADMINLNK`) and the IP address of the XPR server SMTP APL (`PSMTPSERVER`).

```
msiexec /quiet /i LocalForms.MSI  
PWEBADMINLNK="https://XPRServer.company.com/cgi_bin/webassistant/start"  
PSMTPSERVER="10.9.30.17"
```

NOTE:

`PWEBADMINLNK` can also be adjusted via the `Setup.ini` file. In case of an installation via the `Setup.exe` the configuration set in `Setup.ini` overrides the one of the MSI packet.

Test your configured Web Assistant URL before the installation by means of a Web Browser.

Further possible adaptations are described in [Section B.7, “User-defined Installation”](#), on page 1608.

B.3 Installation without Service Provider

You can install the Outlook forms without the Service Provider (MSP) via the public property `IGNOREMSP=1`. The MSP is a precondition for efficient conversation with the XPR server, though. Therefore this option should only be set if another client application has already been set up that contains the MSP.

B.4 Upgrading

In case of an upgrade, all registry values are usually correctly set already. Via the public property `NOOVERWRITE=1` you can instruct the MSI installer not to override any entries in the registry. The disadvantage is that newly accrued registry values are then not written either. Therefore, it may be more useful to override the registry values modified according to [Section B.7, “User-defined Installation”](#), on [page 1608](#) in the registry after the installation.

NOTE:

`NOOVERWRITE` can also be adjusted via the Setup.ini file. In case of an installation via the Setup.exe the configuration set in Setup.ini overrides the one of the MSI packet.

This is exactly what you can achieve via transforms. You find more information about transforms under http://msdn.microsoft.com/library/en-us/msi/setup/about_transforms.asp.

With the MsiTran program you can create transforms that contain the modifications between a genuine and an adjusted MSI. You create a transform with the following command line prompt:

```
Msitran -g original.msi modified.msi transform.mst
```

Subsequently, the `transform.mst` file contains the modifications compared to `original.mst` included in `modified.mst`. To apply such modifications to a new delivery at a later date, invoke the following command:

```
Msitran -a transform.mst neworiginal.msi
```

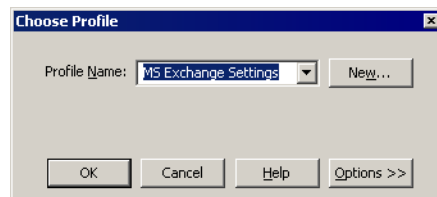
NOTE:

MsiTran is an element of the *Microsoft Windows Installer SDK* component of the *Microsoft Platform SDK*. The *Microsoft Platform SDK* is freely obtainable from Microsoft. The `BIN` folder of the *Microsoft Platform SDK* holds the `MsiTran.exe` program.

B.5 Adding to another User Profile

After the setup program is finished, all files on your system are stored in the folder that you have specified during the installation. After this “initial installation” the forms are now also available to other users by starting the `Formregister.exe` program with the `p` parameter in the directory `\Programs\Common Files\Forms`.

After the program start a window opens in which you first enter the IP address of the XPR server (SMTP APL). Then, in the next window, you select the Outlook profile of the user who also is to deploy the forms on this computer. Confirm your selection with **OK**.



NOTE:

You can suppress the IP address query via the additional parameter `s`. In this case, the IP address globally set with the initial installation is used.

NOTE:

The public property `ADDINFORALL` is not supported for the local Outlook forms.

B.6 Remove Forms for a User Profile

Analog to the procedure in [Section B.5, “Adding to another User Profile”](#) the forms for a user can also be uninstalled. For this purpose, call the `DeInstallBtn.exe` program with parameter `p` from the `\Programs\Common Files\Forms` directory. Afterwards select the Outlook profile of the user who is not to use the forms any longer. Confirm your selection with **OK**.

NOTE:

Via the public property `ADDINFORALL=1` you can already install the Outlook forms for all users of this computer during the installation. If the forms are installed in this way, they cannot be individually removed anymore. `ADDINFORALL` can also be adjusted via the `Setup.ini` file. In case of an installation via the `Setup.exe` the configuration set in `Setup.ini` overrides the one of the MSI packet.

NOTE:

The public property `ADDINFORALL` is not supported for the local Outlook forms.

B.7 User-defined Installation

B.7.1 Automatic Number Filtering

Key Software\Cycos AG\ExchForms Client
Name NoNumberOnlyResolution
Default Value 0

All numeric values entered in the e-mail address field are automatically interpreted as fax G3 address (0). This behavior can be switched off since it may lead to addressing errors, if your address entries in the global or personal address book are not only updated according to names but partly also to code numbers (1).

Key Software\Cycos AG\ExchForms Client
Name WatchIPMNote
Default Value 1

If you set this value to 0, no number entry is accepted in the address field when an e-mail is addressed. The form "Send fax" must then be used for fax transmission. The entry 1 resets this default to normal behavior. A number entry in the address field of an e-mail will then be considered a fax G3 address or a user ID depending on the setting under [NoNumberOnlyResolution](#).

B.7.2 Selecting Forms

In Outlook, all message forms are installed by default. However, you can exclude every single form from the installation. Therefore, set the corresponding entry to 1.

Key Software\Cycos AG\ExchForms Client
Name NoFaxBtn
Default Value 0

1 deactivates the fax icon and form.

Key Software\Cycos AG\ExchForms Client
Name NoSMSBtn
Default Value 0

1 deactivates the SMS icon and form.

Key Software\Cycos AG\ExchForms Client
Name NoFODBtn
Default Value 0

1 deactivates the fax polling icon and form.

Key Software\Cycos AG\ExchForms Client
Name NoVMBtn
Default Value 0

1 deactivates the voicemail icon and form.

Key Software\Cycos AG\ExchForms Client
Name NoWebAssistantBtn
Default Value 0

1 deactivates the Web Assistant icon.

Key Software\Cycos AG\ExchForms Client
Name NoVoiceViewForm
Default Value 0

1 deactivates the Active X object for voice mails.

Key Software\Cycos AG\ExchForms Client
Name NoFaxViewForm
Default Value 0

1 deactivates the Active X object for fax messages.

B.7.3 Changing the Telephone Number

Key Software\Cycos AG\ExchForms Client
Name ChangePhoneNo
Default Value 1

Via this option you can disallow the Microsoft Outlook client user to change the individual phone number. Therefore set the value to 0.

B.7.4 Fax Message Notifications

Key Software\Cycos AG\ExchForms Client\FAX
Name DeliveryReceipt
Default Value 1

Key Software\Cycos AG\ExchForms Client\FAX
Name ReadReceipt
Default Value 1

Normally you may request notices of receipt or read confirmations for fax messages. You can deactivate the option to request such receipts and confirmations here by setting the corresponding values to 0.

B.7.5 SMS Notifications

Key Software\Cycos AG\ExchForms Client\SMS
Name DeliveryReceipt
Default Value 1

Key Software\Cycos AG\ExchForms Client\SMS
Name ReadReceipt
Default Value 0

Normally you may request notices of receipt for SMS messages. You can deactivate the option to request such notices of receipt here by setting the [DeliveryReceipt](#) value to 0. The request for read confirmations is deactivated by default. You should keep this setting since in case of SMS the recipient does not transmit a read confirmation. Even the notice of receipt only means that the SMS message has reached the provider. Since the message is kept there only temporarily, it may not reach the recipient in spite of the notice of receipt. This may already happen if the recipient has his/her cell phone switched off for a few days.

B.7.6 Keeping Area Code "0"

Key Software\Cycos AG\ExchForms Client
Name NoZeroCut
Default Value 0

In most cases the phone number for fax and SMS messages is not suffixed with the leading area code 0 when it is selected from the address book (0). This results in a correctly normalized international phone number. With 1, the area code 0 is maintained. This behavior is required in some countries where this 0 is always dialed.

Example: In case of an Outlook-conformable phone number such as +49 (02404) 901100, the 0 of (02404) is not cut.

B.7.7 Replacing the leading Plus Sign

Key Software\Cycos AG\ExchForms Client
Name SubstituteForPlus
Default Value <Empty string>

Is used to automatically replace the leading + character by any digit combination. For this purpose, write the desired digit combination in the field.

B.7.8 Maximum Number of Characters for SMS Messages

Key Software\Cycos AG\ExchForms Client\SMS
Name TextLength
Default Value 160

This setting is used for restricting the number of characters in an SMS message. This may be required if you have specified an automatic prefix or suffix, for example for SMS messages, on the XPR server. The number of characters of this SMS code automatically enclosed in each message must then be deduced from the maximum number of possible characters.

B.7.9 Mailboxes in the POP3/IMAP Mode

Key Software\Cycos AG\ExchForms Client
Name WatchAllInboxes
Default Value 0

If you run Microsoft Outlook in POP3/IMAP mode and you have several message stores to which fax messages and voicemails are delivered by the XPR server, you have to enter a 1 here. In this way the correct message classes are set for incoming fax messages and voicemails, so that they can be directly displayed in Outlook.

IMPORTANT:

If you enter another value than "0" or "1", the correct message class cannot be set. Then the fax or the voicemail can only be opened as file attachment.

Key Software\Cycos AG\ExchForms Client
Name InboxNames
Default Value Inbox

If [WatchAllInboxes](#) has been set to 1, the inbox folders can be defined here, in which the system searches for fax messages and voicemails in order to set the correct message classes. Enter the inbox name in between the quotation marks. If several inboxes are to be monitored, the names are entered and separated by a semicolon.

Example: `Inbox;Mail from XYZ`

B.7.10 POP3 or IMAP

Key Software\Cycos AG\ExchForms Client
Name IMAPMode
Default Value 0

Default set is the access to the XPR server via POP 3. To set the IMAP mode, alter this value to 1.

B.7.11 No JPEG Fax Attachments

Key Software\Cycos AG\ExchForms Client
Name TifOnlyFaxAttach
Default Value <Does not exist>

If this registry value (REG_SZ) exists with any content, only TIFF attachments are interpreted as fax. Without this value also JPEG attachments are treated as fax.

B.7.12 Disable of Local Content search

Key Software\Cycos AG\ExchForms Client
Name DisableLCSearch
Default Value 0

During the address resolution (send Fax Button or check name), the LocalFormSmtplib looks for the fax number in all personal contacts. This takes much time, if several hundred are available. If this registry value (REG_SZ) is set to 1, the local contact search will be disabled.

C Installation of the Xpressions Outlook Forms for Outlook 2010 and further versions (VSTO Forms)

In order to provide support for Outlook x64 versions, a new Outlook Forms has been created. These new forms use a more recent technology (VSTO) and therefore provide better support for newer Outlook versions. Therefore, only these forms will be supported for Outlook 2010 and further versions.

IMPORTANT: If the system already has the old Xpressions forms installed, those will have to be removed before installing the new ones.

Most of the old forms functionality remains the same and some shortcomings were corrected. Also, the new forms are much easier to install. First of all, there is no need to install server components. There is only the client side installation. Furthermore, there is only one package which may be used both with the Exchange server and SMTP connection. It's only a matter of configuration.

NOTE: Detailed install information can be found in the document *OpenScape Xpressions V7, Client Installations, Installation Guide*, in chapter *Installing the Outlook Forms for Microsoft Outlook 2010 and further versions*.

D Lear

D.1 Definition and Function

This tool is accurately named *King Lear's e-mail canon*, as it serves for testing the transmission of messages and the performance of transactions.

The main task of the Lear tools is to send any test messages within the system. You can indicate different originator or recipient addresses as well as different message sizes. The amount of messages within a freely selectable time interval can also be set. You can test transmission paths of e-mails within the XPR system for efficiency and reliability by executing e.g. load tests in a certain time range. You can use statistics to analyze the sent and received messages for an evaluation of the performance of the transmission of these messages in the XPR system.

Furthermore, it is possible to perform transactions such as establishing a phone call within the system to test the feature here and determine load limits.

D.2 Configuration

Lear's configuration window is started via the XPR monitor. Therefore, select **Lear** in the **Preferences** list and double-click **Set Options**. You can choose from the four tabs **Test**, **Options**, **Statistics** and **Transactions**.

D.2.1 The Test Tab

The **Test** tab defines the details for the performance of a test run.

King Lears email canon!

Test | Options | Statistics | Transactions

Originator: NVS:LEAR/TESTER

Recipient: NVS:FA\G3/49240490181301

? chars in recipient address are replaced by random numbers. NVS:FA\G3/??? causes faxes send to random numbers between 0-999.

Count: 1 Period: 1000 Block: 1

Send <count>*<block> docs, every <period> ms <block> docs

Datafile

☐ Sonnet (15 Lines of text)

☐ Odyssey (complete volume, 620kB text)

☒ Fax 2pg 620kb

☐ Short message (one line of text)

☐ No file

☐ Hello! (16bit WAV Voice, 18kB)

☐ Empty PMF

☐ File (on server):

☐ Set extra PMF-Properties

Edit...

Execute Stop

OK Cancel Apply

The meaning of the fields is explained in the following table:

Field	Description
Originator	This field defines the originator of the test messages. The entry must be an NVS address. The default originator NVS : LEAR is preset.
Recipient	This field defines the recipient of the test messages. The entry must be an NVS address. The address is chosen at random by inserting a certain number of ? characters. The ? characters are replaced by haphazardly selected numbers and form the recipient address. Each ? character represents a digit. "???" can e.g. create the number sequences 000 to 999.
Count	In this field you can determine the number of messages to be sent in a certain time interval. The value must be between 1 and 1000000.
Period	This value defines the time interval during which sending the message is repeated in milliseconds. The entry must be between 1 and 1000000.
Block	The value determines how many messages are sent at the same time. The value of this field must be between 1 and 1000000.

Field	Description
Datafile	This field enables the selection of predefined messages in different sizes and of different types. Furthermore, it is possible to send any file (e.g. from My Documents) as message. The following options are available: • Sonnet (a short piece of text) • Odyssey (a long piece of text) • Short Message (one line for sending an SMS) • Voice (a voicemail) • Fax (a fax message) • No file • Empty file • File on server (a file of your own to be selected on the server)
Set extra PMF-Properties	By ticking this check box you can add additional properties to the files to be sent. It is possible to add certain values to the messages. This mechanism is e.g. used to overwrite values in fax stationery if this is not to be taken from the database.

By clicking the **Execute** button you can start the transmission of the messages and **Stop** it by clicking the corresponding button.

The **XPR Monitor** displays the confirmation messages as well as the errors in the transmission.

D.2.2 The Options Tab

Currently this tab only serves to view the parameters of the logical line `NVS : LEAR` such as formats or the speed. It is not possible to make any changes here.

D.2.3 The Statistics Tab

This tab shows the most important information on the messages and answers that have already been sent and the transactions you have performed. The term documents (Docs) implies your sent test e-mails, whereas a reply (Rep) means a report from the recipient to the originator. Thus an originator sends a “Doc” and receives as response a “Rep”. The XPR monitor logs the process of sending a message or of performing a transaction. Transactions will be explained in the following [Section D.2.4, “The Transactions Tab”](#).

Based on the listed information you can see how many messages were sent and received. In addition, you see how many actions or transactions were successfully or not successfully sent or received. The statistics relate to the Test tab as well as to the Transactions tab.

Furthermore, you can check the MTA Queue load. The MTA is responsible for the administration of the transmission of messages of any type. The queue is a waiting loop for messages processed according to their order of precedence (i.e. sent). In the **Send load** section the messages that are to be sent are displayed, whereas **Report load** shows the responses.

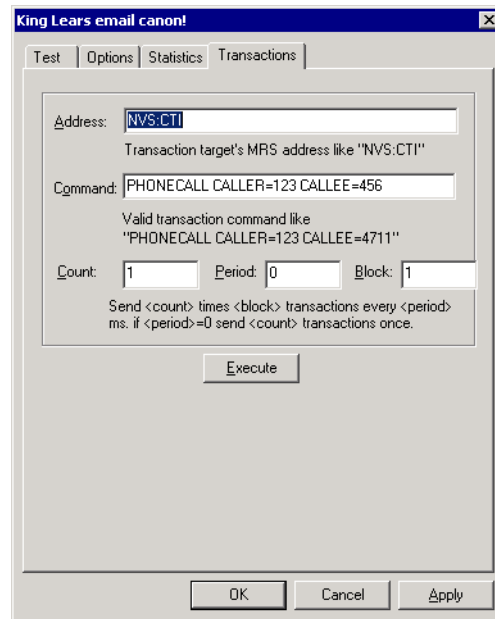
The transmission speed is given in transactions per second and always displays the maximum value at a time.

By clicking the **Reset** button you can reset the statistics to zero. Also clicking the **Cancel** button resets the statistics to zero.

If you click **OK** or **Apply**, the data will be stored, so that the new data will be added to the old data if you continue the testing process.

D.2.4 The Transactions Tab

The last tab **Transactions** allows to execute commands in a certain amount and time. As an example a telephone call within the system can be performed here.



The fields on this tab have the following significance:

Field	Description
Address	In this field you enter the destination address as NVS address. The messages are sent to this address.
Command	This field describes the command you are executing. For our example, the value <code>PHONECALL CALLER=123 CALLEE=456</code> is preset. This describes a telephone call command from 123 (caller) to 456 (callee). It is possible for you to enter other valid commands. You will find further commands in Chapter 17, "CTI APL" .
Count	This value specifies how the indicated transaction is repeated in a certain time interval. This value must be between 1 and 1000000.
Period	The value in this field indicates the time interval during which the transactions are executed in milliseconds. The value must be between 0 and 100000. A 0 in this field provokes that the number of performed actions corresponds to the Count value.
Block	This value indicates how many transactions are executed at the same time in a certain time interval. The value must be between 1 and 1000000.

By clicking the **Execute** button the transaction will be started. After the end of the time period the performance of the transaction will be stopped.

You can view the notifications of your transactions in the **XPR monitor**. Possible errors of the executing operation are listed here.

E Registry Reference

If not stated otherwise, all of the following registry key specifications are relative to HKLM\SOFTWARE\Wow6432Node\PP-COM\MRS.

E.1 Kernel Entries

E.1.1 General Considerations

DocumentationMode [REG_DWORD]

Default:	0
Possible values:	0 – DocumentationMode not active. 1 – DocumentationMode active.

IMPORTANT:

The DocumentationMode key must never be set in an operational system. Once this key has written all sorts of values in the registry, regular operation is no longer possible!

The XPR server writes only the most significant registry keys during the setup to the registry. If DocumentationMode is active, then all registry keys for that server release will be recorded. This feature is exclusively for the documentation of these values, since certain automatisms of the XPR server will no longer function otherwise!

E.1.2 Global Entries

These entries are reproduced from a distributed XPR server to all attached computers. The following values are found in key `MRS Globals`:

AllowDotInName [REG_DWORD]

In order to be backward compatible, by default XPR will not allow a dot in `USER_ID`. By setting (new) `REG_DWORD AllowDotInName` to 1 a dot can be used in the `USER_ID`.

Default:	0
Possible values:	0 – It is not allowed to use a dot in <code>USER_ID</code> . 1 – It is allowed to use a dot in <code>USER_ID</code> .

AllowHyphenInName [REG_DWORD]

In order to be backward compatible, by default XPR will not allow a hyphen in `USER_ID`. By setting (new) `REG_DWORD AllowHyphenInName` to 1 a hyphen can be used in `USER_ID`.

Default:	0
Possible values:	0 – It is not allowed to use a hyphen in <code>USER_ID</code> . 1 – It is allowed to use a hyphen in <code>USER_ID</code> .

AsrShareGrammars [REG_DWORD]

Is correctly created during the installation of the Automatic Speech Recognition. Modifications should only be made during a reinstallation of the Automatic Speech Recognition.

AutoUpdate [REG_DWORD]

Default:	1
Possible values:	0 – Automatic client updates off. 1 – Automatic client updates on.

The functionality for automatic client updates, based on the MSP, can be activated / deactivated here. Furthermore, this mechanism collects data about the installed client software and sends the Windows computer name, the client software name and the operating system version to the XPR server. This information is stored in the database.

AutoUpdateNoAdmin [REG_DWORD]

Default:	1
Possible values:	0 – Notifications for normal users off. 1 – Notifications for normal users on.

In case of automatic client updates activated via [AutoUpdate \[REG_DWORD\]](#) and notifications enabled via [AutoUpdateNotification \[REG_DWORD\]](#) you can disable notifications for users without administrator privilege here. These users cannot update the clients anyway and are only asked by message to contact their administrator.

AutoUpdateNotification [REG_DWORD]

Default:	1
Possible values:	0 – Notification function off. 1 – Notification function on.

In case of automatic client updates activated via [AutoUpdate \[REG_DWORD\]](#) you can disable the notification function here. Consequently, only information about the clients is collected.

BackupDirectory [REG_SZ]

Default:	<XPR Install>\Backup
Possible values:	Directory

Backup directory. Database backups generated by the Standard Maintenance Script are saved to this directory.

CertificateDirectory [REG_SZ]

Default:	<XPR Install>\res\certs
Possible values:	Directory

The SSL certificate which can be used by the SMTP as well as by the WEB APL is written into this directory.

CheckForDateConsistencyOnStart [REG_DWORD]

Default:	1
Possible values:	0 – Do not check date. 1 – Check date.

If active, a check is performed upon starting the XPR server as to whether the current date is between 1995 and 2038 inclusive. If this is not the case, booting the server is refused. This was designed to intercept BIOS errors with the year 2000 switch.

ClusterConfigurationActive [REG_DWORD]

Default:	–
Possible values:	0 – XPR does not run on a cluster system. 1 – XPR runs on a cluster system.

In a cluster system the database automatically runs in a master/slave mode. The slave system is determined by the [LocalSystemList \[REG_MULTI_SZ\]](#).

FastAsyncKernelShutdown [REG_DWORD]

Default:	0
Possible values:	0 – End all XPR services synchronously. 1 – End all XPR services asynchronously.

Normally the XPR server considers dependencies of the services during a Windows shutdown and ends the services in a certain order “synchronously”. All services of the XPR server can be ended simultaneously without considering dependencies. The database is securely shut down, but some losses may occur if e.g. the MTA needs to write to the database. This method should only be used in emergencies.

FolderDirectory [REG_SZ]

Default:	\\<Server>\MrsFolders\$
Possible values:	Share or Directory

The sub-directories `Folder0` to `Folder99` contain documents administered by the XPR server. The directory must be set as share in the event the XPR server is distributed over a number of servers. In this case the directory or share must be given in UNC notation. During the installation, the administrative network share `MrsFolders$` is automatically installed.

InfoStorRecordIDs [REG_SZ]

List of the Record- and Update-IDs for the five databases `JOURNAL`, `CORREL`, `GEB`, `DISTRIB` and `RECH`. Modification of these values leads to database inconsistencies!

Language [REG_SZ]

Default:	–
Possible values:	BRAZILIAN DUTCH ENGLISH FRENCH GERMAN ITALIAN PORTUGUESE SPANISH

The default language the XPR server applies for its status notifications. This also relates to messages visible for the user in the journal or other mail clients such as Microsoft Outlook. If the user receives a message via a reception way in which he/she can enter a differing language, the status notification will then be written or spoken in the language the user has set. This is e.g. the case for TUI.

LicSvcAddress [REG_SZ]

Default:	–
Possible values:	tcpip://<IP address>:13010

IP address of the license service. Via this service, licenses are requested from the HiPath License Management. This IP address normally points to the computer on which the XPR server is installed. For example, in cluster environments or in case of a multihome environment, you need to make sure that this address points to the correct network card. The port 13010 used cannot be modified.

LicSvcTimeout [REG_DWORD]

Default:	5 (seconds)
Possible values:	5 – 60 (seconds)

This is the time in seconds MTA or any APL waits for an answer from License Server.

LocalSystemList [REG_MULTI_SZ]

Default:	–
Possible values:	tcpip://<IP address>:13010
Default:	–
Possible values:	<Name>, <Path>, KERNEL <System index> [SLAVE]

All computers where XPR components are found are listed here. Each line contains the computer name and the XPR installation directory separated by a comma. On one computer the XPR kernel must exist. This is entered via the third parameter `KERNEL` of a line. On non-kernel computers the parameter

system index (SI=) must be given as the third parameter. The index must be unique and assigned sequentially numbered. The kernel computer automatically receives the system index 0. Example:

```

ULYSSES,d:\XPR,KERNEL
DILBERT,d:\XPR,SI=1
ACE488,g:\XPR,SI=2

```

The parameter `SLAVE` is indicated in a cluster system and exported by the value [ClusterConfigurationActive \[REG_DWORD\]](#) to run the slave database on this system.

MaxWaitForNTShutdown [REG_DWORD]

Default:	1000
Possible values:	Milliseconds

Wait time in milliseconds, see [NTShutdownFixActive \[REG_DWORD\]](#).

MonitorDirectory [REG_SZ]

Default:	\\<Server>\MrsMonitor
Possible values:	Share or Directory

Share of the monitor directory used for reloading the configuration modules.

MSClusterNodes [REG_SZ]

The names of computers on which InfoStor can run are entered here comma-separated with an XPR server installed on a Microsoft Cluster Server.

MwiRepeatOnFailure [REG_DWORD]

Default:	0
Possible values:	0: MWI don't use repeat strategy 1: MWI use repeat strategy

The entry should be done for ipapl (HKLM\Software\PP-COM\Mrs\lpapl). For MWI repeat strategy set the value to 1.

NCODirectory [REG_SZ]

Default:	\\<Server>\MrsNCOConfig\$
Possible values:	Share or Directory

Via this share the APLs and the NumberConversionAdmin read and write the NCO configuration. During the installation, the administrative network share `MrsNCOConfig$` is automatically installed.

Modifications to the directory should also be considered in [File Systems \[REG_MULTI_SZ\]](#).

NetworkAliveCheck [REG_DWORD]

Default:	0
Possible values:	0 or 1

If this registry value is set to 1 in the registry of the kernel system, the relevant APLs check on the satellites whether the connection to the kernel MTA via named pipes is set up and works. This check is performed every ten seconds. To enable this, the value is read by a satellite node at the start.

If the check fails and the registry value [NetworkTryReconnect \[REG_DWORD\]](#) is set to 1, the attempt is made to reconnect the kernel MTA exactly once. If this attempt fails, the APLs on the satellite are shut down.

If the check fails and the registry value [NetworkTryReconnect \[REG_DWORD\]](#) is set to 0, the APLs will shut down immediately.

If the watchdog on the kernel computer is active, it will try to relaunch the APLs on the satellite after their shutdown.

NetworkTryReconnect [REG_DWORD]

Default:	0
Possible values:	0 or 1

If this registry value is set to 1 in the registry of the kernel system, the satellites try to re-establish the named pipe if the connection to the kernel MTA via named pipes does not work anymore. If this attempt fails, the relevant APLs are shut down. In case of 0 the APLs would be shut down immediately. To enable this, the value is read by a satellite node at the start. See also [NetworkAliveCheck \[REG_DWORD\]](#).

NonInteractiveServices [REG_SZ]

Default:	NVS:FAXG3,NVS:FAXG4,NVS:VOICE,NVS:EFT,NVS:ISDNCTX, NVS:CIT,NVS:SMS,NVS:PRINTER,NVS:GSM,NVS:SMTP

A comma-separated list of all non-interactive services. The characteristic of a non-interactive service is that the XPR server cannot register the document deletion by the recipient. For messages sent by these services the flag `DELREC` (Deleted by Recipient) would thus never be set. To consider this characteristic in the maintenance script, the `$NONINTERACTIVE` maintenance script variable is defined via this entry.

NTShutdownFixActive [REG_DWORD]

Default:	1
Possible values:	0 – Console Control Handler not active. 1 – Console Control Handler active.

Since the Windows Service Control Manager synchronously notifies one service after another of a shutdown to enable a smooth shutdown by these services, it is possible that a service that does not react to this notification makes the Service Control Manager wait for a reaction forever.

Consequently, all further services do not receive the shutdown notification and are shut down by Windows just the same. They are not given the chance then to duly close databases etc.

Since Microsoft have still not solved this problem, an individual Console Control Handler was implemented. The Console Control Handler receives the shutdown notification from another source, allowing the XPR services to receive the correct shutdown notification, unless sent from the Windows Service Control Manager within the time entered in [MaxWaitForNTShutdown \[REG_DWORD\]](#).

SecurityIdentifier [REG_SZ]

Default:	<Empty>
Possible values:	<Empty> – All local administrators. EVERYONE – No security restrictions. DOMAIN\USER – The user from the domain. DOMAIN\GROUP – The user group from the domain. COMPUTER\USER – The local user on the computer. COMPUTER\GROUP – The local user group.

The Discretionary Access Control List (DACL) is set via this value for all XPR server named pipes. Via these named pipes e.g. the XPR monitor, DBTool and Infotool access the XPR server. The XPR components of a distributed XPR server communicate via these named pipes as well.

The presetting thus means that only local administrators can normally access the XPR server. It is of course possible to integrate domain users in the local administrators group so that the XPR administrator can administer the server remotely.

As presetting alternative a local user account or a domain user account can be specified as well. In this case only the specified user can configure the XPR server. Analog to the user, a local user group or one defined in the domain can also be specified.

We recommend, for example, the integration of a domain user account on the XPR server in the local administrators group. This account would then already be entitled to access via the preset privilege for local administrators. This is particularly useful with a distributed XPR server or cluster system,

since there all services should be started via a user account. So if this account is integrated in the local administrators group on all systems, the XPR server can be administered from all computers via this account.

The `EVERYONE` privilege is only available for maintaining the compatibility to older systems. With this configuration the DACL is not set and everyone authorized to access the XPR server with the tools mentioned.

Problems occur if the distributed XPR server is distributed among two different domains that do not trust each other. As example may serve an XPR server in domain 1 with an Exchange APL in combination with the Exchange server in domain 2. The Exchange APL and the Exchange server then operate on separate computers of course! This configuration can be useful as with a firewall between these domains fewer ports need to be opened. For such a case `EVERYONE` should be set here.

ServiceStartDelay [REG_DWORD]

Default:	0
Possible values:	Seconds

Time period in seconds for the MRS service to wait before starting the NameLoc and other XPR services. This is used when the server does not start automatically at the computer start, and the MRS service reports that the kernel module NameLoc could not be started.

SSL_TLSv1_Enable [REG_DWORD]

Default:	0
Possible values:	0: TLS 1.0 protocol disabled 1: TLS 1.0 protocol enabled

to full security both `SSL_CBC_Enable` and `SSL_TLSv1_Enable` must be set to 0.

By default TLSv1.2 is enabled.

This sets the parameter for Web APL, SMTP APL and IP APL

Refer to Registry keys of

- in Web APL [SSL_TLSv1_Enable \[REG_DWORD\]](#)
- in SMTP APL [SSL_TLSv1_Enable \[REG_DWORD\]](#)
- in IP APL [SSL_TLSv1_Enable \[REG_DWORD\]](#)

SSL_TLSv1_1_Enable [REG_DWORD]

Default:	0
Possible values:	0: TLS 1.1 protocol disabled 1: TLS 1.1 protocol enabled

Used to disable TLS 1.1 on WebApI

This configuration does not affect outgoing connections.

By default TLSv1.2 is enabled.

This sets the parameter for Web APL, SMTP APL and IP APL

Refer to Registry keys of

- in Web APL [SSL_TLSv1_1_Enable \[REG_DWORD\]](#)
- in SMTP APL [SSL_TLSv1_1_Enable \[REG_DWORD\]](#)
- in IP APL [SSL_TLSv1_1_Enable \[REG_DWORD\]](#)

StatisticsClasses [REG_MULTI_SZ]

Default:	*
Possible values:	[<Class> [, <SubClass>]]

This value contains a category respectively subcategory per line, for which statistic information is to be collected. Each APL entered here should generate statistic messages for the specified subcategories.

These statistics messages are then written by the XMR service into an individual log file in the stat directory. These can then be analyzed by the Report APL.

If only <Class> is entered then this APL polls information for all available subcategories. Instead of *Class* an * (asterisk) can be entered which is then interpreted as “all categories”.

SystemName [REG_SZ]

Default:	—

XPR server name.

IMPORTANT:

Since this name is contained in the database records, it may not be changed after the installation. If modified after the installation the kernel will not be able to read the database records.

SystemShutDelay [REG_SZ]

Default:	5
Possible values:	Seconds

Waiting time in seconds. After receiving the last job, the MTA waits this amount of time before it terminates. This makes sure that no jobs are still in the system.

SystemType [REG_SZ]

Default:	–
Possible values:	UMS – Unified Messaging Server VOICE – Voice-only Server

This global parameter controls the behavior of the system as regards send confirmations when a user logs on to VMS/PhoneMail. This behavior depends on whether the system is a Unified Messaging system or a voice-only server system.

Modifications to these settings require an XPR server reboot.

The available selections have the following effects:

- Unified Messaging Server (UMS)

With this selection, notices of receipt are sent according to the settings the user has made in the Web Assistant or in Communications. You must select this setting if the XPR server is connected to Microsoft Exchange or Lotus Notes.

- Voice-only server (VOICE)

With this selection the settings a user has made in the Web Assistant or in Communications for notices of receipt are ignored. Notices of receipt are always sent.

If you use the SMTP APL, select the Unified Messaging server (UMS) option, since the voice-only server option deactivates the settings for notifications and personal filters for e-mails in the Web Assistant.

TransportFormats [REG_SZ]

Default:	TLX,ASC,TXT,FG3,FG4,WAV,AS7,BIN,WAV_A,WAV_MU,PMF
Possible values:	See Appendix A, "Document Formats" .

The formats specified here are registered as valid formats with the router for the SMI transporters MAILBOX (Mail APL), TCPIP (TCP/IP APL), ISDN SMI (ISDN APL) and MODEM (V.24 APL).

UseCAasOrig [REG_DWORD]

Default:	0
Possible values:	1 – Callback access number from the user voicemail protocol as the originator

In order to use the Callback access number from the user voicemail protocol as the originator from the outgoing calls from Xpressions (instead of the users's voice number). IpApl restart is needed after change.

UserDirectory [REG_SZ]

Default:	\\<Server>\MrsUserdata\$
Possible values:	Share or Directory

The user directory must be set as share in the event the XPR server is distributed over a number of servers. In this case the directory or share must be given in UNC notation. During the installation the administrative share `MrsUserdata$` is automatically installed.

Modifications to the directory should also be considered in [File Systems \[REG_MULTI_SZ\]](#).

WebumKey [REG_SZ]

Default:	<random number>

For the Web Message access the URL is generated by means of this random number. If you delete or modify this value, all URLs generated before the modification do not work any more.

E.1.3 Converter

The following values can be found in the key `MRS Globals\Converter`.

AddMimeExtensions [REG_SZ]

Default:	*
Possible values:	* – Supplement all known extensions. – (Blank) Do not supplement extensions. <Extension>[, <Extension>] – Supplement only specified extensions.

If you have MIME attachments, they are flagged with a type. If the file name has no extension, the extension is automatically attached for a known type. Via a comma-separated list it is possible to restrict this automatic attaching of extensions to exactly this list. Via a blank this mechanism can be completely deactivated.

AllowPartialConversion [REG_DWORD]

Default:	0
Possible values:	0 – No partial conversion. 1 – Partial conversion.

Send only if document (Multi Document Format (PMF)) and all attachments can be converted. Otherwise the document will be sent with the convertible attachments. No note for parts that are missing because of an impossible conversion is added.

AlwaysDefaultLanguage [REG_DWORD]

Default:	0
Possible values:	0 – Speech recognition for TTS active. 1 – Always apply default language for TTS.

XPR tries to recognize the language of the text to be put out on the basis of keywords and thus help the applied TTS system with a correct pronunciation. You can disable the speech recognition here if it is unwanted. The default set language will always be used for the output then. See [DefaultLanguage \[REG_DWORD\]](#).

AutodetectPostscript [REG_SZ]

Default:	EXTENDED
Possible values:	NONE – No recognition of postscript in text file. NORMAL – Recognition only if file is postscript. EXTENDED – Extended recognition of postscript code.

With the extended recognition of postscript code a file is considered as postscript, even if the first 30 lines do not include postscript code. This can be the case e.g. for an e-mail.

BinToExt [REG_DWORD]

Default:	0
Possible values:	0 – Deactivated 1 – Activate conversion from BIN to TG3.

If a target allows only one format, an intermediate step must be activated that e.g. assembles an SMTP message with attachment to a common TIFF document. The TIFF document can then be converted to e.g. PDF via [TiffToExternalConverter \[REG_SZ\]](#). This intermediate step can be activated here for messages delivered to the LPR APL.

CheckTIFF [REG_DWORD]

Default:	0
Possible values:	0 – Deactivated 1 – Check TIFF.

When the IP APL receives a fax, it is occasionally forwarded to the MTA though no data was received. The originator receives a correct error report and sends his/her fax anew. But the received TIFF cannot be converted from BIN to TIFF in this case, so that a file with the BIN extension would be delivered to the recipient. This file, however, is of no benefit to the recipient since it does not contain any useful data. The MTA is able to detect this error when it checks the TIFF for valid data before the conversion. An incorrectly delivered fax is in this case ignored and not delivered.

ConverterFont [REG_SZ]

Default:	Lucida Console,18,0,5,0,0,0,0
Possible values:	, <SizeInPoints>, <Bold>, <Left Margin>, <Top Margin>, <Width>, <Height>

Default font for text after fax conversion if fax covers or logos of the no longer supported Client 2.50 are used. Otherwise, the font set in the MTA configuration or defined with the generation of Communications fax templates comes into effect.

CoverDir [REG_SZ]

Default:	\\<Server>\MrsUserdata\$
Possible values:	Share or Directory

Path to the user-specific resources such as fax stationery. Should not be modified.

DarkeningLevel [REG_DWORD]

Default:	0
Possible values:	0 – Deactivated 1 – Dark. 2 – Darker.
Requirement:	FixTif2Fax [REG_DWORD] is set to 1.

Improves the quality of converting a PDF to Fax by GhostScript. Ghostscript must not be used anymore. Disable it, see [DisableGS \[REG_DWORD\]](#).

DcxViewerLowResPatch [REG_DWORD]

Default:	0
Possible values:	0 – Deactivated 1 – Fax G3 always in high resolution after DCX conversion.

Fax G3 documents with a low resolution (200x 100dpi) would be converted to a higher resolution (200x 200 dpi) when the conversion target format is DCX. This is done since many DCX viewers cannot display the lower resolution fax documents.

DDESleep [REG_DWORD]

Default:	0
Possible values:	0 – Speech recognition for TTS active. 0...5000 Milliseconds

The Application Converter prints documents via DDE call. Some applications need more time to implement this call by DDE. Therefore, a waiting period can be taken here after the call. This waiting period is particularly required for slow computers.

DisableGS [REG_DWORD]

Default:	0
Possible values:	0 – “PDF-to-Fax” conversion via GhostScript. 1 – “PDF-to-Fax” conversion via GhostScript disabled.

The conversion of a PDF document to a fax is performed via the always installed GhostScript. This script may, however, not be able to convert any document. In such a case problems can be avoided by disabling the conversion here and trying the normal mechanism for PDF as described in [Section E.1.4, “Application Converter”, on page 1648](#).

IMPORTANT: Ghostscript must not be used anymore.

In order to avoid any vulnerabilities or any conversion issues using Ghostscript, please delete the contents from `res\convert\ghostscript` folder and disable it.

DisableMgo [REG_DWORD]

Default:	0
Possible values:	0 – “PDF-to-Fax” conversion via MgoSoft. 1 – “PDF-to-Fax” conversion via MgoSoft disabled.

The conversion of a PDF document to a fax is performed via the always installed MgoSoft Library. This script may, however, not be able to convert any document. In such a case problems can be avoided by disabling the conversion here and trying the normal mechanism for PDF as described in [Section E.1.4, “Application Converter”, on page 1648](#).

DefaultLanguage [REG_DWORD]

Default:	–
Possible values:	7 – German 9 – English 10 – Spanish 12 – French 16 – Italian 19 – Dutch 22 – Portuguese 25 – Russian

The XPR server attempts by word recognition to determine the language of a sentence to be put out via text-to-speech. If this recognition attempt fails, thus no language could be determined, the language set here is used. A speaker must be installed for the respective language of course.

EmailFaxWidth [REG_SZ]

Default:	800
Possible values:	400 to 1700

Fax width in pixels with fax conversion into an e-mail format (e.g. JPEG to MIME). This parameter enables resolution definition for fax documents.

FaxG3Resolution [REG_SZ]

Default:	200
Possible values:	100 or 200

Standard resolution by postscript to fax conversions for G3 fax.

FaxG4Resolution [REG_SZ]

Default:	200
Possible values:	200, 300 or 400

Standard resolution by postscript to fax conversions for G4 fax.

FaxMonitorLogfile [REG_SZ]

Default:	<Empty>
Possible values:	File name with path

If you need debug outputs of the internal fax printer driver (faxmon.dll), you can specify a text file with path here. Example: `c:\faxmon-output.txt`

FixTif2Fax [REG_DWORD]

Default:	1
Possible values:	0 – Deactivated 1 – Activated.
Requirement:	DisableGS [REG_DWORD] is set to 0.

Invokes the external program FixTif2Fax for correcting the conversion of a PDF to Fax by **MgoSoft library**.

fontHeight [REG_DWORD]

Default:	11
Possible values:	Font size

Font size with text-to-fax conversion. This is meaningless when fax templates are used since it is already implicitly included there.

fontType [REG_SZ]

Default:	Courier New
Possible values:	Name of an installed font type

Font type with text-to-fax conversion. This is meaningless when fax templates are used since it is already implicitly included there.

fontWeight [REG_DWORD]

Default:	400

Font weight with text-to-fax conversion. This is meaningless when fax templates are used since it is already implicitly included there.

GhostscriptPath [REG_SZ]

Default:	<XPR Install>\res\convert\ghostscript
Possible values:	Path

The path in which GhostScript is installed. This path is required for conversions from PostScript to fax. If you want to move the path after the installation, specify the new path here. Or install a new GhostScript version and modify the path for this newer version. GhostScript does not contain special adaptations to XPR.

Ghostscript must not be used anymore,

In order to avoid any vulnerabilities or any conversion issues using Ghostscript, please delete the contents from res\convert\ghostscript folder and disable Ghostscript, see [DisableGS \[REG_DWORD\]](#).

GSPaperSize [REG_SZ]

Default:	<Empty>
Possible values:	<Empty> – Use default page setting. a4 – Use A4 pages. letter – Use Letter pages.

If the document to be converted does not default a page size, the page size set here is used for converting PostScript files to Fax.

LogoGroup [REG_MULTI_SZ]

Default:	–
Possible values:	<User ID>,<Address Pattern>

The XPR user account and originator address are given per line and are separated by comma. These users can then have a fax logo or cover page referenced to this address. All users whose originator address pattern is conform to that of a given LogoGroup definition receive the corresponding fax stationery of the user specified here.

Example: GWUSER,NVS:GW.*/*

margin_b [REG_DWORD]

Default:	200

Setting of the bottom margin with text-to-fax conversion. This is meaningless when fax templates are used since it is already implicitly included there. The default value 200 corresponds to one inch (approx. 2.54 cm).

margin_l [REG_DWORD]

Default:	200

Setting of the left margin with text-to-fax conversion. This is meaningless when fax templates are used since it is already implicitly included there. The default value 200 corresponds to one inch (approx. 2.54 cm).

margin_r [REG_DWORD]

Default:	200

Setting of the right margin with text-to-fax conversion. This is meaningless when fax templates are used since it is already implicitly included there. The default value 200 corresponds to one inch (approx. 2.54 cm).

margin_t [REG_DWORD]

Default:	200

Setting of the top margin with text-to-fax conversion. This is meaningless when fax templates are used since it is already implicitly included there. The default value 200 corresponds to one inch (approx. 2.54 cm).

MaxFirstPagePrintTime [REG_DWORD]

Default:	60
Possible values:	Less than 120 seconds

Time-out, after which an application conversion procedure is considered failed. If during an application conversion (e.g. Microsoft Word to fax) a time-out occurs, one of the following reasons could be the cause:

- MaxFirstPagePrintTime is too short and the server requires more time to convert the first page to fax using the printer driver. In this case the value should be increased.
- More likely is that during the conversion by the MTA Service, the application (e.g. WinWord) itself is used by the MTA to convert the document to a fax with the MTA printing the document by means of the application. A lot of applications are coded unconventionally and become suddenly inactive, e.g. by displaying a dialog box. Here the printing process blocks until the time-out expires. Only the following workaround is possible: In the Service Control Manager the option **Allow Service to Interact with Desktop** is set for the service **XPR Message Router (MTA)** under **Startup**. Subsequently the application is repeated. The MTA visibly starts the application and one can see where the printing operation stalls. Two options are available:
 - a) The problem occurs only once. This can be a one-time initialization. In this case the option can be reset and the application conversion should run correctly in future.
 - b) The problem occurs always. In this case the application cannot be used for automatic conversion.

MaxPopupDialogs [REG_DWORD]

Default:	10

For certain application conversions some dialogs must be confirmed even though the programs are called in a mode described by Microsoft that should be run without interaction. Up to 10 dialogs are confirmed with OK so that the application starts printing.

NoGlobalFaxFormServices [REG_SZ]

Default:	–
Possible values:	<APL>[,<APL>]

All APLs entered here do not use the global system default for fax stationery. The global system default is the fax stationery assigned to user `DEFAULTFAXFORM`. The setting of this virtual user is used if no individual fax stationery has been assigned to the user. This is configured via the Web Assistant in the server settings.

IMPORTANT:

Modifications to this value require an MTA reboot.

PartialConversionServices [REG_SZ]

Default:	–
Possible values:	<XPR Service>[,<XPR Service>]

A list of services can be entered here where partial conversions for the originator is allowed. If, for example, a mail gateway always attaches an object that is not convertible, fax transmission should still be possible.

Example: MS, CC

PcmIsEurope [REG_DWORD]

Default:	–
Possible values:	0 – μ -Law Wave 1 – A-Law Wave
Remark:	See PcmIsWave [REG_DWORD] .

Coding used for Voice format. Available is μ -Law, which is mainly used in the U.S., Canada, Mexico, Hong Kong, Japan, and Taiwan and A-law, which is mainly used in Europe.

NOTE:

With XCAPi A-law is apparently always expected. This value must therefore be set to 1 also in countries where μ -law should actually be set.

PcmIsWave [REG_DWORD]

Default:	1
Possible values:	0 – Compatibility mode for older QNX servers. 1 – 16 Bit 8000Hz Mono Wave-Format.

Voice prompts always have the file extension .pcm, even when a wave is contained within. Depending on the setup, which sets [PcmIsEurope \[REG_DWORD\]](#), these are stored either in a μ -Law or A-Law coding format. If 0 is set here, [PcmIsEurope \[REG_DWORD\]](#) must be set to 1.

PostscriptToBinary [REG_DWORD]

Default:	1
Possible values:	0 – Convert postscript attachment to TIFF. 1 – Do not convert postscript attachment to TIFF.

Normally a postscript attachment is transmitted in binary form to the recipient. If this is not desired and the postscript file shall be converted into a TIFF attachment, this can be configured here.

PreloadedVoices<n> [REG_DW]

Default:	5
Possible values:	<Number of Speakers>

For each language <n> the number of speakers entered here is downloaded in the TTS engine already. Since it can take 20 seconds or even longer to download a speaker, this must be done beforehand. Depending on the TTS engine the required storage space varies with the speaker. Thus you should find a compromise between the number of the previously downloaded speakers and the used storage space.

PrintTextfileWithProgram [REG_MULTI_SZ]

Default:	PDF RTF HTM HTML SAM XML
Possible values:	<Extensions>

Documents the extensions of which are listed here will not be faxed as text documents but given out on the fax printer via a program. Examples are documents in RTF (Rich Text Format) or HTML (Hypertext Markup Language) the formatting instructions of which are contained in the text.

Furthermore, this entry also affects attachment handling by the SMTP APL. Text files must be able to withstand changes to the end-of-line representation according to RFC 822. But often enough they are not, therefore you can specify document extensions here, for which you basically desire binary handling.

You can enter one extension per line.

SapiVoices<n> [REG_BINARY]

Internal value.

StartPrintingTimeout [REG_DWORD]

Default:	120
Possible values:	Seconds

Entire timeout for the conversion to fax by means of the Application Converter. If the called application has not generated a fax document after the time set here, the job is cancelled. As soon as the next repetition, set at the fax protocol, is due, the next conversion attempt is started.

Tiff2Pdfa [REG_DWORD]

Default:	0
Possible values:	0 - Disable the feature 1 - Enables the feature

When enabled in conjunction with the "TiffToExternalConvert" and "TiffToExternalExtension=PDF" keys, it activates the Fax to PDF conversion via MgoSoft Library.

TiffToExternalConverter [REG_SZ]

Default:	–
Possible values:	<External Program> %1 %2

XPR can call an external conversion program that converts a TIFF Fax G3 format document into an arbitrary format. So that this program is invoked, TIFF Bitmap must be selected as target format for fax documents at the recipient. This format is no longer available. The external program, specified in this registry value, is called with the parameters stated here instead. The suffix of the converted file is specified in the registry value [TiffToExternalExtension \[REG_SZ\]](#).

So that this format is also transferred to a client in converted format, the `TIF_BMP` format must be supplemented in the [TransportFormats \[REG_SZ\]](#) value. In parallel verify that the formats `FG3` and `FG4` are not contained in this value. If required, delete them.

The freely available conversion program Fax2PDF quoted in the below example is delivered on the Add-On CD. *<XPR Install>* corresponds to the setup directory of the XPR server.

Example: d:\<XPR Install>\res\convert\Fax2PDF\Fax2PDF %1 %2

Note: In the Web Assistant a fax is always displayed in the JPG format. To also view the result of a conversion set here, you need to activate this option explicitly via [UseTiffToExternalView \[REG_DWORD\]](#).

TiffToExternalExtension [REG_SZ]

Default:	–
Possible values:	<Suffix>

File suffix for the file that is generated by the program specified in the [TiffToExternalConverter \[REG_SZ\]](#) entry.

Example: pdf

UnnecessaryToPrint [REG_MULTI_SZ]

Default:	.vcf .dat
Possible values:	.<Suffix>

File extensions for document types that are not printed or sent as fax. One extension is specified per line. .vcf (with dot!), given in the example, is used by some e-mail programs to attach some sort of business card to the e-mail. Since this business card cannot be printed, it can also not be sent to a fax device.

File attachments with the suffixes specified here are ignored in case of a conversion to a fax message so that no *Partial Conversion Error* is generated.

The file extensions specified here must be linked to an application that indicates that it is able to print this subdocument. With Windows Server this is e.g. not the case for .p7s. As workaround you can change the value (Default) to htmlfile in the .p7s value in HKEY_CLASSES_ROOT.

UseForTextToFaxA4 [REG_DWORD]

Default:	–
Possible values:	0 – Letter format. 1 – A4 format.

Paper format used in conversions from text to fax formats.

UseG4ResolutionForExtension [REG_MULTI_SZ]

Default:	<Empty>
Possible values:	<Suffix>

A page is displayed to the user on the monitor in the ideal format for resolution on the locally installed printer. Normally the Application Converter prints documents via the fax printer driver with a resolution of 200 dpi. This sometimes leads to a different pagebreak, e.g. a Microsoft Excel table displayed to the user on one page is then printed on two fax pages. This is actually an error in the Microsoft operating system. However, it can be avoided.

Since Fax G4 enables a higher resolution, this effect consequently occurs rarely and a conversion from Fax G4 to Fax G3 does not effect the page composition. You can enter one file extension per line here. First, a fax conversion to G4 takes place with accordingly higher resolution to use this effect.

In this case the preset 200 dpi need to be replaced by a higher value of course. We recommend 300 dpi since in most cases printers with 300 dpi or a multiple of 300 dpi are installed, so that the pagebreak comes closest to the display on the user's monitor. Invoke the MTA configurations in the XPR monitor and alter the resolution under Fax Conversion accordingly.

Example: XLS

UseLHTTS [REG_DWORD]

Default:	0
Possible values:	0 – TTS via SAPI 1 – TTS via Lernout & Hauspie

Either the proprietary installed and older Text-To-Speech system by Lernout & Hauspie or a Text-To-Speech system available according to the Microsoft Speech API (SAPI) is used.

UseTiffToExternalView [REG_DWORD]

Default:	0
Possible values:	0 – Do not display PDF in the Web Assistant. 1 – Display PDF in the Web Assistant.

If you have converted a fax to PDF via [TiffToExternalConverter \[REG_SZ\]](#), it will be displayed as picture in the JPG format in the Web Assistant just the same. This corresponds to the Web Assistant philosophy, i.e. usage via a simple web browser at all times without additional problems. By setting this value to 1, the fax that has been converted to PDF will be displayed as attachment in the Web Assistant. Each other conversion format would also be displayed as attachment, similar to PDF. PDF is here only an example of an externally created format.

WaveCodec [REG_SZ]

Default:	<Empty>

This audio codec is used for the option `REMOVECONVERSIONS` in the command `DELDDB` in maintenance scripts. This option can only be set via the MTA configuration from the XPR monitor. See [Section 7.1.1, “Automatic Maintenance”](#), on page 185.

WaveFormat [REG_BINARY]

Most audio codecs support numerous compression rates. The format set here of the Audio Codec set under [WaveCodec \[REG_SZ\]](#) is used. This option can only be set via the MTA configuration from the XPR monitor. See [Section 7.1.1, “Automatic Maintenance”](#), on page 185.

E.1.4 Application Converter

Under the key `MRS Globals\Converter\Faxprint` you can configure whether certain applications are to execute an application conversion to fax and if yes, how they are to do it. For a certain application a `REG_MULTI_SZ` is entered which contains the following values:

Line	Content
1	0 or 1. In case of 0 no application conversion can be performed for the further specified file extensions. This is possible with 1.
2	0 or 1. In case of 0 the method <code>Print</code> , in case of 1 the method <code>PrintTo</code> is used. The latter one is the default method of the application converter.
3 to 10	One file extension can be entered with preceding dot per line. Example: <code>.lwp</code>

NOTE:

An overview of the applications officially supported with the Application Converter can be found in [Section A.8, “Application Conversions”](#), on page 1592.

This is what you do to receive the name of the `REG_MULTI_SZ` for a certain application:

1. Open the window to `HKEY_CLASSES_ROOT` via the Windows registry editor.
2. In this window look for the correct extension. As an example we take `.doc` and find the entry “Word.Document.8”.
3. Now look for “Word.Document.8” in `HKEY_CLASSES_ROOT`.
4. Under the key `HKEY_CLASSES_ROOT\Word.Document.8` the key `shell\Print\command` or `shell\PrintTo\command` should be present. It contains the call to print out a document with the file extension `.doc` using the method `Print` or `PrintTo`. Thus you can verify whether the application supports the selected method.
5. In this case the name of the `REG_MULTI_SZ` should be “Word.Document.8”.

If the selected method does not work you can try another one. If both methods do not work, you can enter another application. Thus you could e.g. enter “Wordpad.Document.1” instead of “Word.RTF.8” for `.rtf`.

The extension `.lwp` of a Lotus WordPro document is an example of the method `PrintTo` not working so that for this method with installed Lotus SmartSuite a registry value must be generated for using the method `Print`. The value would appear like this:

WordPro.Document [REG_MULTI_SZ]

Content:	1 0 .lwp

Thus allowing the application conversion for documents with the file extension .lwp with the method Print via the command entered under HKCR\WordPro.Documentshell\Print\command.

NOTE: On MS Office 2021, 2024 and 365 Apps you may not find Print or Printto registry keys .doc, .docx, .htm or .html on HKEY_CLASSES_ROOT.

In this case you should use e.g following registry key:

```
HKEY_CLASSES_ROOT\Word.Document.12\shell\Printto\command  
(Default) = "C:\Program Files\Microsoft  
Office\Root\Office16\WINWORD.EXE" /j "%1" "%2"
```

E.1.5 License Service

The values you find in key `licsvc` serve for correctly accessing the HiPath license management. They must not be changed.

InstalledProduct [REG_SZ]

Default:	XPR

k1 [REG_SZ]

Example:	roOAcqbTXw0f1PWHk294OGqoGUs=

Internal configuration data for cluster installations. Must not be modified.

k3 [REG_SZ]

Example:	nO9GDIOso2gRpb5odD7ijjHVFz0=

Internal configuration data for cluster installations. Must not be modified.

SiemensProductId [REG_SZ]

Default:	HPXPR

SiemensProductVersion [REG_SZ]

Default:	V7

E.1.5.1 CCF File

The CLA uses the entries in the file

`<XPR Install>\xprlicsvc\HPXPR_V5.0.ccf` for communicating with the HiPath license management (HLM). The `licsvc` service on the XPR server requests the licenses from the CLA, which receives them from the HLM. This text file contains five lines. These are the HLM IP address, the HLM port, the time-out in milliseconds, the number of connection attempts between HLM and the license service and finally an optional Boolean value. If this value is set to `true`, the set number of connection attempts is executed unless an incorrect IP address is reported by error message. In case of `false`, a connection setup is attempted exactly once, independent from the set number of connection attempts.

If the computer on which the HLM was installed receives a new IP address, it must be adjusted here and in [LicSvcAddress \[REG_SZ\]](#).

Example of a created CCF file:

```
172.26.9.46
61740
1000
5
true
```

Besides the above ccf file you find under

`<XPR Install>\xprlicsvc\hlm\License Management Information
\ HPXPR_V6\` the similarly looking file `HPXPR_V6.ccf` created by the HLM.
You must not change this file.

E.1.6 Site Specific Entries

The following values can be found in the key `MRS Globals\Location`.

AccessCode [REG_SZ]

Default:	–

Access number. This number is taken as default for ISDN or modem connection. Individual configuration is possible for ISDN or modem access.

AreaCode [REG_SZ]

Default:	–

Area code without preceding zeros. This number is taken as default for ISDN or modem connection. Individual configuration is possible for ISDN or modem access e.g. numerous service providers.

AreaCodeEscape [REG_SZ]

Default:	–

National prefix. This number is set preceding the [AreaCode \[REG_SZ\]](#) of the recipient when a domestic number is dialed.

Example: 0

Country [REG_SZ]

Default:	–

The country for which the site specific parameters are configured. This is required for the setup to display the correct country with a later update of the XPR server. This is necessary as no unique assignment of the country code to a certain country exists. The United States and Antigua, for example, have the same country code.

CountryCode [REG_SZ]

Default:	–

Country code.

Example: 49

CountryCodeEscape [REG_SZ]

Default:	–

International prefix. This number is prefixed to the [CountryCode \[REG_SZ\]](#) of the recipient when a foreign number is dialed.

Example: 00

DateFormat [REG_SZ]

Default:	–
Possible values:	<Template>

Template is a date display format, which can be composed of various tokens:

Token	Description	Possible Values
%W	Day of Week (capital letters)	['SUN' .. 'SAT']
%w	Day of Week	['SUN' .. 'SAT']
%D	Day	[1 .. 31]
%M	Month	[1 .. 12]
%N	Month	['JANUARY' .. 'DECEMBER']
%n	Month	['JANUARY' .. 'DECEMBER']
%C	Century	[19 .. 20]
%Y	Year	[70 .. 38]

Example: %W %D. %-3.3N %C%02Y

The displayed text depend on the set server language. The date can be used e.g. in fax stationery.

DateFormatLong [REG_SZ]

Default:	–
Possible values:	<Template>

Similar to [DateFormat \[REG_SZ\]](#), but can be selected as long date format for fax stationery.

ExternalLinePrefix [REG_SZ]

Default:	–

External Line.

Example: 0

LocPrefixExtensions [REG_MULTI_SZ]

Default:	* #
Possible values:	<Prefix>

A list with phone numbers or partial phone numbers that remain unchanged when being normalized. For instance, 0240412345 (Alsdorf, Germany) becomes 49240412345.

With corporate networks it is possible that dialing numbers such as 9992<Extension> exist. You can enter the prefix 9992 here so that all numbers beginning with this prefix will not be normalized.

Example:

9992
0111
444

All numbers that begin with 9992, 0111 or 444 will not be normalized. One prefix may be entered per line.

TimeFormat [REG_SZ]

Default:	–
Possible values:	<Template>

Template is a time display format, which can be composed of various tokens:

Token	Description	Possible Values
%02h	Hour	[00..23]
%02h	Hour	[00..12]
%02m	Minute	[00..59]
%02s	Second	[00..59]
%P	Ante/Post meridiem in capital letters	[AM/PM]
%p	Ante/Post meridiem in lower case letters	[AM/PM]

Examples:

%02h:%02m
%02H:%02m %p

The time can be used e.g. in fax stationery.

TimeFormatLong [REG_SZ]

Default:	–
Possible values:	<Template>

Long version of [TimeFormat \[REG_SZ\]](#).

Example: %02h:%02m:%02s

E.1.7 The Router

The following values can be found in the key `MTA`.

AccountingDatabase [REG_DWORD]

Default:	1
Possible values:	0 – GEB database not active. 1 – GEB database active.

Write billing information in the GEB database or not. The billing information is normally collected and analyzed in one place. This is mostly the PBX, so that an additional billing information is not necessary.

AddSendJournalToQuota [REG_DWORD]

Default:	1
Possible values:	0 – Quota calculation without send journal. 1 – Quota calculation with send journal.

Quota calculation with or without send journal.

AutolearnAllfromProperty [REG_DWORD]

Default:	0
Possible values:	0 – Autolearn mode not active. 1 – Autolearn mode active.

The Autolearn mode should be active in the event that *no* user data under XPR is to be administered, and personal fax ID's are desired for fax receipt. When you send documents via Lotus Notes or Microsoft Exchange gateways, the private data from the address book (e.g. IDs, charge infos etc.) is attached to the document and are thus available for sending.

Since a local address book does not exist, a personal fax ID by the standard installation is not available. This can be avoided via the Autolearn option. Here all IDs that have ever been used for sending documents via gateways are learnt by the XPR address book. These answer codes are now available for document reception. If the properties from other services are included with a document they will be retained and imported into the database.

This way receiving voicemails would only be possible as soon as the voice number was e.g. copied from a sent fax message.

Address book replication would be better anyway, since then the required data would be immediately available under XPR.

AutolearnOIDfromProperty [REG_DWORD]

Default:	0
Possible values:	0 – Autolearn mode not active. 1 – Autolearn mode active.

Analog to [AutolearnAllfromProperty \[REG_DWORD\]](#) only the properties of the associated service are copied here. When a fax is sent from Lotus Notes or Microsoft Exchange only the fax data will be retained by the XPR user database.

AutolearnSetPreferred [REG_DWORD]

Default:	0
Possible values:	0 – PREFERRED not set automatically. 1 – PREFERRED set automatically.

The database field PREFERRED is used on the basis of the information received via Autolearn.

BroadcastSlowDown [REG_DWORD]

Default:	0
Possible values:	Milliseconds

With a broadcast the MTA resolves the destination addresses and generates a single send job for each destination address. This may lead to an extreme computer load by harddisk access and CPU load. In such a case you can make the MTA to shortly interrupt the destination address resolution after each single job. So if larger broadcasts cause performance problems in particular as regards the Telephone User Interface (TUI) reply times, increase this value.

Capabilities [REG_MULTI_SZ]

Default:	<Empty>
Possible values:	Complete path to a batch file
Example	C:\OpenScape\xpr\restart-apl.bat

This batch file is invoked rebooting an APL by the MTA fails. Three parameters are handed over to the batch file:

- The host name of the computer on which the APL operates.
- The APL name.
- The process name.

The batch file may have the following content:

```
pskill /accepteula \\%1 %3
```

In this case the external program pskill would be invoked by SysInternals.com for terminating the process on the computer on which this process is running. See [Section 7.6, “Heartbeat Monitor”](#).

CheckCredit [REG_DWORD]

Default:	0
Possible values:	0 or 1

Internal value for optional billing on a public test server.

CheckQuotas [REG_DWORD]

Default:	0
Possible values:	0 – Quota check switched off. 1 – Quota check switched on.

Switch quota check on or off.

ClassMangling [REG_SZ]

Default:	–

If XPR servers are redundantly coupled via Remote System Links (e.g. via TCP/IP and ISDN), a ClassMangling parameter is required. Through the extension of the class the difference in the admission type is given to the router. An address of the type `NVS:NODE.CLASS/USER` is then transformed to `NVS:NODE.CLASS@SSSTTT/USER`. `SSS` are the first three letters of the server name. `TTT` are the first three letters of the transport name.

Example: `%s@%3.3s%3.3s`

In the remote system PERGAMON exists a line `NVS:FAXG3.1`

. This line is now imported twice by the Remote System Link, with the router then having two lines that cannot be differentiated:

```
NVS:FAXG3.1 (Transport: NVS:TCPIP)
NVS:FAXG3.1 (Transport: NVS:ISDNMI)
```

So that the router can differentiate between the lines, the `CLASS`-section of the address (`.1`) is extended:

```
NVS:FaxG3.1@PERTCP
NVS:FaxG3.1@PERISD
```

CompressionType [REG_SZ]

Default:	BZ2
Possible values:	BZ2 – Bzip2 XZ – XZ

Specifies the compression algorithm used by the smart backup. BZ2 is faster and uses less memory at runtime but does not compress as good as XZ. Restore is automatically able to handle both formats.

DocumentLifeTime [REG_DWORD]

Default:	60
Possible values:	1..9999

Maximum document life in days. This value sets the variable \$ (LIFETIME) in the maintenance script. Deletions are initiated after the number of days has expired. The variable can either be given as explicit number in the script or referenced in the registry key by \$ (LIFETIME) . The value in DocumentLifeTime specifies the age limit, so that a document may be deleted by the standard script. This value can also be set in the MTA configuration. Here you can set a 3-day minimum to maintain documents at least over the weekend.

DocumentLifeTimeCompress [REG_DWORD]

Default:	–
Possible values:	1..9999

This value sets the variable \$ (LIFETIMECOMPRESS) in the maintenance Script.

DocumentLifeTimeDeleted [REG_DWORD]

Default:	–
Possible values:	1..9999

This value sets the variable \$ (LIFETIMEDELETED) in the maintenance script.

DocumentLifeTimeEmail [REG_DWORD]

Default:	–
Possible values:	1..9999

This value sets the variable \$ (LIFETIMEEMAIL) in the maintenance Script.

DocumentLifeTimeInbound [REG_DWORD]

Default:	–
Possible values:	1..9999

This value sets the variable \$ (LIFETIMEINBOUND) in the maintenance Script.

DocumentLifeTimeOutbound [REG_DWORD]

Default:	–
Possible values:	1..9999

This value sets the variable \$ (LIFETIMEOUTBOUND) in the maintenance Script.

DocumentLifeTimePassthrough [REG_DWORD]

Default:	–
Possible values:	1..9999

This value sets the variable \$ (LIFETIMEPASSTHROUGH) in the maintenance Script.

DocumentLifeTimeRead [REG_DWORD]

Default:	–
Possible values:	1..9999

This value sets the variable \$ (LIFETIMEREAD) in the maintenance script.

DocumentLifeTimeService [REG_DWORD]

Default:	–
Possible values:	1..9999

This value sets the variable \$ (LIFETIMESERVICE) in the maintenance script.

DocumentLifeTimeUnread [REG_DWORD]

Default:	–
Possible values:	1..9999

This value sets the variable \$ (LIFETIMEUNREAD) in the maintenance script.

DocumentLifeTimeUserdefined [REG_DWORD]

Default:	–
Possible values:	1..9999

This value sets the variable \$ (LIFETIMEUSERDEFINED) in the maintenance script.

EarlyOwnerRecipient [REG_DWORD]

Default:	0
Possible values:	0 – Do not identify recipient early. 1 – Identify recipient early.

When set to 1, the owner of a message (the recipient whose inbound journal contains the message) would be determined at the beginning of the `PREFERRED` evaluation instead of at the end of the routing process.

Advantage: This strategy also works in case the recipient address is not unique. Example: Two users with one TCP/IP address.

File Systems [REG_MULTI_SZ]

List of the directory trees made available to the XPR clients via the XPR file system. The directory `/update` is used for the automatic client software update, `/userdata` contains the user-dependend resources such as cover pages or private greetings, `/logging` contains XPR log files. In cluster environments you should use the corresponding cluster share here.

Required privileges can be attached. The first privilege is for reading and the second is for the writing of objects.

Example:

```
/update;D:\XPR\Client\Update
/userdata;D:\XPR\Client\Update
/logging;D:\XPR\Log;SYS_SERVICE;SYS_SERVICE
/config/nco;C:\OpenScape\xpr\NCO
```

ForceLowerAddresses [REG_SZ]

Default:	PMI-HOSTNAME, SMTP
Possible values:	<Service>[,<Service>]

List of addresses that are always composed of lower case characters.

`NVS:SMTP/ASDF@domain.com` would be transformed to `NVS:SMTP/asdf@domain.com`.

ForceUpperAddresses [REG_SZ]

Default:	<XPR server>, EXCH, GROUP, LMACCOUNT, LN, MAILBOX, PIN, PREFERRED, PRIVILEGES, STAND-IN, VM_AUTH_CODES, VM_USER_OPTIONS,
Possible values:	<Service>[,<Service>]

List of addresses that are always composed of upper case characters.

HeartbeatApls [REG_MULTI_SZ]

Default:	<Empty>
Possible values:	<APL name>[,<process name>]
Example	exumapl exumapl5, exumapl

This entry lists the APLs monitored with the heartbeat monitor. If the APL name deviates from the process name, then it must be specified in addition. See [Section 7.6, “Heartbeat Monitor”](#).

HeartbeatErrFails [REG_DWORD]

Default:	6
Possible values:	6-12

Number of successive heartbeat query errors that lead to an error message by the MTA. This value should be greater than [HeartbeatWarnFails \[REG_DWORD\]](#). See [Section 7.6, “Heartbeat Monitor”](#).

HeartbeatInterval [REG_DWORD]

Default:	30
Possible values:	5-300 <seconds>

Interval in which the APLs listed in [HeartbeatApls \[REG_MULTI_SZ\]](#) are queried. This corresponds to the heartbeat. See [Section 7.6, “Heartbeat Monitor”](#).

HeartbeatRestartFails [REG_DWORD]

Default:	9
Possible values:	9-12

Number of successive heartbeat query errors that make the MTA try a reboot of the affected APL. See [Section 7.6, “Heartbeat Monitor”](#).

HeartbeatWaitTime [REG_DWORD]

Default:	5
Possible values:	5-30 <seconds>

Period in seconds in which an answer from the respective APL is waited for. See [Section 7.6, “Heartbeat Monitor”](#).

HeartbeatWarnFails [REG_DWORD]

Default:	3
Possible values:	3-12

Number of successive heartbeat query errors that lead to a warning by the MTA. See [Section 7.6, “Heartbeat Monitor”](#).

IgnoreOriginatorInGroup [REG_DWORD]

Default:	0
Possible values:	0 – Originator receives his/her own messages to groups. 1 – Originator does not receive his/her own messages to groups.

If a message is sent to a distribution list/group, the originator can be checked as to whether he/she is a member of the distribution list/group. Depending on this membership he/she does not receive his/her own message.

IntRout [REG_SZ]

Default:	SMTP
Possible values:	<Service>[,<Service>]

List of protocols where an address transformation is not required. To prohibit recursion, the router generates a warning message if an address was not modified through a routing rule. This behavior is nevertheless desired by intermediate routing systems. In this case the protocol name (e.g. SMTP) should be entered here. Protocols are to be separated with a comma.

LinkenheilSlowDown [REG_DWORD]

Default:	0
Possible values:	Milliseconds

The transmission of a distribution list is delayed *n* milliseconds per entry in the list.

LowerCaseAddresses [REG_DWORD]

Default:	1
Possible values:	0 – Addresses may not contain lower case. 1 – Addresses may contain lower case.

Allow lower case in addresses. After a conversion, SMTP addresses by the kernel would no longer be processed.

MaintenanceActive [REG_DWORD]

Default:	1
Possible values:	0 – Do not execute maintenance script. 1 – Execute maintenance script.

Execute maintenance script or not.

MaintenanceBackupTemp [REG_SZ]

Default:	–
Possible values:	Directory

Directory to store temporary files required when creating the smart backup. If this value does not exist or is empty, the default directory of the user under whose user account the MTA operates is used. If this account is the local system account, the directory is used for temporary system files.

MaintenanceDontTouch [REG_DWORD]

Default:	0
Possible values:	0 – Set <i>Modification Time</i> . 1 – Do not set <i>Modification Time</i> .

The DELDB function changes the *Modification Time* of all files in the document folders so that the remove function of the maintenance task is under no circumstances able to delete files before their expiry date. If you now back up these files differentially, all files are backed up again though only the *Modification Time* has changed.

MaintenanceLastStart [REG_DWORD]

Default:	–

The time of the last maintenance script performance is filed here with each run. This entry is used by [MaintenanceMonitorDateTime \[REG_DWORD\]](#) and [MaintenanceMonitorYear \[REG_DWORD\]](#) to detect abstruse differences between two start times.

MaintenanceLastUpdateId [REG_DWORD]

Default:	–

Internal value to accelerate the maintenance script operation.

MaintenanceMonitorDateTime [REG_DWORD]

Default:	1
Possible values:	0 – Monitor timer. 1 – Do not monitor timer.

When active, performance of the maintenance script remains undone if more than three days passed between two timer calls. The time between two calls should normally be approx. one minute.

MaintenanceMonitorYear [REG_DWORD]

Default:	1
Possible values:	0 – Do not check year. 1 – Check year.

When active, performance of the maintenance script remains undone if more than five years have passed since the last [MaintenanceLastStart \[REG_DWORD\]](#) entry. This precaution was implemented in view to the upcoming year 2000 as previous tests revealed that some computers would be many years in the future after the turn of the year. In such a case the maintenance script had otherwise immediately deleted the actually current documents.

MaintenanceScript [REG_SZ]

Default:	<XPR Install>\res\maint\maint.scr
Possible values:	<Path and Name of the Maintenance Script>

Location of the maintenance script which defines the periodical tasks of the MTA. See [Section 7.2, “Maintenance Script”, on page 214](#).

MaxHopCount [REG_DWORD]

Default:	10
Possible values:	<Number>

Maximum number of hops before mail is destroyed to prevent recursion. This value must be set high for complicated switching.

MaxLockTime [REG_DWORD]

Default:	60
Possible values:	Seconds

Maximum time a journal entry is allowed to be locked.

MaxPrivateRules [REG_DWORD]

Default:	512

Maximum number of private rules that users can define.

MaxRoutTargets [REG_DWORD]

Default:	1024
Possible values:	16..1024

Maximum number of logical lines that the router can administer.

MinimumBusyTime [REG_DWORD]

Default:	30
Possible values:	10..600 Seconds

Minimum time interval for a repeat strategy in seconds if resources such as lines are in use.

IMPORTANT:

This value has a strong influence on the system performance during peak load periods. If the value is small and many jobs are in the system, a repetition must be attempted more often by the kernel accordingly. This would lead to a useless basic load.

MinimumRejectTime [REG_DWORD]

Default:	30
Possible values:	10..600 Seconds

Minimum time duration in seconds for an attempted repeat after a reject. If the kernel receives a job with repeat strategy smaller than the value defined here, the repetition is executed at the time entered here at the earliest.

MinimumRepeatTime [REG_DWORD]

Default:	30
Possible values:	10..600 Seconds

Minimum time duration in seconds for a repeat attempt. If the kernel receives a job with repeat strategy smaller than the value defined here, the repetition is executed at the time entered here at the earliest.

MonitorDiskUsageAlerts [REG_DWORD]

Default:	1
Possible values:	0 – Monitor hard disk space. 1 – Do not monitor hard disk space.

Monitor hard disk space and warn in case of lack of resources

MonitorMemoryUsageAlerts [REG_DWORD]

Default:	1
Possible values:	0 – Do not monitor free storage space. 1 – Monitor free storage space.

Monitor free storage space and warn in case of lack of resources

MultiAddresses [REG_MULTI_SZ]

Default:	–
Possible values:	<Address pattern>

Normally the router prevents sending a mail to an address via two channels at once. Example: Tow fax messages to the same number. With some addresses it may be meaningful to allow simultaneous transmission. Here an address pattern can be stored for each line for which multiple addressing is to be allowed.

Example: NVS:TCPIP/*

NoNdrOnGlobalList [REG_DWORD]

Default:	0
Possible values:	0 – Non-delivery reports will always be sent. 1 – Non-delivery reports will not always be sent.

Via this value you can deactivate non-delivery reports for messages that were sent to a global distribution list or system-wide broadcast list.

NoOwnerOnNOPREFERRED [REG_DWORD]

Default:	1
Possible values:	0 – Always assign documents to the recipient. 1 – With <code>NOPREFERRED</code> flag do not assign documents to the recipient.

Via this value documents with the `NOPREFERRED` flag cannot be assigned to the recipient. In this way these documents are not reported in his/her inbox either. Thus you can e.g. suppress displaying a sent SMS message in the recipient's inbound journal.

OptimizeQueueSize [REG_DWORD]

Default:	1024
Possible values:	5..1024

Number of waiting loop entries that are RAM-cacheable for queue optimization. The number is directly proportional to the computation time needed by the optimizer. For slower computers this value should be set to 128.

PreferredTransactionAddresses [REG_SZ]

Default:	–
Possible values:	<Service>[,<Service>]

With preferred routing the familiar TUM backend addresses are usually taken for transactions, thus `EXCH` (ExUM APL), `LN` (LN UM APL) and `MAILBOX` (Mail APL). This mechanism prevents, for example, the following: A user has

TCPIP with his/her client IP entered in his/her `PREFERRED` field. With accessing by TUI via the corresponding TUM transactions the attempt would be made to access this client. The mechanism effects an access to one of the above TUM backends instead.

In an Exchange multiline environment, standard addressing via `EXCH` is no longer available, but has been replaced with e.g. `EXCH1` and `EXCH2`. By adding these services they are also considered valid destination addresses for this type of transactions.

PrivilegeDnoServices [REG_SZ]

Default:	FAXG3, FAXG4, VOICE, FAXG3REV, SMS
Possible values:	<Service>[, <Service>]

Here is a list of services that require dialing numbers. The MTA uses this information in different ways: First, the recipient address is normalized with the "Update NCO". These services are then checked for the privileges `SYS_AMT`, `SYS_NATIONAL` and `SYS_INTERNAT`.

Furthermore, an optional credit calculation takes place. For the latter see [CheckCredit \[REG_DWORD\]](#).

ProhibitDoubleHop [REG_DWORD]

Default:	0
Possible values:	0 – No restriction 1 – Maximum one remote system link for exported lines

Lines imported via Remote System Link are no longer exported to other Remote System Links.

IMPORTANT:

Both proxy keys are used to circumvent a Windows bug that does not allow direct opening of a remote proxy on a system within a distributed network. A waiting time of approximately 1ms is required. For security reasons the XPR uses 10 ms by default (see [ProxyOpenDelay \[REG_DWORD\]](#)). If the first attempt fails, then 10 repeat attempts are made with a 50ms interval between attempts (see [ProxyRetryDelay \[REG_DWORD\]](#)).

ProxyOpenDelay [REG_DWORD]

Default:	10
Possible values:	Milliseconds

Waiting time in milliseconds till the first occurrence of open proxy.

ProxyRetryDelay [REG_DWORD]

Default:	50
Possible values:	Milliseconds

Waiting time in milliseconds till a new attempt is made to open the proxy pipe. Maximum number of attempts is 10.

QueueThresh [REG_DWORD]

Default:	1
Possible values:	1

Threshold value from which the database is used for queuing. By default if more than one job is in the queue then the database is used for queuing.

This value may not be modified.

RecursiveDistributionLists [REG_DWORD]

Default:	1
Possible values:	0 – Do not allow recursive distribution lists. 1 – Allow recursive distribution lists.

Normally distribution lists are allowed within distribution lists. This value enables you to deactivate this default behavior.

RecursiveReRout [REG_SZ]

Default:	1
Possible values:	0 – Do not execute routing rules recursively. 1 – Do not execute routing rules recursively.

Normally the routing rules are recursively applied till a modification of the target address no longer occurs. For a non-recursive execution the destination address is finally determined after the first applicable routing rule.

RemoveFromCapaList [REG_SZ]

Default:	–
Possible values:	<Service>[,<Service>]

List of address types not to be reported to the client. The string with the possible XPR server services that is forwarded to the clients is limited to 255 characters. Thus you can actively control which XPR server services are not to be reported in case of an overflow.

RemovePropertiesOnCarbonCopy [REG_DWORD]

Default:	1
Possible values:	0 – Do not delete properties fields on the copy. 1 – Delete properties fields on the copy.

When a carbon copy of a message is generated, the message's properties fields are normally deleted on the copy. If you wish to retain these fields, alter the default setting of this value.

RemovePropertiesOnResend [REG_DWORD]

Default:	0
Possible values:	0 – Do not delete properties fields on a forwarded message. 1 – Delete properties fields on a forwarded message.

When a message is forwarded, the message's properties fields are normally deleted on the forwarded message. If you wish to retain these fields, alter the default setting of this value.

RepeatStandardDeviation [REG_DWORD]

Default:	0
Possible values:	0..100

Standard deviation for kernel repeat strategy. This is a measure for the influence of random factors on the exact duration of the repeat cycle. We suggest not to use this option.

ReRoutLevel [REG_DWORD]

Default:	10

Maximum allowable number of address transformations executed by the kernel during routing rule application. If this value is exceeded, you will receive a respective warning, since an error in the routing rules could lead to an endless recursion. If it is not a matter of such an error, you have to increase the value for complex address modifications by the routing rules.

RoutHeuristic [REG_SZ]

Default:	FRB=10000;FAK=1000;FCN=50;FSQ=2500;FPE=1;FOR=10;FRA=1;FSET=5

Router heuristic. This value may not be modified!

RoutOpt [REG_SZ]

Default:	CHECKMULTI, COMBINEDOCS, NEWOWNER

This value may not be modified!

RoutStrat [REG_SZ]

Default:	RANDOM

This value may not be modified!

StateTimeout [REG_DWORD]

Default:	3600
Possible values:	Seconds

The router maintains an internal list of all addresses currently in the queue, to prevent a second dialing attempt by another document. This value indicates the waiting time before a redial should be attempted, in the event that the address is not free.

SystemStartDelay [REG_DWORD]

Default:	60
Possible values:	Seconds

The MTA spends the time entered here in idle state, before the APLs are released. Subsequently, the MTA waits again for the time entered here, before the system operates for the MTA and puts out the message "System up".

TransactionSlowdown [REG_DWORD]

Default:	20
Possible values:	Milliseconds

Delay time in milliseconds before the next transaction is pushed in the queue. Prevents the output queue to the APL from flowing over (highwater).

UnsecureSMI [REG_DWORD]

Default:	0
Possible values:	0 – Do not accept unsafe SMI connections. 1 – Accept unsafe SMI connections.

Execution of forced validation on SMI transporters. You can switch off the check-up here.

UseOriginalDocOnRout [REG_DWORD]

Default:	0
Possible values:	0 – Do not remove conversions. 1 – Remove conversions.

Normally the PMF representation – if present – of the document with all conversions, cover pages etc. will be sent.

All conversions, fax stationery, etc. can be removed when documents are routed. The routed document consists only of the original documents that were sent upon the first creation of the send job.

UserRemovalExtension [REG_SZ]

Default:	–
Possible values:	<Path including Program> or <Program>

If a program is specified in this value, it is invoked if a user has been deleted by maintenance script in the *OldUserCleanup* task or by InfoTool with the *KillUser* option. This program receives the user ID of the deleted user account as the only command line parameter. If the program is entered without path indication, it must be stored in a directory that is entered in the environment variable `PATH`.

VerifyDocumentDeliveryToApl [REG_DWORD]

Default:	0
Possible values:	0 – Do not monitor document transmission. 1 – Monitor document transmission.

If the MTA transfers a document to an APL that either crashes or is stopped and furthermore does not return a report to the MTA any more, the MTA does not convey this document anew. If you activate this option, the MTA monitors these documents until it receives a report. If no report is delivered due to an APL crash, the documents are handed to the APL once again after it has been restarted.

VirusCheck [REG_DWORD]

Default:	0
Possible values:	0 – Virus check switched off. 1 – Virus check switched on.

Documents and attachments can thus be checked for viruses. The virus checker impedes greatly the routing performance of the kernel.

To activate the virus check, the command line version of the Network Associates virus scanner must be installed in the directory `<XPR Install>\Res\VirScan`. Scan.exe in version 4.0.2 to 4.50 is supported at the moment. All required DLLs and the current *.DAT files must also be copied to this directory. The virus scanner must be licensed!

VirusCheckFileFormats [REG_SZ]

Default:	BIN
Possible values:	<Format>[,<Format>]

When the [VirusCheck \[REG_DWORD\]](#) is enabled, all documents the format of which is contained in the list are checked for viruses. Numerous formats may be appended when separated by a comma. This value must be changed

to BIN,TXT,AS7,ASC, so that also text documents are checked for viruses. This is necessary to recognize e.g. VBS viruses such as “I Love You”. But since a detection significantly lags behind in most cases, the VBS support in Outlook should be switched off. You find a list of possible formats in [Appendix A, “Document Formats”](#).

WriteLoginStat [REG_DWORD]

Default:	0
Possible values:	0 – Do not save last user login. 1 – Save last user login.

The kernel writes the last login date of a user in the Correlation database. The respective key name is `LOGIN_STAT`, the entry a time stamp in the format: “hh:mm:ss DD.MM.YY”. Example:

Classname	Class	Keyname	Key
USER	MK	LOGIN_STAT	06:34:56 04.05.01

Disadvantage: Unnecessary database info replication with the client database at login in systems with numerous users.

This function can be used e.g. for maintenance purposes. In anonymous systems it must be possible to find out when a user has logged in last. This enables deletion of user accounts that have not been used over a specific period.

E.1.8 Automatic Database Import from the Registry

The Message Transfer Agent includes a mechanism that automatically imports data records for the Correlation Database during the start-up once. Therefore, the key `MTA\AutoLoader` is searched for values of the type `REG_MULTI_SZ`. Each value of this type may contain lines of the following type:

```
<Domain>|<Classname>|<Class>|<Keyname>|<Key>
```

| (ASCII 124) serves as separator. These values are imported as strings and should be available in the ANSI character set. The entry `%SERVER%` as `<Domain>` is replaced with the name of the XPR server.

As soon as the data have been imported after the start of the MTA and written in the database, these registry values are deleted. This mechanism is used e.g. by the setup program.

Two reserved names for keys exist below `autoleader` with a special functionality: `Masks` and `Trashcan`. Both can also contain entries of the type `REG_MULTI_SZ`.

`Trashcan`, just like `Autoloader`, may contain correlation data records that are deleted during the MTA start-up. As soon as this has happened, these registry values are deleted.

`Masks` contains values with lines of the following type:

```
<Field>|<Attributes>|<Length>
```

Here the database mask is extended by the fields `<Field>`.

Example: The value `...\AutoLoader\Masks\PROFILE` contains the lines

```
FOO|CHAR|57
BAR|CHAR,UPPER|30
```

Here, during the start of the MTA, the fields `FOO` and `BAR` would be added with these attributes and the entered length of the mask `PROFILE` at the end. Subsequently, this entry will be deleted in the registry, i.e. it is executed once.

E.1.9 Autoreporter

The following values can be found in the key `MTA\AUTOREPORTER`.

DefaultListSet [REG_DWORD]

Default:	–
Possible values:	0 – Default recipient has not been set. 1 – Default recipient has already been set.

After the first start of the MTA the default recipient is set for active alerts. After this default has been set, this value is set to 1. Thus the MTA knows that the default does not have to be set again, even if the list of recipients has been deleted from the MTA configuration.

LogReportPeriodicity [REG_DWORD]

Default:	86400
Possible values:	Days * 86400 Seconds

Number of days in seconds (multiple of 86400), after which the log autoreport is sent.

MinimumTimeBetweenReports [REG_DWORD]

Default:	3600
Possible values:	Seconds

Minimum period in seconds that must pass before an additional report is sent.

ReportList [REG_MULTI_SZ]

Default:	NVS:\$ (NODE) / \$ (ADMINISTRATOR) ; LOG; * NVS:\$ (NODE) / \$ (ADMINISTRATOR) ; ACTIVE; *
Possible values:	<NVS Address> Eventlog; LOG ACTIVE EVENTLOG; <Filter>

A list of recipients with the type and range of the report; separated by semicolon in each case. Each NVS address can be used as recipient. Especially important is the specific address `EventLog`, which writes the log entries in the Windows event log when the type `EVENTLOG` is entered at the same time. Two further type classifications exist: `LOG` collects all corresponding log entries and sends them collectively to the entered recipient. `ACTIVE` sends a message immediately if a log entry belonging to the filter condition comes up. The report range is defined by the filter settings for active alerts of the XPR monitor. A `*` takes all log messages fulfilling the set filter conditions. Entering words separated by comma searches for these words in all log messages and includes the log message into the report, if each of the words is found. If a `!` precedes a word a log message is entered in a report if this word is not found. These search words are a logical and-link.

Example:

Registry Reference

```
NVS:SERVER/ADMINISTRATOR;LOG;*
NVS:SERVER/ADMINISTRATOR;ACTIVE;ERROR,!DIALOG
EventLog;EVENTLOG;*
```

E.1.10 CIT – Computer Integrated Telephony

The following values can be found in the key `MTA\CIT`.

CitActive [REG_DWORD]

Default:	–
Possible values:	0 – CIT disabled. 1 – CIT enabled.

If CIT is active, a corresponding CIT protocol must be defined. This can be done e.g. for the V.24 APL. With installed Notification APL the former Message Waiting Indication form that can be activated here is always switched off.

CitCacheActive [REG_DWORD]

Default:	1
Possible values:	0 – Cache disabled. 1 – Cache enabled.

CIT jobs can be optimized via a cache.

CitCacheActiveForNoCitOff [REG_DWORD]

Default:	1
Possible values:	0 – Cache disabled. 1 – Cache enabled.

The CIT jobs for protocols that do not require resetting the CIT signal can be optimized by a cache.

CitCounter [REG_DWORD]

Default:	0
Possible values:	0 – No counter-based CIT. 1 – Counter-based CIT.

Switch counter-based CIT on or off.

CitMessage [REG_SZ]

This value includes the message for the activated option **Send dynamic text message as CIT**. For more information refer to [Section 7.1.4, “CIT – Message Waiting Indication”, on page 202](#).

CitMessageFile [REG_SZ]

This value contains the name of the voice file with the activated option **Send voice message as CIT**. For more information refer to [Section 7.1.4, “CIT – Message Waiting Indication”, on page 202](#).

CitMessageMode [REG_DWORD]

Default:	–
Possible values:	1 – Option Send dynamic text message as CIT active. 2 – Option Send voice message as CIT active.

For more information refer to [Section 7.1.4, “CIT – Message Waiting Indication”, on page 202.](#)

CitUserBasedMessage [REG_DWORD]

Default:	0
Possible values:	0 – No user-specific files for CIT notification. 1 – User-specific files for CIT notification.

The voice or text file sent as CIT notification can be entered user-dependently. For each user you need to enter the file including its individual text or voice file in the `CITFILE` database field. Text files must be suffixed with `TXT` for this purpose. The files are stored in the XPR server's `UserData` directory tree and entering files is thus performed in relation to this directory. This feature enables among other things various language versions of the CIT notification.

CitUserIsOriginator [REG_DWORD]

Default:	0
Possible values:	0 – Originator of a notification is <code>AUTOREPORTER</code> . 1 – Originator of a notification is the mailbox owner.

Demand: Customer would like billing including all outbound connections.
Problem: No `CallingPartyNumber` is sent with SMS notifications. Only when regular SMS messages are sent. The only difference is that the originator is always `AUTOREPORTER` when SMS notifications are sent. Via this switch the originator for CIT notifications can be set to the mailbox owner, so that billing also works.

HideCitMessages [REG_DWORD]

Default:	1
Possible values:	0 – Do not set <code>HIDE</code> flag. 1 – Set <code>HIDE</code> flag.

The `HIDE` flag is set for all messages created for CIT. So they do not appear in the user's journal.

MaximumCacheTime [REG_DWORD]

Default:	3600
Possible values:	Seconds

Maximum time in the CIT cache.

NoCitOffSignal [REG_SZ]

Default:	SMS,VOICE,SMSB,SMSNL
Possible values:	<Service>,[<Service>]

Protocols for which resetting the CIT signalization is not sensible. It makes sense to delete the telephone LED after the message has been read. For an SMS surely no further SMS is required informing you that the message has been read.

E.1.11 System Networking

The following values can be found in key `MTA\ISC`.

Cipher [REG_DWORD]

For internal use only.

CSEncryption [REG_DWORD]

Default:	1
Possible values:	0 – Encoding not active. 1 – Encoding active.

Activates encoded communication between XPR and Connect Server.

DataPath [REG_SZ]

Default:	Path to the ISC directory
Default:	<XPR Install>\ISC

Path to the ISC directory. In case of a cluster installation this directory should be located on a network drive.

ExportDbFields [REG_MULTI_SZ]

Default:	–
Possible values:	<database field name>

List of additional user database fields sent to remote sites by default in the course of user replication. This default may be changed in the scope of the site configuration.

Some fields like `PASSWORD` and `PIN` are principally excluded from this replication, even if these fields are listed here. Otherwise, the fields usually required are already considered in the scope of the user replication. If required, this default can hereby be extended.

ExportProtocols [REG_MULTI_SZ]

Default:	–
Possible values:	<Service>

List of protocols that can be exported. This is the so-called White List, which overrules the internal Black List.

HeartBeat [REG_DWORD]

Default:	300
Possible values:	Seconds

Interval in seconds in which a heartbeat is sent to a remote site in the network.

OrgAddress [REG_SZ]

Default:	–
Possible values:	<NVS address>

Standard originator address if no local profile is available.

If you have deleted the individual system networking configuration and want to reconnect to an existing network to receive a working profile, you can statically enter the originator address here. Otherwise a local profile needed to be created, which you receive automatically in this procedure.

Profiles [REG_SZ]

Default:	SiteProfiles.dat
Possible values:	<File name>

Name of the file in which the encoded system networking data are stored.

PubKey [REG_SZ]

Default:	PubKey.pem
Possible values:	<File name>

Name of the file under which the local public key is stored.

ReplPollTime [REG_DWORD]

Default:	300
Possible values:	Seconds

Interval in seconds in which the user data are to be replicated. Is used for automatic user data replication only.

SmtpMessageSize [REG_DWORD]

Default:	100
Possible values:	<Number of objects (e.g. user profiles) per replication message>

Scenario: a node with 2000 users is connected to an existing network by system networking. The assumed size of a user profile inclusive name recording be 100 KB. As soon as the automatic user data replication is activated, the data of the 2000 users is sent to the other nodes of the network as one message of size 200 MB. This message would neither be accepted by a SMTP server nor SMTP Relay.

Therefore, the data to be transmitted is sent in several submessages. The number of objects to be transmitted in one message is set here. In our scenario only messages of the size 100*100 KB would be created, i.e. with a size of about 10 MB. The biggest object to be transmitted is the name announcement. Consequently, this is a good measure to define the approximate maximum size of the replication messages. We know from

previous experience that the average message size is 5 MB in case of a default of 100. This, however, as one-time peak during the first activation of the replication. Later modifications result in clearly smaller messages.

If the messages were too big and thus not accepted by the recipient, the transmission would be attempted again and again in a new message. The replication messages are deleted after the transmission attempt, so that only the replication does not work, but there will be no hard disk overflow.

UseOldConnectServerFormat [REG_DWORD]

Default:	–
Possible values:	0 – Use newer connect server protocol. 1 – Use protocol of the connect server v2.5.

Connect server protocol used.

E.1.12 Line Cache

The following values can be found in the key `MTA\LineCache`.

CacheActive [REG_DWORD]

Default:	1
Possible values:	0 – Line cache of the MTA disabled. 1 – Line cache of the MTA enabled.

Switch line cache of the MTA on or off.

LineCacheVersion [REG_DWORD]

Line cache version.

LogicalLines [REG_MULTI_SZ]

Here the MTA memorizes all lines it knows and their states subject to [CacheActive \[REG_DWORD\]](#). So when the XPR server starts, the MTA knows them already. Consequently, there will be no illegal addresses because specific lines are made known by an establishing Remote System Link at a later date.

E.1.13 Remote System Links

The following values can be found in the key `MTA\RemoteSystemLinks`.

AutoBiDirectionalLinks [REG_DWORD]

Default:	0
Possible values:	0 – Do not create backlink automatically. 1 – Create backlink automatically.

Remote System Links are always directed. If a system establishes a Remote System Link to a remote system, the system can send mail to the remote system but not vice versa. Via this value a backlink can automatically be created, so that this link becomes bidirectional.

EmailSecurityLevel [REG_DWORD]

Default:	0
Possible values:	0 – Reject messages with missing privilege. 1 – Accept messages to <code>NVS : <System name></code> without privilege. 2 – As 1, but additionally check <code>SYS_USER</code> at the recipient.

If you configure a Remote System Link, you can configure it wrongly in a way that it has no privileges and every message coming from this system is rejected. With 1 all messages addressed to the e-mail address `NVS : <system name>` are delivered even with missing privileges. With 2 an additional check is performed as to whether the recipient address has the `SYS_USER` privilege, thus a real user is very likely to be on the own XPR server.

ForceAuthentication [REG_DWORD]

Default:	1
Possible values:	0 – Password not required. 1 – Password required.

Each Remote System Link normally must log in with a password. Therefore a user account needs to be created with the name of the own system on the remote server. Its password and privileges will then be used for authentication.

GlobalLink [REG_DWORD]

Default:	0
Possible values:	0 – Maximally export via a hop. 1 – Export lines with attribute <code>GLOBAL</code> via several hops.

Some logical lines such as the e-mail address `NVS : <system name>` have the `GLOBAL` attribute. Via this switch lines with this attribute can be exported via several hops. Then delivering a message via several systems as interstation would be possible.

A hop corresponds to the connection via a Remote System Link. If a server imports a line and exports it then to a further system via Remote System Link, these would be two hops.

Normally lines are only exported via one hop.

ImportedFields [REG_SZ]

Default:	VOICE, NAME, VM_USER_OPTIONS
Possible values:	<Field>[,<Field>]

This field contains comma-separated field names of the user database that are imported by the other system with a Remote System Link. Importing rules are:

- If ImportedFields contains field names, only the fields entered here are imported.
- All fields listed in the [NotImportedFields \[REG_SZ\]](#) value are generally not imported.

The default for ImportedFields contains the fields required e.g. for a voicemail server. The previous default setting (importing all fields except the ones explicitly listed in [NotImportedFields \[REG_SZ\]](#)) often caused problems. Since adding required fields is easier than deleting wrongly imported fields, this changed behavior was implemented.

LinkList [REG_MULTI_SZ]

Default:	–
Possible values:	<i><connection address>; <synchronization interval>; <number of redials>; <encrypted password>; <configured address book replication>; <imported logical lines></i>

Per line a link to a remote system is listed. The settings of a Remote System Link can best be entered via the MTA configuration of the XPR monitor. See [Section 7.1.2, “Remote System Link”, on page 195](#).

Example:

```
NVS:TCPIP/NVS20;CSync=120,10;Rep=3;Pwd=3701913046;OPT=TIME
```

Every 120 seconds a connection attempt is made to system NVS20PPC over TCP/IP transport. If the connection is made within a 10-second period, then the Remote System Link is established. If not, then another attempt would be made 120 seconds later. After three unsuccessful attempts, no further attempts would be made to establish a connection. If the connection is successful, the encrypted password is sent. The password should be entered using the MTA configuration in the XPR monitor. Validation on the other side of the link is done through use of a pseudo account. This corresponds to the procedure of privilege validation via trusted domains. Lastly, the system time is set to that of the remote system. All logical lines on the server NVS20PPC would be imported.

The available logical NVS addresses correspond to those lines provided by the MTA.

MaximumReplicationRecordsPerTransaction [REG_DWORD]

Default:	500

Maximum number of database records that can be replicated per transaction.

NotImportedFields [REG_SZ]

Default:	CIT,MAILBOX,NEWMSGs
Possible values:	<Field>[,<Field>]

This field contains comma-separated field names of the user database that are not imported by the other system with a Remote System Link.

Via the CIT field you can control e.g. new-message notifications that are exclusively to be initiated on the home server. Thus this field should not be imported. The MTA stores the number of new messages in the NEWMSGs field. So that this field is correctly reset and not overwritten with incorrect values by e.g. a correlation database synchronization, it should be specified here as well.

Please note that these two database fields only come to bear with the MTA's notification function. A new mechanism exists with the Notification APL. The Notification APL enables especially in True Unified Messaging environments new-message notification in Microsoft Exchange or Lotus Notes. All database fields of type NOT_* should be listed here as well. In any case, this should never be added to the value [ImportedFields \[REG_SZ\]](#).

RemoteLocalServices [REG_SZ]

Default:	TCPIP,SPX,IPX,MAILBOX,PIPE,STAND-IN
Possible values:	<Service>[,<Service>]

If a replication is set in *Adapt routing information* mode, the PREFERRED addresses are adjusted in case of addresses that have one of the services – i.e. they are users of the remote server – specified here as preferred.

Example: The database record "USER XYZ PREFERRED TCPIP" is replicated by the remote server. On the local server the entry "USER XYZ PREFERRED <remote server name>" and an additional entry "USER XYZ <remote server name>XYZ" are created from this in the *Adapt routing information* mode. The mail routing now occurs automatically to the remote system user XYZ.

ReportEncapsulation [REG_DWORD]

Default:	0
Possible values:	0 – Do not encapsulate reports in documents. 1 – Encapsulate reports in documents.

Repeat options are not available for reports sent over a remote system link. Reports will be lost if the first transmission is not successful.

If the reports are encapsulated in documents, so that repeat options are possible, this problem is avoided. The reports can then be processed by the remote system.

UseTrustedDomains [REG_DWORD]

Default:	1
Possible values:	0 – Do not use trusted domain user for validation. 1 – Use trusted domain user for validation.

Remote system links normally validate themselves against each other using Trusted Domain User.

A pseudo user must be set up with a user name that corresponds to the system name of the remote system. This pseudo-user receives all required privileges as needed for documents transmission over the remote system link. Additionally, this pseudo user must have the privilege `SYS_ACTASDOMAIN`. This validation is used, for example, when further costs are accumulated by a routing where the originator does not have the necessary authority.

IMPORTANT:

Trusted domain users constitute a – rather improbable – security risk in that the identity of the remote system is not checked. A value of 0 deactivates this function.

E.1.14 Routing Rules

The following values can be found in the key `MTA\RULES`.

Awake [REG_MULTI_SZ]

The awake rules. See [Section 7.1.3, “Routing Rules”, on page 200](#).

AwakeCustomBackup [REG_MULTI_SZ]

Possible storage of a user defined set of awake rules. If during the setting of the MTA, a different set of awake rules is installed in the XPR monitor, these rules would be stored here. A later resetting to user-defined rules would assume these values. See [Section 7.1.3, “Routing Rules”, on page 200](#).

AwakeType [REG_DWORD]

Default:	–
Possible values:	0 – No automatic new rerouting of documents. 1 – Unread incoming documents sent to Postmaster. 2 – User defined new rerouting rules.

This value represents the awake rules setting in the MTA configuration. See [Section 7.1.3, “Routing Rules”, on page 200](#).

CarbonCopy [REG_MULTI_SZ]

The Carbon Copy Rules. See [Section 7.1.3, “Routing Rules”, on page 200](#). These rules become active only if a [CarbonMode \[REG_SZ\]](#) is specified.

CarbonCopyCustomBackup [REG_MULTI_SZ]

Possible storage of a user defined set of carbon copy rules. If in the MTA settings in the XPR monitor carbon copy rules other than these user-defined ones are switched to, the server will store the user-defined rules here. A later resetting to user-defined rules would assume these values. See [Section 7.1.3, “Routing Rules”, on page 200](#).

CarbonCopyType [REG_DWORD]

Default:	–
Possible values:	0 – No Carbon Copy. 1 – Carbon Copy on default printer. 2 – Carbon Copy on the printer set in the user database. 3 – User-defined Carbon Copy Rules.

This value represents the carbon copy rules setting in the MTA configuration. See [Section 7.1.3, “Routing Rules”, on page 200](#).

CarbonMode [REG_SZ]

See [Section 7.4.7.2, “Carbon Copy Rules \(Send Copies\)”, on page 258](#).

CarbonModeBackup [REG_SZ]

Possible storage of the [CarbonMode \[REG_SZ\]](#) value for setting a user-defined set of carbon copy rules. See [Section 7.1.3, "Routing Rules", on page 200](#).

MaxCarbonCopy [REG_DWORD]

Default:	64
Possible values:	0..1024

Maximum number of carbon copy rules. Furthermore, the total size of the rules must not exceed 32kB.

MaxPreConvRules [REG_DWORD]

Default:	64
Possible values:	1..64

Maximum number of predictive conversion rules in the [PredictiveConversion \[REG_MULTI_SZ\]](#) value with the absolute maximum being 64.

MaxReRouteRules [REG_DWORD]

Default:	64
Possible values:	1..1023

Maximum number of routing rules in the [Rerouting \[REG_MULTI_SZ\]](#) value.

PredictiveConversion [REG_MULTI_SZ]

Default:	–
Possible values:	<NVS Address>=<Format>

Here you can specify one rule per line that has an early conversion into a given format performed for specific target addresses. See [Appendix A, "Document Formats"](#) for the valid format tokens.

Examples:

```
"^NVS:FAXG3 (/.*)?$"=TG3
```

This line means that all messages addressed to NVS:FAXG3/<Number> are converted already before the routing to TG3. This can be used, for example, to also deliver Microsoft Word documents as fax when they are sent to the fax number of a XPR user. Such documents would actually not be converted owing to routing optimization. If you simply enter NVS:FAXG3/* here instead of the regular expression specified, this rule is internally converted into the regular expression "NVS:FAXG3 (/.*)?". This expression would match NVS:FAXG3 as well as NVS:FAXG3/<String>. Thus it also matches addresses of type NVS:FAXG3REV/<Number> and leads with them to a conversion error. This internal conversion error will be fixed as soon as possible.

NVS:SERVER/LST:FAX*=FG3

Documents sent to a distribution list the name of which begins with FAX are converted to fax before distribution to the single recipients is performed. This may result in a considerable performance advantage.

Privileges [REG_MULTI_SZ]

Default:	SYS_SERVICE,NVS:FAXG3/+49900*
Possible values:	<Privilege>, <Address Pattern>

Addresses the format of which corresponds to the listed <Address Patterns> require the respective privilege. The default privileges can be made a prerequisite for all telematics services via [PrivilegeDnoServices \[REG_SZ\]](#). Additional privileges required by addresses can also be stored here. Many manufactures use expensive service numbers such as 0900 in Germany for updated information. For service personnel to poll such information from a server by fax-on-demand a privilege could be assumed.

Example: SYS_SERVICE,NVS:FAXG3REV/+49900*

Rerouting [REG_MULTI_SZ]

The Routing Rules. See [Section 7.1.3, "Routing Rules", on page 200](#).

ReroutingCustomBackup [REG_MUTLI_SZ]

Possible storage for user defined routing rules sets. If during the setting of the MTA a different set of routing rules is installed in the XPR monitor, these rules would be stored here. A later resetting to user-defined rules would assume these values. See [Section 7.1.3, "Routing Rules", on page 200](#).

RoutingType [REG_DWORD]

Default:	–
Possible values:	0 – User-defined routing 1 – Default routing 2 – SAP-inbound routing 3 – Fax server inbound routing

This value represents the routing rules setting in the MTA configuration. See [Section 7.1.3, "Routing Rules", on page 200](#).

E.1.15 Session Monitoring

The following values are found in the key `MTA\SESSIONS`.

OtherTimeout [REG_DWORD]

Default:	600
Possible values:	Seconds

As administrator, you can view in the Web Assistant the currently logged-in users as well as a history of the logged-in clients. The clients, though, need not log off from the XPR server. Therefore, a client that was shut down without explicit log-off would still be considered active. To evade this problem, a client is implicitly assumed logged off after some time. Since the clients usually query the server as to whether new messages are to be retrieved in regular intervals, you can still determine the desired information via the aforementioned time limit.

Under [WebTimeout \[REG_DWORD\]](#) you can set this time limit for all clients connected via the Web APL and here separated for all other logon options.

WebTimeout [REG_DWORD]

Default:	600
Possible values:	Seconds

See [OtherTimeout \[REG_DWORD\]](#).

E.1.16 Services

The following values can be found in the key `Services`.

Access Protocol Layers [REG_MULTI_SZ]

Default:	–
Possible values:	<XPR Service>,[<Windows Server>]

List of the installed XPR APL's. As soon as the kernel has been successfully started, the *XPR Administrator* service will use this list to start-up the system. The computer where the service is started may be entered as parameter after the comma. Default is the local machine with nothing following the comma.

Example:

```
MailApl,  
PipeApl,  
FiApl,  
IsdnApl,
```

AplDelay [REG_MULTI_SZ]

Default:	–
Possible values:	ConApl,<time in minutes> NotApl,<time in minutes>

Set this registry key order to delay any Xpressions service initialization when starting up Xpressions.
This is used specially on Failover Cluster installations.
In case of a failover scenario NotApl and ConApl should be started only after the voicemail is reestablished for the users.

with syntax:
apl name,delay in minutes

Example:
ConApl,5
NotApl,10

Kernel [REG_MULTI_SZ]

Default:	NameLoc, CfgSvc, XmrSvc, InfoStor, MTA,
Possible values:	<XPR Service>.[<Windows Server>]

Kernel services to be started at the time of the server start. The computer on which the service is started may be entered as parameter after the comma. You find more details about how to proceed in case of a distributed XPR server in [Section 7.7, “Distributed XPR Server”, on page 272](#). Default is the local machine with nothing following the comma.

MaxRetries [REG_DWORD]

See [Section 7.5, “Watchdog Process”, on page 267](#).

Recover-Kernel [REG_MULTI_SZ]

See [Section 7.5, “Watchdog Process”, on page 267](#).

Recover-<Computer name>-<Service> [REG_MULTI_SZ]

See [Section 7.5, “Watchdog Process”, on page 267](#).

Recover-<Service> [REG_MULTI_SZ]

See [Section 7.5, “Watchdog Process”, on page 267](#).

WatchdogActive [REG_DWORD]

Default:	1
Possible values:	0 – Deactivate watchdog 1 – Activate watchdog

Activate or deactivate watchdog.

WatchdogRestartSystemDelay [REG_DWORD]

See [Section 7.5, “Watchdog Process”, on page 267](#).

WatchdogRetryDelay [REG_DWORD]

See [Section 7.5, “Watchdog Process”, on page 267](#).

E.1.17 Database

If database files (*.DAT) are contained in the Infostor directory that contain information about the individual database entries, a database recovery is possible. If a recovery fails due to damaged index files (*IDX), the files can be removed from the Infostor directory. The index files will be recreated automatically at the next server start.

IMPORTANT:

Depending upon the size of the database, the recovery could take from several minutes to several hours. During the database recovery the XPR server may not be shut down, since a recovery is no longer possible after an interruption!

The following values can be found in the key `InfoStor`.

CompactDatabases [REG_DWORD]

Default:	0
Possible values:	0 – Inactive. 1 – Compact databases at start.

If you set this value to 1, the databases are compacted at the next start of the InfoStor service. All deleted data records that were previously only marked accordingly are physically removed. Furthermore, the indices are newly created. This minimizes the databases' and indices' size, which improves the performance.

IMPORTANT:

This operation requires at runtime free memory on the harddisk, which equals three times the size of the database files.

IMPORTANT:

We urgently recommend to create a backup file of the databases before the operation.

NOTE:

Depending on the database size this operation may take some time, thus considerably delaying the start of the entire system.

DatabaseDirectory [REG_SZ]

Default:	<XPR Install>\InfoStor
Possible values:	Directory

Path to the database directory.

InvalidateKeys [REG_MULTI_SZ]

Default:	E_LOGIN_WEB=4294967295 PASSWORD=4294967295 PIN=4294967295 VM_PIN_01=4294967295 VM_PIN_02=4294967295 VM_PIN_03=4294967295 VM_PIN_04=4294967295 VM_PIN_05=4294967295 VM_PIN_06=4294967295 VM_PIN_07=4294967295 VM_PIN_08=4294967295 VM_PIN_09=4294967295 VM_PIN_10=4294967295 POP-PASSWORD=4294967295 PMI-PASSWORD=4294967295
Possible values:	KEYNAME=<Dummy>

One field name of the user database may be entered per line. The contents of these fields are not transmitted to clients, so that it is not possible to access sensitive data such as the users' passwords by exporting an MSP database on a client.

JournalLayout [REG_DWORD]

Default:	–

Internal version number of the Journal database layout. If this database layout is modified, the database must be updated accordingly. The version number is then used as flag to signify whether a possibly necessary update has been performed already.

MaintenanceDelay [REG_SZ]

This entry corresponds with the Maintenance Priority slide control for performing the Maintenance Script in the MTA configuration of the XPR monitor.

MaxLockTime [REG_SZ]

Default:	60
Possible values:	Seconds

Maximum lock time for journal database entries.

E.1.18 Important User Accounts

The following values can be found in the key `InfoStor\Accounts`.

Administrator [REG_SZ]

Default:	–

Definition of the administrator (user account and encrypted password). If the XPR database is fully deleted ([DatabaseDirectory \[REG_SZ\]](#) directory is empty), then this user would be automatically reentered. The user retains the password given at the time of the installation. In addition, this user account is also used by the `$ (ADMINISTRATOR)` variable of the maintenance script.

LoginPolicy [REG_SZ]

Default:	–
Possible values:	XPR – XPR authentication WINLMKRB – Windows authentication

See [Section 4.8.1, “Authentication Mode in the XPR Server”](#), on page 140.

PostMaster [REG_SZ]

Default:	–

Definition of the user (user name and encrypted password) that receives all non-deliverable mail. If the XPR database is fully deleted ([DatabaseDirectory \[REG_SZ\]](#) directory is empty), then this user would be automatically reentered. The user retains the password given at the time of the installation. In addition, this user account is also used by the `$ (POSTMASTER)` variable of the maintenance script.

E.1.19 Extended Message Reporter Service

The following values can be found in the key `XmrSvc`.

AutoReportFilter [REG_MULTI_SZ]

Default:	<code>*,*,FE</code>
Possible values:	<code><Module>, <Topics>, FEWID1234A</code>

Filter for the active alert reports generated by the MTA. The MTA uses the log entries generated by the XPR server and passes through this filter for its active alert reports when they meet the criteria of its own filter. Log entry formats correspond to those described in the [LogFileFilter \[REG_MULTI_SZ\]](#).

DiagAddress [REG_SZ]

Default:	–

Maps the **Server Address** parameter in the OSVTM dialog of the XPR monitor.

DiagFilter [REG_MULTI_SZ]

Default:	<code>*,*,G lpapl,*,FEWA</code>
Possible values:	<code><Module>, <Topics>, FEWID1234A</code>

Defines the filter for the log messages sent to the OpenScape Voice Trace Manager. The format corresponds to the one described with [LogFileFilter \[REG_MULTI_SZ\]](#).

The G in first line corresponds to the new *Diagnostic Message* category used only here. This category is intended for an expansion planned for the case that the IP APL receives a special SIP call that requests a diagnosis in the SIP header. In this case, the diagnosis information is sent to the OpenScape Voice Trace Manager via this mechanism.

See also [Section 6.5.4, “OpenScape Voice Trace Manager \(OSVTM\)”](#), on page 177.

DiagNeName [REG_SZ]

Default:	–

Maps the **Element Name** parameter in the OSVTM dialog of the XPR monitor.

DiagNodeId [REG_SZ]

Default:	–

Maps the **Node ID** parameter in the OSVTM dialog of the XPR monitor.

DiagPassword [REG_SZ]

Default:	–

Maps the **Password** parameter in the OSVTM dialog of the XPR monitor.

DiagPath [REG_SZ]

Default:	–

Maps the **Path** parameter in the OSVTM dialog of the XPR monitor.

DiagPeriod [REG_DWORD]

Default:	5
Possible values:	5 to 60 minutes

Interval in which information is sent to the OpenScape Voice Trace Manager. See also [Section 6.5.4, “OpenScape Voice Trace Manager \(OSVTM\)”, on page 177](#).

DiagUser [REG_SZ]

Default:	–

Maps the **User** parameter in the OSVTM dialog of the XPR monitor.

FlushAfterWrite [REG_DWORD]

Default:	1
Possible values:	0 – Write buffer after several messages. 1 – Write buffer after each message.

After each writing in the log file the buffer is emptied, thus the file is physically written from the memory onto the hard disk. This operation affects the performance, but if you change this value and the XMR service has a problem, the last messages in the log file might get lost.

LogFileFilter [REG_MULTI_SZ]

Default:	*, *, FEWA
Possible values:	<Module>, <Topics>, FEWID1234A

Filter for the XPR log file. Modules, topics, and filters that are to be entered in the log are written on a line and separated with a comma. The filters are indicated by letters or digits: Fatal Errors (F), Errors (E), Warnings (W), Information (I), Debug Messages (D), Debug Level 1 to 4 (1, 2, 3, 4), Privileged Messages (A). For each message the flag *Privileged Messages* can be set in addition to the actual class. This is mostly done for information messages.

This log is in the [LogFilePath \[REG_SZ\]](#) directory.

For all modules and topics Fatal Error, Error and Warning messages are written to the log. Additionally, info messages where no topic can be assigned are in the log. None of the assigned topics is the default topic.

LogFilePath [REG_SZ]

Default:	<XPR Install>\Log
Possible values:	Directory

The log files of the XPR server are written into the path specified here.

IMPORTANT:

If you modify this path, you need to change the following Maintenance Script entry also:

```
Remove path=$(Root)\log age=60 option=x,recursiv
```

LogServer [REG_DWORD]

Default:	1
Possible values:	0 – Do not create topic <i>LogServer</i> . 1 – Create topic <i>LogServer</i> .

The topic *LogServer* is created by the XMR service. All reports sent with the *LogServ* program from the XPR SDK utilities to the XMR service appear under this topic. This program can be used to write messages from the batch jobs in the XPR log. Thus also from within the XPR maintenance script, for example. Assistance is given for this program when you start *LogServ* without parameters.

This program is not included in the standard delivery, but can be obtained for projects by ftp.

MaxLines [REG_DWORD]

Default:	1024
Possible values:	32..4096

Maximum number of lines administered by the XMR service.

ModuleCache [REG_MULTI_SZ]

Internal cache.

SnmpMode [REG_DWORD]

Default:	1
Possible values:	0 – Do not create messages in the event display. 1 – Create messages in the event display. 2 – Create messages via System Info SNMP Agent .

This mechanism automatically creates messages in the Windows event display for the most important error messages. These messages may then trigger SNMP traps via standard tools. In the following you see a message overview:

Crash of a process:

```
[<name of XPR server>/XMR]: Process <name of process> is
probably crashed
```

Low memory warning:

```
[<name of XPR server>/MTA/Watchdog]: Free memory: <free
memory in per cent> %, physical memory <free memory in kB>
kB - SHUTDOWN AT 2% or physical less than 512kb
```

Not enough memory (XPR stops operation!):

```
[<name of XPR server>/MTA/Watchdog]: Free memory: <free
memory in per cent> %, physical memory <free memory in kB>
kB - SHUTDOWN
```

Enough memory available again (XPR continues operation except if there is not enough disk space):

```
[<name of XPR server>/MTA/Watchdog]: Free Memory: <free
memory in per cent> %, physical memory <free memory in kB>
kB, error condition resolved
```

Low disk space warning:

```
[<name of XPR server>/MTA/Watchdog]: Free space on <name
of disk drive>: <free disk capacity in per cent> % -
SHUTDOWN AT 1% if not 100MB free
```

Not enough disk space (XPR stops operation!):

```
[<name of XPR server>/MTA/Watchdog]: Free space on <name
of disk drive>: <free disk capacity in per cent> % -
SHUTDOWN
```

Enough disk space available again (XPR continues operation except if there is not enough memory):

```
[<name of XPR server>/MTA/Watchdog]: Free space on <name
of disk drive>: <free disk capacity in per cent> %, error
condition resolved
```

Layer 1 of ISDN board down:

```
[<name of XPR server>/IsdnApl/EiconIDI]: IdiMessageInput:
Layer 1 of controller '<number of controller>' (<name of
controller>) is down!
```

Layer 1 of ISDN board up again:

```
[<name of XPR server>/IsdnApl/EiconIDI]: IdIMessageInput:
Layer 1 of controller '<number of controller>' (<name of
controller>) is active
```

The following message covers different errors concerning the connection to the SMS service provider:

```
[<name of XPR server>/SmsIPapl/Connection]: Socket error:
'<socket error text>'
```

Error during login to the SMS service provider:

```
[<name of XPR server>/SmsIPapl/UCP]: Failed to open
session: Error: <error code>, '<error text>'
```

Successful login to the SMS service provider (this message should also clear all alarms concerning socket errors of the SmslpApl):

```
[<name of XPR server>/SmsIPapl/UCP]: Session successfully
opened
```

Connection to LDAP server could not be established:

```
[<name of XPR server>/LdapApl/Ldap]: [<name of ldap
connection>] ldap_bind to <hostname> for <username>
failed: <ldap specific error string>
```

Connection to LDAP server established

```
[<name of XPR server>/LdapApl/Ldap]: [<name of ldap
connection>] ldap_bind OK (user:<username>)
```

Attribute of user cannot be replicated because its value is not unique (e.g. fax and voicemail numbers must be unique):

```
[<name of XPR server>/LdapApl/Ldap]: [<name of ldap
connection>] MRS-Attribute <attribute>: value '<value>'
not written (not unique)
```

ExchApl has lost the connection to the Exchange server:

```
[<name of XPR server>/ExchApl/Mail Gateway]:
MrsCheckExchangeRunning: connection to the server lost
```

ExchApl has reconnected to the Exchange server:

```
[<name of XPR server>/ExchApl/Mail Gateway]:
MrsCheckExchangeRunning: OK
```

TUM login failed (unable to open Exchange mailbox):

```
[<name of XPR server>/ExUmApl/UM]: session logon failed
for user '<user name>'
```

TUM login successful:

```
[<name of XPR server>/ExUmApl/UM]: session logon succeeded
for user '<user name>'
```

Outgoing link to notes server broken

```
[<name of XPR server>/LnApl/Connection]: <domain>: No
access to <outgoing link> on server <server> any longer.
```

```
[<name of XPR server>/LnApl/IBX Replicator]: ->Notes:
Outbound connection collapsed. Replication not possible.
```

[<name of XPR server>/LnApl/IBX Replicator]: ->Notes:
Insufficient rights on the outbound connection.
Replication not possible.

[<name of XPR server>/LnApl/CTI]: ->Notes: Cannot open the
outbound connection. CTI Journal replication not possible.

[<name of XPR server>/LnApl/CTI]: ->Notes: Insufficient
rights on the outbound connection. CTI Journal replication
not possible.

[<name of XPR server>/LnApl/CTI]: ->Notes: Outbound
connection collapsed. CTI Journal replication not
possible.

Outgoing link to notes server (re)established:

[<name of XPR server>/LnApl/Connection]: <domain>: Access
to <outgoing link> on server <server> granted.

[<name of XPR server>/LnApl/IBX Replicator]: ->Notes:
Outbound connection restored! Replication possible!

[<name of XPR server>/LnApl/IBX Replicator]: ->Notes:
Access rights on outbound connection are now OK

[<name of XPR server>/LnApl/CTI]: ->Notes: Access rights
on cti outbound connection are now OK

[<name of XPR server>/LnApl/CTI]: ->Notes: Outbound
connection with Notes Server reestablished.

Database problems:

[<name of XPR server>/LnUmApl/Notification]: OpenDatabase:
The server <<servername>> is not available`

[<name of XPR server>/LnUmApl/Notification]: OpenDatabase:
API error <<error number>> => <<error string>>

[<name of XPR server>/LnUmApl/UM]: OpenDatabase: The
server <<servername>> is not available`

Database problems have been resolved:

[<name of XPR server>/LnUmApl/Notification]: OpenDatabase:
The server is available again

[<name of XPR server>/LnUmApl/UM]: OpenDatabase: The
server is available again

CTI link down:

[<name of XPR server>/CtiApl/<topic, e.g. H8000_CSTA for
OpenScape Voice>]: Restarting of CTI link '<name of CTI
link>' ...

CTI link up again:

[<name of XPR server>/CtiApl/<topic, e.g. H8000_CSTA for
OpenScape Voice>]: CTI link '<name of CTI link>' is up
again ...

SnmptapFilter [REG_SZ]

Default:	–
Possible values:	FEWID1234A

The [System Info SNMP Agent](#) can trigger SNMP traps directly. To enable this you need to set [SnmptapMode \[REG_DWORD\]](#) to 2 and specify a logging filter here. Log entry formats correspond to those described in the [LogFileFilter \[REG_MULTI_SZ\]](#).

NOTE: The SnmptapFilter registry key is used to specify what kind of log messages are going to generate traps.

E.1.20 SNMP Agents

XPR uses several SNMP agents. An SNMP agent delivers an interface and a database for information. These are used to monitor network devices and processes that deploy SNMP. The SNMP agent collects the information and delivers it to a management system upon request.

When the Windows SNMP service starts, it also starts the SNMP agents registered with it. These agents then load the files associated to them with the definition of the Management Information Base (MIB). An MIB is a formal description of objects. Each object represents a specific information. This information is stored as a set of MIB variables. You can access MIB objects by SNMP and they can be managed via a network management system. The management console via which the SNMP inquiries are posted to remote devices usually loads such MIB files.

NOTE: SNMP Agent writes the following files into system %TEMP% folder

```
xpragent-#####.log
snmplic-#####.log
```

Those files are created every day and are not deleted by default. Depending on the amount of system warnings these files size can increase quickly.

You can change the location of the log files by defining a System Environment Variable named %TRIVIAL_LOG_PATH% (e.g. C:\OpenScape\xpr\log)

Windows SNMP Service restart is needed.

For the time being, the following SNMP agents are supplied:

- License Info SNMP Agent

Provides the licenses used in the scope of the Software Subscription Licensing Model in the Common Management Portal (CMP). The license information is reported to the CMP by SNMP. This way the service can retrieve the corresponding information in the CMP. See [Section E.1.20.2, “License Info SNMP Agent \(CMP Usage Tracking\)”](#), on page 1705.
- System Info SNMP Agent

Provides via SNMP the same information displayed by means of the SystemInfo tool. See [Section 32.16, “SystemInfo”](#), on page 1561. The information is retrieved via the Web APL.

This agent can also trigger SNMP traps for information usually written in the logging file. To enable this you need to set `SnmpMode [REG_DWORD]` to 2 and specify a logging filter with `SnmpTrapFilter [REG_SZ]`. As filter we recommend e. g. FEW (Fatal errors (F), Error (E) and Warnings (W)).

E.1.20.1 Windows SNMP Service

The Windows SNMP service is a requirement for installing the SNMP agents. As the case may be, install it retrospectively:

Add or Remove Windows Components > Management and Monitoring Tools > Details > Simple Network Management Protocol and WMI SNMP Provider.

The SNMP service must be configured:

1. **Start > Run > services.msc**
2. In the properties of the Windows SNMP service add on the **Security** page the community "Public" with at least read access. If access shall be possible from other computers, select the corresponding option.
3. Restart the Windows SNMP service.

E.1.20.2 License Info SNMP Agent (CMP Usage Tracking)

You find the MIB file `SEN-LICENSE-MGR.mib` in
`<XPR Install>\res\snmpagent.`

If the SNMP port of the CMP deviates from the default 161, it must be changed. To do this you need to edit the `SERVICES` file in the directory
`%SYSTEMROOT%\SYSTEM32\DRIVERS\ETC.` Please proceed as follows:

1. Open the file with a text editor and look for the following line:
`snmp 161/udp #SNMP`
2. Change the port number according to the default in the CMP.
3. Save the file.
4. Restart the Windows SNMP service.

NOTE:

Owing to restrictions of the HiPath license management the available time with licenses that have not been used yet is reported as zero.

The following values can be found in the key
`SnmpLicenseAgentXpr\CurrentVersion.`

Pathname [REG_SZ]

Default:	<XPR Install>\bin\SnmpLicenseAgentXpr.dll
Possible values:	<Path>\SnmpLicenseAgentXpr.dll

Path and file name of the SNMP license agent. This is a so-called *Extension Agent* in the form of a DLL loaded by the Windows SNMP service.

You find the following values in the key `SnmpLicenseAgentXpr`.

ProductId [REG_SZ]

Default:	Content of SystemName [REG_SZ]
Possible values:	<String>

The product ID reported to the CMP. This is the name of the XPR server by default. If you wish to see another product ID, you can set this here.

E.1.20.3 System Info SNMP Agent

You find the MIB file `xpressionscmp.mib` in
 <XPR Install>\res\snmpagent.

The following values are contained in key `SnmpAgentXpr\CurrentVersion`.

Pathname [REG_SZ]

Default:	<XPR Install>\bin\SnmpAgentXpr.dll
Possible values:	<path>\SnmpAgentXpr.dll

Path and file name of the SNMP license agent. This is a so-called *Extension Agent* in the form of a DLL loaded by the Windows SNMP service.

E.2 Entries of the ABC APL

The following values can be found in the key `AbcApl`.

Address [REG_SZ]

Default:	–
Possible values:	<IP address>

PBX IP address. This value maps the **IP Address** field in the ABC APL configuration dialog. See [Chapter 25, “MWI to Alcatel 4400 \(ABC APL\)”](#).

AdjustedNotAplSettings [REG_DWORD]

Internal value. Must not be manually modified.

DisplayNameEmail [REG_SZ]

Default:	E-mail
Possible values:	<String>

Name for messages of type e-mail displayed in the telephone menu.

DisplayNameFax [REG_SZ]

Default:	Fax
Possible values:	<String>

Name for messages of type fax displayed in the telephone menu.

DisplayNameSMS [REG_SZ]

Default:	SMS
Possible values:	<String>

Name for messages of type SMS displayed in the telephone menu.

DisplayNameVoice [REG_SZ]

Default:	Voice
Possible values:	<String>

Name for messages of type voicemail displayed in the telephone menu.

LogicalLineClass [REG_SZ]

Default:	4400
Possible values:	<String>

Class portion of the logical line registered at the MTA by the ABC APL.

LogicalLineNode [REG_SZ]

Default:	MWI
Possible values:	<String>

Node portion of the logical line registered at the MTA by the ABC APL. Should not be modified.

MinUpdateInterval [REG_DWORD]

Default:	300
Possible values:	0 – Do not send any update requests to the Notification APL any more >0 – Period in milliseconds

This switch defines the time interval in milliseconds that must be at least between two notification update requests to the Notification APL. Such a request to the Notification APL is only sent if a lost connection between the ABC APL and the Alcatel PBX has been reestablished. Then the Notification APL sends the current MWI state for each user. Since this can result in an increased system load in case of a high number of users, the update frequency can be controlled by the new switch.

MrsNodeName [REG_SZ]

Default:	<XPR server name>
Possible values:	<String>

XPR server name. Should not be modified.

Port [REG_DWORD]

Default:	2533
Possible values:	<IP Port>

Port number for the ABC-A protocol at the Alcatel PBX. This value maps the **IP Port** field in the ABC APL configuration dialog. See [Chapter 25, “MWI to Alcatel 4400 \(ABC APL\)”](#).

E.3 Entries of the Con APL

You find the following values in the key ConApl.

The WebClient Service can be modified using the registry path
HKLM\SYSTEM\CurrentControlSet\services\XPRWebClient

If not stated otherwise, all of the following registry key specifications are relative to HKLM\SOFTWARE\Wow6432Node\PP-COM\MRS.

BindAddress [REG_SZ]

Default:	-
Possible values:	IP-address

Here the bind address of the TCP/IP protocols to be used by the Web server is specified. The Connection APL serves as web server for processing requests by XML-RPC.

CertificateDirectory [REG_DWORD]

Default:	-
Possible values:	Directory

The SSL certificate used in case of an encrypted transmission by HTTPS is in this directory.

HTTP_Port [REG_DWORD]

Default:	10000
Possible values:	Port number

Determines the port of the HTTP connection via which the RPC connection is enabled.

ListenerTimeout [REG_DWORD]

Default:	60
Possible values:	5-300

Period in seconds in which the Connection APL keeps a connection open. If no answer or request is received within this period, the connection is closed.

MaxClientsThreads [REG_DWORD]

Default:	8
Possible values:	Any whole positive number

This value determines the maximum number of threads that the client may execute.

MaxNumDocsRequest [REG_DWORD]

Default:	100
Possible values:	-1 – All messages 1...n – number of messages

When *OpenScape Web Client* retrieves voicemails from the Mail APL, only the first 100 messages in the inbox are considered. The available voicemails are filtered from these 100 messages and displayed in the *OpenScape Web Client*.

If you wish to consider more messages you can increase this value or set it even to “All messages”. If a user has received a large number of messages, this may lead to a time-out, though. If not all messages of a user have been retrieved after 60 seconds to filter them for voicemails, the function terminates and no voicemails are displayed to the user.

MaxServerThreads [REG_DWORD]

Default:	8
Possible values:	Any whole positive number

This value determines the maximum number of threads that the server may execute.

VoiceMailsOnly [REG_DWORD]

Default:	1
Possible values:	0 or 1

This entry serves for finding and rectifying errors. Default value 1 activates the voicemail-only transmission. Value 0 deactivates this function and admits all message types in case of an XML-RMP request.

Verbosity [REG_DWORD]

Default:	-1
Possible values:	Whole-number values from -1 to 5

With this entry you can determine the display of the exchanged call information. With value -1 no other outputs are delivered than requests. Value 0 activates the additional display of arguments of the invoked methods. The values 1 to 5 activate XML-RPC-internal representations.

PinToProcessor [REG_DWORD]

Default:	0
Possible values:	0, 1, 2, 3, ...
Remark:	0 = off 1 = CPU 0 2 = CPU 1 etc.

Registry Path is

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\XPRWebClient

If the customer is experiencing intermittent long delays in accessing OpenScape Web Client pages it is recommended to use this switch.

You need to select one of your logical processors (beginning with number 1) for the value of PinToProcessor followed by a restart of your Xpressions services in order to bind the Java processes for the WebClient services to this processor.

StartDelay [REG_DWORD]

Default:	0
Possible values:	Any whole positive number (e.g 5)

Registry Path is

HKLM\SOFTWARE\Wow6432Node\PP-COM\MRS\ConApl

This value will define the time in (decimal) minutes that the processing of jobs will be paused after the service startup.

NOTE: This registry key must be used in Microsoft Cluster environments in place of the registry key:

HKLM\SOFTWARE\Wow6432Node\PP-COM\Services\AplDelay

XpressionsFolder [REG_DWORD]

Default:	0
Possible values:	0: disable Xpression folder access 1: enable Xpression folder access

Enables access to PhoneMail Xpressions folder from WebClient

E.4 CSTA APL Entries

The following values are found in the key `CSTAAPL`:

BindAddress [REG_SZ]

Default:	<Server IP address>:1040-
Possible values:	<IP address>:<Port number>

Contains the values of the **IP address** field and of the preset port number, which were entered on the Connectivity tab of the configuration pages in the XPR monitor.

ComfortTransferApplication [REG_SZ]

Default:	-
Possible values:	Phone number

Contains the value of the phone number field for the comfort transfer, which was entered on the Phone Numbers tab of the configuration pages in the XPR monitor.

DeflectTimeout [REG_DWORD]

Default:	10
Possible values:	0 to 9999 seconds

Contains the value of the redirection time-out field for a parking loop, which was entered on the Phone Numbers tab of the configuration pages in the XPR monitor. Value 0 deactivates this feature.

LogMask [REG_DWORD]

Default:	0x00000000
Possible values:	<0xFFFFFFFF0 ... 0xFFFFFFFF>

Defines the settings of the logged messages in the XPR monitor. The following messages are not activated by default and can be activated by setting their associated bits:

- Bit 0: Transport layer (topic 'TCP<linkname>' or 'ISDN<linkname>')
- Bit 1: Topic 'CstaL6<linkname>' Debug 2
- Bit 2: Topic 'CstaL6<linkname>' Debug 3

With the following bits complete topics can be switched on. Since the number of topics is limited, this procedure can be useful when several CTI links are used:

- Bit 3: Topic '<linkname>DBG'
- Bit 4: Topic 'PBX<linkname>DBG'

ParkingDevice [REG_SZ]

Default:	-
Possible values:	Phone number

Contains the value of the real phone number field for a parking loop, which was entered on the Phone Numbers tab of the configuration pages in the XPR monitor.

ParkingLoop [REG_SZ]

Default:	-
Possible values:	Phone number

Contains the value of the virtual phone number field for a parking loop, which was entered on the Phone Numbers tab of the configuration pages in the XPR monitor.

PortList [REG_MULTI_SZ]

Default:	1040
Possible values:	Port number

One configured port number is listed per line.

SendSnapshot [REG_DWORD]

Default:	0
Possible values:	0 – Send snapshot to CTI APL disabled. 1 – Send snapshot to CTI APL active.

All snapshot commands are either sent directly to the CTI APL or dealt with within the CSTA APL.

E.5 Entries of the CTI APL

Since many of the registry values described in the following only apply when certain CTI protocols are used, the line *CTI Protocol* is introduced for each registry key starting from [Section E.5.2, “Registry Keys for CTI Links”, on page 1728](#). This line indicates for which CTI protocols the respective key is used.

IMPORTANT:

The modification of parameters should always be made in the configuration dialog of the XPR monitor. Only in some exceptional cases manual modifications directly performed in the registry become necessary.

The registry values in this chapter are structured in the following format:

- [Section E.5.1, “General Registry Keys”, on page 1720](#)
- [Section E.5.2, “Registry Keys for CTI Links”, on page 1728](#)
- [Section E.5.3, “Registry Values for the HiPath 4000”, on page 1758](#)

E.5.1 General Registry Keys

The following general registry values of the CTI APL are found under the following key:

HKLM\SOFTWARE\Wow6432Node\PP-COM\MRS\CTIAPL

ACL_AccessListCheck [REG_DWORD]

Default:	1
Possible values:	0 – Check deactivated 1 – Check activated

The possibility to control telephone devices in a CTI environment can be restricted for XPR users. This is done via the definition of telephone access privileges in *Communications*. Individual access groups are defined for each controllable telephone device all XPR users authorized for control have been assigned to. If no privileges for the telephone access via CTI have been defined systemwide, the control of telephone devices is unrestricted. Cf. the user manual *Communications*.

ACL_AccessListCheck activates the verification whether an XPR user is authorized as user of an access group

- to set a monitor point for monitoring the respective telephone device
- to establish a CTI-based communication relation via the XPR server to the respective telephone device

ACL_AccessProtoList [REG_Multi_SZ]

Default:	<Empty string>
Possible values:	<List of NODE addresses>
Remark:	Works in combination with ACL_AccessListCheck [REG_DWORD] .

Defines a list of NODE addresses that are authorized to establish communication relations via CTI. One address entry per line is allowed.

CheckACLAccessForAllLocation [REG_DWORD]

Default:	0
Possible values:	0 – Verification on the basis of the dialed phone number 1 – Verification on the basis of the dialed and localized phone number
Remark:	Works in combination with ACL_AccessListCheck [REG_DWORD] .

Specifies the phone number used as basis for checking the access authorization of an XPR user.

There are two options:

- Only on the basis of the phone number actually dialed in the CTI transaction
- On the basis of the phone number actually dialed and normalized.

CheckComputerNameField [REG_SZ]

Default:	<Empty string>
Remark:	This value must not be changed.

Switch for internal tests.

CheckMonitorLimit [REG_DWORD]

Default:	0
Possible values:	0 – Check disabled 1 – Check number of monitor points
Remark:	Works in combination with MaxMonitor [REG_DWORD] .

Activates the check as to how many monitor points of a user are simultaneously active.

CheckMonitorTimer [REG_SZ]

Default:	23:59
Possible values:	hh:mm
Remark:	Works in combination with CheckMonitorLimit [REG_DWORD] .

Indicates the time at which the warning of a user exceeding the maximum number of monitor points is written in the log file.

GetPhoneFrom [REG_SZ]

Default:	<Empty string>
Possible values:	DATABASE, BOTH, CLIENT
Remark:	Works in combination with UseFieldForPhone [REG_SZ] .

To transmit CTI transactions between a CTI client and the XPR server the transactions are packed in classic XPR messages. Thus the receiving XPR server knows the originator address in the NVS header as well as the originator number in the actual CTI transaction.

Example:

XPR message with the originator address: NVS:<Server name>/USER1.
Contained CTI transaction: PHONECALL Caller=110 Callee=223

In this example a telephone connection is to be established by *USER1*. The phone numbers of the packed CTI transaction define that this connection is to be established from the telephone device with the phone number *110* to the device with the phone number *223*. The XPR server now offers the possibility to determine the originator phone number for the desired communication connection on the basis of the transaction or NVS originator information.

Originator address in transaction

The XPR server establishes a communication connection between the telephone devices with the extensions 110 and 223.

Originator address in NVS header

If the originator address in the NVS header possesses a valid address format, the XPR server performs a look-up on the basis of the user ID contained within in the XPR user database. Since the entered user ID must be one of an existing XPR user, he/she will find the corresponding entry and the phone number assigned to him/her there. Accordingly, a communication connection between the thus identified telephone device and the device with the extension 223 is established.

By default, the phone number of the found user is searched in the **PHONE** database field. This setting can be modified in the registry value **UseFiledForPhone**.

GrantsPrivilegeToWatcher [REG_DWORD]

Default:	0
Possible values:	0 – telephone status display can be restricted 1 – Telephone status display cannot be restricted

So that XPR users can restrict the display of their telephones stati in the XPR server CTI clients for other users, this value must be set to **1**.

HicomAplCompatible [REG_DWORD]

Default:	1
Possible values:	0 – XPR server establishes one log. line via the HICOM APL 1 – XPR server establishes two log. lines via the HICOM APL

Ensures the compatibility to older versions of the HICOM APL, which establish two logical lines to the connected PBX.

IgnoreCallType [REG_DWORD]

Default:	0
Possible values:	0 - 'Call Type' is evaluated. 1 - 'Call Type' is ignored.

The XPR server can execute the phone number normalization on the basis of the transmitted 'call type'.

IgnoreCallType defines whether the 'call type' transmitted by the PBX is evaluated by the XPR server for normalization or whether it is ignored.

LogUID_Tree [REG_DWORD]

Default:	0
Possible values:	0 – No output of all UID information 1 – Output of all UID information

The unique ID defines a logical connection ID that is identical for all subscribers taking part in a defined communication relation. The XPR server stores the unique IDs of all communication relations in a designated list - the UID Tree.

Example:

In a telephone conference with four conversation partners the XPR server stores an automatically generated unique ID for each of the subscribers in addition to the individual call ID. The unique ID is identical for all four subscribers and is administered in the UID tree.

LogUID_Tree defines whether in the case of logging the UID tree content is also put out.

MaxMonitor [REG_DWORD]

Default:	30
Possible values:	<Number of monitor points>
Remark:	Works in combination with CheckMonitorLimit [REG_DWORD] .

Specifies the maximum number of simultaneously active monitor points of a user. The user's own monitor point for his/her telephone is not taken into account here. This value is used only if the database field [MAX_MONITOR](#) has not been specified for the user or user group.

ModifyLocation [REG_DWORD]

Default:	1
Possible values:	0 – No support of # and * as location prefix element 1 – Support of # and * as location prefix element

The XPR server supports the use of the # and * characters as location prefix elements. Using them, the cryptic special commands of the *Hicom 150* could, for example, be dialed from a CTI client. In this case no normalization would be performed.

MultiPBXAutoLearnMode [REG_DWORD]

Default:	1
Possible values:	0 – Deactivates the MultiPBX 'AutoLearn' mode 1 – Activates the MultiPBX 'AutoLearn' mode

Activates the MultiPBX 'AutoLearn' mode (cf. [Section 17.3.6, "Multi PBX "AutoLearn" Mode", on page 1065](#)).

The 'AutoLearn' mode enables connecting several PBX systems to one XPR server. The CTI APL learns independently the distribution of the applied extensions among the connected PBX systems. The extension numbers can be arbitrarily distributed among the PBXs but must be unique.

MultiPBXAutoLearnModeWithoutLocation [REG_DWORD]

Default:	0
Possible values:	0 – Normalized Addressing 1 – Extension Addressing

The MultiPBX 'AutoLearn' mode can process pure extension addressing without the respective location definition. In this case the CTI APL searches all configured CTI links for the subscriber with the addressed extension. Cf. [Section 17.3.6, "Multi PBX "AutoLearn" Mode", on page 1065](#).

In the default setting the CTI APL expects the transfer of a destination number in normalized form. In this case only the CTI links of the corresponding location are searched for the desired subscriber.

MwiRefreshAllLinks [REG_DWORD]

Default:	0
Possible values:	0 – Deactivates the retransfer of the MWI status information 1 – Activates the retransfer of the MWI status information
Remark:	For <i>Hicom 300</i> and <i>Hipath 4000</i> . Works in combination with CIT-RefreshTime [REG_SZ] .

The PBX Hicom 300 and Hipath 4000 do not save the current state of the MWI signal (LED) of the single telephones. Therefore, this status information is lost e.g. during a restart of a module or the PBX itself. The XPR server can therefore be configured in a way that all MWI status information is to be reset once a day in the connected PBX.

MwiRefreshAllLinks activates the retransmission mechanism for all configured CTI links.

StatCtiCall [REG_DWORD]

Default:	1
Possible values:	0 – Deactivates saving CTI CALL statistics 1 – Activates saving CTI CALL statistics

The XPR server stores statistic information by default under *<XPR Install>\<Statistic directory>\st<date>.log*. A new statistic file is created for each day.

StatCtiCall activates saving a statistic entry for each performed communication connection in the file *st<date>.log*. Thereby all important information about the respective connection is documented.

StatCtiEvents [REG_DWORD]

Default:	1
Possible values:	0 – Deactivates saving CTI EVENT statistics 1 – Activates saving CTI EVENT statistics

The XPR server stores statistic information by default under *<XPR Install>\<Statistic directory>\st<date>.log*. A new statistic file is created for each day.

StatCtiEvents activates saving a statistic entry for each performed CTI event in the file *st<date>.log*.

StatDevEvents [REG_DWORD]

Default:	1
Possible values:	0 – Deactivates saving DEV EVENT statistics 1 – Activates saving DEV EVENT statistics

The XPR server stores statistic information by default under *<XPR Install>\<Statistic directory>\st<date>.log*. A new statistic file is created for each day.

StatDevEvents activates saving a statistic entry for each change of the device state from ALIVE to DEAD or from DEAD to ALIVE in the file `st<date>.log`.

TransBreak [REG_DWORD]

Default:	25 [Milliseconds]
Possible values:	<Time> [Milliseconds]
Remark:	Works in combination with TransMax [REG_DWORD] .

The CTI APL can restrict the execution of CTI transactions.

TransBreak defines the time interval, during which a maximum of **TransMax** CTI transactions are processed.

TransMax [REG_DWORD]

Default:	3
Possible values:	<Number>
Remark:	Works in combination with TransBreak [REG_DWORD] .

The CTI APL can restrict the execution of CTI transactions.

TransMax defines the number of CTI transactions that are processed in the time interval **TransBreak**.

UniqueCallId [REG_DWORD]

Default:	<Unique Call ID>
Possible values:	<Unique Call ID>
Remark:	Must not be modified.

The XPR server generates for each connection group a corresponding unique call ID that will be required for referencing the connection group later on.

UniqueCallId serves for caching the last used unique call ID.

UseFieldForPhone [REG_SZ]

Default:	<Empty string>
Possible values:	<Name of an XPR database field>
Remark:	Is only evaluated, if the entry in GetPhoneFrom [REG_SZ] is DATABASE or BOTH.

Defines from which XPR database field a telephone device number is to be read. If this field cannot be found, an entry in the **PHONE** database field is searched for.

UseOldTSAPIStack [REG_DWORD]

Default:	0
Possible values:	0 – Activates the new TSAPI protocol stack 1 – Activates the old TSAPI protocol stack
Remark:	The setting may only be modified by the producer's personnel or their official partners. As long as there are nor arguments against it, you should always use the new TSAPI protocol stack.

Besides the TSAPI protocol stack used so far, the CTI APL contains a new TSAPI protocol stack.

UseOldTSAPIStack defines whether this new TSAPI protocol stack or the stack of the previous server version is used.

If value **0** is selected here, no expanded settings are available in the TSAPI channel settings of the CTI APL.

Use<Protocol>_<CTI Link name> [REG_DWORD]

Default:	0
Possible values:	0 – Deactivates the corresponding CTI link 1 – Activates the corresponding CTI link

The XPR server creates a registry key with a name in the form Use<Protocol>_<CTI-Linkname> for each configured CTI link.

Example:

UseCSTA_H150CSTA for the CTI link named *H150CSTA*, which uses the CTI protocol *CSTA*. Such a key defines whether the associated CTI link is active.

E.5.2 Registry Keys for CTI Links

Depending on the applied CTI protocol, one additional key with the name of this CTI link can exist for the respective CTI links.

The following general registry values of the CTIAPL are found under the following key:

HKLM\SOFTWARE\Wow6432Node\PP-COM\MRS\CTIAPL\<CTI link>

AllowedNumberChars [REG_SZ]

Default:	01234567890*#
Possible values:	<any characters>
CTI protocol:	CSTA, TSAPI, TAPI

The CTIAPL can check phone numbers for illegal characters, since not every application can process any character strings without problems.

AllowedNumberChars defines all characters that may be included in a transmitted phone number. If this key remains empty, the phone number check is deactivated.

AssociatedNormPublic [REG_DWORD]

Default:	0
Possible values:	0, 1
CTI protocol:	CSTA
Remark:	For <i>Hicom 150</i> .

In case of older Hicom PBXs the number of the caller and of the callee must be manipulated in certain cases, if a number exists in the **Associated...** CSTA field.

If a PBX number or the location exists twice in the normalized phone number and the **Associated...** field exists in the CSTA trace of the corresponding event, set **AssociatedNormPublic** to **1**.

AutoLearnerTimeout [REG_DWORD]

Default:	10 [Seconds]
Possible values:	<Time> [Seconds]
CTI protocol:	CSTA, TSAPI, TAPI

The multi PBX “AutoLearn” mode is based on setting monitor points in the active PBXs. To set such a monitor point in a PBX, the XPR server sends a corresponding transaction to the PBX concerned. This PBX then reports to the XPR server whether or not the monitor point could be set. If in the meantime the CTI link between XPR server and PBX was interrupted, the XPR server cannot receive the reply.

So that the XPR server need not unnecessarily wait for the reply already sent, a period can be defined in **AutoLearnerTimeout**, after which the XPR server stops waiting for the reply.

AutoReconnectAfterConsultation [REG_DWORD]

Default:	0 (HiPath 4000), 2 (others)
Possible values:	0 – Maintain ‘Hold’ if busy 1 – No longer used 2 – Finish ‘Hold’ if busy and switch back to subscriber
CTI protocol:	CSTA, TSAPI
Remark:	Is in case of TSAPI only valid for the new TSAPI protocol stack (cf. UseOldTSAPIStack [REG_DWORD]).

Defines whether a subscriber will be immediately connected to the caller when a consultation call attempt has ended with ‘Busy’.

BindAddress [REG_SZ]

Default:	<Empty string>
Possible values:	<IP address>
CTI protocol:	CSTA

The XPR server system of a CTI environment can be equipped with several LAN cards. If in such a case the CTI communication with the connected PBX system(s) occurs via TCP/IP, then for each CTI link must be specified via which LAN card the respective PBX can be reached.

BindAddress defines the IP address of the LAN board via which the primary IP address ([HostName \[REG_SZ\]](#)) of the associated PBX can be reached.

If this value remains empty in a Multi-NIC environment, the LAN board transferred to the XPR server by the WinSocket of the Windows operating system as the first one is used.

Since the result from this is unpredictable, we recommend in a Multi-NIC environment to always specify one of the available LAN boards via its IP address.

BindAddress2 [REG_SZ]

Default:	–
Possible values:	<IP address>
CTI protocol:	CSTA
Remark:	Must be added to the registry manually if required. Works in combination with: • HostName2 [REG_SZ] • Port2 [REG_DWORD].

Defines the IP address of the LAN board via which the secondary IP address ([HostName2 \[REG_SZ\]](#)) of the associated PBX can be reached.

If this value remains empty in a Multi-NIC environment, the LAN board transferred to the XPR server by the WinSocket of the Windows operating system as the first one is used.

Since the result from this is unpredictable, we recommend in a Multi-NIC environment to always specify one of the available LAN boards via its IP address.

BlindConferenceDelayTime [REG_DWORD]

Default:	0 [Milliseconds]
Possible values:	<Time> [Milliseconds]
CTI protocol:	CSTA

The XPR server may initiate conferences in two ways:

- as common conference with a connected subscriber and a second subscriber who is already on hold while the conference is being set up
- as blind conference with a connected subscriber and a second subscriber who is merely defined via his/her phone number while the conference is being set up

Though users will find the second option easier to handle, PBXs do in most cases not support this type of a conference setup. Therefore, the XPR server first establishes a consultation with the second subscriber independently. Subsequently, it initiates automatically the desired conference.

Some PBXs, though, cannot immediately initiate a conference with the consulted subscriber after establishing a consultation. Therefore, a period can be defined with **BlindConferenceDelayTime**, in which the XPR server delays the conference initiation after the consultation has been established.

CallId [REG_DWORD]

Default:	<Call ID>
Possible values:	<Call ID>
CTI protocol:	CSTA, TSAPI, TAPI
Remark:	Must not be modified.

The XPR server generates for each connection a corresponding call ID that will be required for referencing the connection later on.

CallId serves for caching the call ID used last.

CallTransferDelay

Default:	250 [Milliseconds]
Possible values:	<Time> [Milliseconds]
CTI protocol:	CSTA
Remark:	For <i>Alcatel 4200</i> .

Defines a delay time the XPR server waits before executing a configured call diversion.

Capabilities [REG_MULTI_SZ]

Default:	Diverse options
Possible values:	Diverse options
CTI protocol:	CSTA, TSAPI, TAPI

Defines the features (e.g. DIVERSION, PHONECALL, ...) of all telephones of this CTI link. Since no device-specific settings are supported, the logical intersection of features of all device types should be defined. Otherwise, the CTI APL allows features on the respective CTI link that cannot be represented by some devices.

If in the CTI APL device profiles are defined (cf. [Section 17.3.5, "Device Profiles", on page 1059](#)), the settings made here are not evaluated, since the information of the device profiles is administered in the Correlation Database of the XPR server.

CAPI_ControllerNr [REG_DWORD]

Default:	1
Possible values:	<Controller number>
CTI protocol:	CSTA

Defines the number of the ISDN controller via which the CTI communication to the respective PBX takes place.

CAPI_ControllerIndex [REG_DWORD]

Default:	1
Possible values:	<Index number>
CTI protocol:	CSTA

Defines the index number of the ISDN line on the ISDN controller via which the CTI communication to the respective PBX takes place.

CAPI2032.DLL [REG_SZ]

Default:	CAPI2032.DLL
Possible values:	<Name of the CAPI.DLL>
CTI protocol:	CSTA

Defines the name of the CAPI.DLL if the CTI communication to the respective PBX is enabled via an ISDN connection.

CheckTimeValue [REG_DWORD]

Default:	60 [Seconds]
Possible values:	<Time> [Seconds]
CTI protocol:	TSAPI
Remark:	Is only valid for the old TSAPI protocol stack (cf. UseOldTSAPIStack [REG_DWORD]).

Different PBX systems offer the XPR server the option to retrieve information about the current communication relations.

CheckTimeValue defines the time interval in which the CTI APL retrieves this information about the current communication relations and synchronizes them with the connections known in the CTI APL. This prevents an erroneously signalled connection end from unintentionally binding system resources in the CTI APL.

CIT-Beep [REG_DWORD]

Default:	0
Possible values:	0 - No acoustic signal 1 - Acoustic signal
CTI protocol:	CSTA
Remark:	For <i>Hicom 300</i> and <i>Hipath 4000</i> .

Defines whether the telephone is to put out an acoustic signal to signalize a new message.

CIT-Display [REG_DWORD]

Default:	0
Possible values:	0 - No display 1 - Permanent display 2 - Temporary display (mostly about 5 seconds)
CTI protocol:	CSTA
Remark:	For <i>Hicom 300</i> and <i>Hipath 4000</i> .

Defines whether a display is to be put out on the telephone when a new message is signalized. If desired, you can select between the options of a permanent or temporary display.

CIT-LED [REG_DWORD]

Default:	0
Possible values:	0 – No MWI display by LED <LED number on the telephone>
CTI protocol:	CSTA
Remark:	For <i>Hicom 300</i> and <i>Hipath 4000</i> .

Defines whether an LED is to be addressed on the telephone when a new message is signalized. If this is desired, the corresponding LED to be used for displaying this information can be specified via this entry and the LED number on the telephone.

The selected LED may not be used for any other features.

CIT-RefreshTime [REG_SZ]

Default:	<Empty string>
Possible values:	<hh:mm>
CTI protocol:	CSTA, TSAPI, TAPI
Remark:	• For <i>Hicom 300</i> and <i>Hipath 4000</i>. • Works in combination with MwiRefreshAllLinks [REG_DWORD]. • Updates the MWI information only if the counter-based CIT of the XPR server is used. NOT APL usage does not support any mailbox LED update. This requires the settings: – HKLM\SOFTWARE\Wow6432Node\PP-COM\MRS\MTA\CIT\CitActive=1 – HKLM\SOFTWARE\Wow6432Node\PP-COM\MRS\MTA\CIT\CitCounter=1.

The PBX Hicom 300 and Hipath 4000 do not save the current state of the MWI signal (LED) of the single telephones. Therefore, this status information is lost e.g. during a restart of a module or the PBX itself. The XPR server can therefore be configured in a way that all MWI status information is transferred once a day to the connected PBX.

CIT-RefreshTime defines the time at which all MWI status information is transferred to the connected PBX.

CitSF [REG_DWORD]

Default:	Depending on the applied PBX
Possible values:	0 – Deactivates the MWI Signal 1 – Activates the MWI Signal
CTI protocol:	CSTA, TSAPI, TAPI
Remark:	Works in combination with CitSFAddr [REG_SZ] .

The XPR server supports the transmission of the MWI signal to the connected PBX. This enables notifying the user of the addressed telephone about incoming messages.

CitSF enables the MWI signal on the respective CTI link.

CitSFAddr [REG_SZ]

Default:	NVS : MWI . <Name of the CTI link>
Possible values:	NVS : MWI . <Name of the CTI link>
CTI protocol:	CSTA, TSAPI, TAPI
Remark:	Works in combination with CitSF [REG_DWORD] .

The XPR server supports the transmission of the MWI signal to the connected PBX. This enables notifying the user of the addressed telephone about incoming messages.

CitSFAddr defines the name of the logical line via which MWI signaling is to take place.

CSTAVersion [REG_SZ]

Default:	<Version number>
Possible values:	<Version number>
CTI protocol:	CSTA
Remark:	For <i>Alcatel 4200</i> .

Defines the version of a producer-dependent `CSTA.DLL`, which may be used.

CstaDll [REG_DWORD]

Default:	csta.dll
Possible values:	<File name>
CTI protocol:	CSTA, TSAPI

Defines the name of the `CSTA.DLL`.

CtiTeleActive [REG_DWORD]

Default:	0
Possible values:	0 – Deactivates forwarding of incoming calls 1 – Activates forwarding of incoming calls
CTI protocol:	CSTA, TSAPI, TAPI

The option *Forwarding incoming Calls*, which is a voicemail system feature, must be activated here for the IP APL to support it. Consequently, relevant requests by the TUI and the *Web Assistant* are not handled via the IP APL but via the CTI APL.

DBFieldForMWI [REG_SZ]

Default:	CIT
Possible values:	<XPR database field>
CTI protocol:	CSTA, TSAPI, TAPI

Defines the field in the XPR user database in which the address for Message Waiting Indication is stored.

DontLocalize [REG_DWORD]

Default:	0
Possible values:	0 – UseTypeInternational = false. No normalization 1 – UseTypeInternational = true. Normalization to E.164.
CTI protocol:	CSTA, TSAPI, TAPI

Defines whether the phone numbers are normalized by the XPR server. By setting, the NCO variable [UseTypeInternational](#) is temporarily overwritten.

DontLocalizeInternal [REG_DWORD]

Default:	0
Possible values:	0 – Activates the phone number normalization for internal phone numbers 1 – Deactivates the phone number normalization for internal phone numbers
CTI protocol:	CSTA, TSAPI, TAPI

Defines whether internal phone numbers are normalized by the XPR server. For OpenScape Voice this value must be set to **1**, since this PBX expects phone numbers in a format that can be directly dialed.

DontSendDead [REG_DWORD]

Default:	0
Possible values:	0 – 'DEAD' messages are not suppressed 1 – 'DEAD' messages are suppressed
CTI protocol:	CSTA, TSAPI
Remark:	Is in case of TSAPI only valid for the new TSAPI protocol stack (cf. UseOldTSAPIStack [REG_DWORD]).

To clear a communication connection, the respective CTI client is normally notified about the actual connection termination with a DEAD message.

DontSendDead defines whether 'DEAD' messages are suppressed.

ExtPrefix [REG_SZ]

Default:	<Empty string>
Possible values:	<Number Sequence>
CTI protocol:	CSTA, TSAPI, TAPI

Some PBX systems forward besides the actual phone number information an additional digit to the XPR server during the dialing process. This digit may be e.g. a tie trunk number or a specific escape code for an existing corporate network in which several PBX systems are networked.

The XPR server is able to reject such an additionally forwarded digit during the phone number information analysis.

ExtPrefix defines the string of digits that are to be rejected during the phone number information evaluation by the XPR server.

FirstLoadDelay [REG_DWORD]

Default:	2 [Seconds]
Possible values:	<Time> [Seconds]
CTI protocol:	TSAPI
Remark:	Is only valid for the old TSAPI protocol stack (cf. UseOldTSAPIStack [REG_DWORD]).

Defines a delay for setting a monitor point on the PBX of the corresponding CTI link.

FirstPlayMessageDevice [REG_SZ]

Default:	<Empty string>
Possible values:	<Index number>
CTI protocol:	CSTA
Remark:	Works in combination with LastPlayMessageDevice [REG_SZ] .

Some PBX systems support analog announcement ports for the playback of voice messages (e.g. in contact center environments). Depending on the PBX it may be possible to control these ports via CTI functionalities. Addressing these announcement ports is often effected in a coherent index block.

FirstPlayMessageDevice defines the first index number of such an announcement port block.

HostName [REG_SZ]

Default:	<IP address>
Possible values:	<IP address>
CTI protocol:	CSTA
Remark:	Possibly in combination with HostName2 [REG_SZ]

Defines the (primary) IP address of the associated PBX. If a service to resolve host names is available in the TCP/IP network used, also the PBX host name can be entered here.

If the relevant PBX can be reached via a redundant IP address, this redundant IP address can be configured under the registry value [HostName2 \[REG_SZ\]](#).

HostName2 [REG_SZ]

Default:	–
Possible values:	<IP address>
CTI protocol:	CSTA
Remark:	Must be added to the registry manually if required. Works in combination with: • HostName [REG_SZ] • Port2 [REG_DWORD] • BindAddress2 [REG_SZ].

Defines besides the primary IP address ([HostName \[REG_SZ\]](#)) a redundant IP address of the associated PBX. If a service to resolve host names is available in the TCP/IP network used, also the PBX host name can be entered here.

If the associated PBX cannot be reached under the primary IP address ([HostName \[REG_SZ\]](#)), the CTI APL attempts to reach the PBX under the redundant IP address. If the PBX cannot be reached under the redundant IP address either, the CTI APL takes turns in the attempt to reach the PBX under the primary and the redundant IP address.

IsBChannel

Default:	1
Possible values:	0 - Uses the D-channel 1 - Uses the B-channel
CTI protocol:	CSTA
Remark:	For <i>Octopus 180</i> with ISDN connection.

Defines whether the B- or D-channel of the ISDN connection is used for the CTI communication.

LastPlayMessageDevice [REG_SZ]

Default:	<Empty string>
Possible values:	<Index number>
CTI protocol:	CSTA
Remark:	Works in combination with FirstPlayMessageDevice [REG_SZ] .

Some PBX systems support analog announcement ports for the playback of voice messages (e.g. in contact center environments). Depending on the PBX it may be possible to control these ports via CTI functionalities. Addressing these announcement ports is often effected in a coherent index block.

LastPlayMessageDevice defines the last index number of such an announcement port block.

License [REG_DWORD]

Default:	0
Possible values:	0 – TAPI client license 1 – TAPI server license 2 – CSTA server license
CTI protocol:	CSTA
Remark:	For <i>Alcatel OmniPCX Office</i> .

Defines which licenses are used in the PBX.

Three options can be realized:

- The 'TAPI client' license is used in the PBX (only two monitor points can be set).
- The 'TAPI server' license is used in the PBX.
- The 'CSTA server' license is used in the PBX.

LicKey [REG_DWORD]

Default:	–
Possible values:	<License Keys>
CTI protocol:	CSTA

Defines a license key for the CTI connection of some PBX systems.

LineSleep [REG_DWORD]

Default:	0 [Milliseconds]
Possible values:	<Time> [Milliseconds]
CTI protocol:	TAPI

After it has been started, the CTI APL starts all logical lines of the configured CTI links successively.

LineSleep defines a delay that is to pass between opening two lines.

LinkMaster [REG_DWORD]

Default:	0
Possible values:	0 – Does not define the respective CTI link as link master 1 – Defines the respective CTI link as link master
CTI protocol:	CSTA, TSAPI, TAPI
Remark:	Exactly one CTI link may be defined as link master.

In an environment with several CTI connections ideally all phone numbers of CTI requests should be forwarded to the CTI APL in normalized form. In many cases, however, there is a major system delivering the local respectively internal numbers.

LinkMaster defines the CTI link via which the XPR server is connected to this major system.

LoadBackupDelay [REG_DWORD]

Default:	5 [Seconds]
Possible values:	<Time> [Seconds]
CTI protocol:	TSAPI
Remark:	Is only valid for the old TSAPI protocol stack (cf. UseOldTSAPIStack [REG_DWORD]).

The CTI APL stores the information about all set monitor points in a backup file. Thus it is possible to reset the original state of the device monitoring after a restart.

LoadBackupDelay defines a delay that has to pass after the start of the APL before it begins with the reimport process.

LocalLine [REG_DWORD]

Default:	1
Possible values:	0 – CTI link may be represented via RSL 1 – CTI link may not be represented via RSL
CTI protocol:	CSTA, TSAPI, TAPI

Several XPR servers can be networked via so-called Remote System Links (RSL). Logical lines of an XPR server are then mapped on another server, which is connected via RSL, so that this remote server can also access them.

LocalLine defines whether the respective CTI link is mapped on the remote XPR server in case of RSL.

Login_Delaytime [REG_DWORD]

Default:	2000 [Milliseconds]
Possible values:	<Time> [Milliseconds]
CTI protocol:	CSTA
Remark:	For <i>Alcatel OmniPCX Office</i> . Works in connection with Number_of_TAPI-Links [REG_SZ] and Logout_Delaytime [REG_DWORD] .

When an *Alcatel OmniPCX Office* is used, several parallel connections between the XPR server and the PBX can be established.

Login_Delaytime defines which time the XPR server waits between the setup of two of these connections.

LoginID [REG_SZ]

Default:	<Empty string>
Possible values:	<Account name>
CTI protocol:	TSAPI
Remark:	Works in combination with Password [REG_SZ] .

For the CTI communication between the XPR server and the PBX, a user account is implemented in the PBX.

LoginID defines the name of this user account with which the CTI APL needs to log on to the PBX.

Logout_Delaytime [REG_DWORD]

Default:	2000 [Milliseconds]
Possible values:	<Time> [Milliseconds]
CTI protocol:	CSTA
Remark:	For <i>Alcatel OmniPCX Office</i> . Works in connection with Number_of_TAPI-Links [REG_SZ] and Logout_Delaytime [REG_DWORD] .

When an *Alcatel OmniPCX Office* is used, several parallel connections between the XPR server and the PBX can be established.

Logout_Delaytime defines how long the XPR server waits between the shutdown of two of these connections.

MaxLoadBackup [REG_DWORD]

Default:	3
Possible values:	<Number of monitor points>
CTI protocol:	CSTA, TSAPI
Remark:	Is in case of TSAPI only valid for the new TSAPI protocol stack (cf. UseOldTSAPIStack [REG_DWORD]).

The CTI APL stores the information about all set monitor points in a backup file. Thus it is possible to reset the original state of the device monitoring after a restart.

MaxLoadBackup defines the number of monitor points read in one block from the backup file and subsequently set when the CTI APL starts. The CTI APL downloads a new block from the backup file every two seconds and sets the respective monitor points in the corresponding PBX.

MaxLoadBackup [REG_DWORD]

Default:	3
Possible values:	<Number of monitor points>
CTI protocol:	CSTA, TSAPI
Remark:	Is in case of TSAPI only valid for the new TSAPI protocol stack (cf. UseOldTSAPIStack [REG_DWORD]).

The CTI APL stores the information about all set monitor points in a backup file. Thus it is possible to reset the original state of the device monitoring after a restart.

MaxLoadBackup defines the number of monitor points read in one block from the backup file and subsequently set when the CTI APL starts. The CTI APL downloads a new block from the backup file every two seconds and sets the respective monitor points in the corresponding PBX.

MaxMonRange [REG_DWORD]

Default:	100
Possible values:	<Number of monitor points in one phone number range>
CTI protocol:	TSAPI
Remark:	Is only valid for the old TSAPI protocol stack (cf. UseOldTSAPIStack [REG_DWORD]).

Under TSAPI it is possible to set static monitor points in a coherent phone number range.

MaxMonRange defines the maximum size of a range of static monitor points. Therefore no oversized ranges can be indicated for setting monitor points.

MonDelay [REG_DWORD]

Default:	500 [Milliseconds]
Possible values:	<Time> [Milliseconds]
CTI protocol:	CSTA, TSAPI
Remark:	Is in case of TSAPI only valid for the new TSAPI protocol stack (cf. UseOldTSAPIStack [REG_DWORD]).

Defines a delay for setting a monitor point on the PBX of the corresponding CTI link.

MonitorLimit [REG_DWORD]

Default:	0
Possible values:	0 – No verification <Number of monitor points>
CTI protocol:	CSTA, TSAPI, TAPI

Defines the maximum number of monitor points that are to be set on the respective CTI link.

MonitorTimeout [REG_DWORD]

Default:	15 [Seconds]
Possible values:	<Time> [Seconds]
CTI protocol:	CSTA, TSAPI, TAPI
Remark:	Is in case of TSAPI only valid for the new TSAPI protocol stack (cf. UseOldTSAPIStack [REG_DWORD]).

If a CTI client initiates setting a monitor point in a PBX, status information about the required device is regularly transmitted to the client by the XPR server via the CTI transaction MONITORSTATUS. The CTI client confirms the reception of each of these transactions. Only after the CTI client has deleted the respective device monitoring or logs off from the XPR server, the XPR server stops these regular transmissions.

MonitorTimeout defines a timeout, during which a CTI client must confirm a MONITORSTATUS message. If this is not the case, the XPR server assumes that the CTI client has failed to log off and is no longer active. As a result, the XPR server stops the transmissions.

MPCallCause [REG_DWORD]

Default:	0xFFFFFFFF (4294967295)
Possible values:	<Call Cause>
CTI protocol:	TSAPI
Remark:	This value must not be modified.

Some PBX systems support the connection of an additional telephone device (slave) to an existing device (master). The additional device can then be reached under the same phone number as the master.

MPCallCause defines in this environment whether a 'DELIVERED' event is suppressed for the 'MULTIPLECALL' transaction at the master of a *Bosch* PBX.

MulapPrefix [REG_SZ]

Default:	**
Possible values:	<Mulap-Prefix>
CTI protocol:	TAPI
Remark:	For <i>Hicom 150</i> .

The Hicom 150 uses a so-called *Mulap* group to which the telephone devices belong. For outgoing calls the Hicom150 only notes the <MulapNumber>. The phone number of the respective telephone device is stored in the **REDIR** field.

MulapPrefix defines the prefix used for the definition of a Mulap number.

NetType [REG_DWORD]

Default:	0
Possible values:	0 – ISDN 1 – LAN
CTI protocol:	CSTA

Defines the medium used for the CSTA connection.

NodeNumber [REG_DWORD]

Default:	–
Possible values:	<HiPath 3000 node number>
CTI protocol:	CSTA

If optiClient is used with a HiPath 3000, calls may get lost in the call journal if the HiPath 3000 is used with an open number plan.

NodeNumber must in this case defined the node number of the HiPath 3000.

NoSpeaker [REG_DWORD]

Default:	0
Possible values:	0 – Automatic activation of loudspeaker/microphone possible 1 – No automatic activation of loudspeaker/microphone possible
CTI protocol:	CSTA, TSAPI, TAPI

In a CTI environment the loudspeaker and the microphone of the receiving telephone device can be automatically activated for incoming calls.

NoSpeaker defines whether this option is provided on the respective CTI link.

NotSupported_Device [REG_MULTI_SZ]

Default:	<Empty string>
Possible values:	<List of device extensions>
CTI protocol:	CSTA, TSAPI, TAPI

Defines which telephone devices may not be monitored by setting monitor points.

Number_of_TAPI-Links [REG_SZ]

Default:	25
Possible values:	<Number of TAPI links>
CTI protocol:	CSTA
Remark:	For <i>Alcatel OmniPCX Office</i> . Works in connection with Login_Delaytime [REG_DWORD] and Logout_Delaytime [REG_DWORD] .

When an *Alcatel OmniPCX Office* is used, several parallel connections between the XPR server and the PBX can be established.

Number_of_TAPI-Links defines how many parallel connections are set up by the XPR server.

NumMaxConnections [REG_DWORD]

Default:	256
Possible values:	<Maximum number of connections>
CTI protocol:	TSAPI
Remark:	Is only valid for the old TSAPI protocol stack (cf. UseOldTSAPIStack [REG_DWORD]).

TSAPI drivers normally allow only a number of CTI links limited by the licenses.

NumMaxConnections defines the maximum number of connections that are allowed for the TSAPI driver of the respective CTI link.

NumMaxMonitors [REG_DWORD]

Default:	256
Possible values:	<Maximum number of monitor points>
CTI protocol:	TSAPI
Remark:	Is only valid for the old TSAPI protocol stack (cf. UseOldTSAPIStack [REG_DWORD]).

PBX systems normally allow only a number of monitor points limited by the licenses.

NumMaxMonitors defines the maximum number of monitor points that can be set in the connected PBX.

NumMaxTrans [REG_DWORD]

Default:	256
Possible values:	<Maximum number of transaction relations>
CTI protocol:	TSAPI
Remark:	Is only valid for the old TSAPI protocol stack (cf. UseOldTSAPIStack [REG_DWORD]).

The TSAPI stack administers all current transaction relations in a list that is restricted in its length. For this reason, the XPR server can only set up a restricted number of transactions to the connected PBX at the same time.

This restriction applies especially to the setting of monitor points of several CTI clients.

Example:

In a CTI environment exist 30 users who have activated their CTI client, and who monitor the states of 10 PBX terminal devices each.

If all users start their computers at the same time in the morning, the result is 300 transaction relations. This value exceeds the default setting of 256. As a result, the 'first' 25 users see all stati of the desired devices. The 26th user can only see 6 states. The limit of 256 is thus reached. All other users do not see any current state at all.

NumMaxTrans defines the maximum number of transaction relations that can be administered via the applied TSAPI stack.

NumMaxXmrLines [REG_DWORD]

Default:	64
Possible values:	<Maximum number of displayed lines>
CTI protocol:	CSTA, TSAPI, TAPI

Defines the maximum number of logical lines that are displayed in the XPR monitor.

PabxManufacturer [REG_SZ]

Default:	Depending on the connected PBX
Possible values:	<Manufacturer name>
CTI protocol:	CSTA, TSAPI, TAPI
Remark:	This value must not be modified.

Defines the manufacturer name of the connected PBX that is used for the internal distinction of the PBX-dependent features.

PabxModel [REG_SZ]

Default:	Depending on the connected PBX
Possible values:	<Model name>
CTI protocol:	CSTA, TSAPI, TAPI
Remark:	This value must not be modified.

Defines the model name of the connected PBX that is used for the internal distinction of the PBX-dependent features.

Password [REG_SZ]

Default:	<Empty string>
Possible values:	<Password>
CTI protocol:	TSAPI
Remark:	Works in combination with LoginID [REG_SZ] .

For the CTI communication between the XPR server and the PBX, a user account is implemented in the PBX.

Password defines the password of this user account with which the CTI APL needs to log on to the PBX.

PbxRelease [REG_SZ]

Default:	6.3
Possible values:	6.3 6.4
CTI protocol:	CSTA
Remark:	For <i>Octopus E300/800</i> This value should only be modified in exceptional cases.

Defines the Login procedure that the CTI APL uses for the login at the connected PBX.

Since software version 6.4 of the Octopus E300/800 a new login procedure has been used. By default, the CTI APL tries to set up the connection to the PBX via the login procedure of version 6.3. If an error occurs, the new procedure of version 6.4 is used with the next attempt. If this second login is successful, the content of the registry value **PbxRelease** is automatically modified to **6.4**. Accordingly, the CTI APL tries to log in at the PBX with the 6.4 procedure after a restart.

PhoneNumber [REG_SZ]

Default:	Depending on the applied PBX
Possible values:	<Extension>
CTI protocol:	CSTA

Defines the extension via which the CTI communication between the XPR server and PBX takes place, if the respective CTI links are realized via an ISDN connection.

PhoneSetStatus [REG_DWORD]

Default:	0
CTI protocol:	TAPI
Remark:	For <i>Hicom 150</i> . Is no longer used and must not be changed.

Defines the applied CTI mode of the connected PBX.

PlayMessage_withIndex [REG_DWORD]

Default:	1
Possible values:	0 – Access announcement port by telephone number 1 – Access announcement port by 'index'
CTI protocol:	CSTA
Remark:	For <i>Hicom 150</i> with HPCO call center

Defines in which form announcement ports are accessed.

Port [REG_DWORD]

Default:	Depending on the applied PBX
Possible values:	<IP Port>
CTI protocol:	CSTA

Defines the TCP port for the primary IP address ([HostName \[REG_SZ\]](#)), via which the CTI communication between XPR server and PBX is handled, if the relevant CTI links are enabled via a LAN connection.

Port2 [REG_DWORD]

Default:	–
Possible values:	<IP Port>
CTI protocol:	CSTA
Remark:	Must be added to the registry manually if required. Works in combination with: • HostName2 [REG_SZ] • BindAddress2 [REG_SZ].

Defines the TCP port for the secondary IP address ([HostName2 \[REG_SZ\]](#)) via which the CTI communication between XPR server and PBX is handled.

PrivateProfile [REG_DWORD]

Default:	Depending on the applied PBX
Possible values:	<Bit mask>
CTI protocol:	TSAPI
Remark:	This value must not be modified and is only valid for the old TSAPI protocol stack (cf. UseOldTSAPIStack [REG_DWORD]).

To initiate a CTI link and for the configuration of a TSAPI interface a PBX profile can be created for each CTI link depending on the applied PBX.

Via a bitmask the following seven attributes can be configured for the connection to the PBX:

- **0x0001:** PBX_PRIVPROFILE_QUERYAUTH
- **0x0002:** PBX_PRIVPROFILE_ACSSETESR
- **0x0004:** PBX_PRIVPROFILE_QUERYCALLMON
- **0x0020:** PBX_PRIVPROFILE_ENUMSERVER
- **0x0040:** PBX_PRIVPROFILE_SNAPSHOTDELAY
- **0x0080:** PBX_PRIVPROFILE_CALLTIMER

Depending on the PBX type used, the XPR server allocates this key already with an individually adjusted value.

RepeatPhysMonitor [REG_DWORD]

Default:	0
Possible values:	0 – No repeated setting <Time> [Seconds] (more than 30 seconds)
CTI protocol:	CSTA, TSAPI
Remark:	Is in case of TSAPI only valid for the new TSAPI protocol stack (cf. UseOldTSAPIStack [REG_DWORD]).

Some PBX systems recognize monitor points after a certain time as no longer active. In this case the XPR server allows reactivating all current monitor points by resetting them in the PBX in fixed time intervals.

RepeatPhysMonitor defines an interval, after which the XPR server resets all current monitor points in the PBX. The set time must be at least 30 seconds.

SendDelayTime [REG_DWORD]

Default:	Depending on the applied PBX
Possible values:	<Time> [Milliseconds]
CTI protocol:	CSTA

Diverse PBX systems can only process a certain number of commands in a given time.

SendDelayTime defines a period the XPR server waits after a command for a connected PBX before sending the next command to the respective PBX.

ServerID [REG_SZ]

Default:	Depending on the applied PBX
Possible values:	<Server ID>
CTI protocol:	TSAPI

Defines the server ID of the XPR server for login to the PBX driver. It is composed of default expressions that may be completed with system parameters such as server name.

StdTransTimeout [REG_DWORD]

Default:	10000 [Milliseconds]
Possible values:	<Time> [Milliseconds]
CTI protocol:	TAPI

Defines a timeout during which internal transactions – mostly to the PBX – must be receipted.

Supported_Device [REG_MULTI_SZ]

Default:	<Empty string>
Possible values:	<List of device extensions>
CTI protocol:	CSTA, TSAPI, TAPI

Defines which telephone devices may be monitored by setting monitor points.

TRType [REG_DWORD]

Default:	1
Possible values:	1 - Transport via LAN (TCP/IP) 2 - Transport via V.24 3 - Transport via ISDN
CTI protocol:	CSTA

Defines which type of the physical transport layer is used for the respective CTI link.

TrunkLineEnd [REG_SZ]

Default:	<Empty string>
Possible values:	<Calling number>
CTI protocol:	CSTA

For some PBX systems it is possible to monitor trunk lines as well as telephone devices with the help of CTI functionality. The trunk lines to be monitored must exist in a coherent phone number block.

TrunkLineEnd defines the last trunk phone number of the number block that is to be monitored with the help of CTI features.

TrunkLineStart [REG_SZ]

Default:	<Empty string>
Possible values:	<Calling number>
CTI protocol:	CSTA

For some PBX systems it is possible to monitor trunk lines as well as telephone devices with the help of CTI functionality. The trunk lines to be monitored must exist in a coherent phone number block.

TrunkLineEnd defines the first trunk phone number of the number block that is to be monitored with the help of CTI features.

TryOpenUnknownLines [REG_DWORD]

Default:	Depending on the applied PBX
Possible values:	0 – PBX does not send error message 1 – PBX sends error message
CTI protocol:	TAPI

Defines whether an error message is sent by the connected PBX, if the XPR server tries to set a monitor point on a telephone device that is unknown to the PBX.

UseAcDnIs [REG_DWORD]

Default:	0
Possible values:	0 – CSTASiemensPrivateData not supported 1 – CSTASiemensPrivateData supported
CTI protocol:	CSTA

In some cases, the optiClient displays the extensions of an ACD group's agents instead of the group number. If this occurs, you can set this value to 1 to activate the CSTASiemensPrivateData feature with a HiPath 4000.

UseAcdProxy [REG_DWORD]

Default:	1
Possible values:	0 – Does not use ACD proxy 1 – Uses ACD proxy
CTI protocol:	TAPI
Remark:	For <i>Hicom 150</i> with contact center

Defines whether the ACD proxy of the PBX is to be used.

UseACSE [REG_DWORD]

Default:	0
Possible values:	0 – Do not use ACSE 1 – Use ACSE
CTI protocol:	CSTA
Remark:	For <i>HiPath 4000 V5</i> .

This switch must be set for *CAP Inside* in case of a connection to HiPath 4000 V5.

UsePbxUID [REG_DWORD]

Default:	0
Possible values:	0 – XPR server generates individual UID 1 – Uses UIDs of the PBX
CTI protocol:	CSTA
Remark:	For Hicom 150 only.

The *Unique ID* defines a logical connection ID that is identical for all subscribers taking part in a defined communication relation. The XPR server stores the unique IDs of all communication relations in a designated list - the UID Tree.

Example:

In a telephone conference with four conversation partners the XPR server stores an automatically generated unique ID for each of the subscribers in addition to the individual call ID. The unique ID is identical for all four subscribers and is administered in the UID tree.

UsePbxUID defines whether the UIDs forwarded from the PBX to the XPR server are copied by the server or newly created by it.

Wait_of_ISDN_Send_receipt [REG_DWORD]

Default:	1
Possible values:	0 – Does not wait for ISDN command receipt 1 – Waits for ISDN command receipt
CTI protocol:	CSTA

Defines whether the command receipt of the ISDN transport layer is awaited after a CAPI command has been forwarded before the next command is sent.

WatchdogTimeout [REG_DWORD]

Default:	Depending on the connected PBX
Possible values:	<Time> [Seconds]
CTI protocol:	CSTA, TSAPI
Remark:	Is in case of TSAPI only valid for the new TSAPI protocol stack (cf. UseOldTSAPIStack [REG_DWORD]).

Different PBX systems offer the XPR server the option to retrieve information about the current communication relations.

WatchdogTimeout defines the time interval during which the CTI APL retrieves this information about the current communication relations and synchronizes it with the connections known in the CTI APL. This prevents an erroneously signalled connection end from unintentionally binding system resources in the CTI APL.

WithCallCenter [REG_DWORD]

Default:	1
Possible values:	0 – No integrated contact center application exists 1 – Integrated contact center application exists
CTI protocol:	CSTA
Remark:	For <i>Hicom 150</i> with contact center

Defines whether the PBX provides an integrated contact center application via which the XPR server can request and maybe modify the agent's state.

If no integrated contact center application exists, this key must be set to **0**. Otherwise the CTI APL requests the agent states from the PBX. This leads to extensive error messages in the XPR monitor.

XmrLogMask [REG_DWORD]

Default:	0xFFFFFFFF8
Possible values:	<0xFFFFFFFFE0 ... 0xFFFFFFFF>
CTI protocol:	CSTA, TSAPI, TAPI

Defines the log message settings in the XPR monitor.

The following log messages are not activated by default and can be activated by setting their corresponding bits:

- **Bit 0:** Transport Layer (Topic 'TCP<*link name*>' or 'ISDN<*link name*>')
- **Bit 1:** Topic 'CstaL6<*link name*>' Debug 2
- **Bit 2:** Topic 'CstaL6<*link name*>' Debug 3

With the following bits complete topics can be switched on. Since the number of topics is limited, this procedure can be useful when several CTI links are used:

- **Bit 3:** Release of the topic '<*link name*>DBG'
- **Bit 4:** Release of the topic 'PBX<*link name*>DBG'

E.5.3 Registry Values for the HiPath 4000

The following general registry values of the CTI APL are found under the following key:

HKLM\SOFTWARE\Wow6432Node\PP-COM\MRS\CTIAPL\HP4000

TransferringDeviceClearTime [REG_DWORD]

Default:	500 [Milliseconds]
Possible values:	<Time> [Milliseconds]
Remark:	For Hicom 4000 only.

If an existing call is forwarded by a terminal device of a HiPath 4000 (FORWARD), the HiPath 4000 creates erroneously a new undirected connection on the terminal device after the forwarding. The user of the terminal device must then manually close this connection. For example by picking up or replacing the receiver.

TransferringDeviceClearTime defines a period in which the CTI APL immediately terminates each new call for the forwarding device after the forwarding.

E.6 Entries of the DB APL

You find the following values in the key `DbAp1`.

ADOCommandTimeout [REG_DWORD]

Default:	30
Possible values:	10 to 180 seconds

Maps the configuration option **Time-out of commands** in the registry. See [Section 26.3.2, “MS ODBC Time-Out”, on page 1238](#).

ADOConnectionTimeout [REG_DWORD]

Default:	15
Possible values:	5 to 60 seconds

Maps the configuration option **Time-out of connection** in the registry. See [Section 26.3.2, “MS ODBC Time-Out”, on page 1238](#).

GarbageConnectionTimeout [REG_DWORD]

Default:	30
Possible values:	30 to 180 seconds

Maps the configuration option **Time-out of connection** in the registry. See [Section 26.3.1, “DB APL Time-Out”, on page 1237](#).

MaxConnectionCount [REG_DWORD]

Default:	200
Possible values:	0 to 9000

Maps the configuration option **Max. no. of connections** in the registry. See [Section 26.3.3, “Miscellaneous”, on page 1238](#).

MaxThreadPoolCount [REG_DWORD]

Default:	50
Possible values:	10 to 1000

Maps the configuration option **Max. no. of threads** in the registry. See [Section 26.3.3, “Miscellaneous”, on page 1238](#).

RDBASyncRequestTimeout [REG_DWORD]

Default:	5
Possible values:	1 to 30 seconds

Maps the configuration option **Time-out of sync. requests** in the registry. See [Section 26.3.1, “DB APL Time-Out”, on page 1237](#).

ThreadPoolTimeOut [REG_DWORD]

Default:	20
Possible values:	10 to 60 seconds

Maps the configuration option [Time-out of threads](#) in the registry. See [Section 26.3.1, “DB APL Time-Out”, on page 1237](#).

E.7 Entries of the FI APL

The following values can be found in the key `FiApl`.

MaxAddressCount [REG_DWORD]

Default:	16
Possible values:	<Number>

Maximum number of destination addresses in a header. If you enter more destination addresses, you will receive a warning in the log file and the message will not be delivered to the redundant addresses.

ResPath [REG_SZ]

Default:	<XPR Install>\Res\FiApl
Possible values:	Share or Directory

Path to the script resources. Especially in cluster systems it is reasonable to set this path on a released directory since otherwise the script needs always to be updated on both systems.

Protocols [REG_MULTI_SZ]

Default:	–

List of the active protocols. For every protocol there is an individual registry key under the key `FIAPL` containing the protocol name. The number of protocols is restricted to 32.

E.7.1 Protocol Specific Settings

Each protocol listed under [Protocols \[REG_MULTI_SZ\]](#) has its own individual registry key in the `FiApl` key. In each of these keys the following values are found.

BodyDelay [REG_DWORD]

Default:	–
Possible values:	<i>Seconds</i>

Break between reading/writing of the header and the corresponding body file in seconds. This is to ease race conditions in certain Novell network environments.

CheckPrivileges [REG_DWORD]

Represents the configuration option **Check Privileges** in the registry. See [Section 28.2.1, “Host -> FI APL”, on page 1423](#).

EnableIncoming [REG_SZ]

Represents the configuration option **Enable Incoming messages** in the registry. See [Section 28.2.2, “File Interface APL to the Host”, on page 1425](#).

EnableReports [REG_SZ]

Represents the configuration option **Reports > Filter** in the registry. See [Section 28.2.2, “File Interface APL to the Host”, on page 1425](#).

HdrInDir [REG_SZ]

Represents the configuration option **Header directory** in the registry. See [Section 28.2.2, “File Interface APL to the Host”, on page 1425](#).

HdrOutDir [REG_SZ]

Represents the configuration option **Poll directory** in the registry. See [Section 28.2.1, “Host -> FI APL”, on page 1423](#).

HdrPattern [REG_SZ]

Represents the configuration option **Header pattern** in the registry. See [Section 28.2.1, “Host -> FI APL”, on page 1423](#).

IncFaxFormat [REG_SZ]

Represents the configuration option **Fax format** in the registry. See [Section 28.2.2, “File Interface APL to the Host”, on page 1425](#).

IncFileSuffix [REG_SZ]

Represents the configuration option **Incoming messages > Suffix** in the registry. See [Section 28.2.2, “File Interface APL to the Host”, on page 1425](#).

MaxPerPoll [REG_DWORD]

Represents the configuration option **Maximum per poll** in the registry. See [Section 28.2.1, “Host -> FI APL”, on page 1423](#).

PollRate [REG_DWORD]

Represents the configuration option **Poll rate** in the registry. See [Section 28.2.1, “Host -> FI APL”, on page 1423](#).

PrivData [REG_SZ]

Represents the configuration option **PrivData field size** in the registry. See [Section 28.2.1, “Host -> FI APL”, on page 1423](#).

RemoveHeader [REG_SZ]

Represents the configuration option **Delete Header** in the registry. See [Section 28.2.1, “Host -> FI APL”, on page 1423](#).

RepFileSuffix [REG_SZ]

Represents the configuration option **Reports > Suffix** in the registry. See [Section 28.2.2, “File Interface APL to the Host”, on page 1425](#).

SendFormats [REG_SZ]

Default:	–
Possible values:	<XPR Format> [; <XPR Format>]

This list displays the valid document and data formats for the logical line logged in by this protocol. These formats are described in [Appendix A, “Document Formats”](#) of this manual. If a document is forwarded to this protocol by the MTA then, as the case may be, a conversion into one of the formats indicated here is performed. The PMF format should additionally be entered with documents carrying attachments. All format entries occur in upper case letters and separated with a semicolon.

Example: TG3 ; PMF

TxtInDir [REG_SZ]

Maps the **Body directory** configuration option in the registry. See [Section 28.2.2, “File Interface APL to the Host”, on page 1425](#).

TxtOutDir [REG_SZ]

Maps the **Body directory** configuration option in the registry. See [Section 28.2.1, “Host -> FI APL”, on page 1423](#).

E.8 HPM APL Entries

The following values can be found in the key `HpmApl`.

AttributeMapping [REG_SZ]

Maps the configuration options of the **Binding of Attributes** tab in the registry. See [Section 20.3.2, “Binding of Attributes”, on page 1173](#).

EmailForOff365 [DWORD]

Default:	0
Possible values:	0 – email attribute will not be used for OFF365 1 – email attribute will be used for OFF365

When set to 1 `HpmApl` will use the 'email' attribute also to set the 'OFF365' field to configure the mapping of the user's email address to the OFF365 field via `HpmApl`.

GivenNameMandatoryBug [REG_DWORD]

Default:	1
Possible values:	0 – Option disabled. 1 – Do not integrate givenname attribute in table.

This value serves for fixing an attribute assignment error. The **givenname** (first name) attribute in the element manager cannot be replaced with a matching attribute in the XPR system since no attribute exists for a user's first name. This option prevents the integration of the attribute in the assignment table. Therefore, the value of this entry should always be 1.

PropertiesUrl [REG_SZ]

Maps the configuration options of the **URL to User Attributes** tab in the registry. See [Section 20.3.3, “URL to User Attributes”, on page 1174](#).

ResourceField [REG_SZ]

Default:	HPMRES
Possible values:	Valid, unique name

Describes the name of the correlation database field in which the mailbox names (user resources) are stored.

TcpIpPort [REG_DWORD]

Default:	4444
Possible values:	<IP Port>

Maps the configuration options of the **Element Manager** tab in the registry. See [Section 20.3.1, “Element Manager”, on page 1172](#).

UseHttps [REG_DWORD]

Default:	1
Possible values:	0 – Unencrypted communication. 1 – Encrypted communication.

This entry controls secure communication between the HiPath User Management and the XPR server.

UserNotifications [REG_SZ]

Default:	0
Possible values:	0 – Do not send XPR modifications. 1 – Send XPR modifications. (Not supported)

This entry determines whether a notification is sent to the HPM UM system in case of user data modifications in the XPR system.

ValidateExpr [REG_SZ]

Possible values:	<Regular expression>

Based on this regular expression, the syntax of the entries in value [AttributeMapping \[REG_SZ\]](#) is checked. This is to exclude errors in case of someone manually modifying this value in the registry.

E.8.1 Replication

The AddressUpdated value in key `HpmApl\Replication` is an internal value in which the HPM APL registers the already transmitted data records modifications by means of an ID. Consequently, not all data are transmitted each time but only the current modifications.

E.9 LDAP APL Entries

The following values can be found in the key `LdapApl`.

DiscardGarbageBlobs [REG_DWORD]

Default:	0
Possible values:	0 or 1

The Active Directory (AD) may contain corrupt binary objects, which cannot be read via the API. Normally, such objects are ignored and simply not read. If problems still arise though, you can set this value to 1. The LDAP APL then deletes corrupt binary objects it has found in the AD.

MRS-NonDeleteAtts [REG_MULTI_SZ]

Default:	PASSWORD, GROUP, PIN
Possible values:	Attributes

Specifies the user attributes in the XPR system that must not be deleted. Exception: a user is deleted completely.

MRS-NonSyncAtts [REG_MULTI_SZ]

Default:	–
Possible values:	Attributes

Specifies the user attributes in the XPR system that must not be overridden. Consequently, such attributes override the corresponding value of the XPR system only if they do not exist there yet. Please note that a modification to these attributes in the directory service at a later date after the initial replication does not lead to a modification of these attributes in the XPR database any more.

ResPath [REG_SZ]

Default:	–
Possible values:	Path

Path to the `res\ldap` directory. Especially on cluster systems you will want to maintain adapted scripts in only one place. Here you can adapt the corresponding path for such systems.

E.9.1 Server Section

The following values can be found in the key `LdapApl\Server\<server name>`:

AttributeMap [REG_MULTI_SZ]

Defines the attributes with their IDs in the LDAP and XPR system and the corresponding interrelationships. The specifications correspond to the entries on the **Attributes** configuration tab.

BindDomain [REG_SZ]

Default:	–
Possible values:	Valid domain name

Defines the domain name. This involves the settings that you perform under **Domain** on the **Login** configuration tab.

BINDMethod [REG_SZ]

Default:	NTLM
Possible values:	NTLM, SIMPLE, Negotiate

Defines the method set for connecting the server. This involves the settings that you perform under **Authentication type** on the **Login** configuration tab.

BindPassWort [REG_SZ]

Default:	–
Possible values:	Valid password

Defines the user password in encoded format. This involves the settings that you perform under **Password** on the **Login** configuration tab.

BindUserName [REG_SZ]

Default:	–
Possible values:	Valid user name

Defines the user name. This involves the settings that you perform under **User name** on the **Login** configuration tab.

CreateDsEntries [REG_DWORD]

Default:	0
Possible values:	0 or 1

Specifies whether or not new users can be defined in the directory server. A 0 does not allow this whereas it is possible with a 1. This does **not** involve the settings that you can perform on the **Global Settings** configuration tab. New users should be directly defined in the directory server.

CreateMrsEntries [REG_DWORD]

Default:	0
Possible values:	0 or 1

Defines whether new users can be generated in the XPR system. A 1 confirms this whereas a 0 prevents user generation. This involves the settings that you can perform on the **Global Settings** configuration tab.

DefaultMRSValues [REG_MULTI_SZ]

Example:	PIN:1234321 GROUP:USER
Possible values:	<Attribute>: <Value>

Here you can set default values for database fields. If such fields do not exist yet for a newly replicated user, they are generated with these values. This value does not affect users already replicated.

DeleteDsEntries [REG_DWORD]

Default:	0
Possible values:	0 or 1

Specifies whether or not users can be deleted in the directory server. A 0 does not allow this whereas it is possible with a 1. This setting **cannot** be controlled via a configuration tab. You should administer users directly in the directory server. For this reason we recommend to keep the default setting 0.

DeleteMrsEntries [REG_DWORD]

Default:	0
Possible values:	0 or 1

Defines whether users can be deleted in the XPR system. A 1 confirms this whereas a 0 prevents user deletion. This involves the settings that you can perform on the **Global Settings** configuration tab.

DS-Attributes [REG_BINARY]

Specifies the attributes available in the directory server. You can have them listed in the XPR monitor via the **Query DS Attributes** button of the **Login** configuration tab. We expressly do not recommend attribute modifications since this may lead to a faulty directory structure.

DS-AttributesSize [REG_SZ]

Depends on DS-attributes and specifies the memory that attributes require in the directory server at this point in time.

DS-Type [REG_SZ]

Default:	–
Possible values:	Active Directory, DirX, <Unknown>

Specifies the directory service with which LDAP operates. This involves the settings that you can perform on the **Login** configuration tab.

Enable [REG_DWORD]

Default:	1
Possible values:	0 or 1

Defines whether an LDAP server is enabled. A 1 enables an LDAP server whereas a 0 deactivates it.

E-ScriptName [REG_SZ]

Default:	–
Possible values:	<none>, adrepl, ExRepl, tsys, <your own E Script>

Defines the E-script used. This involves the settings that you can perform on the **Global Settings** configuration tab.

HostName [REG_SZ]

Default:	–
Possible values:	Valid server name

Defines the name of the host via which the LDAP communication is handled. This involves the settings that you perform under **Server IP address** on the **Login** configuration tab.

PollIntervall [REG_DWORD]

Default:	0
Possible values:	0 to 9999999999 sec.

Defines the poll interval length. This involves the settings that you perform under **Polling interval** on the **Search** configuration tab.

PollSchedule [REG_MULTI_SZ]

Default:	–
Possible values:	<Day> = <Time>

Defines the schedule settings. This involves the settings that you perform under **Schedule** on the **Search** configuration tab.

PortNumber [REG_DWORD]

Default:	389
Possible values:	389 or 636

Defines the port via which the LDAP communication is handled. Port 389 describes the default connection without encryption, while Port 636 is intended for the SSL encryption. This involves the settings that you perform under **Port number** on the **Login** tab. See also [UseSSL \[REG_DWORD\]](#).

SaveDsUSN [REG_DWORD]

Default:	0
Possible values:	0 or 1

Defines whether a UNS is generated in the directory server upon modifying the attributes. A 1 allows this and a 0 prevents UNS generation. This involves the settings that you perform under **Save UNS** on the **Global Settings** configuration tab.

SaveMrsUpdateId [REG_DWORD]

Default:	0
Possible values:	0 or 1

Defines whether an update ID is generated in the XPR upon modifying the attributes. A 1 allows this and a 0 prevents ID generation. This involves the settings that you perform under **Save Update-ID** on the **Global Settings** configuration tab.

SearchFolders [REG_MULTI_SZ]

Default:	DC=<domain name>, DC=local(homeMDB=*)
Possible values:	Distinguished names entries for searching

Specifies the search settings defined on the **Search** configuration tab.

SearchPageSize [REG_DWORD]

Default:	0
Possible values:	0 to 9999999999

Defines the entries per page. This involves the settings that you perform under **Entries per page** on the **Search** configuration tab.

SearchTimeout [REG_DWORD]

Default:	120
Possible values:	Seconds

Defines the maximum search duration. This involves the settings that you perform under **Max. search duration** on the **Search** configuration tab.

UseSSL [REG_DWORD]

Default:	0
Possible values:	0 or 1

With 1 the connection to the directory server is encoded by SSL. As soon as SSL is activated via this value, the LDAP APL automatically resets the port used to 636.

WriteToDs [REG_DWORD]

Default:	0
Possible values:	0 or 1

Defines whether modifications are integrated in the directory server file. A 1 confirms this, a 0 does not allow modification saving. This involves the settings that you perform under **Write changes to DS** on the **Gobal Settings** configuration tab.

WriteToMrs [REG_DWORD]

Default:	0
Possible values:	0 or 1

Defines whether modifications are integrated in the XPR directory. A 1 confirms this, a 0 does not allow modification saving. This involves the settings that you perform under **Write changes to MRS** on the **Global Settings** configuration tab.

E.10 Entries of the LEAR APL

The following values can be found in the key `Lear`.

Block [REG_DWORD]

Default:	1
Possible values:	{1, 2, ..., 1000000}

Specifies the value for the **Block** field on the **Test** tab.

Count [REG_DWORD]

Default:	1
Possible values:	{1, 2, ..., 1000000}

Specifies the value for the **Count** field on the **Test** tab.

Filename [REG_SZ]

If you select an individual file on your server in the **Datafile** field of the **Test** tab, the name of this file is stored here.

Freq [REG_DWORD]

Default:	–
Possible values:	{1, 2, ..., 1000000}

Specifies the value for the **Period** field on the **Test** tab.

Originator [REG_SZ]

Default:	NVS:LEAR/TESTER
Possible values:	NVS:<Service>/<Address>

Specifies the originator address of the messages. Is defined in the **Originator** field of the **Test** tab.

PMF-Properties [REG_MULTI_SZ]

Default:	–
Possible values:	<Name>;<Value>

Determines the additional PMF properties of a selected file. The entries for these values are made in the **Extra Properties** dialog and listed here.

Recipient [REG_SZ]

Default:	NVS:<Servername>/POSTMASTER
Possible values:	NVS:<Server name>/<Address>

Specifies the recipient address of the messages. Is defined in the **Recipient** field of the **Test** tab.

SetPmfProps [REG_DWORD]

Default:	0
Possible values:	{0, 1}

Determines whether further PMF properties are added to a selected file. This entry is made by ticking off the **Set extra PMF-Properties** field on the **Test** tab. In case of 1 the tick is set, with 0 it is not.

StatMsgRec [REG_DWORD]

Represents the value for **Docs sent**, thus for sent messages, on the **Statistics** tab.

StatMsgSend [REG_DWORD]

Represents the value for **Docs rcv**, thus for received messages, on the **Statistics** tab.

StatRepFail [REG_DWORD]

Represents the value for **Rep fail**, thus for messages not received, on the **Statistics** tab.

StatRepOk [REG_DWORD]

Represents the value for **Rep ok**, thus for successfully received messages, on the **Statistics** tab.

StatRepRec [REG_DWORD]

Represents the value for **Rep rcv**, thus for received messages, on the **Statistics** tab.

StatRepSend [REG_DWORD]

Represents the value for **Rep sent**, thus for sent messages, on the **Statistics** tab.

TransBlock [REG_DWORD]

Default:	1
Possible values:	{1, 2, ..., 1000000}

Specifies the value for the **Block** field on the **Transactions** tab. Indicates the number of transactions.

TransCmd [REG_SZ]

Default:	PHONECALL CALLER=123 CALLEE=456
Possible values:	<Transaction>

Specifies the value for the **Command** field on the **Transactions** tab.

TransCount [REG_DWORD]

Default:	1
Possible values:	{1, 2, ..., 1000000}

Specifies the value for the **Count** field on the **Transactions** tab. Indicates the number of transaction repetitions within a specific period.

TransPeriod [REG_DWORD]

Default:	0
Possible values:	{0, 1, 2, ..., 1000000}

Specifies the value for the **Period** field on the **Transactions** tab. Indicates the length of the period for executing the transactions. In case of value 0, **Count** is executed once.

TransRec [REG_SZ]

Default:	NVS:CTI
Possible values:	NVS:<Service>

Specifies the transactions target address. Is determined in the **Address** field of the **Transactions** tab.

Type [REG_DWORD]

Default:	1
Possible values:	{1,2,3,4,5,6,7,8}

Indicates the type of the selected file for the message. The following options are available:

1. Sonnet (15 lines of text)
2. Odyssey (complete volume, 620kb text)
3. Short message (one line of text)
4. File (on server)
5. Hello! (33kB PCM Voice)
6. No file
7. Empty PMF
8. Fax 2pg 620kb

E.11 Entries of the LPR APL

The following values are found in the key `LprApl`.

ApiVersion [REG_SZ]

LPR APL version number

BindAddress [REG_SZ]

Default:	–
Possible values:	<IP address>

IP address the LPR APL binds to in case of a multi-homed-system.

MaxPrintChannels [REG_DWORD]

Default:	100
Possible values:	<Maximum number of channels>

Maximum number of printers that can be addressed simultaneously. The printers are administered dynamically, so that no channel is opened for a printer until a print job for this printer exists. As soon as all jobs from a printer's queue have been processed, the channel with the queue for this printer is closed again.

MaxQueueSize [REG_DWORD]

Default:	20
Possible values:	<Maximum queue size>

As soon as a print job exists for a printer and, consequently, a channel has been opened, a new queue is established for the jobs to this printer that will follow.

PrinterType [REG_SZ]

Default:	lp

Name of the printer type for the LPR protocol. This is a normal element of the LPR protocol.

SleepTimeAfterPrint [REG_DWORD]

Default:	0
Possible values:	<Milliseconds>

Waiting time until the next print job is sent. Some printers work very slowly and in this case the delay caused by this parameter may be helpful.

TCP-Log [REG_DWORD]

Default:	0
Possible values:	0 – No special debug output. 1 – Special debug output.

When the special debug output is active, all sent data are put out in debug level 2 and all received data are put out in debug level 3.

Repeats_1 [REG_DWORD]

Default:	3
Possible values:	<Number>

Defines a repeat strategy for dialing

By the values [Repeats_1 \[REG_DWORD\]](#) and [RepeatTime_1 \[REG_DWORD\]](#) a parameter of the format <number>–<interval> is specified. This specification defines how often and in which interval the attempt is made to deliver messages. The <number> parameter describes the number of delivery attempts to be performed and the associated <interval> parameter indicates the seconds between the single delivery attempts previously defined.

Up to five different dial intervals are run through.

[Repeats_1 \[REG_DWORD\]](#) defines the <number> of the first repeat interval.

RepeatTime_1 [REG_DWORD]

Default:	30
Possible values:	<Seconds>

See [Repeats_1 \[REG_DWORD\]](#). This parameter defines the <interval> of the first repeat interval in seconds.

Repeats_2 [REG_DWORD]

Default:	3
Possible values:	<Number>

See [Repeats_1 \[REG_DWORD\]](#). This parameter defines the <number> of the second repeat interval.

RepeatTime_2 [REG_DWORD]

Default:	30
Possible values:	<Seconds>

See [Repeats_1 \[REG_DWORD\]](#). This parameter defines the <interval> of the second repeat interval in seconds.

Repeats_3 [REG_DWORD]

Default:	3
Possible values:	<Number>

See [Repeats_1 \[REG_DWORD\]](#). This parameter defines the <number> of the third repeat interval.

RepeatTime_3 [REG_DWORD]

Default:	30
Possible values:	<Seconds>

See [Repeats_1 \[REG_DWORD\]](#). This parameter defines the <interval> of the third repeat interval in seconds.

Repeats_4 [REG_DWORD]

Default:	3
Possible values:	<Number>

See [Repeats_1 \[REG_DWORD\]](#). This parameter defines the <number> of the fourth repeat interval.

RepeatTime_4 [REG_DWORD]

Default:	30
Possible values:	<Seconds>

See [Repeats_1 \[REG_DWORD\]](#). This parameter defines the <interval> of the fourth repeat interval in seconds.

Repeats_5 [REG_DWORD]

Default:	3
Possible values:	<Number>

See [Repeats_1 \[REG_DWORD\]](#). This parameter defines the <number> of the fifth repeat interval.

RepeatTime_5 [REG_DWORD]

Default:	30
Possible values:	<Seconds>

See [Repeats_1 \[REG_DWORD\]](#). This parameter defines the <interval> of the fifth repeat interval in seconds.

E.12 Entries of the Mail APL

The following values can be found in the key `MailApl`.

AllowRecursiveAwake [REG_DWORD]

Default:	0
Possible values:	0 – Do not use awake rules recursively 1 – Use awake rules recursively

Apply awake rules repeatedly or not

AutoAwake [REG_DWORD]

Default:	–
Possible values:	0 or 1

If the Mail APL is to perform time monitoring of the journal entries on the basis of the awake rules, this value is automatically set to 1.

CitJournal [REG_DWORD]

Obsolete.

CtiJournal [REG_DWORD]

Default:	–
Possible values:	0 or 1

Activate Server CTI Journal (1). This occurs automatically when the first activation request arrives, which is one reason why you should not activate the [DocumentationMode \[REG_DWORD\]](#) with a real server. This value would then be written with default 0 and not automatically internally changed to value 1 any more in case of a retrospective CTI provider installation.

CtiJournalAllCalls [REG_DWORD]

Default:	0
Possible values:	0 or 1

Calls are normally only logged in the CTI journal when the caller transmits a calling number. If you set this switch to 1, also those calls are included in the journal that were not accompanied with a calling number.

This switch only works if [NewCtiJournal \[REG_DWORD\]](#) is set to 1.

CtiJrnLoadDelay [REG_DWORD]

Default:	300
Possible values:	Milliseconds

Delays setting of monitor points with the Mail APL start. In case of a large number of users, especially the PBX and the SMI queues of the MTA may otherwise get overloaded as the PBX does not accept the requests fast enough.

CtiLogBlackList [REG_MULTI_SZ]

Default:	–
Possible values:	<Number>

Via this value an exclusion list can be defined so that for the numbers specified there no CTI journal entries are logged. An example would be the numbers of the individual voicemail server.

One number is entered in each line. Numbers can contain question marks as dummy characters representing arbitrary digits. 2?? would be a valid entry for all numbers beginning with 2 and consisting of a maximum of three digits.

CtiLogUnknown [REG_DWORD]

Default:	0
Possible values:	0 or 1

In case of an activated CTI journal, entries that do not deliver calling numbers can be logged as well (1).

This switch only works if [NewCtiJournal \[REG_DWORD\]](#) is set to 0.

DatabasePollRate [REG_DWORD]

Default:	60
Possible values:	Seconds

Polling rate in which the database is processed by the awake rules. The poll rate must always be less than the minimum value entered as the age condition. If an age condition is specified for an age of 10 seconds, the poll rate must be set to 1 second. If age is in days, then a polling rate of 3600 seconds is sufficient.

DbBackend [REG_DWORD]

Default:	1

Required for the MSP configuration module. Must not be modified.

DefaultAwakeAge [REG_DWORD]

Default:	5
Possible values:	1..90 days

If an awake rule uses the macro \$ (AGE) then this value will be used.

DistribDefaultsSets [REG_DWORD]

Default:	–
Possible values:	0 or 1

Automatically set to 1 by the Mail APL after the Default Distrib Setup has been installed.

DistribLinePathlist [REG_MULTI_SZ]

Default:	NVS:DIS,/userdata,LOGICAL NVS:SFOD,/userdata/sfod/FaxFiles,LOGICAL NVS:STOD,/userdata/sfod/FaxFiles,LOGICAL
Possible values:	<NVS Address>, <Path>, [LOGICAL PHYSICAL]

Paths are specified for every address defined under [DistribLineProtocols \[REG_MULTI_SZ\]](#). The directory can either be a logical directory under the share \\<XPR Install>\MrsUserData\$ or a physical directory on the XPR server. When specifying a logical directory, a / is used as separator for the path, and a \ in case of physical directories.

Example:

```
NVS:FOD,/userdata/fod,LOGICAL
NVS:XXX,e:\temp,PHYSICAL
```

If a document was sent to NVS:XXX/old\a.b the file a.b would be stored in the directory e:\temp\old\.

DistribLineProtocols [REG_MULTI_SZ]

Default:	NVS:DIS;SF,OUT;2048000;0;* NVS:SFOD;SF,OUT;2048000;0;FG3 NVS:STOD;SF,OUT;2048000;0;TG3
Possible values:	<Line-Address>;<Attributes>;<Speed>;<Preference>;<Formats>

A protocol is defined for every line.

- <Line-Address>

NVS:<Node>, with <Node> being an arbitrary protocol name that has not been used otherwise yet.

- <Attribute>

Should be set to SF, OUT. Through this attribute the line is defined for outgoing traffic and store-and-forward services.

- <Speed>

Transmission rate of the line. Since files are only transferred within a local network, a transmission rate of 2048000 can be entered.

- <Preference>

Through the use of this parameter preferences can be assigned to logical lines used by the router. The larger the value of the line <<Preference>>, the higher its rate of usage by the router (-100< <<Preference>> < 100).

- <Format>

This comma-separated list specifies the document and data formats valid for this logical line. These formats are described in [Appendix A, "Document Formats"](#) of this manual. If wildcards (*) are used, the file remains unchanged and copied to its destination.

DoAddressBookConsistencyCheck [REG_DWORD]

Default:	1
Possible values:	0 or 1

Activate (1) or deactivate (0) address book consistency checks.

EnterDeflectCallinCtiJournal [REG_DWORD]

Default:	0
Possible values:	0 or 1

With a call arriving at device A but being routed to device B via DEFLECT or PICKUP, the CTI journal of device A used to feature "not reached" as entry for the call. This was confusing since the call did reach a partner.

This behavior has been changed, so that by default no entry is made in the CTI journal for these calls. This, however, requires the following:

- The connection to the PBX must occur via Raw CSTA of the CTI APL.
- With “ConnectionCleared“ the PBX must state the reason for clearing a connection in the “CAUSE“ field.
- The extended CTI logging [NewCtiJournal \[REG_DWORD\]](#) is active.

Setting this value to 1 activates the former logging again.

KeepFirstCallee [REG_DWORD]

Default:	0
Possible values:	0 or 1

It is usually the number of the actually reached device that is logged in the CTI journal. If a phone number suppression is active on this device, no number is displayed. When you set this switch to 1, the originally called number is always logged in the CTI journal.

MaxAwake [REG_DWORD]

Default:	16
Possible values:	0..256

Maximum number of awake rules. Memory is reserved for the number of awake rules entered here.

NewCtiJournal [REG_DWORD]

Default:	1
Possible values:	0 or 1

The old CTI journal could simultaneously administer only one call for each terminal device. Therefore, not all connections were entered in the CTI journal during a call. Consequently, there was no indication of e.g. a consultation being performed during a call or of a subscriber taking part in a conference.

Therefore, an extended CTI logging has been introduced. Here all calls of a terminal device are entered as separate calls in the CTI journal. In other words, if a consultation is executed during a call, two calls are entered in the CTI journal. The former CTI journal structure did not provide the option to enter further information such as “consultation” or “conference”. Setting this switch to 0 activates the former type of CTI logging.

PhoneField [REG_SZ]

Default:	PHONE
Possible values:	PHONE or PHONE#

In old versions the device number was gathered from the variable `PHONE#` of the correlation database for the CTI journal. Since characters (+ - / ()) other than numbers can be entered here as separators, problems occurred. Because of this, the device number is read in from the `PHONE` variable. This variable contains the normalized number.

This function is only active with the extended CTI logging (see [NewCtiJournal \[REG_DWORD\]](#)). If you enter `PHONE#` here again, the Mail APL shows the former behavior with respect to the database field used.

RefreshCtiMonitor [REG_DWORD]

Default:	600
Possible values:	300 to 86400 Seconds

All seconds specified here are newly set as CTI monitor points at the CTI provider (CTI APL). In this way the server CTI journal is regularly restarted if e.g. the CTI provider does no longer know the monitor points set here because of a hard stop/start (crash). When a CTI provider stops/starts in a normal manner, the monitor points should not get lost.

ResetCITonRead [REG_DWORD]

Default:	0
Possible values:	0 or 1

Via this switch you can have the address `NVS:MAILBOX` logged in with the `RCIT` flag (1). Thereby the Message Waiting Indication (MWI) is also reset when a user has entered `MAILBOX` in the `PREFERRED` field, but reads the message e.g. under Exchange (inbox replication with Integrated Messaging), via Ergo over the TUM interface of the Mail APL or with the Web APL.

SupportEC [REG_DWORD]

Default:	0
Possible values:	0 or 1

Activate (1) or deactivate (0) support for printer embedded codes in the Mail APL.

TumBackend [REG_DWORD]

Default:	1
Possible values:	0 or 1

Determines whether (1) or not (0) the Mail APL as True Unified Messaging (TUM) Backend provides the corresponding functionality. If this entry is not present or set to 1, the TUM functionality is provided. If the value is set to 0, the TUM functionality is not available, neither dynamically upon request.

TumQueueSize [REG_DWORD]

Default:	128

Size of the transaction queue for TUM transactions.

TumSingleSession [REG_DWORD]

Default:	1
Possible values:	0 – Option disabled. 1 – Option enabled.

Represents the option **Restrict the number of TUM sessions that are active at the same time to one session per user** from the configuration. See [Section 11.6, “True Unified Messaging \(TUM\)”, on page 888](#).

TumWorkerThreads [REG_DWORD]

Default:	2
Possible values:	1...8

Number of available workerthreads. An incoming TUM transaction is assigned to a (vacant) workerthread that processes the transaction then. The more threads are simultaneously available, the more requests can be processed in parallel. The number of workerthreads has nothing to do with the number of simultaneous sessions.

UseAlcatelTwinDevice [REG_DWORD]

Default:	0
Possible values:	0 – No special entry handling. 1 – Summarize Alcatel Twin Device entries.

The Alcatel Twin Device consists of a normal and a mobile phone. A call is always signaled on both phones and can be answered at will. The PBX delivers for each of the phones the corresponding entries. A call answered on one device will be reported as not accepted on the other device. In the server CTI journal such information can be combined to a single entry, so that only one entry per call is available in the journal. This value must be set to 1 for this purpose.

UseRecipientForNdr [REG_DWORD]

Default:	0
Possible values:	0 – NDR sender is postmaster. 1 – NDR sender is original recipient.

If this switch is set, in cases of undelivered documents not the postmaster account is used as the sender of the non-delivery report (NDR) but the original recipient. This only applies, if the sender has activated delivery notifications for the document.

VanityNumber [REG_SZ]

Default:	NAME
Possible values:	NAME or VM_HI_DSP_NAM or <DISABLED>

Source field for vanity number generation. See [Section 11.11, “Vanity Number Support”, on page 895](#).

E.12.1 Printer Embedded Codes

These settings default the key values that can be entered in documents for the embedded codes. All settings can be conveniently performed via the XPR monitor. See [Section 11.5, “Printer Embedded Codes”, on page 884](#). Please note that the settings made here only apply for the user-defined style (see [Style \[REG_DWORD\]](#)).

The following values can be found in the key MailApl\PEC.

BeginTag [REG_SZ]

Default:	<
Possible values:	<Char>

Initiates a PEC sequence.

DateFormat [REG_DWORD]

Default:	0
Possible values:	0 - YYYY MM DD 1 - DD MM YYYY 2 - MM DD YYYY

There are currently three defaulted formats for selection with the token specified in [DateSeparator \[REG_SZ\]](#) to be placed in between for separation in each case.

DateSeparator [REG_SZ]

Default:	.
Possible values:	<Char>

Token which separates the single date components. In case of a dot thus e.g. 18.4.2002 for 18 April 2002.

EndTag [REG_SZ]

Default:	>
Possible values:	<Char>

Terminates a PEC sequence.

Fax [REG_SZ]

Default:	Fax
Possible values:	<String>

Keyword to set a recipient's fax number.

FaxStationery [REG_SZ]

Default:	FaxStationery
Possible values:	<String>

Keyword for setting the fax stationery for this document.

FromName [REG_SZ]

Default:	From
Possible values:	<String>

Keyword to specify the originator's name.

FromUid [REG_SZ]

Default:	Uid
Possible values:	<String>

Keyword to specify the XPR originator's ID.

PreserveDocument [REG_DWORD]

Default:	0
Possible values:	0 - Remove PEC from the created PS file 1 - Leave PEC in the created PS file unchanged

The Printer Embedded Codes are usually removed from the created PostScript file. In case of binary sequences in the PostScript file as they occur e.g. in images, the binary sequence may be erroneously recognized as PEC sequence. Because white characters on a white background are often used

for PEC sequences, you can leave the PEC sequences under this condition in the PostScript file without changing the print result. Consequently, set this value to 1.

PrioHigh [REG_SZ]

Default:	High
Possible values:	<String>

Keyword to set a high send priority.

PrioKey [REG_SZ]

Default:	Prior
Possible values:	<String>

Keyword to specify the priority.

PrioLow [REG_SZ]

Default:	Low
Possible values:	<String>

Keyword to set a low send priority.

PrioNormal [REG_SZ]

Default:	Normal
Possible values:	<String>

Keyword to set the normal send priority.

PrioUrgent [REG_SZ]

Default:	Urgent
Possible values:	<String>

Keyword to set the highest send priority.

SendDate [REG_SZ]

Default:	SendDate
Possible values:	<String>

Keyword to set the send date.

SendTime [REG_SZ]

Default:	SendTime
Possible values:	<String>

Keyword to specify the send time.

SepTag [REG_SZ]

Default:	=
Possible values:	<Char>

This token separates the keyword from the assigned value in a PEC sequence.

Sms [REG_SZ]

Default:	SMS
Possible values:	<String>

Keyword for a recipient's SMS number.

Smtp [REG_SZ]

Default:	smtp
Possible values:	<String>

Keyword for a recipient's Internet e-mail address.

Style [REG_DWORD]

Default:	–

This value represents the keyword setting in the configuration. If set to **User-defined**, the additional PEC values are activated.

Subject [REG_SZ]

Default:	Subject
Possible values:	<String>

Keyword for the message subject.

ToName [REG_SZ]

Default:	To
Possible values:	<String>

Keyword for a recipient.

E.13 Notification APL Entries

The following values can be found in the key `NOTAPL`.

InitialProcMode [REG_DWORD]

Maps the configuration option **Initial processor mode** in the registry.

This key describes the startup behaviour of the NotApl-processor. On systems with large user numbers the initialization of the MWI leds may consume vast resources. If set to 2, the initial MWI requests sent by the backends are ignored in order to avoid these high load scenarios. If set to 4, only Webum messages will be processed. If set to 1, only MWI requests are handled on startup, value 7 lets the processor handle any request of the backend.

The complete list of possible values is:

- 0 - None
- 1 - only MWI
- 2 - only Notification
- 3 - MWI and Notification
- 4 - only Web Message Access
- 5 - MWI and Web Message Access
- 6 - Notification and Web Message Access
- 7 - All

MaxBackendConnections [REG_DWORD]

Maps the configuration option **Max. number of back-end connections** in the registry.

MaxScheduleTimeout [REG_DWORD]

Maps the configuration option **Processor update** in the registry.

MemoryMapCPURelease [REG_DWORD]

Default:	0
Possible values:	0 – Switched off; maximum CPU utilization. 1 – Minimum CPU load up to 10 – Stepwise increase of the CPU utilization.

If a customer reports the problem that the Notification APL uses the computer to full capacity so that other processes do not receive sufficient computing time, you can decrease the load with values between 1 and 10 here. Since the customer environment plays an important role in this context, you can only find out the ideal value by trying.

MinimumJobDistance [REG_DWORD]

Maps the configuration option **Minimum job distance** in the registry.

MWIForEmail [REG_DWORD]

Maps the configuration option [Signal MWI for E-mail](#) in the registry.

MWIForFax [REG_DWORD]

Maps the configuration option [Signal MWI for Fax](#) in the registry.

MWIForVoice [REG_DWORD]

Maps the configuration option [Signal MWI for Voice Mail](#) in the registry.

MWIStrngFormat [REG_SZ]

Maps the configuration option [MWI text definition](#) in the registry.

PendingJobQueueSize [REG_DWORD]

Maps the configuration option [Max. number of outstanding jobs](#) in the registry.

ResetMwi [REG_DWORD]

Default:	0
Possible values:	0 – Do not reset MWI at the APL start. 1 – Reset MWI at the APL start.

At the APL start the MWI LEDs are not reset. This helps avoiding an increased system load at the start, but MWI display inconsistencies may then occur.

If you want to reset the MWI LEDs at the start, [MinimumJobDistance \[REG_DWORD\]](#) will be considered. This reduces the enormous system load to some degree, when all telephones configured for MWI are addressed at one go.

SignalAnyChange [REG_DWORD]

Maps the configuration option [Signal any change of box](#) in the registry.

StartDelay [REG_DWORD]

Default:	0
Possible values:	Any whole positive number (e.g 5)

Registry Path is

HKLM\SOFTWARE\Wow6432Node\PP-COM\MRS\NotApl

This value will define the time in (decimal) minutes that the processing of jobs will be paused after the service startup.

NOTE: This registry key must be used in Microsoft Cluster environments in place of the registry key:

HKLM\SOFTWARE\Wow6432Node\PP-COM\Services\ApIDel

TaRepTimeout [REG_DWORD]

Maps the configuration option **Distance** in the registry.

TextStringFormat [REG_SZ]

Maps the configuration option **Definition for all additional text protocols** in the registry.

TransactionRepititions [REG_DWORD]

Maps the configuration option **Max. number of Repetition** in the registry.

TransactionTimeout [REG_DWORD]

Maps the configuration option **Failure time for transactions** in the registry.

Verbose [REG_DWORD]

Maps the configuration option **Verbose mode** in the registry.

VoiceProtocols [REG_MULTI_SZ]

Maps the configuration option **Voice protocols** in the registry.

WebumActive [REG_DWORD]

Maps the configuration option **Web Message Access** in the registry.

WebumConfidential [REG_DWORD]

Maps the configuration option **Flag messages as confidential** in the registry.

WebumOriginator [REG_DWORD]

Maps the configuration option **Message originator** in the registry.

WebumStringFormat [REG_MULTI_SZ]

Maps the configuration option **Text for Web Message Access** in the registry.

E.14 Entries of the Presence APL

The following values can be found in the key `PresenceApl`.

CalendarRefreshMinutes [REG_DWORD]

Default:	–
Possible values:	0 – Feature disabled. Minutes – Regular calendar data update.

This value maps the options [Use the Exchange or Lotus Notes calendar for the presence calendar profile](#) and [Refresh the calendar of a monitored user every](#) in the Presence APL configuration dialog. See [Section 21.3.1.1, “The TUM Calendar”, on page 1199](#).

DefaultPrivileges [REG_SZ]

Default:	D6010	
Possible values:	Privilege mask:	
	PHONE	0x80000
	Presence Profile	0x40000
	Online Status	0x10000
	Location	0x08000
	Comment	0x04000
	Busy	0x02000
	Private Comment	0x01000
	Appointment Subject	0x00080
	Divert Business phone	0x00040
	Since	0x00020
	Next Profile	0x00010

Default privileges for the presence status. Every user may normally monitor the presence status of another user. This includes the telephone status (Busy/Free) and the presence status set by the user. This value is used for a new user but can be customized by the user at a later date if the administrator does not prevent this by [OverwriteDefaultPrivileges \[REG_DWORD\]](#). User-individual settings are written in the Correlation and found in the following entry:

```
<Domain/Alias> USERINFO <User ID> PRESENCE_PRIVS <Privilege>
```

The default value is composed of *Busy*, *Comment*, *Online Status*, *Phone*, *Presence Profile* and *Next Profile*.

OverwriteDefaultPrivileges [REG_DWORD]

Default:	0
Possible values:	0 – Feature disabled. 1 – Overwrite individual user settings.

You can use this value to overwrite the individual user settings by the value in [DefaultPrivileges \[REG_SZ\]](#). This enables administrators to deny users the option to assign individual privileges. If the default is not changed, everybody may monitor all telephones.

RtcPassword [REG_SZ]

Default:	–

This value maps the **Password** option in the Presence APL configuration dialog. See [Section 21.3.1.2, “The Live Communications Server Tab”, on page 1200](#).

RtcServerName [REG_SZ]

Default:	–

This value maps the **Server Name or IP Address** option in the Presence APL configuration dialog. See [Section 21.3.1.2, “The Live Communications Server Tab”, on page 1200](#).

RtcSingInName [REG_SZ]

Default:	–

This value maps the **Login ID** option in the Presence APL configuration dialog. See [Section 21.3.1.2, “The Live Communications Server Tab”, on page 1200](#).

RtcSingUserName [REG_SZ]

Default:	–

This value maps the **User Name** option in the Presence APL configuration dialog. See [Section 21.3.1.2, “The Live Communications Server Tab”, on page 1200](#).

E.15 Entries of the Print APL

The following values can be found in the key `PrintApl`.

BadPrinterCreateDC [REG_DWORD]

Default:	0
Possible values:	0 or 1

Some printer drivers show abnormal behavior when the CreateDC function is called in the usual way, which can lead among other things to a Print APL crash. If this is the case, set this value to 1 and check whether the thus activated diversion is a sufficient corrective. At any rate the used printer driver is to be updated first!

EmailAddresses [REG_MULTI_SZ]

Default:	NVS:LN.*/ NVS:EXCH.*/ NVS:SMTP.*/ NVS:MS.*/ NVS:CC.*
Possible values:	NVS : <Protocol> . * / *

The addresses specified here are recognized by the Print APL as e-mail addresses. In addition to those listed here the default address `NVS : <Servername>` is recognized. This is used for filling the `%serv` variable with the word e-mail instead of the cryptic address portion. This variable can be used in the `DocInfoLine` for printing document information.

RetryOnError [REG_DWORD]

Default:	0
Possible values:	0 or 1

If this switch is set to 1, the Print APL activates a repeat strategy for failed print jobs. These jobs are then twice repeated after 30 seconds, subsequently twice again after two minutes if an error message is issued. This serves to avert an error of the Windows printer spooler that, under load, does occasionally not accept any documents any more.

E.15.1 Default Printer-Settings

The following settings under

`HKLM\Software\Wow6432Node\PP-COM\MRS\PrintApl` are default settings for all installed printers. These settings are used for the installation of new printers as well as for all other printers whose settings do not vary from those of the default.

Address [REG_SZ]

Default:	NVS:PRINTER/DEFAULT

The MTA uses this entry to recognize whether the option **Set as default printer** has been set for one of the configured printers. If the *Carbon Copy Rules* are set to *Incoming faxes are copied to the default printer* in the MTA, this printer is addressed. Must not be modified.

DocInfoLine1 [REG_SZ]

Maps the configuration option **Document info** in the registry. See [Section 22.1, “Printer Settings”, on page 1212](#).

DocInfoLine2 [REG_SZ]

Maps the configuration option **Document info** in the registry. See [Section 22.1, “Printer Settings”, on page 1212](#).

DocInfoLine3 [REG_SZ]

Maps the configuration option **Document info** in the registry. See [Section 22.1, “Printer Settings”, on page 1212](#).

DocInfoLine4 [REG_SZ]

Maps the configuration option **Document info** in the registry. See [Section 22.1, “Printer Settings”, on page 1212](#).

DocOverlapFooter [REG_DWORD]

Maps the configuration option **Document info overwrites document body** in the registry. See [Section 22.1, “Printer Settings”, on page 1212](#).

DocPrintInfo [REG_SZ]

Maps the configuration options **None**, **Top** or **Bottom** in the registry for **Document info**. See [Section 22.1, “Printer Settings”, on page 1212](#).

FaxPrintMode [REG_SZ]

Maps the configuration option **Fax mode** in the registry. See [Section 22.1, “Printer Settings”, on page 1212](#).

Formats [REG_SZ]

Represents the configuration option **Formats** in the registry. See [Section 22.1.1, “Supported File Formats”, on page 1214](#).

NumberOfCopies [REG_DWORD]

Maps the configuration option **Number of copies** in the registry. See [Section 22.1, “Printer Settings”, on page 1212](#).

TelexBanner [REG_DWORD]

Maps the configuration option **Telex banner** in the registry. See [Section 22.1, “Printer Settings”, on page 1212](#).

E.15.2 Individual Printer Settings

Each printer has a key under the key `PrintApl\Devices`.

Each printer can be configured in the same manner as with the default printer. For that reason, only the entries that differ from those of the default printer have been listed below.

Address [REG_SZ]

Maps the mandatory printer address in the registry, which is composed by the configuration option **Address** and **Name**. See [Section 22.1.2, “Printer Properties”, on page 1214](#).

DeviceName [REG_SZ]

Mandatory printer name. For network printers the complete name of the Share. Example: `\\OLYMP\QMS 1060 Print System`

IsDefault [REG_DWORD]

Default:	–
Possible values:	0 or 1

This value may only be used for one printer and is set to 1 when the printer is declared as the default printer. If no printer is set as default, the first listed printer will be used and this value is set accordingly for this printer.

If more than one printer has been set as default, a warning is generated in the log and the first listed printer used as default. A corrected value will be returned to the registry.

LineName [REG_SZ]

Maps the configuration option **Pringer** in the registry. See [Section 22.1.2, “Printer Properties”, on page 1214](#).

NovellNetworkPrinter [REG_DWORD]

Default:	0
Possible values:	0 or 1

When set to 1 an attempt to query the global data of the printer will not be made. Apparently, this data is not always available from Novell network printers and an error report is generated upon access. To work around this the default value is used.

UseDefaults [REG_DWORD]

Represents the configuration option **Use default settings** in the registry. See [Section 22.1.2, “Printer Properties”, on page 1214](#).

E.16 Entries of the Report APL and Report Schedule APL

The Report APL and the Report Schedule APL both access the values of the registry entries in the `RepAPL` key. In the `RepScheduleAPL` key no entries are stored, so that this key stays empty.

E.16.1 General Entries

You find the following registry entries in the `RepAPL` key:

Access mode [REG_SZ]

Default:	ADO
Possible values:	ADO or CodeBase

This value contains the access mode for the database connection. The mode is defined on the configuration pages of the Report APL.

ConnectionString [REG_SZ]

Default:	-
Possible values:	-

The Report APL configuration is stored here encrypted in hexadecimal representation.

CRDOTNET [REG_DWORD]

Default:	1
Possible values:	0 – RDC API 1 – Crystal Reports.NET SDK API

With *Crystal Reports XI* the *RDC API* is used, which is not supported anymore from *Crystal Reports 2008*. As of *Crystal Reports 2008* the *Crystal Reports.NET SDK API* will be used instead. Since the Report Schedule APL cannot recognize the installed version of *Crystal Reports*, this switch must be used to make known the use of *Crystal Reports 2008*. A parallel installation of *Crystal Reports XI* and *Crystal Reports 2008* is not supported and may lead to unforeseen errors when reports are generated.

As of *Crystal Reports 2008*, the RDC API used by the *Crystal Reports Viewer* and shipped on the XPR product carrier is not supported by Crystal Reports anymore. The viewer can therefore not be used anymore. As alternative, you can use the *Crystal Reports Viewer* to be downloaded under <http://www.sap.com/solutions/sapbusinessobjects/sme/reporting/viewer/index.epx>. When using *Crystal Reports 2008*, the file format for the *Crystal Reports Viewer* changes to `.rpt`, so that the viewer can display this format.

The previous file format (*.rep*) cannot be generated with *Crystal Reports 2008*. However, you can rename the old reports after *.rpt*. The new viewer is then able to recognize these and displays them as well.

Please be aware that the resource consumption of the *Crystal Reports.NET SDK API* is significantly higher. So, if possible, stick to the older Crystal Reports with the RDC API in case of upgrades while maintaining older hardware.

Note: By default RepScheduleApl generates with output file settings “TXT” a file with extension “TTX” (for Trados TagEditor).

When CRDOTNET is set to 0 then RepScheduleApl generates a file with extension “TXT”.

DbStatDir [REG_SZ]

Default:	-
Possible values:	File path

The file path specified here overrides the defined file path from which the Report APL obtains the log files of type *st<dd.mm.yy.>.log*. Do not confuse the registry entry with the DataBaseDirectory entry (see [Appendix E.16.4.3, “Database Directory Statistics”](#)): The file path in which the log files of type *st<dd.mm.yy.>.log* are stored cannot be modified here. The file path is defined, from which the Report APL obtains the log files. By default no path is specified here, since the Report APL automatically accesses the path *<XPR install>\stat*.

ExportIVRStatistics [REG_DWORD]

Default:	0
Possible values:	0 or 1

This entry refers to the export of statistical *IVR raw data* of the *VOGUE* script to database tables of the configured SQL server. The data supply statistical information about the properties and the behavior of configured applications and boxes in the *Application Builder*. The export of all possible raw data to the database tables of an SQL server is disabled by default with value 0 but can be activated with value 1. The export may only be activated with an SQL server configured in the Report APL. The IVR raw data are stored in two SQL database tables. One database table stores the data *IVR Application*, the other one the data *IVR Box*.

FixedStFile [REG_SZ]

Default:	-
Possible values:	-

This registry key has an internal function and must not be modified.

BIRT_RUNTIME [REG_SZ]

Default:	<XPR Install>\ReportEngine
Possible values:	File path

The path specified here must contain the BIRT runtime component as well as possible external Java applications, since the Report Schedule APL can access these in this path only. Please be sure to install BIRT updates in the path specified here.

CRRunTime [REG_DWORD]

Default:	-
Possible values:	-

This registry key has an internal function and must not be modified.

E.16.2 Runtime Engine

Because of the high system resources required by report generating that may perhaps influence other components negatively, a runtime engine is needed. The default behavior of this engine suspends the generating of the reports all 5 seconds for a second. This mechanism allows other system components unhindered access to the system resources. The runtime behavior of the Report APL can be influenced by the following values in the key `RepAp1`.

TimerThreadRunTime [REG_DWORD]

Default:	5
Possible values:	Cycles

This entry specifies the number of the intervals during which the report generating is active. The value must be greater or equal 1.

TimerThreadSleepTime [REG_DWORD]

Default:	1
Possible values:	Cycles

This entry indicates the number of intervals during which the report generating is inactive. The value must be greater or equal 1.

TriggerThreadSleepTime [REG_DWORD]

Default:	1000 ms
Possible values:	Milliseconds

This entry specifies the time interval in milliseconds. The value must be greater or equal 10 for being accepted.

Export Interval [REG_DWORD]

Default:	5
Possible values:	0 to 1440

With this value you specify a time interval in minutes after the expiration of which a database export is automatically performed. The temporarily last raw data are exported. Precondition is that the Report APL is not busy with an export and raw data are available. Value 0 deactivates this feature. If a value higher than 1440 minutes is entered, the maximum value of 1440 minutes is used. This entry is not valid for the **InfoStor** databases *Journal*, *Geb* or *Correl*. Such databases are only exported in case of a report generation in the Report Schedule APL.

WatchdogStateSave[REG_DWORD]

Default:	-
Possible values:	Watchdog state

This entry must not be modified. The feature is internally used by the Report APL to restore the Watchdog state after a system crash.

E.16.3 Manual Entries

The following entries can be added in the `RepAPL` key manually to enable the export of specific data to database tables by the Report APL. You find a detailed description of the function of these entries in [Section 27.10, “Basics on the Raw Data Database Tables”](#).

ExportNCOLocation [REG_DWORD]

Default:	0
Possible values:	0 or 1

This entry activates(1) or deactivates (0) the export of NCO location information to Report APL database tables.

ExportMrsUsers [REG_DWORD]

Default:	0
Possible values:	0 – No export; existing export table is deleted. 1 – Export activated. 2 – No export; existing export table is kept.

You can use this entry to have the data of users and groups exported to the database tables of the Report APL.

E.16.4 Database

The following values can be found in the key RepAp1\DB.

Time Selections [REG_MULTI_SZ]

Default:	-
Possible values:	Digits,Path,Century,Year,Month,Day,Hour,Minute,Second,Timezone,Century,Year,Month,Day,Hour,Minute,Second,Timezone

The first parameter Digits specifies the data base exports that can be found under the second parameter Path. The other parameters define the included time range.

SlowDownCorrel [REG_DWORD]

Default:	1
Possible values:	Whole numbers greater than zero

We recommend not to change this value!

With value 1 a delay is performed with each data readout run from the Correl Database. With value 2, this function is executed only with every second run. This behavior is controlled correspondingly with greater values. Thus greater values enable increasing the data run performance. This, however, will effect the performance of other system components. Since such effects have not been tested, we expressly recommend not to use a value greater than 1.

SlowDownGeb [REG_DWORD]

Default:	1
Possible values:	Whole numbers greater than zero

We recommend not to change this value!

With value 1 a delay is performed with each data readout run from the charges database. With value 2, this function is executed only with every second run. This behavior is controlled correspondingly with greater values. Thus greater values enable increasing the data run performance. This, however, will effect the performance of other system components. Since such effects have not been tested, we expressly recommend not to use a value greater than 1.

SlowDownJournal [REG_DWORD]

Default:	1
Possible values:	Whole numbers greater than zero

We recommend not to change this value!

With value 1 a delay is performed with each data readout run from the journal database. With value 2, this function is executed only with every second run. This behavior is controlled correspondingly with greater values. Thus greater values enable increasing the data run performance. This, however, will effect the performance of other system components. Since such effects have not been tested, we expressly recommend not to use a value greater than 1.

EnableOldStyleDbExport [REG_DWORD]

Default:	0
Possible values:	0 or 1

This entry activates (value = 1) or deactivates (value = 0) the type of data export from databases if CodeBase is used and is obsolete with using ADO and SQL.

EnableNewStyleDbExport [REG_DWORD]

Default:	0
Possible values:	0 or 1

This entry activates (value = 1) or deactivates (value = 0) this type of data export from databases. Two additional tables for the recipients and the received information are created in this process. This entry can only be used for CodeBase and is obsolete with using ADO and SQL.

E.16.4.1 Storage of the Event Files

The Report APL performs an automatic saving of the processed event data, since this is automatically deleted in the <XPR Install>\Stat directory after having been processed. The default setting is the <XPR Install>\Log directory. In this directory the automatic XPR server maintenance deletes all data older than 60 days. This default can be changed in the maintenance script. If the event data is to be stored for a longer time, you should provide appropriate saving programs. Via the following two entries the saving can be switched off and/ or the directory, into which the saving is performed can be modified. The entries can be modified any time.

BackupDirectory [REG_SZ]

Default:	<XPR Install>\Log
Possible values:	Local directory

This entry contains the path to the server log files and can be replaced by every valid local database path.

BackupSettings [REG_SZ]

Default:	1
Possible values:	0 – Saving not active 1 – Saving active

Switch backup of statistics log files on or off.

E.16.4.2 Regular Database Maintenance

CompressDbSettings

Default:	1, YYYY.MM.DD.03.00.00
Possible values:	0 1, YYYY.MM.DD.hh.mm.ss

The Report APL performs a daily database maintenance. Via this entry the maintenance may be switched off and/ or the default time (3 o'clock) may be modified. The setting is switched on or off via the switch 1 (on) or 0 (off). The value YYYY.MM.DD.hh.mm.ss determines the next database maintenance time. The maintenance serves to remove entries that are marked as deleted physically from the database and the index files. Respectively marked entries are entries having exceeded the maximum usability time. This parameter may be modified any time.

E.16.4.3 Database Directory Statistics

DatabaseDirectory [REG_SZ]

Default:	<XPR Install>\Stat
Possible values:	Local directory

Via this entry the directory may be determined in which the statistic database is generated and maintained. The value may only be modified when the Report APL is shut down. All statistic databases generated up to this time must be copied from the root path into the new directory by hand before the Report APL is restarted.

UpdateDbSettings[REG_SZ]

Default:	1, YYYY.MM.DD.01.00.00
Possible values:	switch, YYYY.MM.DD.hh.mm.ss

This entry specifies the time when databases are again generated from the raw data. Furthermore, the update feature can be switched on or off via this entry (Switch 1 = on , 0 = off).

Use Foreign Exports [REG_DWORD]

Default:	-
Possible values:	0 or 1

This parameter specifies whether database exports from other report jobs are to be used for caching.

E.16.5 Job

The following values can be found in the key `RepAp1\Job`.

JID [REG_DWORD]

Default:	-
Possible values:	<Number>

The biggest ID of all defined report jobs.

Job List [REG_MULTI_SZ]

Default:	-
Possible values:	Job ID

A list of all defined report jobs.

E.16.6 Configuration of the single Jobs

One key exists per job `RepAp1\Job\<JID>` with the following values.

CR Export Destination [REG_SZ]

Default:	No default value. Path changes depending on the installation.
Possible values:	Path\file name

This value defines where the exported report file is stored and how the file is named. The extension depends on the selected export format and will be automatically attached. Configure this value on the Extensions tab. See [Section 27.6.4.6, “Step 6 - Selecting a Folder”, on page 1327](#).

Example: `d:\<XPR Install>\res\crw\out\output`

CR Export Format [REG_DWORD]

Default:	1
Possible values:	0 - Crystal Report (Extension: REP) 1 - Rich Text Format (RTF) 2 - Hypertext Markup Language (HTM) 3 - Tab Separated Values (TSV) 4 - Comma Separated Values (CSV) 5 - Text (TXT) 6 - Tab Text (TXT) 7 - Winword Document (DOC) 8 - Excel 5 Sheet (XLS) 9 - Fax G3 (FG3) 10 - Fax G4 (FG4) 11 - Fax G3 TIFF (FAX) 12 - Fax G4 TIFF (FAX)

This value specifies the export format of the report. This is determined on the Export tab. See [Section 27.6.4.5, “Step 5 - Selecting a Format”, on page 1326](#).

CR Export Mode [REG_DWORD]

Default:	0
Possible values:	0 - File 1 - Lotus Notes (planned extension) 2 - Microsoft Exchange (planned extension)

The default setting is exported into a file. The exported reports can also be directly delivered to Lotus Notes or Microsoft Exchange (planned extension). The Export mode can be configured on the Export tab. See [Section 27.6.4.5, “Step 5 - Selecting a Format”, on page 1326](#).

CR Layout [REG_SZ]

Default:	-
Possible values:	Path\file name

Here the report layout is configured which has been created by the Crystal Report Designer. The file must always end with rpt.

Example: d:\<XPR Install>\res\crw\Dbase.rpt

DB Data Sources [REG_DWORD]

Default:	7
Possible values:	1 - Correlation 2 - Journal 4 - Charges 8 - eXtended Statistics

The data sources used here. If more than one source is used, the values of these sources are to be added. These data sources are selected when you choose a new layout. See [Section 27.6.4.1, "Step 1 - Introducing Layouts", on page 1321](#)

DB Export Destination [REG_SZ]

Default:	-
Possible values:	File path

Here the data is stored that is generated by exporting from the data sources. The path must end with a backslash.

Example: d:\<XPR Install>\res\crw\in\

DB Export Hidden [REG_DWORD]

Default:	0
Possible values:	0 or 1

With 1 also journal entries with a hidden flag are exported. This value represents the option **Export data records from journal incl. HIDDEN flags** (Export tab). See [Section 27.6.4.6, "Step 6 - Selecting a Folder", on page 1327](#).

DB Export only [REG_DWORD]

Default:	0
Possible values:	0 or 1

With 1 only an export of the data sources takes places. This is useful for creating a basis for generating new report layouts. This value represents the option **Create Database Export only** (Extensions tab). See [Section 27.6.4.6, "Step 6 - Selecting a Folder", on page 1327](#).

DB Time in day from [REG_DWORD]

Default:	19,0,1,1,0,0,0,99,
Possible values:	Age,year,month,day,hour,minute,second,timezone,

With this entry you specify the start date of a time range from which the data are used for report generation. This value corresponds to the configuration of the **Time range** option in the **Export** tab of the Report Schedule APL configuration tabs (see [Section 27.5.1, "Reports Tab"](#)).

DB Time in day to [REG_DWORD]

Default:	19,0,1,1,0,0,0,99,
Possible values:	Age,year,month,day,hour,minute,second,timezone,

With this entry you specify the end date of a time range up to which the data are used for report generation. This value corresponds to the configuration of the **Time range** option in the **Export** tab of the Report Schedule APL configuration tabs (see [Section 27.5.1, "Reports Tab"](#)).

DB Time Select Fixed Offset [REG_DWORD]

Default:	0
Possible values:	0 - Current 1 - Last complete 2 - Penultimate complete ...

A time range is selected and only data of this period is exported from the data sources. This applies only to data sources where this is useful. This offset is required if DB Time Select Mode possesses a value between 6 and 10, that means a fixed time unit is configured. With the value 0 no access to a cache database takes place. Already exported data is stored in a cache database and must perhaps not be exported again. This relative offset can be entered on the Export tab. See [Section 27.6.4.5, "Step 5 - Selecting a Format"](#), on [page 1326](#).

DB Time Select from [REG_SZ]

Default:	19,0,1,1,0,0,0,99,
Possible values:	Age,year,month,day,hour,minute,second,timezone,

All values must consist of 2 ciphers. This entry is required if DB Time Select Mode possesses the value 1, 2 or 5. It determines the offset of the time range.

DB Time Select Mode [REG_DWORD]

Default:	0
Possible values:	0 - Export of all available data records 1 - Start time until end time 2 - Start time + offset 3 - End time - Offset 4 - Current time - Offset 5 - Start time until current time 6 - Time unit in hours 7 - Time unit in days 8 - Time unit in weeks 9 - Time unit in months 10 - Time unit in years

The mode of the time range definition is configured here. For all values including the current time no caching takes place. Select the **Time Range for Data Sources** on the Export tab. See [Section 27.6.4.5, “Step 5 - Selecting a Format”, on page 1326](#).

DB Time Select Range [REG_DWORD]

Default:	1
Possible values:	Any value

This entry is required if DB Time Select Mode possesses the value 2, 3 or 4. It determines the offset of the time range.

DB Time Select to [REG_SZ]

Default:	20,99,12.31,23,59,59,99,
Possible values:	Age,year,month,day,hour,minute,second,timezone,

All values must consist of 2 ciphers. This entry is required if DB Time Select Mode possesses the value 1 or 3. It determines the end time of the time range.

Description [REG_SZ]

Default:	Default value after installation
Possible values:	Arbitrary alphanumerical value

Text description of the report.

Error Handling [REG_DWORD]

Default:	0
Possible values:	Not defined yet.

Error handling for failed reports. Not implemented yet.

ID [REG_DWORD]

Default:	No default value
Possible values:	A number

This number is a unique job name. At the same time this job ID forms the name of this key in the Windows registry. A list of all configured jobs can be found in the value Job List.

Last Result [REG_DWORD]

Default:	6
Possible values:	0 - Error 1 - None 2 - Active 3 - Executing 4 - Ready 5 - Canceled 6 - Stopped

This value is set with those report jobs that are repeated in regular intervals. It shows the status of the last performed cycle.

Name [REG_SZ]

Default:	-
Possible values:	Arbitrary alphanumerical value

Short name of the report job.

Recipients [REG_MULTI_SZ]

Default:	-
Possible values:	0 or 1 <NVS address>

A recipient for this report job is specified here per line. Via this flag each address can be activated separately. Select the recipient in the Recipient tab. See [Section 27.6.4.4, "Step 4 - Selecting a Recipient", on page 1325](#).

Repeat Custom Days [REG_DWORD]

Default:	0
Possible values:	<Number>

In case of a user-defined repeat interval the offset is stored here in days.

Repeat Custom Hours [REG_DWORD]

Default:	0
Possible values:	<Number>

In case of a user-defined repeat interval the offset is stored here in hours.

Repeat Custom Minutes [REG_DWORD]

Default:	0
Possible values:	<Number>

In case of a user-defined repeat interval the offset is stored here in minutes.

Repeat Mode [REG_DWORD]

Default:	0
Possible values:	0 - None 1 - Hourly 2 - Daily 3 - Weekly 4 - Monthly 5 - Yearly 6 - User-defined

Repeat mode for this report job. No repetition means the report job is executed only once. For a user-defined repetition at least one of the three Repeat Custom ... values must be greater than 0. Configure the repeat mode on the Times tab. See [Section 27.6.4.3, “Step 3 - Setting an Execution Time”, on page 1324](#).

Start Now [REG_DWORD]

Default:	0
Possible values:	0 or 1

With 1 the report job is performed at once, otherwise at the start time configured in the value Start Time.

Start Time [REG_SZ]

Default:	-
Possible values:	Age,year,month,day,hour,minute,second,timezone,
Remark:	All values must consist of 2 ciphers.

This is the start time the report job is performed.

Status [REG_DWORD]

Default:	6
Possible values:	0 - Error 2 - Active 3 - Executing 4 - Ready 5 - Canceled 6 - Stopped

A report job possesses a uniquely defined status at all times.

E.16.7 Layouts

The following values can be found in the key `RepApl\Layout`.

Count [REG_DWORD]

Default:	-
Possible values:	<Number>

The number of available report layouts. This value corresponds to the number of existing default layouts.

Location [REG_SZ]

Default:	-
Possible values:	File path

All report layouts must be in this directory. Please note that a `\` must end the task.

Example: `d:\<XPR Install>\res\work\crw\`

E.16.8 Layout Configuration

One key exists per job `RepApl\Layout\<Layout No.>` with the following values.

Comment [REG_SZ]

Default:	-
Possible values:	<String>

Comment on this default layout.

Data Sources [REG_DWORD]

Default:	For older layouts 7, for newer layouts 8
Possible values:	1 - Correlation 2 - Journal 4 - Charges 8 - eXtended Statistics

Here the data sources used in the text are mentioned. If more than one source has been used, the values of these sources are to be added.

Name [REG_SZ]

Default:	-
Possible values:	File name

This is the file name of the default layout. The file type (extension) must be `RPT`.

Example: `SysDsn.RPT`

E.17 SMS-Connector Entries

E.17.1 Global Values

Global values refer to all configured APL connections. They are only read at the APL start, so that modifications require a reboot of the APL. The following values are found in the key `SMSIPAPL`.

MaxLicenses [REG_DWORD]

Default:	0
Possible values:	defines the number licenses to be consumed by SmslpApl

This registration key defines the number of licenses to be consumed by SmslpApl.

If the registry does not exist or the value is 0 (zero) then SmslpApl uses the maximum number of licenses on startup.

Also if the value is greater than the available licenses then SmslpApl will use the maximum number of licenses on startup.

PrefetchBuffering [REG_DWORD]

Default:	0
Possible values:	0 – Buffer switched off. 1 – Buffer active.

Some providers support only relatively small queues. This slows down the transmitting power of the XPR server in cooperation with the MTA considerably. You can avoid this by activating an APL-wide buffer for 64 messages here. In this way the SMS Connector is enabled to accept up to 64 messages while one message is being sent.

RepeatStrategy [REG_SZ]

Default:	3-12;10-60;12-300;3-3600
Possible values:	<number of repeats>-<seconds>;<number of repeats>-<seconds>;...

You can change the strategy for repeating short message transmission here. You can specify up to five blocks. Each of them indicates the number of repeats and the respective interval between the repeats. The default is three repeats every 12 seconds, then 10 repeats after one minute, then 12 repeats after five minutes, then three repeats after one hour.

The strategy defaulted here applies for all SMS lines.

SmsOriginatorPropertyName [REG_SZ]

Default:	<Empty>
Possible values:	PMF property

The SMS Connector tries to determine the originator ID of an outgoing SMS message by querying the user database. If this is not possible, the set [Default Originator](#) is used.

By specifying a PMF property you can reset the SMS message originator address to something else. For example, the `ORIGINATOR_FAXG3` setting would set the FAX G3 number of the originator as originator ID.

Settings of this type should always be performed by the Professional Services since they are familiar with PMF properties.

NOTE:

This feature does not work in combination with a GSM box, since in this case the number of the implemented SIM card is used.

SmsValidityTime [REG_DWORD]

Default:	0
Possible values:	Seconds

This value indicates the validity of the message from the time it was sent in seconds. In case of 0 the maximum setting is not transmitted in the OTO51 protocol element to the message center, so that the center keeps its default setting. This default setting is usually 48 hours.

If you modify this value, always verify that the message center actually supports this feature. Different errors may occur:

- You do not receive an error report.
- The provider ignores the setting.
- You receive an OK report but the provider does not deliver the SMS message without feedback.
- ...

Possibly desired values should always be arranged with the provider.

A step by step test gives information about the functionality:

1. Set the value to 6 hours (21600)
2. Send an SMS message to your own cell phone to ensure that messages are generally received.
3. Switch your cell phone off and send an SMS message to your cell phone. After 6 hours you should receive an error report.

4. Switch your cell phone off and send an SMS message to your cell phone. Switch your cell phone on after 7 hours. The SMS message should not be delivered by the provider any more.

In the XPR monitor you can analyze the process on debug level 4 under the “Connection” topic in more detail. This topic contains a hexdump of the communication. With the freely obtainable protocol description for EMI/UCP you can read this hexdump.

E.17.2 Connection-specific Values

For each configured connection, a key `SMSIPAPL\<Connection>` is defined. Within this key the following values may exist:

Adapter [REG_SZ] (GSM)

Maps the configuration option **Mailbox Type** in the registry.

Address [REG_SZ]

Maps the configuration option **Connection Address** in the registry.

BindAddress [REG_SZ] (UCP)

Default:	<Empty>
Possible values:	<IP address>

In case of several computer IP addresses you can enter here the originator address used for the delivery to the provider.

BlackList [REG_MULTI_SZ]

Default:	<Empty>

Here you can enter one number in normalized format per line. * may be used as wildcard.

Example:

```
+39*  
+49172*
```

Prevents SMS transmissions to Italy or Vodafone Germany. In the latter case the prefix must begin with +49172, though. Since the customers of cellphone network providers may keep their number when they become subscribers to another provider, prefixes do not determine specific providers any more.

BulkSenders [REG_MULTI_SZ]

Default:	<Empty>

Requesting delivery confirmations may incur costs depending on the contract. Therefore you can selectively decide **not** to enforce a delivery confirmation for specific send jobs. You can do this via two different ways:

1. Enter here the normalized number of an originator who may not request delivery confirmations. * may be used as wildcard. See also [BlackList \[REG_MULTI_SZ\]](#).
2. If the message contains the SMS_DELIVERY_NOTIFICATIONS PMF property with value 0, no delivery confirmations will be requested. This PMF property could be created e. g. by adjusting the Professional Services.

The SMS_DELIVERY_NOTIFICATIONS PMF property does not only allow to deactivate delivery notifications for an explicit send process, but also to specify how delivery confirmations are to be handled for this send process.

SMS_DELIVERY_NOTIFICATIONS is a bit mask that can be allocated as follows:

Requesting delivery confirmations: 0x00000010

Delivery confirmations also as message: 0x00000020

If you want to specify which delivery confirmations are desired, the following values are available:

Successfully delivered: 0x00000001

Not delivered: 0x00000002

Buffered: 0x00000004

If you do not specify any of these values, the default value of the message center is used. This is usually 0x00000007.

If you set explicit delivery confirmations, you should only drop the “buffered” confirmation. The XPR server will otherwise not notice the completion of a send process any more. All send processes would thus be acknowledged negatively after some time.

CaseSensitiveSearch [REG_DWORD]

Default:	0
Possible values:	0 – Convert into capital letters. 1 – Do not convert into capital letters.

The search for a recipient normally converts the search term into capital letters first, before the corresponding database field in the Correlation database is searched. Here you can disable this conversion, so that you can also use upper and lower case writing to search e. g. the NAME field. However, a recipient will then only be found if the writing matches exactly the one in the database.

Cost [REG_DWORD]

Default:	0
Possible values:	<Cent>

The amount entered here is written in the GEB charges database per sent SMS message. This enables user-based billing.

DailyLimit [REG_DWORD]

Maps the configuration option [Daily Send Limit](#) in the registry.

DBInField [REG_SZ]

Default:	<Empty>
Possible values:	<Field name of the user database>

Description of the user database field via which received SMS messages can be assigned to a user. If this value is empty, then *SMS#* is used internally. This is particularly useful in the interaction with [DBOutField \[REG_SZ\]](#).

DBOutField [REG_SZ]

Default:	DBInField [REG_SZ]
Possible values:	<Field name of the user database>

The content of the database field referenced here is prefixed to a message enclosed by [LimLeft \[REG_SZ\]](#) and [LimRight \[REG_SZ\]](#). If this value is not available in the registry, the database field set for [DBInField \[REG_SZ\]](#) is used. If this value is written in the registry without content, then this feature is disabled.

By default, the recipient of an SMS message can thus simply reply and need only copy the portion of the message framed by the characters set under [Recipient restriction](#) to his/her reply.

See also [Prefix Originator Identification](#).

DefaultOriginator [REG_SZ] (UCP)

Maps the configuration option [Default Originator](#) in the registry.

DefaultRecipient [REG_SZ]

Maps the configuration option [Default recipient address](#) in the registry.

Enabled [REG_DWORD]

Maps the configuration option [Start this connection automatically](#) in the registry.

ForcedIdentification [REG_DWORD]

Maps the configuration option [Prefix Originator Identification](#) in the registry.

FromAddressNPI [REG_DWORD] (GSM)

Default:	0
Possible values:	0 – Unknown 1 – Telephone/ISDN (E.163/E.164) 3 – Data (X.121) 4 – Telex (F.69) 8 – National 9 – Private 10 – Ermes

The numbering plan indicator used by the GSM client for the FromAddress property.

FromAddressTON [REG_DWORD] (GSM)

Default:	0
Possible values:	0 – Unknown 1 – International 2 – National 3 – Network-specific 4 – Subscriber number 5 – Alphanumeric

The number type used by the GSM client for the FromAddress property.

GsmDeviceCheckRate [REG_DWORD] (GSM)

Default:	30
Possible values:	0 – Deactivate check. 15 - 300 seconds

The following parameters of the connected GSM device are queried in regular intervals: PIN, activity, network registration, signal quality, service availability and charge of battery.

If problems are noticed here, the GSM device will be rebooted. If three consecutive reboots do not lead to an improvement, this line is terminated and, depending on [SnmpMode \[REG_DWORD\]](#), an SNMP trap triggered.

Setting 0 deactivates these checks.

GSMInitString [REG_SZ] (GSM)

Default:	<Empty>
Possible values:	<Initialization command>

The contents of this value is sent to the GSM device as first command and serves to initialize the device.

Identity [REG_SZ] (SMPP, UCP)

Maps the configuration option **ID** in the registry.

InternalData [REG_BINARY]

Contains internal data such as the encrypted PIN code to access the GSM SIM boards or the statistics that can be retrieved in the XPR monitor.

KeepAliveTimer [REG_DWORD]

Maps the configuration option **Keep-Alive Interval** in the registry.

LimLeft [REG_SZ]

Default:	#
Possible values:	--, #, \$, %, &, **, [, {, <, <String>

Maps the left portion of the **Recipient restriction** configuration option to the registry. If nothing is set, # is used. Besides the directly selectable characters you can also enter any individual character combination.

LimRight [REG_SZ]

Default:	<Empty>
Possible values:	--, #, \$, %, &, **,], }, >, <String>

Maps the right portion of the **Recipient restriction** configuration option to the registry. If nothing is set, # is used. Besides the directly selectable characters you can also enter any individual character combination.

LogFile [REG_SZ] (GSM, SMPP)

Default:	<Empty>
Possible values:	<Path and file name>
Example:	c:\temp\mylogfile.log

If this value is not empty, all GSM or SMPP commands and replies are logged in the referenced file.

LongSmsMode [REG_DWORD]

Maps the configuration option **Long SMS mode** in the registry.

MailNotificationFlags [REG_DWORD]

Default:	3
Possible values:	Mask that may be composed of the following values: 1 – Successfully delivered. 2 – Not delivered. 4 – Buffered.

This mask specifies for which cases delivery confirmations are sent as message in case of activated **MailReports [REG_DWORD]**. The default setting of 3 (1+2) means that a report is sent as message to the originator for successfully and not delivered SMS messages. If an invalid value, for example 0, is entered here, the default of 3 is always assumed.

MailReports [REG_DWORD]

Default:	0
Possible values:	0 – Delivery confirmations as message are deactivated. 1 – Delivery confirmations as message are activated.

If delivery notifications are generally activated in the SMS Connector via [Delivery Notifications – Default](#) or [Delivery Notifications – Specific](#), they are transferred to the MTA in the internal XPR server format. Besides delivering this normal report you can instruct the SMS Connector to provide the originator with a detailed message in addition. Using [MailNotificationFlags \[REG_DWORD\]](#) you can filter the delivery confirmation as message.

MapperTable [REG_SZ]

Maps the configuration option [Fonts](#) in the registry.

MaxRestartAttempts [REG_DWORD]

Default:	3
Possible values:	<Number>

Maximum number of attempts to restart the connection to the GSM device.

MessageStorage [REG_DWORD] (GSM)

Default:	0
Possible values:	0 – Retrieve messages from all storage locations. 1 – Retrieve messages from the SIM memory. 2 – Retrieve messages from the device memory. 3 – Retrieve messages from the SIM and device memory. 4 – Retrieve messages from the special report memory.

SMS messages are usually retrieved from all available storage locations of a GSM adapter. The special report memory is only available for advanced GSM adapters.

MidMapperSize [REG_DWORD]

Maps the configuration option [Size of index table](#) in the registry.

NotificationFlags [REG_SZ]

Maps the precise setting of the [Delivery Notifications – Specific](#) option in the registry.

PollRate [REG_DWORD] (GSM, SMPP)

Default:	90 (GSM), 5 (SMPP)
Possible values:	<Seconds>

Maps the configuration option [Poll rate](#) in the registry. In case of SMPP this value cannot be set via the GUI and need not be modified in the normal case either. It is a time interval for polling newly received messages.

Protocol [REG_SZ]

Maps the configuration option **Protocol** in the registry.

ReconnectInterval [REG_DWORD]

Maps the configuration option **Reconnect Interval** in the registry.

ReportsStorage [REG_DWORD] (GSM)

Default:	0
Possible values:	0 – Retrieve messages from all storage locations. 1 – Retrieve messages from the SIM memory. 2 – Retrieve messages from the device memory. 3 – Retrieve messages from the SIM and device memory. 4 – Retrieve messages from the special report memory.

This value is for advanced GSM adapters only: If delivery notifications are required for outgoing SMS messages and advanced GSM adapters that have a special report memory are used at the same time, a special storage location may have to be specified from which the delivery notifications are retrieved.

The setting depends on the hardware used. GSM telephones usually store the delivery notifications in their integrated device memory only. Therefore, do not make any settings for such devices here.

RequestNotifications [REG_DWORD]

Maps the configuration options **Delivery Notifications – None**, **Delivery Notifications – Default** and **Delivery Notifications – Specific** in the registry.

RetryInterval [REG_DWORD] (UCP)

Maps the configuration option **Retry Delay** in the registry.

SendSubjectOnly [REG_DWORD]

Default:	0
Possible values:	0 – Send message body as SMS 1 – Send message subject as SMS

Send subject or body of a message as SMS

SendTimeout [REG_DWORD] (GSM)

Default:	15
Possible values:	5 - 60 seconds

Time in seconds that may be spent waiting for an answer from the provider.

SerBaudRate [REG_DWORD] (GSM)

Default:	0
Possible values:	0.1200 - 115200

Baudrate of the serial interface. In case of 0 the value of the current communication connection is copied. If required, this value must be manually created. This is required for e.g. Falcom boxes, since the SMS Connector cannot connect them otherwise.

ServerTimeout [REG_DWORD] (SMPP)

Default:	2000
Possible values:	<Milliseconds>

Time-out in milliseconds for the server used for all network operations.

ServiceCenter [REG_SZ] (SMPP, UCP)

Maps the configuration option [Message Center](#) in the registry.

SessionPassword [REG_SZ]

Maps the configuration option [Session Password](#) in the registry.

SmsCenter [REG_SZ] (GSM)

Maps the configuration option [SMS Center](#) in the registry.

SmsDigest [REG_SZ]

Maps the configuration option [SMS Digest](#) in the registry.

SMSDontDeleteMessages [REG_DWORD]

Default:	0
Possible values:	0 – Remove retrieved messages from the SIM card 1 – Do not remove retrieved messages from the SIM card

This parameter states whether received messages are to be deleted from the SIM card. For testing purposes it can be activated so that the messages are maintained. In real operation this switch must be set to 0 since only a maximum of 15 messages can be saved on the SIM board.

SmsLogsRecipient [REG_SZ]

Maps the configuration option [Statistics Recipient](#) in the registry.

SmsPrefix [REG_SZ]

Maps the configuration option [SMS prefix](#) in the registry.

SmsSuffix [REG_SZ]

Maps the configuration option [SMS suffix](#) in the registry.

SourceRouting [REG_DWORD]

Default:	1
Possible values:	0 – Source routing deactivated. 1 – Source routing activated.

The SMS Connector usually attempts to independently determine the recipient of an SMS message based on specific criteria. See also [Section 14.5.4.1, “Determining the Recipient”, on page 1024](#). This technique is called source routing.

In case of SMS messages this technique is mostly useful since routing is usually performed via one or via a relatively small number of central numbers. But if an entire phone number range is transmitted via a provider connection, each recipient has already assigned a unique phone number. In this case you can deactivate the source routing here.

SystemAddressRange [REG_SZ] (SMPP)

Default:	<Empty>

See <http://www.activexperts.com/support/xmstoolkit/index.asp?kb=Q4240050>.

SystemCharSet [REG_DWORD] (SMPP)

Default:	0
Possible values:	0 – Use default character set of the SMSC 1 – Use GSM character set (IA5) 2 – Use ASCII character set 3 – Use ISO 8859-1 character set 4 – Use JIS character set 5 – Use Cyrillic character set 6 – Use Hebrew character set 7 – Use Japanese character set (ISO 2022) 8 – Use Greek character set (ISO 8859-7)

Character set used. This character set should only be modified upon special SMPP provider request.

SystemDestinationNPI [REG_DWORD] (SMPP)

Default:	0
Possible values:	0 – Automatic recognition 1 – Telephone/ISDN (E.163/E.164) 3 – Data (X.121) 4 – Telex (F.69) 6 – Land Mobile (E.212) 8 – National 9 – Private

The numbering plan used by the SMPP server.

SystemDestinationTON [REG_DWORD] (SMPP)

Default:	0
Possible values:	0 – Automatic recognition 1 – International 2 – National 3 – Network-specific 4 – Subscriber number 5 – Alphanumeric 6 – Abbreviated

The type of number used by the SMPP server.

SystemMode [REG_DWORD] (SMPP)

Maps the configuration option [System Mode](#) in the registry.

SystemSourceAddress [REG_SZ] (SMPP)

Default:	<Empty>
Possible values:	<SMS number>

The individual SMS number connected to this SMPP provider access. Normally you need not set this value since the number is automatically transmitted to the recipient.

But if you want to transmit an alphanumeric display name with a maximum of 11 characters instead of the number, then set this value. In this case the [SystemSourceTON \[REG_DWORD\] \(SMPP\)](#) value should also be set to 5. This feature is not supported by all providers, though.

Furthermore, you may have received several SMS numbers in case of an SMPP provider. The number to be used here must then be entered.

SystemSourceNPI [REG_DWORD] (SMPP)

Default:	0
Possible values:	0 – Automatic recognition 1 – Telephone/ISDN (E.163/E.164) 3 – Data (X.121) 4 – Telex (F.69) 6 – Land Mobile (E.212) 8 – National 9 – Private

The numbering plan used by the SMPP client.

SystemSourceTON [REG_DWORD] (SMPP)

Default:	0
Possible values:	0 – Automatic recognition 1 – International 2 – National 3 – Network-specific 4 – Subscriber number 5 – Alphanumeric 6 – Abbreviated

The type of number used by the SMPP client.

SystemThroughput [REG_DWORD] (SMPP)

Default:	0
Possible values:	<Number of messages>

This value lets you restrict the number of sent messages per second. 0 means no restriction.

SystemType [REG_SZ] (SMPP)

Default:	<Empty>

SMSC provider type. SMPP is set by default. Valid values can be: SMPP, VMS, OTA or an empty string. If something must be set here, please consult your SMPP provider for the desired setting.

ToAddressNPI [REG_DWORD] (GSM)

Default:	0
Possible values:	0 – Unknown 1 – Telephone/ISDN (E.163/E.164) 3 – Data (X.121) 4 – Telex (F.69) 8 – National 9 – Private 10 – Hermes

The numbering plan indicator used by the GSM client for the ToAddress property.

ToAddressTON [REG_DWORD] (GSM)

Default:	0
Possible values:	0 – Unknown 1 – International 2 – National 3 – Network-specific 4 – Subscriber number 5 – Alphanumeric

The number type used by the GSM client for the ToAddress property.

Truncate [DWORD]

Default:	0
Possible values:	0 – disable 1 – enable

by enabling (set to 1) this registry key only the first 160 characters of a SMS message will be sent. Further characters will be omitted.

Unicode [REG_DWORD] (GSM and SMPP)

Default:	0
Possible values:	0 – do not convert message to Unicode 1 – convert message to Unicode

This will set the SMS messages to be sent as Unicode for GSM and SMPP protocols.

UseDecimalIdForReports [REG_DWORD] (SMPP)

Default:	0
Possible values:	0 – Use hexadecimal format 1 – Use decimal format

The message centers use different formats for the Message Reference field. This value must be adjusted for using decimal format.

WindowSize [REG_DWORD]

Default:	1

This is the number of parallel send jobs that can be transferred to the provider without confirmation. Marking up this value may increase the performance but this is only permitted when explicitly allowed by the provider!

E.18 Entries of the SMTP APL

The following values can be found in the

HKLM\Software\Wow6432Node\PP-COM\MRS\SmtplAp1 key.

AuthIncoming [REG_DWORD]

Represents the configuration option **Use sender addresses to authorize gateway access** in the registry. See [Section 12.1.1.2, “E-Mail”, on page 899](#).

BindAddress [REG_SZ]

Represents the configuration option **Use BIND address** in the registry insofar that an entered IP address is stored here. The entry [UseBindAddress \[REG_DWORD\]](#) decides if it is used. See [Section 12.1.1.1, “General Settings”, on page 898](#).

Via the registry entries [Receive_BindAddress \[REG_SZ\]](#), [Pop3_BindAddress \[REG_SZ\]](#) and [Imap4_BindAddress \[REG_SZ\]](#) you can bind the single services SMTP server, POP3 server and IMAP4 server also to different IP addresses.

BuildCC [REG_DWORD]

Default:	0
Possible values:	0 – Do not create a cc field 1 – Create a cc field

If a message was sent to several recipients, a corresponding cc field with the other addressees is integrated in the SMTP header for the message to be sent. The recipient will then also see all addresses a copy was delivered to. Furthermore, he/she can write a reply to all.

DefaultSapUsers [REG_MULTI_SZ]

Default:	<Empty>
Possible values:	USER;domain

In case of an SAP connection you can specify here one XPR user ID for an SMTP domain per line. This determines the privileges and stationery for fax messages sent from SAP via the SMTP APL. For more information refer to the *SAP R/3 Gateway* manual.

DocReps [REG_SZ]

Default:	3-60,4-3000,0-0,0-0,0-0
Possible values:	<Number of transmission attempts>-<Interval in seconds>

Repeat Strategy. These parameters define how often and at which interval delivery attempts are to be made by the router. Delivery attempts are successively executed, whereby the first parameter is the number delivery

attempts to be made and the second parameter the time interval in seconds between delivery attempts. Up to five different repeat strategies can be indicated.

Default are 3 attempts in a 60 seconds interval, subsequently 4 additional attempts in a 3000 seconds interval (50 minutes).

DontRelay [REG_MULTI_SZ]

Default:	<Empty>
Possible values:	<Hostname> [':<Port>]

An Internet e-mail received by the XPR server cannot be forwarded to another internal sender if a relay host has been configured. Here you can enter an exception list for this case. In the list a <Hostname> can be entered per line that cannot be reached via the relay or is not to be sent to it directly. Here transmission is performed to all entered domains directly and not via the relay host.

Furthermore, the port used for transmission can optionally be entered for dedicated addresses here. The entry `domain.net:24` e.g. sends all messages to `domain.net` via the port 24.

ForceStartTLS [REG_DWORD]

Default:	0
Possible values:	0 – Allows unencrypted logging 1 – Enforce the connection via the 'STARTTLS'

Enabling this key will block unencrypted login and sending plain text mails to the XPR server by enforcing the connection via 'STARTTLS'.

HostName [REG_SZ]

Default:	Qualified host name of the XPR server.
Possible values:	Qualified host name or domain

Maps the **Hostname** configuration option in the registry. See [Section 12.1.1.1, “General Settings”, on page 898](#).

Imap4_BindAddress [REG_SZ]

Default:	<Empty>
Possible values:	[IP Address]

The IP address over which the IMAP4 server is to be connected. In most cases this is the TCP/IP address of the computer. In a multi-host system with numerous addresses, the desired address can be given. With this, the entry in [BindAddress \[REG_SZ\]](#) for the IMAP 4 server can be overwritten. However, it is also valid, if [BindAddress \[REG_SZ\]](#) is not set.

Imap4_Enable [REG_DWORD]

Represents the configuration option **Enable IMAP4 server** in the registry. See [Section 12.1.4, “IMAP4 Server”, on page 907](#).

Imap4_IgnoreCopy [REG_MULTI_SZ]

Represents the configuration option **Mailboxes that should not be copied automatically** in the registry. See [Section 12.1.4, “IMAP4 Server”, on page 907](#).

Imap4_JEntriesPerFetch [REG_DWORD]

Default:	64
Possible values:	<Number>

Number of the journal entries that are transmitted at once. In case of very large journals, composing the journal entries could cause a timeout, if they are collected first and then transmitted all at once. Through this, the transmission starts earlier and the timeout is avoided.

Imap4_MaxLogins [REG_DWORD]

Default:	8
Possible values:	<Number>

Maximum number of logins per user that may be executed at once. Practically all IMAP clients known at the moment execute e.g. one login per folder of the user, since this is the simplest way to retrieve the different folders in parallel.

Imap4_MaxMailboxes [REG_DWORD]

Default:	16
Possible values:	<Number>

Maximum number of folders, an IMAP user is allowed to create on the XPR server.

Imap4_maxPerIp [REG_DWORD]

Default:	0
Possible values:	0 – corresponds to (Imap4_nThreads / 2) >0 – individual setting

A client (IP address) can occupy by default only half of the maximum allocable IMAP connections to the XPR server. Further requests will be rejected.

Imap4_nThreads [REG_DWORD]

Represents the configuration option **Max. no. of concurrent connections** in the registry. See [Section 12.1.4, “IMAP4 Server”, on page 907](#).

Imap4_Outbox [REG_SZ]

Represents the configuration option **Folder for sent items** in the registry. See [Section 12.1.4, “IMAP4 Server”, on page 907](#).

Imap4_Port [REG_DWORD]

Default:	143
Possible values:	<IP Port>

Represents the configuration option **IMAP4 server port** in the registry. See [Section 12.1.4, “IMAP4 Server”, on page 907](#). The configuration dialog only displays this value whereas here you can change to another port.

Imap4_PortSSL [REG_DWORD]

Default:	993
Possible values:	<IP Port>

Here you can switch the TCP port on which the SMTP APL handles incoming IMAP 4 requests encrypted by SSL.

Imap4_PreLoginTimeout [REG_DWORD]

Default:	10
Possible values:	<Seconds>

After a connection to the IMAP port has been established, the XPR server waits for the login for this time and would otherwise cancel the connection. Without this timeout the timeout entered in [Imap4_Timeout \[REG_DWORD\]](#) would take effect and, in the normal case, the login would 666 seconds be waited for. Thus, this parameter improves the XPR server behavior in case of a denial of service attack considerably.

Imap4_Timeout [REG_DWORD]

Represents the **Client inactivity timeout** configuration option in the registry. See [Section 12.1.4, “IMAP4 Server”, on page 907](#).

Imap4_Trash [REG_SZ]

Default:	<Empty>
Possible values:	<IMAP folder>

Name of the IMAP4 folder in which deleted messages are stored.

Example: Trash

LogicalLineClass [REG_SZ]

Default:	<Empty> – Installed on the kernel computer <Systemindex> – Installed on satellite
Possible values:	<String>

Each SMTP APL logs in its logical trunks in the form `NVS:SMTP.<Class>`. The class corresponds to the computer's system index where the SMTP APL is running. So several SMTP APLs could be installed in a distributed system and these could be distinguished from the trunks logged in at the MTA via the class. Via this registry parameter an own <Class> for the trunks of this SMTP APL can be declared. If you want to install the SMTP APL on a computer several times, you need to enter something different here in order to be able to distinguish. For example `in` for one SMTP APL and `out` for the other.

This information is e.g. analyzed by the Web Assistant when the SMTP, POP3 and IMAP4 servers are displayed.

MxCacheMaxAge [REG_DWORD]

Default:	300
Possible values:	<Seconds>

Normally, the SMTP APL first fetches all MX entries for the destination domain for a send job. Afterwards, these computers would be tried one after another corresponding to their priority. The configured repeat strategy would be applied. If a lot of send jobs are to be transmitted to one domain at once, the SMTP APL remembers for the time set here, if e.g. the host with the highest priority is not available at the moment. Then it would no longer be considered for messages subsequently sent to this domain. Via this cache the following faulty behavior is avoided:

Company X has 3 MX entries: A with Prio 1, B with Prio 2, C with Prio 3.

Supposedly MX A is not available. For each transmission to company X the first attempt would be to reach A, after 60 seconds B would be tried. If you now address a distribution list with a lot of recipients of company X, the outbound mail traffic would practically be paralyzed, since transmission to A would be tried first and it takes some time to cancel this attempt.

Via this cache this time is wasted only in the first transmission attempt. All following ones lead immediately to successful transmission via the second working MX entry.

MxCacheMaxEntries [REG_DWORD]

Default:	512

Maximum number of entries in the cache of the MX entries. See [MxCacheMaxAge \[REG_DWORD\]](#).

MxCacheNumFailSkip [REG_DWORD]

Default:	5

Number of attempts an MX entry in the cache is not used after a failed attempt. See [MxCacheMaxAge \[REG_DWORD\]](#).

Netmap [REG_MULTI_SZ]

Represents the **Firewall** configuration option in the registry. See [Section 12.1.1.2, “E-Mail”, on page 899](#).

NoVpimSubject [REG_DWORD]

Default:	0
Possible values:	0 – Send spoken subject 1 – Do not send spoken subject

The VPIM specification allows for a message's subject to be sent as additional voice file. For the XPR this is in most cases a “Voice mail: 17 seconds”. You can disable this default behavior via this switch, so that in case of VPIM the subject is not transmitted.

PMI_NoDBLookup [REG_DWORD]

Default:	0
Possible values:	0 – Determine recipient from the SMTP database field 1 – Take recipient directly from header

The recipient can directly be taken from the message header and then be forwarded to the MTA. Thus further editing is possible via the routing rules.

PMI_NotifyPostmaster [REG_DWORD]

Default:	0
Possible values:	0 – No action 1 – Forward undeliverable messages to postmaster

Messages retrieved via POP3 mail import that cannot be delivered are forwarded to the postmaster account.

Pop3_BindAddress [REG_SZ]

Default:	<Empty>
Possible values:	[IP Address]

The IP address over which the POP3 server is to be connected. In most cases this is the TCP/IP address of the computer. In a multi-host system with numerous addresses, the desired address can be given. With this, the entry in [BindAddress \[REG_SZ\]](#) for the POP3 server can be overwritten. However, it is also valid, if [BindAddress \[REG_SZ\]](#) is not set.

Pop3_Enable [REG_DWORD]

Represents the configuration option **Enable POP3 server** in the registry. See [Section 12.1.3, “POP3 Server”, on page 905](#).

Pop3_maxPerIp [REG_DWORD]

Default:	0
Possible values:	0 – corresponds to (Pop3_nThreads / 2) >0 – individual setting

A client (IP address) can occupy by default only half of the maximum allocable POP connections to the XPR server. Further requests will be rejected.

Pop3_nThreads [REG_DWORD]

Maps the **Max. no. of concurrent connections** configuration option in the registry. See [Section 12.1.3, “POP3 Server”, on page 905](#).

Pop3_Port [REG_DWORD]

Default:	110
Possible values:	<IP Port>

Represents the configuration option **POP3 server port** in the registry. See [Section 12.1.3, “POP3 Server”, on page 905](#). The configuration dialog only displays this value whereas here you can change to another port.

Pop3_PortSSL [REG_DWORD]

Default:	995
Possible values:	<IP Port>

Here you can switch the TCP port on which the SMTP APL handles incoming POP3 requests encrypted by SSL.

Pop3_Timeout [REG_DWORD]

Represents the **Client inactivity timeout** configuration option in the registry. See [Section 12.1.3, “POP3 Server”, on page 905](#).

Pop3Delete [REG_SZ]

Default:	POPPER
Possible values:	POPPER or RECIPIENT

The XPR POP3 server marks messages retrieved via POP3 client with a specific deletion flag `DELETE_POPPER`. This flag provokes that these messages are not retrieved during the next request with a POP3 client. However, in other clients such as e.g. Communications these messages are still displayed as new messages.

If you change this registry value to `RECIPIENT`, the XPR server behavior is adapted. The “Deleted by recipient” flag is set and thus this message is no longer displayed in any other client.

In the user database this setting can be individually entered in the `POP-DELETEFLAG` field for each user, if a behavior differing from the default is desired for some users. This field then also has to be entered in the database and the entry mask has to be extended accordingly.

See also [LeaveMsgOnServer \[REG_DWORD\]](#).

Pop3FlgRead [REG_DWORD]

Represents the **Flag as read after retrieval** configuration option in the registry. See [Section 12.1.3, “POP3 Server”, on page 905](#).

Pop3Formats [REG_SZ]

Represents the configuration option of the **Formats** page in the registry. See [Section 12.1.6, “Formats”, on page 911](#).

Pop3MaxMsgs [REG_DWORD]

Represents the **Max. no. of messages per poll** configuration option in the registry. See [Section 12.1.3, “POP3 Server”, on page 905](#).

Pop3MaxSize [REG_DWORD]

Represents the **Maximum messages size** configuration option in the registry. See [Section 12.1.3, “POP3 Server”, on page 905](#).

Pop3NonStdTo [REG_SZ]

Default:	<Empty>
Possible values:	<SMTP Header field>

You can enter a keyword in this field that is used like `TO` (recipient), `CC` (Carbon Copy; recipient of a copy) or `BCC` (Blind Carbon Copy; recipient of a copy the other recipients do not know of). This is then used for POP3 mail import.

Please note that the other delivery fields are skipped if this keyword exists in the message header. A message that is to be sent to several recipients is thus only delivered to the recipient entered in this specific field. This measure is required, since a message would otherwise be delivered more than once to the same recipient.

Example: `X-RCPT-TO`

Pop3PollType [REG_DWORD]

Default:	0
Possible values:	0 – Default, as explained below 1 – Mail import individual for each user 2 – Mail import for entire domains/user groups

XPR checks for the account for which the POP3 mail import is executed, whether it has an entry in the `GROUP` field of the user database. If yes, this account is considered a user for who the retrieved messages are intended. If no, the account is considered a pseudo account where the incoming messages still need to be delivered to the correct recipient. Via this entry this behavior can be explicitly controlled.

Receive_AllowRelay [REG_MULTI_SZ]

Represents the **Trusted Domains** configuration option in the registry. See [Section 12.1.1.2, “E-Mail”, on page 899](#).

Receive_AutoLearn [REG_DWORD]

Represents the **Autolearn names of senders in user database** configuration option in the registry. See [Section 12.1.1.2, “E-Mail”, on page 899](#).

Receive_BindAddress [REG_SZ]

Default:	<Empty>
Possible values:	[IP Address]

The IP address over which the SMTP server is to be connected. In most cases this is the TCP/IP address of the computer. In a multi-host system with numerous addresses, the desired address can be given. With this, the specification in [BindAddress \[REG_SZ\]](#) can be overwritten for the SMTP server. However, it is also valid, if [BindAddress \[REG_SZ\]](#) is not set.

Receive_CheckUserExist [REG_DWORD]

Default:	0
Possible values:	0 – No action 1 – Check recipient addresses for existence

If this switch is enabled, the SMTP APL checks already before the reception whether the recipient exists in the XPR user database and rejects the reception otherwise.

This can cause the following problem: The SMTP APL checks the properties of the `SMTP` field in the user database. If the attribute of this field is `LOWER`, the addresses of the incoming mails are normed to lower case and then compared to the `SMTP` field.

If the field has neither a `LOWER` nor an `UPPER` attribute and the `SMTP` field contains the user's mail address e.g. in lower case and the originator wrote everything in upper case or both in upper and lower case, the message is rejected by the SMTP APL.

Thus one of the attributes should be added to the `SMTP` field in the user database, if you would like to use this feature.

Receive_Enable [REG_DWORD]

Represents the **Enable inbound mail** configuration option in the registry. See [Section 12.1.1.2, “E-Mail”, on page 899](#).

Receive_EnableVRFY [REG_DWORD]

Default:	0
Possible values:	0 – VRFY inactive 1 – VRFY active

The SMTP command VRFY can be enabled, so that the users of the XPR server can be retrieved. Since this is normally considered as security problem, this command is normally not available and is answered with the message “502 VRFY not implemented”.

Receive_ESMTP_Capabilities [REG_MULTI_SZ]

Default:	<Empty>
Possible values:	8BITMIME AUTH DSN SIZE STARTTLS

Normally, all ESMTP features supported by the SMTP APL are indicated during the connection setup. By explicit indications this declaration can be restricted to the ones entered here during the connection setup. One feature is specified per line.

Different switches are represented on the interface. On the one hand the configuration option **Activate ESMTP**. See [Section 12.1.1.1, “General Settings”, on page 898](#). This option activates or disables ESMTP. If you want to deactivate single ESMTP features, the switch must be active and the unwanted features must not be listed here.

Via the AUTH token the **Enable client authorization** configuration option is mapped in the registry. See [Section 12.1.1.2, “E-Mail”, on page 899](#). This function also depends on the **Activate ESMTP** option.

Receive_LocalHosts [REG_MULTI_SZ]

Represents the **Local Domains** configuration option in the registry. See [Section 12.1.1.2, “E-Mail”, on page 899](#).

Receive_MaxNotAuthAttempts [REG_DWORD]

Default:	3

If more than the number of not-allowed attempts entered here are executed during a connection, the connection is canceled. SPAM senders sometimes attempt to find out valid addresses simply by trial and error. Through this, they must often re-establish the connection, which complicates collecting addresses.

Receive_maxPerIp [REG_DWORD]

Default:	0
Possible values:	0 – corresponds to (Receive_nThreads / 2) >0 – individual setting

A client IP address can occupy by default only half of the maximum allocable SMTP connections to the XPR server. Further requests will be rejected.

Receive_MaxSize [REG_DWORD]

Default:	0
Possible values:	0 – No restriction <Bytes> – Maximum message size

If this value is not 0, the size of the message to be received is queried. If the value specified here is exceeded, receiving will be rejected.

Receive_nThreads [REG_DWORD]

Represents the **Max. no. of concurrent inbound connections** configuration option in the registry. See [Section 12.1.1.2, “E-Mail”, on page 899](#).

Receive_Port [REG_DWORD]

Represents the **SMTP port** configuration option in the registry. See [Section 12.1.1.1, “General Settings”, on page 898](#).

Receive_Separator [REG_SZ]

Default:	;

This entry applies to the option for modifying SMTP addresses to configure a fax cover page. For this reason you can enter information to this effect in the comment part of an SMTP address:

FAXG3/123456 (\$FAXSTATIONARY=XXX; \$dbo (NAME) =Mister) @mrssrv

According to RFC 822 a comment is structured as follows:

comment = "(" *(ctext / quoted-pair / comment) ")"

ctext = <any CHAR excluding "(", ")", "\", & CR, & including linear-white-space>

CHAR = <any ASCII character>

Thus the default ';' is a legal character to separate the XPR information within this comment. Since the Internet Mail Connector (IMC) cuts off Microsoft Exchange addresses after a ';', you need to use another separator for messages running via this connector. This can be set here. We do not recommend ',' as separator, since then problems with addresses of the type ...(\$dbo(NAME)=User, Rainer)... would occur. Alternatively, we recommend a character such as '|'.

Receive_Timeout [REG_DWORD]

Represents the **Inactivity timeout for mail receipt** configuration option in the registry. See [Section 12.1.1.2, "E-Mail", on page 899](#).

Receive_UseFrom [REG_DWORD]

Default:	0
Possible values:	0 – Take originator address from the MAIL FROM field 1 – Take originator address from the FROM field

By default, the address in the MAIL FROM field is used as originator of a received message. For larger customers, sometimes the following is contained in the header of the mail:

```
MAIL FROM: <Hostname_of_the_Originator@domain.org>
DATA
From: "User Name" <user@domain.org>
```

Alternatively, the address from the FROM field can be used, so that a correct user authentication can be realized and reports about possible non-transmission will arrive at the originator's.

ReceivedForDepth [REG_DWORD]

Default:	1
Possible values:	1 to 10

Search depth for recipient addresses in combination with the [UseReceivedFor \[REG_DWORD\]](#) option.

ReducedLineName [REG_DWORD]

Default:	0
Possible values:	0 – Register logical line with class 1 – Register logical line without class

Owing to the database structure, the length of SMTP addresses is in case of the XPR server restricted to 63 characters. This includes the logical line NVS:SMTP.0/, so that actually only 52 characters can be used for an SMTP address. This value enables omitting the class when registering the logical line with the MTA: NVS:SMTP/. This saves two lines, so that 54 characters are available then.

The restriction to a maximum of 54 characters thus also refers to the length of the Connect Server FQDN.

RelayAllowedSecs [REG_DWORD]

Default:	0
Possible values:	0 – No receiving restriction <Seconds> – SMTP after POP

With a 0, everyone can send messages via the SMTP APL who is allowed to via relaying. In many cases relaying is disabled for practically all TCP/IP addresses. To allow users connected to the server by IMAP or POP the message transmission, you can enter a period here. Within this period these users may send messages by IMAP or POP via the SMTP server after a corresponding login. This feature is also known under the name SMTP after POP.

RelayHost [REG_SZ]

Represents the **Send mail via relay host** configuration option in the registry. See [Section 12.1.2, “Outgoing E-mail”, on page 903](#).

ReportReps [REG_SZ]

Default:	2-60,4-180,0-0,0-0,0-0
Possible values:	<Number of transmission attempts>-<Interval in seconds>

Repeat dialing strategy for reports. These parameters define how often and at which interval delivery attempts are to be made by the router. Delivery attempts are successively executed, whereby the first parameter is the number delivery attempts to be made and the second parameter the time interval in seconds between delivery attempts. Up to five different repeat strategies can be indicated. Via this value you can set several attempts for the various report types such as e.g. Non Delivery Reports (NDR).

Default are 2 attempts in a 60 seconds interval, subsequently 4 additional attempts in a 180 seconds interval (3 minutes).

SAP_Enable [REG_DWORD]

Default:	1
Possible values:	0 – SMTP gateway to SAP R/3 not active. 1 – SMTP gateway to SAP R/3 active.

Activates the SMTP gateway for fax and SMS to SAP R/3. For more information refer to the *SAP R/3 Gateway* manual.

Send_AuthMethods [REG_MULTI_SZ]

Default:	<Empty>
Possible values:	CRAM-MD5 LOGIN PLAIN

Normally, all authentication methods supported by the SMTP APL are indicated during the connection setup. By explicit indications this declaration can be restricted to the ones entered here during the connection setup. One method is entered in each line. See also [Section 12.2.1.2, “Authentication according to RFC 2554”](#), on page 916.

Send_MaxOut [REG_DWORD]

Maps the **Max. no. of concurrent connections** configuration option in the registry. See [Section 12.1.2, “Outgoing E-mail”](#), on page 903.

Send_Ras [REG_SZ]

Represents the **Send mail by schedule** configuration option in the registry. See [Section 12.1.2, “Outgoing E-mail”](#), on page 903.

Send_RequireSSL [REG_MULTI_SZ]

Default:	<Empty>
Possible values:	<Host name> : <Keystrength>

List of servers, to which transmission is only possible via a connection secured with SSL/TLS. Thus no one can pass off as the server, if he does not possess the respective SSL certificate. The servers entered here are also checked, whether the host name corresponds to the entered host name. The <Key strength> entry is optional.

Two possible attacks to a secure connection where this measure would come into effect could be:

- If the STARTTLS command that is exchanged between the servers was intercepted and a secure connection would thus not be accomplished. In this case the setup of a non-secure connection would be rejected if the counterpart is not listed here.
- If the MX entry points at a host other than the recipient SMTP server, an unsecured connection would not be established either.

Example: `host.company.com:1024`

SendFormats [REG_SZ]

Maps the configuration option **Fax** and **Voicemail Formats** in the registry. See [Section 12.1.2, “Outgoing E-mail”](#), on page 903.

SendTest_Data [REG_BINARY]

For internal use only.

SendTimeout [REG_DWORD]

Represents the **Inactivity timeout** configuration option in the registry. See [Section 12.1.2, “Outgoing E-mail”, on page 903](#).

SSL_CertificateFile [REG_SZ]

Maps the configuration option **Certificate file** in the registry. See [Section 12.1.5, “Secure Sockets”, on page 909](#).

SSL_Enable [REG_DWORD]

Maps the configuration option **Enable Secure Sockets** in the registry. See [Section 12.1.5, “Secure Sockets”, on page 909](#).

SSL_PassPhrase [REG_SZ]

Represents the **Passphrase for private key** configuration option in the registry. The password is entered here encrypted so that at any rate it must be specified via the configuration from within the XPR monitor. See [Section 12.1.5, “Secure Sockets”, on page 909](#).

SSL_PrivateKeyFile [REG_SZ]

Maps the configuration option **Private key file** in the registry. See [Section 12.1.5, “Secure Sockets”, on page 909](#).

SSL_TLSv1_Enable [REG_DWORD]

Default:	0
Possible values:	0: TLS 1.0 protocol disabled 1: TLS 1.0 protocol enabled

to full security both SSL_CBC_Enable and SSL_TLSv1_Enable must be set to 0.

By default TLSv1.2 is enabled.

SSL_TLSv1_1_Enable [REG_DWORD]

Default:	0
Possible values:	0: TLS 1.1 protocol disabled 1: TLS 1.1 protocol enabled

Used to disable TLS 1.1 on WebApl
This configuration does not affect outgoing connections.

By default TLSv1.2 is enabled.

SSL_TrustedCaFile [REG_SZ]

Represents the configuration option **Trusted certificates list** in the registry. See [Section 12.1.5, “Secure Sockets”, on page 909](#).

SSL_VerifyClientCert [REG_DWORD]

Represents the **Verify client certificates** configuration option in the registry.
See [Section 12.1.5, “Secure Sockets”, on page 909](#).

SSL_VerifyServerCert [REG_DWORD]

Represents the **Verify server certificates** configuration option in the registry.
See [Section 12.1.5, “Secure Sockets”, on page 909](#).

UseBindAddress [REG_DWORD]

Maps the **Use Bind address** configuration option in the registry insofar as it is decided here whether an IP address that is entered in [BindAddress \[REG_SZ\]](#) is used. See [Section 12.1.1.1, “General Settings”, on page 898](#).

UseReceivedFor [REG_DWORD]

Default:	0
Possible values:	0 – Default 1 – Use <code>For</code> field from “Received” header as recipient address

For POP3 mail import you can use the `For` field from the “Received” header as recipient address. This option has been desired by a customer. It was thus possible for him/her to avoid the faulty provider configuration. The first `For` entry in the header is normally the one searched for. This was, however, not the case with a provider. You can therefore use the registry value [ReceivedForDepth \[REG_DWORD\]](#) to default a search depth, so that e.g. the first three `For` entries of the header are checked for a valid recipient address.

VPIM_Enable [REG_DWORD]

Default:	1
Possible values:	0 – VPIM disabled 1 – VPIM active

Switch VPIM protocol on or off.

E.18.1 POP3 Mail Import Time Schedules

Under the key `Smtpl\PopSchedules` an additional key with the schedule name is specified for each defined schedule. In these keys the following values can be found:

LeaveMsgOnServer [REG_DWORD]

Default:	0
Possible values:	0 – Delete messages at the provider 1 – Do not delete messages at the provider

If you retrieve messages via POP3 mail import, you can configure via this switch if they are to be deleted at the provider or if the messages are still to be stored on the provider server. See also [Pop3Delete \[REG_SZ\]](#).

PhoneBookEntry [REG_SZ]

The **Name** from the RAS address book.

PollEveryNMinutes [REG_DWORD]

Default:	<Empty>
Possible values:	1... <Minutes>

Via the configuration in the XPR monitor always only 15-minute intervals can be set, with polling at the beginning of the set period. If this registry value is added, the polling rate can be controlled within the range of minutes.

Within a 15-minute interval set by XPR monitor, polling occurs at the beginning of this period and subsequently all n minutes. n corresponds to the value set here.

Consecutive periods forming a larger active period are considered one period, thus for example with 10 minutes set here polling occurs at the beginning of this period and then every 10 minutes.

RasPassword [REG_SZ]

The encryptedly stored RAS password.

TimeSched [REG_BINARY]

The schedule in binary format. The specific editor in the SMTP APL configuration is to be used via the XPR monitor. See [Section 12.1.7.3, “Active Schedules”](#), on page 913.

WaitDisconnect [REG_DWORD]

Default:	0
Possible values:	0 – clear RAS connection immediately. 1 – do not clear RAS connection.

Maps the configuration options **Disconnect immediately after sending and receiving new mail** and **Wait until RAS phone book idle time has expired before disconnecting** in the registry. See [Section 12.1.7.3, “Active Schedules”](#), on page 913.

E.19 Entries of the TCP/IP APL

E.19.1 Firewall

The following values can be found in the key `TcpApl\Firewall`.

Netmap [REG_MULTI_SZ]

Represents the **Firewall** configuration option in the registry. See [Section 15.2, “Firewall Mechanism”, on page 1028](#).

E.19.2 Line

The following values can be found in the key `TcpApl\Line`.

HighWaterThreshold [REG_DWORD]

Default:	85 Percent
Possible values:	50 ... 100 Percent

When this value is reached, the SMI queue sets all outgoing lines to busy till the value given in [LowWaterThreshold \[REG_DWORD\]](#) falls below. During this time no further data are sent to the transport. The percent value refers to the value [SmiQueueSize \[REG_DWORD\]](#).

LowWaterThreshold [REG_DWORD]

Default:	45 Percent
Possible values:	0...90 Percent

See [HighWaterThreshold \[REG_DWORD\]](#).

ShortholdTime [REG_DWORD]

Default:	60 Seconds
Possible values:	15...3600

Connection time-out. If no data are transferred within the time entered here, a disconnect will be initiated.

SmiQueueSize [REG_DWORD]

Default:	512
Possible values:	256...2048

Number of SMI jobs that can be queued. The values [LowWaterThreshold \[REG_DWORD\]](#) and [HighWaterThreshold \[REG_DWORD\]](#) refer to this number.

E.19.3 Line Admin

The following values can be found in the key `TcpApl\LineAdmin`.

ShowSubLineInfo [REG_DWORD]

Default:	0
Possible values:	0 – Do not show sublines 1 – Show sublines

Determines whether individual connections are displayed below the TCP/IP Line Information in the XPR monitor. Entries are *ignored* after the 256th line, as well as sub-line entries. This is done to reduce XPR monitor workload.

IMPORTANT:

This feature should not be activated in a production system, since the XMR service increases the server load significantly.

E.19.4 NwPlugTcp

The following values can be found in the key `TcpApl\NwPlugTcp`.

BindAddress [REG_SZ]

Default:	0.0.0.0
Possible values:	IP address

If the XPR server has several network cards or IP addresses, we suggest that the TCP/IP APL be bound to a single IP address. If the computer has, for example, the IP address 192.168.9.44 (primary) and 194.77.158.10 (secondary), the TCP/IP APL would be bound to the primary IP address, since this represents the default IP address. Clients from the 194.77.158 network would not be able to log in to the server. In this example the BindAddress would be set to 194.77.158.10.

A warning is generated by the TCP/IP APL at booting when a BindAddress is specified that does not exist on the computer. In this case there is *no* fall-back on the default IP address. The entry 0.0.0.0 corresponds to the default IP address of the computer.

IoPort [REG_DWORD]

Default:	8944
Possible values:	<IP Port>

The server monitors the TCP/IP socket for connection requests. This value should never be modified since clients already configured would not be able to find or establish a connection to the server.

TunPort [REG_DWORD]

Default:	8945
Possible values:	<IP Port>

If the MSP was set to encrypted connections, it previously consults the TCP/IP APL which port to use. The port set here is then returned and the connection established via the STunnel program.

If you modify this port here, you need to change the “List” port for STunnel as well. For this purpose, adjust the corresponding port number for `accept = 8945` in the `<XPR Install>\bin\stunnel\stunnel.conf` file.

The certificate required for the SSL connection is automatically created with the TCP/IP APL installation and also stored in the `<XPR Install>\bin\stunnel` directory.

E.20 Registry Keys of the Telematics APLs

The telematics APLs use the TeleReg API for the registry administration (c.f. [Section 10.1.1, “Telematics Program Libraries”, on page 526](#)). This API provides functions that administer various information of the different Telematic APLs. Possible dependencies are automatically checked.

IMPORTANT:

All entries administered by the TeleReg API should only be modified through the appropriate module in the XPR monitor. If you do not proceed like this, the modifications performed might be overwritten by the configuration module, since it caches all entries and checks for consistency.

The registry values in this chapter are structured in the following format:

- [Registry Keys of the TeleReg](#)
- [ISDN APL Registry Keys](#)
- [IP APL Registry Keys](#)

E.20.1 Registry Keys of the TeleReg

This section describes the registry values of the TeleReg. The information is structured in the following manner:

- [General Entries](#)
- [Blobs \(Binary Large Objects\)](#)
- [Devices](#)
- [Trunk Groups](#)
- [Extension number ranges](#)
- [Protocols](#)

E.20.1.1 General Entries

The following general registry values of the different APLs can be found under the

HKLM\Software\Wow6432Node\PP-COM\MRS\<APL>

key.

BuiltInDtmf [REG_DWORD]

Default:	0
Possible values:	APL-dependent

Defines in which manner the DTMF recognition occurs.

CfgCompress [REG_DWORD]

Default:	1
Possible values:	0 – Uncompressed data transmission 1 – Compressed data transmission 2 – Compressed data transmission with data verification

Defines how the transmission of configuration data between the APL and the XPR monitor is performed.

Transmission of configuration data can be compressed or uncompressed. Furthermore, it is possible to activate a text mode. This mode decompresses the compressed data before transmission to check the correctness of the data compressing.

Checked<n> [REG_DWORD]

Default:	APL-dependent
Possible values:	0 – Deactivates the respective option 1 – Activates the respective option
Remark:	In connection with <i>CheckName<n></i> [REG_SZ].

The TeleReg-API provides four tuples [(Checked<1>, CheckName<1>) ... (Checked<4>, CheckName<4>)] for self-defined use by the respective APL. Each of these tuples realizes a logical switch. Its switch name is administered in CheckName<n> and the corresponding state of activation in Checked<n>.

By use of the APL a respective check box is displayed in the configuration dialog with the name indicated by the APL. For Checked<n>=1 this check box is selected.

CheckName<n> [REG_SZ]

Default:	<APL-specific services>
Possible values:	<APL-specific services>
Remark:	In connection with <i>Checked<n></i> [REG_DWORD].

The TeleReg API provides four tuples of the format [(Checked<1>, CheckName<1>) ... (Checked<4>, CheckName<4>)]. Their use can be defined by the using APL itself.

CliMode [REG_DWORD]

Default:	2
Possible values:	0 – Transmission of the normalized phone number 1 – Transmission of the extension 2 – Transmission of the information from the database field CostInfo 3 – No transmission

Defines which information is transmitted as calling line identification (CLI) by the XPR server to the connected PBX. The following three options exist:

- Transmission of the normalized international phone number of the respective user.
- Transmission of a user-specific value that is stored in the **CostInfo** field of the XPR user database.
- Transmission of the extension of the respective user, if no entry has been made in the **CostInfo** field.
- No CLI transmission.

Cost [REG_DWORD]

Default:	12
Possible values:	<Number> [1/100 of the local currency]

Defines the amount of a billing pulse in 1/100 of the local currency.

DestNumberPlan [REG_DWORD]

Default:	0x00
Possible values:	0x00 – Unknown number plan 0x01 – ISDN number plan (E.164) 0x02 – Number plan (E.163) 0x03 – Data number plan (according to X.121 [21]) 0x04 – Telex number plan (according to F.69 [22]) 0x08 – National standard number plan 0x09 – Private number plan

Defines the numbering plan of the target number via a seven-digit bitmask.

DestNumberType [REG_DWORD]

Default:	0
Possible values:	0 – Complete phone number transmission ('en-bloc') 1 – International phone number 2 – National phone number 4 – Local (Directory) number plan 5 – Continuous phone number transmission ('overlap')

Internal setting for testing the ISDN and PBX connection.

FaxLicences [REG_DWORD]

Default:	<Number of licensed fax channels>
Possible values:	<Number of licensed fax channels>
Remark:	No modification allowed

Defines the number of the allowed fax channels.

This value is preset by the licenses you purchased. Modifications cause an error message because of license infractions.

FaxResources [REG_DWORD]

Default:	<Number of detected fax channels>
Possible values:	<Number of detected fax channels>

Defines the number of fax channels found by the hardware detection.

LineLicences [REG_DWORD]

Default:	<Number of licensed lines>
Possible values:	<Number of licensed lines>
Remark:	No modification allowed

Defines the number of the allowed lines.

This value is preset by the licenses you purchased. Modifications cause an error message because of license infractions.

LineResources [REG_DWORD]

Default:	<Number of detected lines>
Possible values:	<Number of detected lines>

Defines the number of lines found by the hardware detection.

An S₀ bus corresponds to two lines for instance.

OrigNumberPlan [REG_DWORD]

Default:	0x00
Possible values:	0x00 – Unknown number plan 0x01 – ISDN number plan (E.164) 0x02 – Number plan (E.163) 0x03 – Data number plan (according to X.121 [21]) 0x04 – Telex number plan (according to F.69 [22]) 0x08 – National standard number plan 0x09 – Private number plan

Defines the numbering plan of the originator number via a seven-digit bitmask.

OrigNumberType [REG_DWORD]

Default:	0
Possible values:	0 – Complete phone number transmission ('en-bloc') 1 – International phone number 2 – National phone number 4 – Local (Directory) number plan 5 – Continuous phone number transmission ('overlap')

Internal setting for testing the ISDN and PBX connection.

QueryBilling [REG_DWORD]

Default:	1
Possible values:	0 – Deactivates billing 1 – Activates billing

Defines whether billing is activated.

If billing is deactivated, no charges are displayed, even in the case of outgoing calls through the public exchange.

SupportedDevices [REG_MULTI_SZ]

Default:	APL-dependent
Possible values:	<Device names>

Defines which device names are displayed in the configuration dialog of the respective APL.

VoiceLicences [REG_DWORD]

Default:	<Number of licensed voice channels>
Possible values:	<Number of licensed voice channels>
Remark:	No modification allowed

Defines the number of allowed Full Duplex voice channels. Modifications cause an error message because of license infractions.

VoiceResources [REG_DWORD]

Default:	<Number of detected voice channels>
Possible values:	<Number of detected voice channels>

Defines the number of voice resources (Full Duplex voice channels) found via hardware detection.

E.20.1.2 Blobs (Binary Large Objects)

Every registry entry administered by the TeleReg API may contain a reference to a Blob. Blobs are binary data ranges in which programmer-defined data may be stored.

Used blobs can be found in the registry under the following key:

HKLM\Software\Wow6432Node\PP-COM\MRS\<APL>\Blobs

E.20.1.3 Devices

A device corresponds to the physical interface of an interface board (ISDN APL) or a configured TAPI driver (IP APL) of the XPR server system. In case of a physical interface the device is composed of a defined number of logical communication channels. E.g. an S0 interface consists of 2 logically separated channels or an S2M interface consists of up to 30.

For each of these devices a consecutively numbered key n exists under the

HKLM\Software\Wow6432Node\PP-COM\MRS\<APL>\Devices

key. These contain respectively the following registry values that describe the properties of the individual physical interfaces.

AddDialOutLen [REG_DWORD]

Default:	0
Possible values:	<Number of digits>

Defines the number of digits that are added to the dialing string for outgoing calls.

If, for example, a PBX system has two tie lines 82 and 83, then a call from 8247 to 8311 is simply transferred locally within the PBX and not through the public exchange. Some PBXs are not capable of this and must transfer the call via public exchange in such a case. This number of digits is then added.

Blob [REG_DWORD]

Default:	0
Possible values:	<Data range index>

Defines the index number of the used blob data range.

Caps [REG_DWORD]

Default:	Device-dependent
Possible values:	<Bit mask>

Defines the capabilities of the respective device.

Each device administered by the TeleReg API has certain capabilities. These are listed as bit masks with the appropriate capability:

0x0001: Device masters speech.

0x0002: Device can recognize DTMF tones.

0x0004: Device can send and receive Fax G3 documents.

0x0008: Device can poll documents from a fax-on-demand server.

0x0010: Device may act as fax-on-demand server.

0x0020: Device can send and receive Fax G4 documents.

0x0040: Device can poll documents from a Fax G4 fax-on-demand server.
(Protocol does not exist yet, hence not defined for G4.)

0x0080: Device can act as Fax G4 fax-on-demand server.
(Protocol does not exist yet, hence not defined for G4.)

0x0100: Device masters Euro-Filetransfer transmissions.

0x0200: Device masters teletext transmissions.

0x0400: Device can transmit raw data.

0x0800: Device masters MWI.

Channels [REG_DWORD]

Default:	Device-dependent
Possible values:	<Number of physical channels>

Defines the number of physical channels of the relevant device.

Example: S_{2m} corresponds to 30.

Description [REG_SZ]

Default:	<Empty string>
Possible values:	<Device description>

Defines an optional description of the relevant device.

FaxG3 [REG_DWORD]

Default:	Device-dependent
Possible values:	<Number of Fax G3 lines>

Defines the number of Fax G3 lines of the relevant device.

Handle [REG_DWORD]

Default:	<Handle>
Possible values:	<Handle>
Remark:	No modification allowed

Defines the internal handling of the relevant device.

Lines [REG_DWORD]

Default:	Device-dependent
Possible values:	<Device name>

Defines the number of lines supported by the relevant device.

Example: An S₀-Bus includes 2 lines.

Name [REG_DWORD]

Default:	Device-dependent
Possible values:	<Device name>

Defines the device name that is also used for the XPR monitor display.

Example: D/300SC-E1

PrefixedAni [REG_DWORD]

Default:	0
Possible values:	0 – ANI transmission with external line prefix 1 – ANI transmission without external line prefix

Defines whether the own phone number (Automatic Number Identification - ANI) is used with the prefixed digit for outside dialing from the device. This form is used e.g. for a uniform acquisition of billing data.

Private [REG_MULTI_SZ]

Default:	Device-dependent
Possible values:	<Initialization entry per line>

Defines APL-specific configuration data. One specific entry is made per line in the form *Label*>=<Value>. <Label> determines the respective setting name and <Value> the desired content of the respective setting.

PrivateMode [REG_DWORD]

Remark:	APL-dependent

State [REG_DWORD]

Default:	Device-dependent
Possible values:	<Bit mask>

Defines the state of the relevant device.

Every entry in the registry administered by the TeleReg API has a “state”. These entries are in the form of a bitmask and with the following bit settings that can be combined:

0x01: Activates the device.

0x02: The device must still be updated in the registry.
(This bit is used internally only.)

0x04: The device is removed from the registry, if the bit 0x08 is not set additionally.

0x08: The device remains always in the registry, even if it is not active and has been flagged as deleted by a configuration module.
(This bit is used by certain standard protocols e.g. Fax G3.)

0x10: The device is already available in the registry.
(This bit is internally used by a configuration module so that it does not recreate the entry completely but modifies it if required.)

Type [REG_DWORD]

Default:	Device-dependent
Possible values:	0 – S2m device (Primary Rate Interface – PRI) 1 – S0 device (Basic Rate Interface – BRI) 2 – Analog device 3 – Unknown device

Defines the type of the respective device.

E.20.1.4 Trunk Groups

A trunk group describes the summary of several ¹ logical, bidirectional communication channels of a single device. Only channels of a coherent section can be summed up to one trunk group.

Each single trunk group is assigned one of the configured protocols.

For each trunk group a consecutively numbered key *m* exists under the

HKLM\Software\Wow6432Node\PP-COM\MRS\<APL>\Devices\ *n*

key of the associated device. In this key you find the following values that define all properties of the relevant trunk group.

BaudRate [REG_DWORD]

Default:	0
Possible values:	<Baudrate>

Defines the transmission rate of the respective logical line. This way certain lines can be prioritized in the MTA.

Blob [REG_DWORD]

Default:	0
Possible values:	<Index of the data range>

Index number of the Blob data range.

BoundProtocols [REG_DWORD]

Default:	0
Possible values:	<Bit mask>

Specifies a bit mask that defines the protocols supported on the relevant line. 32 protocols per bit mask are supported. Consequently, four of these bit masks are required for the maximum of 128 supported protocols. The values **BoundProtocols**, **BoundProtocols1**, **BoundProtocols2** and **BoundProtocols3** serve this purpose. All supported protocols are listed by the TeleReg API as enumerated entry *n* under the key
HKLM\Software\PP-COM\MRS\<APL>\Protocols.

Bit 0x1 corresponds to the first listed protocol with the key 01, 0x2 to the second, 0x4 to the third etc. If 7 protocols are available and all protocols of a line are supported, **BoundProtocols** would have value 0x7f.

1. In extreme cases such a trunk group can include only one communication channel.

BoundProtocols1 [REG_DWORD]

Default:	0
Possible values:	<Bit mask>

See [BoundProtocols \[REG_DWORD\]](#).

BoundProtocols2 [REG_DWORD]

Default:	0
Possible values:	<Bit mask>

See [BoundProtocols \[REG_DWORD\]](#).

BoundProtocols3 [REG_DWORD]

Default:	0
Possible values:	<Bit mask>

See [BoundProtocols \[REG_DWORD\]](#).

Cost [REG_DWORD]

Default:	0
Possible values:	<Charges>

Defines the amount for a line-specific billing pulse in $\frac{1}{100}$ of the local currency.

An entry made here overwrites the value entered globally under General Settings ([Cost \[REG_DWORD\]](#)) for the relevant line.

EndChannel [REG_DWORD]

Default:	Device-dependent
Possible values:	<Channel number>
Remark:	In connection with StartChannel [REG_DWORD] .

Defines the physical channel last used, if only a part of the physically existing channels is used.

NumChannels [REG_DWORD]

Default:	Device-dependent
Possible values:	<Channel number>

Specifies the number of channels that the relevant line is to use at the most.

OAD [REG_DWORD]

Default:	0
Possible values:	<Index number>

Defines the index number of the originator address (OAD) belonging to the respective line.

The TeleReg API administers all available OAD numbers as consecutively numbered key n under the key:

HKLM\Software\Wow6432Node\PP-COM\MRS\<APL>\OADs.

The entry made under **OAD [REG_DWORD]** serves as reference to the key number to be used for the respective line. If no index number is indicated, the OAD with the lowest index number would be used.

PermMask [REG_DWORD]

Default:	0
Possible values:	0 – No restrictions. 1 – Allow only inbound calls. 2 – Allow only outbound calls. 3 – Allow inbound and outbound calls.

Defines restrictions for the respective line concerning inbound and outbound calls.

StartChannel [REG_DWORD]

Default:	1
Possible values:	<Channel number>
Remark:	In connection with EndChannel [REG_DWORD] .

Defines the physical channel first used, if only a part of the physically existing channels is used.

State [REG_DWORD]

Default:	Device-dependent
Possible values:	<Bit mask> (see description)

Defines the status of the respective line.

Every entry in the registry administered by the TeleReg API has a “state”. These entries are in the form of a bitmask and with the following bit settings that can be combined:

0x01: Activates the relevant line.

0x02: The relevant line must still be updated in the registry.

(This bit is used by an internal configurations module only.)

- 0x04: The relevant line is removed from the registry, if the bit 0x08 is not set additionally.
- 0x08: The relevant line remains always in the registry, even if it is not active and has been marked as deleted by a configuration module.
(This bit is used by certain standard protocols e.g. Fax G3.)
- 0x10: The relevant line already exists in the registry.
(This bit is internally used by a configuration module so that it does not recreate the entry completely but modifies it if required.)

E.20.1.5 Extension number ranges

Each phone number dialed in the XPR server must be within the range indicated here with its extension, so that the incoming call can be accepted by the respective APL.

If the board delivers an ISDN Service Indicator it will be checked against a list of applicable protocols.

The following registry values are found under the

HKLM\Software\Wow6432Node\PP-COM\MRS\<APL>\Extensions

key.

EnableRegSz [REG_DWORD]

Default:	1
Possible values:	0 – START/END in the format REG_DWORD. 1 – START/END in the format REG_SZ.
Remark:	Only change for compatibility reasons.

Defines whether the values of the registry keys **Start [REG_SZ]** and **End [REG_SZ]** of the extension ranges in the format REG_SZ or REG_DWORD are written the registry.

The **REG_DWORD** option is only implemented for compatibility reasons. Normally the setting **1 (REG_SZ)** should be used. Thus, also extension number ranges with leading zeros would be possible.

For each supported service normally one extension number range must be configured. All configured ranges are numbered ascendingly and stored as a separate key with their respective number under the key

HKLM\Software\Wow6432Node\PP-COM\MRS\<APL>\Extensions

as a separate key. In each of these keys the following values are found.

Blob [REG_DWORD]

Default:	0
Possible values:	<Index of the data range>

Index number of the Blob data range.

Description [REG_DWORD]

Default:	<Empty string>
Possible values:	<Description>

Defines a description of the respective extension number range.

End [REG_SZ]

Default:	999
Possible values:	<Extension>
Remark:	In connection with <i>Start</i> [REG_SZ].

Defines the bottom limit of the respective extension number range.

MSN [REG_SZ]

Default:	<Empty string>
Possible values:	<MSN>

Defines an MSN under which the XPR server can be reached.

OAD [REG_DWORD]

Default:	0
Possible values:	<Index number>

Defines the index number of the originator address (OAD) belonging to the respective extension number range.

The TeleReg API administers all available OAD numbers as consecutively numbered key *n* under the key:

HKLM\Software\Wow6432Node\PP-COM\MRS\<APL>\OAD.

The entry performed under **OAD** serves in this context as reference to the key number to be used for the relevant extension range. If no index number is indicated, the OAD with the lowest index number would be used.

Protocol [REG_DWORD]

Default:	0x1
Possible values:	<Index number>

Defines the index number of the protocol belonging to the respective extension number range.

Each supported protocol is listed by the TeleReg API as consecutively numbered key *n* under the

HKLM\Software\Wow6432Node\PP-COM\MRS\<APL>\Protocols

key.

The entry performed under **Protocol** serves in this context as reference to the key number to be used for the relevant extension range.

Start [REG_SZ]

Default:	100
Possible values:	<Extension>
Remark:	In connection with End [REG_SZ] .

Defines the top limit of the respective extension number range.

State [REG_DWORD]

Default:	0x01
Possible values:	<Bit mask>

Defines the status of the respective extension number range.

Every extension number range administered in the registry administered by the TeleReg API has a “state”. These entries are in the form of a bitmask and with the following bit settings that can be combined:

0x01: Activates the extension range.

0x02: The extension range must be updated in the registry.
(This bit is used by an internal configurations module only.)

0x04: The extension range is removed from the registry, if the bit 0x08 is not set additionally.

0x08: The extension range remains always in the registry, even if it is not active and has been flagged as deleted by a configuration module.
(This bit is used by certain standard protocols e.g. Fax G3.)

0x10: The extension range is already available in the registry.
(This bit is internally used by a configuration module so that it does not recreate the entry completely but modifies it if required.)

VarDigits [REG_DWORD]

Default:	0
Possible values:	0 – Deactivates variable extension number length 1 – Activates variable extension number length

Defines whether the respective extension number range can have a variable amount of numbers.

If variable extension number length is allowed, a call with numbers less than the maximum length is accepted after a short waiting period.

Example:

With an extension range of 700000 to 999999 (**Start**=700000; **End**=999999) and variable extension number length the extensions 7–9, 70–99, 700–999,..., 700000–999999 are permissible.

E.20.1.6 Protocols

Protocols are services supported by the respective APL. For each installed protocol a consecutively numbered key n exists under the

HKLM\Software\Wow6432Node\PP-COM\MRS\<APL>\Protocols

again a consistently numbered key n exists. This contains the following values.

Attributes [REG_MULTI_SZ]

Default:	APL-dependent
Possible values:	<Attribute>
Remark:	Modifications can cause system restrictions or system failures

Defines a list of the valid attributes of the protocol. Each line of the list includes a protocol attribute.

The list is preset by default during the installation of the APL, so that modifications are not considered useful. Adding further attributes can restrict the system functions or even lead to system failures depending on the type of the line.

All in all, the following attributes are available with the restriction depicted above:

- *AUTOLEARN:*
On the relevant logical line the originator attributes are copied to the XPR user database.
(No longer supported AutoLearn mode.)
- *AUTOREG:*
New users on the respective logical line are automatically copied to the XPR user database.
- *COST:*
Activating the cost input for outbound messages via the respective logical line. Ensuing transmission costs will be stored in the XPR charges database.
- *DLG:*
The respective logical line allows 'Dialog' communication.
- *DOCSYNC:*
Activating document synchronization on the relevant logical line.
- *GLOBAL:*
The relevant logical line is not reported to the clients.
- *IN:*
Allowing inbound traffic via the relevant logical line.

- *LOCAL:*
The relevant logical line is not exported to other XPR servers connected via Remote System Link.
- *OUT:*
Allowing outbound traffic via the relevant logical line.
- *PABX:*
(Reserved for planned extensions.)
- *PRIV:*
Activates the privilege check on the relevant logical line.
- *RCIT*
Activates the CIT signal resetting when a read confirmation comes in on the relevant logical line.
- *SF:*
Activates the Store-and-Forward transmission of documents on the relevant logical line.
- *SMITR:*
Configures the relevant logical line as SMI transport for the connection of XPR clients or for Remote System Links.
- *TRANSACTION:*
Activates XPR transactions via the relevant logical line.
- *VALORG:*
Activates the validation of originators via the respective logical line.
- *VALREC:*
Activates the validation of recipients via the relevant logical line.

AttributesAllowed [REG_DWORD]

Default:	Protocol-dependent
Possible values:	<Bit mask>
Remark:	In connection with <i>EditPerm</i> [REG_DWORD].

Defines the attributes allowed for the respective protocol via a bitmask.

Every protocol administered by the TeleReg API possesses attributes. The entries made in this registry key are only considered when the attributes bit is set in **EditPerm**.

Blob [REG_DWORD]

Default:	0
Possible values:	<Data range index>

Index number of the Blob data range.

CapMask [REG_DWORD]

Default:	Protocol-dependent
Possible values:	<Bit mask>
Remark:	In connection with <i>Caps</i> [REG_DWORD].

Defines the interface board properties required for the relevant protocol via a bitmask. This listed properties allow the configuration module to determine if a protocol can be supported by this interface board. The following values are supported:

0x0001: Device masters speech.

0x0002: Device can recognize DTMF tones.

0x0004: Device can send and receive Fax G3 documents.

0x0008: Device can poll documents from a fax-on-demand server.

0x0010: Device may act as fax-on-demand server.

0x0020: Device can send and receive Fax G4 documents.

0x0040: Device can poll documents from a Fax G4 fax-on-demand server.
(Protocol does not exist yet, hence not defined for G4.)

0x0080: Device can act as Fax G4 fax-on-demand server.
(Protocol does not exist yet, hence not defined for G4.)

0x0100: Device masters Euro-Filetransfer transmissions.

0x0200: Device masters teletext transmissions.

0x0400: Device can transmit raw data.

0x0800: Device masters MWI.

CheckMailbox [REG_DWORD]

Default:	0
Possible values:	0 – Deactivates the XPR database check. 1 – Activates the XPR database check.

Defines whether a call is only accepted if an entry with the dialed phone number exists for the user in the XPR database.

ContMsg [REG_SZ]

Default:	'Continuation of an interrupted fax transmission'
Possible values:	<single-line message>

Defines a single-line message that is faded in as first line in a fax message if the transmission has been interrupted and the connection is reestablished.

Example: Continuation of an interrupted message.

Description [REG_SZ]

Default:	<Empty string>
Possible values:	<Description>

Defines a description of the respective OAD.

DispPerm [REG_DWORD]

Default:	APL-dependent
Possible values:	<Bit mask>

Defines the release of certain windows or window elements for the GUI via a bitmask. The definition is performed via the respective APL.

The settings are in detail:

0x0001: Page identification /ID

0x0002: Header for fax transmission on the **ID** page

0x0004: Identification for fax transmission on the ID page

0x0008: Page **Attribute** (in Expert Mode only)

0x0010: Page **Format** (in Expert Mode only)

0x0020: Page **Repetitions**

0x0040: Page **Private**

0x0080: Page **Fax G3**

0x0100: Option *Document chaining* on the **Fax G3** page

0x0200: Option *Retransmission* on the **Fax G3** page

0x0400: Page **Fax G4**

0x0800: Option *Retransmission* with Fax G3 after failed attempt on the **Fax G4** page.

0x1000: Option *Use T.70 Network Layer* on the **Fax G4** page.

0x2000: Option *Receipt of fax documents for existing mailboxes only* on the **Fax G3** page.

DocReps [REG_SZ]

Default:	3-60;2-120;1-300;0-0;0-0
Possible values:	<Number>-<Interval> (list separated by semicolon)

Defines a repeat strategy for dialing

The entered parameters in the form <Number>-<Interval> determine how often and in which time periods delivery attempts are performed for messages. The parameter <Number> describes the number of the delivery attempts to be performed and the associated parameter <Interval> the distance in seconds between the single delivery attempts that have been defined before.

If several parameters separated by comma are indicated, they will be executed one after another. Up to five different repeat strategies can be indicated.

Example: 3-60;2-90;0-0;0-0,0-0

In this example, three delivery attempts are made in 60-second intervals and another two in 90-second intervals each.

EditPerm [REG_DWORD]

Default:	Protocol-dependent
Possible values:	<Bit mask>

Specifies via a bitmask for which registry values of the relevant protocols modifications are possible.

The registry keys to be released for modifications are in detail:

0x0001: *Name* [REG_SZ]

0x0002: *FriendlyName* [REG_SZ]

0x0004: *Description* [REG_SZ]

0x0008: *Attributes* [REG_MULTI_SZ]

0x0010: *Formats* [REG_SZ]

0x0020: *Private* [REG_MULTI_SZ]

0x0040: *ParamBlock* [REG_SZ]

0x0080: *DocReps* [REG_SZ]

0x0100: *ScriptName* [REG_SZ].

EditPermGenerated [REG_DWORD]

Remark:	Corresponds to <i>EditPerm</i> [REG_DWORD], but is only valid for generated protocols and thus protocols derived from another protocol.

FaxG3Chain [REG_DWORD]

Default:	1
Possible values:	0 – Deactivates chaining of documents 1 – Activates chaining of documents
Remark:	Chaining of documents only works if the APL has not yet transmitted all data of the previous fax message to the interface board. If this has already been done, the respective APL initiates the connection termination. In this case it is not possible to attach an additional message.

Defines using the chaining of documents.

In Fax G3 send mode the documents of several fax send jobs can be chained. Required for this chaining is that the recipient, the document format and the send resolution are identical for all relevant documents.

FaxG3Resend [REG_DWORD]

Default:	0
Possible values:	0 – First document page as start page after send cancelation. 1 – Interrupted document page as start page after send cancelation.

Defines which document page continues the fax transmission, if the previous transmission of the same document has been interrupted unexpectedly.

FaxG4FaxG3 [REG_DWORD]

Default:	0
Possible values:	0 – Output of a Fax G4 error protocol. 1 – Fax G3 delivery of Fax G4 messages.

Defines the behavior in the case that a Fax G4 send job cannot be transmitted as FaxG4.

Possible options are output of a corresponding error protocol or the new attempt to send the FaxG4 as FaxG3 message. The latter requires the installation of the FAX G3 protocol.

FaxG4T70 [REG_DWORD]

Default:	0
Possible values:	0 – ISO8208 as layer 3 fax protocol. 1 – T70NL as layer 3 fax protocol.
Remark:	Works in combination with G4UseIso8208 [REG_DWORD] .

Defines which B3 protocol is used as layer 3 protocol for the Fax G4 message transmission.

Possible options are T70NL (activates the B3 protocol T90NL, which is compatible to T70NL) or ISO8208. In case of doubt, always select ISO8208, because you cannot send a Fax G4 message from a T70NL connection to an ISO8208 connection.

If this registry key is not activated, the XPR server checks the entry of the registry key [G4UseIso8208 \[REG_DWORD\]](#) and derives from this the layer 3 protocol to be used.

FaxId [REG_SZ]

Default:	Fax G3: '<CountryCode><AreaCode><AccessCode>0' Fax G4: '<CountryCode><AreaCode><AccessCode>0=<SystemName>'
Possible values:	<Fax ID>

Defines the default ID of the fax protocol.

For Fax G3 this ID must correspond to the standard T.30 and may thus only include digits, blanks and the '+' character. For Fax G4 and ISDN teletex the format requirements of the standard F.200 must be respected.

The setting made under this registry key is applied if no individual fax ID has been found for the transmitting user in the XPR user database.

Example:

+49 2404 9876543 (Fax G3 with T.30)

49-1234567890=FIRMA (Fax G4 with F.200)

Formats [REG_SZ]

Default:	Protocol-dependent
Possible values:	<Document format> and/or <Data format>

Defines the valid document and data formats for the respective protocol.

The supported formats are described in [Appendix A, "Document Formats"](#).

FormatsAllowed [REG_DWORDS]

Default:	Protocol-dependent
Possible values:	<Bit mask>
Remark:	In connection with <i>EditPerm</i> [REG_DWORD].

Defines the document and data formats for the relevant protocol via a bitmask.

The entries made in this registry key are only considered when the attributes bit **Formats** is set in the registry value *EditPerm* [REG_DWORD].

FriendlyName [REG_SZ]

Default:	Protocol-dependent
Possible values:	<Protocol name>

Specifies a readable name for the relevant protocol. For each protocol a unique protocol name must be assigned.

Headline [REG_SZ]

Default:	Protocol-dependent
Possible values:	<Fax G3 header>
Remark:	Then entry length may not exceed 32 characters .

Specifies the Fax G3 header that is displayed on each page of a fax message.

MultiMaster [REG_DWORD]

Default:	0
Possible values:	0 – No other protocols can be derived. 1 – Other protocols can be derived.

Defines whether other protocols can be derived from the respective protocol.

Name [REG_SZ]

Default:	<Empty string>
Possible values:	<Node name>

Defines the node name used in a logical NVS address of the format NVS:<Node>/<User> for the relevant protocol.

Example:

NVS:FAXG3/+490123456789

NeedConference [REG_DWORD]

Default:	0
Possible values:	0 – <i>Conversation Recorder</i> without CorNet 1 – <i>Conversation Recorder</i> with CorNet

This value must be set to 1 for using the *Conversation Recorder* protocol with CorNet-NQ (ISDN APL) or CorNet-IP (IP APL).

ParamBlock [REG_SZ]

Default:	Protocol-dependent
Possible values:	<Script parameter>

Defines script parameters that are transmitted for the respective protocol. Depending on the protocol, one specific entry per line separated by a blank is performed.

1. PlayWave

- MAX_REC_TIME
Maximum recording time in seconds.
Default: 300 [seconds]
- START_DELAY
Defines the start delay for message playback.
Default: 10 [tenth of a second]

Example: MAX_REC_TIME=200 START_DELAY=5

Private [REG_MULTI_SZ]

Default:	<Empty string>
Possible values:	<Initialization entry per line>

Defines APL-specific configuration data. One specific entry is made per line in the form *Label*==<Value>. <Label> determines the respective setting name and <Value> the desired content of the respective setting.

PrivateMode [REG_DWORD]

Remark:	APL-dependent

ScriptName [REG_SZ]

Default:	Protocol-dependent
Possible values:	<File Name> (without extension)

Defines the file name (without extension) of the script belonging to this protocol.

Example: SFOD

SI [REG_SZ]

Default:	Protocol-dependent
Possible values:	<CIP>:<SI>

Defines the CIP values of the CAPI 2.0 and the values of the service indicators that are accepted for the relevant protocol.

The entry is made in the format <CIP>:<SI>. The first expression describes the CIP value that is used for message transmission. <SI> defines the sub indicator formerly used by the German 1TR6 protocol, but which has no significance today.

Valid CIP values are:

- 1: Speech
- 4: 3.1kHz Audio
- 5: 7kHz Audio
- 16: Telephony
- 17: Fax G3
- 18: Fax G4

In the Benelux states transmission problems might occur since a lot of recipients expect the CIP value 1 (speech) differing from the CAPI standard. To solve this problem the value SI can be modified in the entry for the Fax G3 protocol.

State [REG_DWORD]

Default:	<Empty string>
Possible values:	<Bit mask>

Defines the state of the respective protocol.

Each protocol that is administered in the registry by the TeleReg API has a "state". These entries are in the form of a bitmask and with the following bit settings that can be combined:

- 0x01:** Activates the protocol
- 0x02:** The protocol must still be updated in the registry.
(This bit is used by an internal configurations module only.)
- 0x04:** The protocol is removed from the registry, if the bit 0x08 is not set additionally.
- 0x08:** The protocol remains always in the registry, even if it is not active and has been flagged as deleted by a configuration module.
(This bit is used by certain standard protocols e.g. Fax G3.)

0x10: The protocol is already available in the registry.
(This bit is internally used by a configuration module so that it does not recreate the entry completely but modifies it if required.)

Type [REG_DWORD]

Default:	Protocol-dependent
Possible values:	See remarks.

Defines the type of the respective protocol.

Valid values for the protocol type are:

- 0: Unknown protocol type
- 1: Sending and receiving Fax G3
- 2: Fax G3 polling
- 3: Fax G3 fax-on-demand server
- 4: Fax G4
- 7: Euro-Filetransfer server
- 8: Euro-Filetransfer client
- 9: Sending and receiving voice mail
- 10: Script-based protocol based on the programming language D
- 11: Script-based protocol based on the programming language E
- 12: Script-based protocol based on the programming language GSM
- 13: Message Waiting Indication (MWI)
- 14: ISDN Teletex
- 15: SMI transport
- 16: Computer Telephony Integration (CTI).

E.20.2 ISDN APL Registry Keys

This section describes the ISDN APL registry values. Only the entries available in addition to the TeleReg entries are depicted in detail. The registry entries of the TeleReg API are correspondingly marked and described in [Section E.20.1, “Registry Keys of the TeleReg”](#), on page 1860.

The information is structured in the following manner:

- [General Entries](#)
- [Blobs \(Binary Large Objects\)](#)
- [Devices](#)
- [Trunk Groups](#)
- [Extension number ranges](#)
- [Protocols](#)
- [Voice and Fax-on-Demand Systems](#)

E.20.2.1 General Entries

The following general registry values are found under the key:

HKLM\Software\Wow6432Node\PP-COM\MRS\IsdnAp1

ALawCoding [REG_DWORD]

Remark:	Not used at the moment.

AlcatelDiscKey [REG_SZ]

Default:	<Empty string>
Possible values:	0
Remark:	Must not be modified.

Special configuration for Alcatel PBX project.

Ap1Index [REG_DWORD]

Default:	<APL index>
Possible values:	<APL index>

Defines the logical index of an ISDN APL that unambiguously designates each ISDN APL of an XPR installation. The APL index corresponds to the system index of an XPR node. The system index of the kernel node is *0*, the system index of the first satellite *1* etc.

The XPR addresses of the logical lines also derive from the APL index.

Example: `NVS:FAXG3.I1.0101`

The '1' that follows the denominator 'I' describes the APL index plus 1. In our example we thus deal with the ISDN APL of the XPR node with the system index 0 – thus a kernel node APL.

The APL index can e.g. be used to logically summarize the ISDN APLs of several XPR satellites of a location. For this, the APL indices of the respective APLs must simply be set to the same value in the registry.

Example:

We assume the presence of two XPR satellites with the system indices 3 and 4 in one location. The APL indices of the ISDN APLs then also read 3 and 4 by default. Derived from this, the associated fax lines of the ISDN APLs on these satellites have the denominators `NVS:FAXG3.I4.0101` or

`NVS:FAXG3.I5.0101`.

If the registry value **ApIIndex** is set to 3 on both XPR satellites, the fax lines on both satellites will be labeled `NVS:FAXG3.I4.0101` and can thus be addressed together via Routing Rules.

BuiltInDtmf [REG_DWORD]

Default:	0
Possible values:	0 – Disables the DTMF software detection 1 – Enables the DTMF software detection 2 – Enables the DTMF hardware detection 3 – Enables the DTMF soft and hardware detection

Defines whether DTMF recognition is performed via the XPR server software detection or via the ISDN board.

If Cornet T is to be configured of the ISDN APL, this value should be set to 2. In the event that this results in DTMF recognition problems, we recommend setting 3.

CapiQueueSize [REG_DWORD]

Default:	1
Possible values:	[1 ... 64]
Remark:	The configured default value should be sufficient for productive systems. If the default value is not sufficient in a system, this system should undergo a thorough performance check.

Specifies the size of the data queue in which incoming CAPI messages are buffered for the ISDN APL. The value of **CapiQueueSize [REG_DWORD]** is based on units of 64 CAPI messages in each case.

Example: If **CapiQueueSize**=4, the data queue has a size of 4×64=256 CAPI messages.

If this queue is allocated for 75%, the following message of the ISDN APL points this out in the XPR monitor:

```
"CapiQueue W [dev:4] Please use the reg-key 'CapiQueueSize'
to set a multiplication factor (1-64) for the base queue size
(64) which better fits to the load of this system.
QueueMaxSize[64] QueueMsgs[51]"
```

In this message

- QueueMaxSize[64]
describes the currently configured size of the data queue.
- QueueMsgs[51]
describes the maximum number of CAPI messages that have simultaneously come in up to now.

Always change the value of **CapiQueueSize [REG_DWORD]** in steps of 1 and not in larger steps. Then check whether the XPR monitor still issues the message of the 75%-limit transgression.

NOTE:

If for **CapiQueueSize [REG_DWORD]** a value greater than **16** is configured, the ISDN APL uses value **1** for the data queue size.

CfExplicit [REG_DWORD]

Default:	1
Possible values:	0 – Deactivates ECT 1 – Activates ECT

Defines whether the feature *Explicit Call Forwarding (Explicit Call Transfer)* is activated.

ECT realizes a direct link between two subscribers in a PBX. Before, single connections have been established to them via the connected XPR server.

ECT is also known under the name *Path Replacement* .

CfgCompress [REG_DWORD]

Remark:	<i>TeleReg.</i> See CfgCompress [REG_DWORD] .

Checked<n> [REG_DWORD]

Remark:	<i>TeleReg.</i> See Checked<n> [REG_DWORD] .

CheckEiconStatus [REG_DWORD]

Default:	1
Possible values:	0 – Deactivates the Eicon line state 1 – Activates the Eicon line state

Defines whether line state information of the Sangoma Diva(R) ISDN board(s) are queried by the ISDN APL.

The ISDN APL can query status information about the lines of an Sangoma Diva(R) ISDN board via an ISDN driver interface (IDI). If this feature is activated, this information can be displayed in the XPR monitor under the respective physical lines.

CLIMode [REG_DWORD]

Remark:	<i>TeleReg.</i> See CliMode [REG_DWORD] .

Cost [REG_DWORD]

Remark:	<i>TeleReg.</i> See Cost [REG_DWORD] .

CtiLayerActive [REG_DWORD]

Default:	1
Possible values:	0 – Deactivates the CTI Computer Telephony Integration protocol 1 – Activates the CTI Computer Telephony Integration protocol

Defines whether the CTI Computer Telephony Integration protocol is started during booting the relevant ISDN APL.

CtiSwitchMode [REG_DWORD]

Default:	0
Possible values:	0 – Controlled transfer 1 – Blind transfer

When invoking the PHONECALL CTI transaction, the CTI Computer Telephony Integration protocol of the ISDN APL assumes that with this invocation various parameters are transferred. If one of these parameters is missing, a default value is used instead.

CtiSwitchMode defines the default value for the Parameter Switch Mode of the PHONECALL CTI transaction.

CtiSwitchType [REG_DWORD]

Default:	0
Possible values:	0 – Software switch 1 – Hardware switch

When invoking the PHONECALL CTI transaction, the CTI Computer Telephony Integration protocol of the ISDN APL assumes that with this invocation various parameters are transferred. If one of these parameters is missing, a default value is used instead.

CtiSwitchType defines the default value for the Parameter Switch Type of the PHONECALL CTI transaction.

CtiTimeout [REG_DWORD]

Default:	10 [Seconds]
Possible values:	<10...120> [seconds]

When invoking the PHONECALL CTI transaction, the CTI Computer Telephony Integration protocol of the ISDN APL assumes that with this invocation various parameters are transferred. If one of these parameters is missing, a default value is used instead.

CtiTimeOut defines the default value for the TimeOut parameter of the PHONECALL CTI transaction.

DatusLeast [REG_SZ]

Remark:	No longer used. Retained for reasons of compatibility.

DefaultCli [REG_SZ]

Default:	<Empty string>
Possible values:	<Calling number>

This number is reported as Calling Party Number for outbound calls of the PBX if the originator ID is unknown. Used also for cost evaluation within the PBX telephone system.

DestNumberPlan [REG_DWORD]

Remark:	<i>TeleReg.</i> See DestNumberPlan [REG_DWORD] .

DestNumberType [REG_DWORD]

Remark:	<i>TeleReg.</i> See DestNumberType [REG_DWORD] .

DialInfoTimeout [REG_SZ]

Default:	10 [Seconds]
Possible values:	<Time> [Seconds]

If a phone number is transferred to the XPR system, this time is waited after each dialed extension digit for possible further extension digits. In case this time is exceeded once, the XPR server starts assigning the phone number received until then to a configured protocol. If this is not possible, the incoming call is rejected.

DialMode [REG_SZ]

Default:	<Empty string>
Possible values:	<Calling number>
Remark:	Value must not contain blanks.

Here the PIN-supervision is parameterized. The dial string is so manipulated that a destination phone number is for example prefixed with a PIN code. This code can be used for billing.

Example: ##4<DB (CostInfo) , COST>%s

DialPlan [REG_DWORD]

Default:	0x80
Possible values:	<Phone number type>

Defines the D-channel phone number type.

The default value is 0x80 (unknown).

DirectStationSelect [REG_DWORD]

Default:	0
Possible values:	0 – Enables access to Settings 1 – Disables access to Settings

Defines whether or not the PBX is allowed to access the settings of the registry values *FaxCallFwAllowed* and *VoiceCallFwAllowed* when a voice or fax message is forwarded.

If this registry value does not exist, the default value is used.

DisableEiconLevelDelimiter [REG_DWORD]

Default:	1
Possible values:	0 – Activates the Eicon Voice Limiter 1 – Deactivates the Eicon Voice Limiter

Defines whether or not the Sangoma Diva(R) (Eicon) Voice Limiter is enabled.

DisableL1DownOnMonitor [REG_DWORD]

Default:	0
Possible values:	0 – Activates the display of the layer-1 status in the XPR monitor 1 – Deactivates the display of the layer-1 status in the XPR monitor

Defines whether or not the layer-1 status of ISDN APL lines is displayed in the XPR monitor.

DiversionCtrlParty [REG_SZ]

Default:	4711
Possible values:	<Diversion Controlling Party Number>

Defines the diversion controlling party number the CTI Light protocol uses for the *Remote Call Forwarding* feature.

If a user wants to adopt an existing call diversion from the former diversion target to another PBX, three phone numbers must be forwarded:

1. From Phone number of the current rerouting destination
2. TO: Phone number of the new rerouting destination
3. DIVERSIONCTRLPARTY: Phone number of the redirected phone

DlgFlags [REG_DWORD]

Remark:	Must not be modified.

Defines which registers are displayed in the configuration dialog of the APL.

DM [REG_SZ]

Default:	0x00
Possible values:	<Bit mask>
Remark:	Must never be set during operation!

Defines a bitmask for the error attempts. Additional low level debug information.

DO [REG_SZ]

Default:	SCOWIN
Possible values:	<File name>
Remark:	Must not be set during operation!

Specifies the debug output file. If the debug bit mask [DM \[REG_SZ\]](#) is set, the debug output is written to this file.

DT [REG_SZ]

Default:	0
Possible values:	<Time> [Seconds]

Low Level Debug Time-out. With a value of **0** the log file would be written till the hard disk is full. With another setting a new log file is generated every **DT** seconds.

DtmfPeriods [REG_DWORD]

Default:	1
Possible values:	<1...5> [x15 milliseconds + 15 milliseconds]
Remark:	The default value should not be modified!

This is the number of 15 millisecond periods (**1** corresponds to e.g. 30 milliseconds, **5** to 90 milliseconds) in which a DTMF tone is continually recognized, so that it can be reported as recognized. Operational testing has proven that a value of 1 provides optimal results.

ECT [REG_DWORD]

Default:	0
Possible values:	0 – Explicit Call Transfer deactivated 1 – Explicit Call Transfer activated
Remark:	The feature must be supported by the applied ISDN board and the PBX for the activation on the XPR server.

Controls the activation of the feature Explicit Call Transfer.

You must test for each solution whether this feature is supported by the applied components in the respective scenario (tie line, bus communication).

Sangoma Diva(R) ISDN boards support this feature. For PBXs, it has been tested with a Hicom 150 and a Tenovis Integral 33xE. The latter does not support this feature for tie lines.

EnableChangePartnerEvt [REG_DWORD]

Default:	1
Possible values:	0 – Evaluation of change partner events deactivated 1 – Evaluation of change partner events activated

PBXs send a so-called change partner event to a subscriber if the conversational partner of this subscriber changes during a call. This happens, for example, after forwarding a call.

The registry value defines whether such change partner events are evaluated by the ISDN APL.

Example:

1. Subscriber A calls subscriber B.
2. Subscriber B establishes a consultation and reaches a XPR server voicebox. The PBX signals B's phone number as caller to the XPR server.
3. Subscriber B now connects the reached voicebox with subscriber A.
4. The connected subscriber thus changes and so does the connected phone number for the XPR server. The PBX signals this change to the XPR server by a change partner event.

EricssonUseCCN [REG_DWORD]

Default:	0
Possible values:	0 – Originator phone number is not determined from user-user-information 1 – Originator phone number is determined from user-user-information

Networked Ericsson PBXs do not transfer the originator phone number of a connection as correct ANI information during the connection establishment. In such a case the ISDN APL is able to determine the originator phone number from the user-user-information, which is also exchanged during the connection establishment.

This registry value defines whether the originator phone number is determined from the user-user-information.

FakeOriginator [REG_DWORD]

Default:	0
Possible values:	0 – Originator number and destination number may be identical 1 – In case of identity, the originator number is replaced with * characters
Remark:	May be used in connection with FakeOriginatorPrefixes [REG_MULTI_SZ] .

With some PBXs problems occur if originator and destination number are identical. If this value is set, the identical originator number is replaced with the * character.

FakeOriginatorPrefixes [REG_MULTI_SZ]

Default:	–
Possible values:	<list of phone numbers; one per line>
Remark:	Requires entry 1 in the FakeOriginator [REG_DWORD] registry value.

With some PBXs problems occur if originator and destination number are identical. Therefore you can insert a * character in the originator number. The position in which this character appears is determined by the prefix list defined here. The * character is always inserted after the applicable prefix.

Example:

089722 and 089622 are defined as prefixes and all with the same originator and destination number occurs – e.g. 08972256789.

The originator number is supplemented and consequently reads 089722*56789.

The same originator and destination number 08977256789 or 04472256789 would not be supplemented since none of the prefixes defined here matches them.

FaxCallFwAllowed [REG_DWORD]

Default:	1
Possible values:	0 - No support of fax forwarding via keyboard 1 - Support of fax forwarding via keyboard

Defines whether the PBX allows to forward a fax message via the keyboard (CorNet-NQ protocol).

If this registry value does not exist, the default value is used.

FaxG3CheckStationID [REG_DWORD]

Default:	0
Possible values:	0 – Disables the fax ID check of the fax device 1 – Activates the fax ID check of the fax device
Remark:	This feature should only be activated in exceptional cases

Before a Fax G3 message is sent by the XPR server, the Fax G3 ID of the addressed fax device can be compared to the dialed phone number. The respective phone numbers are normalized before the comparison.

If the fax ID and the addressed phone number do not comply, the connection will be terminated without sending the fax message. Afterwards, a journal entry will be created for the sending XPR user documenting that the message has not been sent.

If fax ID and addressed phone number comply, the fax message is sent.

Format examples:

- Works as ID for all fax devices:
+492404901100, 492404901100 or +49 (2404) 901
- Works as ID for fax devices in the same area:
2404901100
- Works as ID for fax devices in an area of the same country:
2404901100
- Works as ID for fax devices in another country:
00492404901100

IMPORTANT:

Since the fax ID configuration of a remote fax device is normally not in the configuration realm of the sending device, the activation of this feature can cause an increased number of fax messages that are not delivered.

FaxLicences [REG_DWORD]

Remark:	<i>TeleReg</i> . See FaxLicences [REG_DWORD] .

FaxResources [REG_DWORD]

Remark:	<i>TeleReg</i> . See FaxResources [REG_DWORD] .

FilterSMSDialString [REG_DWORD]

Default:	1
Possible values:	0 – Does not allow special characters in SMS addresses 1 – Allows special characters in SMS addresses

Defines whether the ISDN APL allows addresses with special characters for the SMS protocol and filters these when they come up.

Basically, all clients should deliver normalized numbers, since the MTA routing rules might otherwise not be effective. However, especially with SMS from Outlook a message might be delivered with the help of this filter.

G3ErrorHandle [REG_DWORD]

Default:	0
Possible values:	0 – OK message after the end of the fax transmission 1 – OK message after the fax message transmission to the MTA

Defines when the message 'End of Transmission OK' is transmitted to the Fax G3 originator.

G4ReplyNcpi [REG_DWORD]

Default:	0
Possible values:	0 – Deactivates CONNECT_B3_RESP with Ncpi 1 – Activates CONNECT_B3_RESP with Ncpi

Defines whether a CONNECT_B3_IND with CONNECT_B3_RESP and Ncpi is answered.

G4UseIso8208 [REG_DWORD]

Default:	0
Possible values:	0 – Activates T90NL as layer 3 fax protocol 1 – Activates ISO8208 as layer 3 fax protocol.
Remark:	Works in combination with FaxG4T70 [REG_DWORD] .

Defines which B3 protocol is used as layer 3 protocol for the Fax G4 message transmission.

Possible options are the protocols T90NL (compatible to T70NL) and ISO8208.

This entry is only evaluated, if the registry key [FaxG4T70 \[REG_DWORD\]](#) has not been activated.

IgnoreMwiOffResponse [REG_DWORD]

Default:	0
Possible values:	0 – Interprets the error message code 0x3603 1 – Ignores the error message code 0x3603

Defines whether the MWI error message code 0x3603 is interpreted or ignored.

If an LED of a telephone device that is already switched off is to be switched off, the error code 0x3603 is reported back via an 'INFO_IND' message. This error code can be ignored if desired. In this case an OK message is transmitted to the network protocol of the XPR server instead of the error.

This error may occur for example with HiPath PBXs.

IgnoreOADType [REG_DWORD]

Default:	0
Possible values:	0 – Transmitted value of the ISDN numbering plan is used 1 – Type 'Unknown' is used as ISDN numbering plan

For ISDN a transmitted telephone number always consists of three components. The type, the numbering plan and the actual phone number.

The numbering plan determines the phone number structure. So if, according to the numbering plan, you receive a national phone number, this number must be delivered from the PBX to the ISDN APL without external prefix etc. Many PBXs modify the transmitted phone number in such a way that the caller can immediately be called back. Where applicable this is done by supplementing the number with the required external prefix. In this case the PBX must set the numbering plan to 'Unknown'. If the latter is not performed by the PBX owing to an error, you can set this value to 1. The XPR server will then ignore the incorrect numbering plan specification.

A special feature of the ISDN card properties configuration is the option 'Automatic number identification with external prefix', which can be activated for incoming calls. However, this option only becomes operative when the numbering plan has been forwarded as 'Unknown'. Also here this value then helps bringing to bear the setting made.

IgnoreUnknownDiscCauses [REG_DWORD]

Default:	1
Possible values:	0 – Errors with unknown causes are rated as errors 1 – Errors with unknown causes are ignored

By default the ISDN APL does not recognize errors with unknown causes as errors.

This registry value specifies whether the ISDN APL ignores errors that do not contain information about the cause.

IncReject[REG_DWORD]

Default:	0x15
Possible values:	<ETSI (DSS1) Reject Code>

Defines the ETSI (DSS1) Reject Code.

IntlDialMode [REG_DWORD]

Default:	1
Possible values:	0 – Allows any phone number length 1 – Expects international phone number format

Defines whether the ISDN APL expects phone numbers in international phone number format (min. 10 digits) or not. In the latter case the ISDN APL also accepts pure extensions.

LineLicences [REG_DWORD]

Remark:	<i>TeleReg.</i> See LineLicences [REG_DWORD] .

LineMonitorBytesRefreshSec [REG_DWORD]

Default:	1 [second]
Possible values:	<1 ... 10> [seconds]

Specifies for all ISDN APL lines in which intervals the display for incoming and outgoing data amounts in the XPR monitor is updated.

LineResources [REG_DWORD]

Remark:	TeleReg. See LineResources [REG_DWORD] .

LocalizeNumberForRcc [REG_DWORD]

Remark:	Not used at the moment.

LocPrefixExtensions [REG_MULTI_SZ]

Default:	<Empty string>
Possible values:	<List of phone numbers>
Remark:	An entry here is only useful when settings for the ISDN APL are to be configured differently than that of the global settings under MRS Globals\Location\LocPrefixExtensions.

Defines a list with dialing numbers or partial dialing numbers not modified by the normalization. Normally, all phone numbers are normalized to an international phone number.

Example: 0123456789 becomes 49123456789

With corporate networks, escape codes could precede network-internal phone numbers (e.g. 9992<extension parts>). Such escape codes can be indicated in this key, so that all numbers starting with this digit are not normalized.

Example:

9992

0111

444

In this case all phone numbers starting with 9992, 0111 or 444 are not modified during phone number normalization.

MaxConnectTime [REG_DWORD]

Default:	60 [minutes]
Possible values:	<Time> [minutes]

Defines a time after which each connection still active is terminated.

MaxG3Speed [REG_DWORD]

Default:	5
Possible values:	See description

Defines the maximum transmission rate of a G3 fax document.

Possible values are:

0: Max. possible transmission rate

1: 2400 Baud

2: 4800 Baud

3: 7200 Baud

4: 9600 Baud

5: 14400 Baud

6: 33600 Baud

MaxLengthForAreaOad [REG_DWORD]

Default:	0x8
Possible values:	<Phone number length>
Remark:	Is used in combination with MinLengthForExternalOad [REG_DWORD] .

Sometimes telephone numbers are provided with the additional 'Call type' information by the ISDN switching exchange. Thus for example a local number is transmitted with the additional information 'in local area network'. See for example I ETSI EDSS1-300-102-1.

If you applied the normal normalization routine to such a number, often a number being not correctly normalized would be delivered.

In order to have these numbers normalized correctly, the ISDN APL treats numbers that are provided with 'Call type' information and are between **MinLengthForExternalOad** and **MaxLengthForAreaOad** (included) with their phone number length separately.

MaxRedirLength [REG_DWORD]

Default:	0
Possible values:	<applied length of redirecting number>

Voice mail boxes are often addressed via Redirecting Numbers. Thus, not every user needs his/her own voice mail number but his/her telephone number may simply be used. Cf. [Section 10.1.5, "Redirecting Numbers", on page 551](#).

If the value of this parameter is greater than **0**, only the last MaxRedirLength digits of a number that has been signaled by the PBX via a Redirecting Number are used.

The button has been added for a client whose PBX reported the extensions of the Redirecting Numbers either with 4 or 8 digits. Via this switch a constant length of 4 correct digits has been configured.

MaxSuppServiceCnt [REG_DWORD]

Default:	0x5
Possible values:	<0x1 ... 0xFFFFFFFF>

Defines how many FACILITY_REQ messages are sent by the ISDN APL.

The ISDN APL sends GETSUPPORTSRV requests to the applied Sangoma Diva(R) board in a 30s interval. The respective Sangoma Diva(R) board then generates GETSUPPORTSRV replies via which the APL determines the ISDN board capacity.

MaxSuppServiceCnt defines how many of these GETSUPPORTSRV requests are sent to the Sangoma Diva(R) board. If this counter has expired, no further requests are performed via the ISDN APL.

The default entry **5** determines that 5 requests are performed within the first 150 seconds.

MinLengthForExternalOad [REG_DWORD]

Default:	0x7
Possible values:	<Phone number length>

See [MaxLengthForAreaOad \[REG_DWORD\]](#).

MinRedirectedLen [REG_DWORD]

Default:	5
Possible values:	<Phone number length>

Defines the minimum phone number length a *Redirected Number* must have if it is transmitted.

MwiListSize [REG_DWORD]

Default:	4096
Possible values:	256 ... 65535

The APL buffers MWI notifications to be sent to a connected PBX in a list. When the list is full, the APL does not accept the next MWI notification by the MTA until a notification could be sent from the list.

MwiListSize defines the length of the relevant list.

NoInboundNormalize [REG_DWORD]

Default:	0
Possible values:	0 – Activates the normalization for incoming communication 1 – Deactivates the normalization for incoming communication

Defines whether the phone numbers of incoming communication requests are normalized.

NormTransAni [REG_DWORD]

Default:	1
Possible values:	0 – Transfer ANI is forwarded as local phone number 1 – Transfer ANI is forwarded in a normalized way

Defines whether the transfer ANI is passed on to the PBX either normalized or as local phone number.

NotDecrRptCntCodes [REG_MULTI_SZ]

Default:	<List of error codes>
Possible values:	<List of error codes>
Remark:	Is possibly used in combination with <i>NotRepeatCodes</i> [REG_MULTI_SZ].

If the ISDN APL performs an action directed to the connected ISDN system, an error code is returned if this action fails. This error code is defined in hexadecimal format and consists of 4 digits in total.

The APL can react in three different ways if such an error code is returned:

1. Countdown of the repeat counter and repetition of action
2. Repetition of the action without modification of repeat counter
3. No repetition of the action

For all error codes that have been defined in the registry value **NotDecrRptCntCodes**, option 2 is used in case of the respective error. If an error has neither been defined here nor in the registry value **NotRepeatCodes**, the APL uses error option 1.

The codes that are to be defined in this registry value must correspond to the error codes of specifications *ETS 300 102-1* and *Common-ISDN-API Version 2.0*. If several error codes are listed at the same time, they must be separated by a line break.

NotRepeatCodes [REG_MULTI_SZ]

Default:	<List of error codes>
Possible values:	<List of error codes>
Remark:	Is possibly used in combination with <i>NotDecrRptCntCodes</i> [REG_MULTI_SZ].

If the ISDN APL performs an action directed to the connected ISDN system, an error code is returned if this action fails. This error code is defined in hexadecimal format and consists of 4 digits in total.

The APL can react in three different ways if such an error code is returned:

1. Countdown of the repeat counter and repetition of action
2. Repetition of the action without modification of repeat counter
3. No repetition of the action

For all error codes that have been defined in the registry value **NotRepeatCodes**, option 3 is used in case of the respective error. If an error has neither been defined here nor in the registry value **NotDecrRptCntCodes**, the APL uses error option 1.

The codes that are to be defined in this registry value must correspond to the error codes of specifications *ETS 300 102-1* and *Common-ISDN-API Version 2.0*. If several error codes are listed at the same time, they must be separated by a line break.

NumberTypeMode [REG_DWORD]

Default:	0
Possible values:	0 – No phone number is normalized 1 – Normalizes destination number 2 – Normalizes originator number 3 – Normalizes destination and originator number

Defines via a two-digit bitmask whether phone numbers in a communication request are normalized and which ones.

If the normalization of a phone number is activated, its number type is set to the value 'International' accordingly.

OadIndicator [REG_DWORD]

Default:	0x80
Possible values:	See description

Defines via a two-parts bitmask whether destination number, originator number and redirected number are displayed at the device.

The value assignments of the respective bits 6 and 7 are (bit 8 is always **1**):

- 0 0 (0x80): Display allowed
- 0 1 (0xA0): Display not allowed
- 1 0 (0xC0): Phone number not available
- 1 1 (0xE0): Reserved

OadLicStyle [REG_DWORD]

Default:	0
Possible values:	0, 1

IMPORTANT:

A manual modification of this value can cause a malfunction of the XPR server.

Is required for the license compatibility of the XPR server.

OldCostInfo [REG_DWORD]

Default:	0
Possible values:	0 – No normalization of the value in field COSTINFO 1 – Normalization of the value in field COSTINFO
Remark:	This field is ignored when the setting 'local extension' is selected.

Defines whether the number of the cost center entered in the **COSTINFO** field is normalized.

If the former incorrect behavior is required for compatibility reasons, this value can be set to **1**.

OldStyleConnInd [REG_DWORD]

Default:	0

If parts of the dialed extension are missing with old CAPI 2.0 boards, this value can be set to **1**.

OrigNumberPlan [REG_DWORD]

Remark:	<i>TeleReg.</i> See OrigNumberPlan [REG_DWORD] .

OrigNumberType [REG_DWORD]

Remark:	<i>TeleReg.</i> See OrigNumberType [REG_DWORD] .

OutCallHoldAllowed [REG_DWORD]

Default:	0: "Cannot be put on hold"
Possible values:	0: "Cannot be put on hold" 1: "Can be put on hold"

Set this key to clear the 'Hold-not-Allowed' classmark bit.

Setup message extract with IsdnApl default (OutCallHoldAllowed = 0)

Classmarks

Feature Indicator

- Cannot be put on hold
- Can indicate display info
- Change of service not allowed
- Can activate Message Waiting Callback
- User-to-user information transport possible

Access capabilities

- Can access long distance public network
- Can access local public network

Setup message extract with IsdnApl OutCallHoldAllowed = 1

Classmarks

Feature Indicator

- Can be put on hold
- Can indicate display info
- Change of service not allowed
- Can activate Message Waiting Callback
- User-to-user information transport possible

Access capabilities

- Can access long distance public network
- Can access local public network

\PhoneNrSilenceLength [REG_DWORD]

Default:	200 [Milliseconds]
Possible values:	<Time> [Milliseconds]

Defines the pause length between single digits with announcing phone numbers to a user.

PrioClass [REG_DWORD]

Default:	0x80
Possible values:	0x020 – Normal priority 0x040 – Idle priority 0x080 – High priority 0x100 – Realtime priority
Remark:	Modifications are not recommended.

Specifies the ISDN APL priority class. Leave the default setting for this value because higher priorities may block the complete Windows system and lower ones may also cause problems.

IMPORTANT:

The ISDN APL does not work with the idle priority (0x40).

PrioThread [REG_DWORD]

Default:	0x1
Possible values:	2 – Highest 1 – Above Normal 0 – Normal -1 – Below Normal -2 – Minimal
Remark:	This value must not be modified.

Priorities of several special threads that administer board events.

QueryBilling [REG_DWORD]

Remark:	<i>TeleReg.</i> See QueryBilling [REG_DWORD] .

ReportVoiceOKAfterConn [REG_DWORD]

Default:	0x1
Possible values:	0 – OK report after complete playback of a voice mail 1 – OK report after start of the voice mail playback

The voice protocol is often used for putting out received voice messages at a telephone. If the recipient puts the phone down before having listened to the entire message, this message is reported as not correctly delivered and, as the case may be, the MTA initiates a repetition of the call.

If this switch was set to **1**, 'OK' would be reported to the MTA already when the recipient answers the phone and thus listens to at least a part of the message.

Restart [REG_DWORD]

Default:	0x1
Possible values:	0 – Watchdog may restart board drivers 1 – Watchdog may not restart board drivers
Remark:	Is not supported by all ISDN boards. This value should only be modified for testing purposes.

Defines whether the internal watchdog will restart the card driver when errors occur.

Rout1 [REG_SZ]

Remark:	Not used at the moment.

ShowSecretNumber [REG_DWORD]

Default:	0
Possible values:	0 – Presentation-restricted numbers are not displayed 1 – Presentation-restricted numbers are displayed

Defines whether numbers are displayed anyhow for which the bit for *Presentation restricted* has been set in the *Presentation Indicator* field.

Thus this value can be used to evade calling number suppression.

SimulResDw [REG_SZ]

Default:	<Empty string>

Setting for manufacturer quality assurance to simulate system errors

SkipRedirectingDigits [REG_DWORD]

Default:	0
Possible values:	<applied length of redirecting number>

Here you can enter the number of the first *n* digits you wish to cut off of the 'Redirecting Number'. On the other hand there are PBXs that do not correctly transmit the Redirecting Number and with a negative offset entered here the correct number can be obtained.

With e.g. a Tenovis system the 'Redirecting Clause' element was not transmitted and this could be made up for with the value -1.

See on this topic also [Section 10.1.5, “Redirecting Numbers”, on page 551](#).

SmiShortHold [REG_DWORD]

Default:	60 [Seconds]
Possible values:	<Time> [Seconds]
Remark:	Exists for compatibility reasons

This entry has the same meaning as the private entry “ShortHold” of the ISDN SMI protocol (cf. [Private \[REG_MULTI_SZ\]](#)). The ISDN APL uses this entry in case the private one cannot be found.

Otherwise the entry exists only for compatibility reasons and should be deleted in favor of the private entry.

SmsProviderList [REG_MULTI_SZ]

Default:	491771167,49177,TAP 491771167,49178,TAP 491771167,49163,TAP 491712521001,49171,TAP,T90 491712521001,49170,TAP,T90 491712521001,49175,TAP,T90 491712521001,49151,TAP,T90 491712521001,49160,TAP,T90 491722278000,49172,UCP 491722278000,49173,UCP 491722278000,49174,UCP 491722278000,49162,UCP 491722278000,49152,UCP 49109001797673425,49179,TAP,LT 49109001797673425,49176,TAP,LT 31653141414,31651,UCP 31653141414,31653,UCP 31654545000,31654,UCP 31703328662,3170,UCP 3275161622,3275,UCP
Possible values:	<SMSC phone number>,<network access>,<transport protocol>

Defines the list of Short Message Service Centers (SMSC) that take on SMS message transfer when the SMS protocol is used.

Each list line consists of:

- The access phone number of the respective SMSC
- The associating network access number, which is the first part of a SMS number
- The transport protocol that is possible via the relevant access

Example: 491712521001,49175,TAP,T90

All SMS messages the destination numbers of which begin with 49175, are sent to the SMSC with the access number 491712521001. The transmission may occur with the protocols TAP or T90.

If the network access number for the SMSC can in our example also be addressed in the format 0175... or 0049175..., additional entries must be made in the provider list for these alternatives:

491712521001,0175,TAP,T90

491712521001,49175,TAP,T90

491712521001,0049175,TAP,T90

If special characters are to be transmitted in SMS messages via the provider T-Mobile, the protocol T90 must be replaced with the protocol TMB for the network access numbers of this provider.

Example: 491712521001,49175,TAP,TMB

SSCTAbortable [REG_DWORD]

Default:	1
Possible values:	0 – Deactivates Single Step Call Transfer Abort 1 – Activates Single Step Call Transfer Abort

The signaling protocols QSIG and CorNet NQ implement the forwarding version Single Step Call Transfer (SSCT). This can divert an existing connection to another destination without occupying another B-channel.

Normally, a diversion initiated via SSCT cannot be canceled by the initiator. This means that the respective forwarding process can only be canceled by a timeout in the respective PBX, if the new destination e.g. does not accept the connection.

To solve this problem the feature *SSCT Cancel* (also called *SSCT Abort*) has been implemented e.g. for CorNet NQ of the HiPath 4000 V.2. This feature also enables the initiator to cancel a forwarding process. Such an initiator can be e.g. a voice mail protocol or the VOGUE script that can initiate the cancellation of a forwarding process via a configurable time-out.

If a PBX is used that does not support *SSCT Cancel*, this feature must be deactivated in the ISDN APL, since otherwise malfunctions may be the result. Therefore, set the entry in the registry value **SSCTAbortable** to **0**.

StdCharging [REG_DWORD]

Default:	1
Possible values:	0 – No user-dependent phone number for billing 1 – User-dependent phone number for billing

Defines whether a user-specific phone number is adopted from the XPR database field COSTINFO for billing.

SupportedDevices [REG_MULTI_SZ]

Default:	<Current device list>
Possible values:	<Device names>

Defines which device names are displayed in the configuration dialog of the APL.

TakeOriginalType [REG_DWORD]

Default:	1
Possible values:	0 – Does not use the original phone number type 1 – Uses the original phone number type

Defines whether the phone number type of the original originator phone number is used for the new originator number in a diverted call.

TransBreak [REG_DWORD]

Default:	25 [Milliseconds]
Possible values:	<Time> [Milliseconds]
Remark:	Is used in combination with <i>TransMax</i> [REG_DWORD].

Defines the time during which the *TransMax* [REG_DWORD] XPRtransactions are performed.

TransMax [REG_DWORD]

Default:	5
Possible values:	<Transaction number>
Remark:	Is used in combination with <i>TransBreak</i> [REG_DWORD].

Defines the maximum number of XPR transactions that are performed within the time *TransBreak* [REG_DWORD].

UseCallPartySubaddress [REG_DWORD]

Remark:	Not used at the moment.

UseCapiDll [REG_DWORD]

Default:	0
Possible values:	0 – CAPI Calls via Kernel Driver Interface 1 – CAPI Calls via CAPI2032.DLL
Remark:	Internal value. Must not be modified.

Defines whether CAPI calls are performed via CAPI2032.DLL or the kernel driver interface.

UseCtiMonitorPoint [REG_DWORD]

Default:	0
Possible values:	0 – No monitor point is set on the APL 1 – A monitor point is set on the APL
Remark:	If CAD is to be used, no phone number recognition may be configured in the ISDN APL for outgoing connections. Cf. ISDN settings > Outbound > Use following ID.

To administer Call Attached Data (CAD) correctly, the CTI APL must be informed when a call status changes in the ISDN APL. To this, the CTI APL must set a monitor point on the ISDN APL.

If this registry value is set to **1**, such a monitor point will be configured.

UseSecondCallingPartyNumber [REG_DWORD]

Default:	0
Possible values:	0 – APL evaluates the first of the transferred phone numbers 1 – APL evaluates the second of the transferred phone numbers

During the establishment of a call rerouting some PBXs transfer a phone number field with two calling party numbers to the XPR server.

This value defines which of these two phone numbers the APL is to evaluate as Redirected Number.

UserUserSupported [REG_DWORD]

Default:	1
Possible values:	0 – Activates using the uinfo information 1 – Deactivates using the uinfo information

The ISDN APL uses the uinfo information for its internal voice protocol. This information element is not supported by all PBXs (e.g. not by Alcatel 4400). In such a case processing this information element must be deactivated.

UseSameCardForECT [REG_DWORD]

Default:	1
Possible values:	0 – ECT only on the same ISDN board 1 – ECT also between different ISDN boards

Defines whether the Explicit Call Transfer feature may also be activated for calls of different ISDN boards.

ECT realizes a direct link between two subscribers in a PBX. Before, single connections have been established to them via the connected XPR server. ECT is also known under the name *Path Replacement*.

UseTransferAni [REG_DWORD]

Default:	1
Possible values:	0 – Accepts possible forwarding restriction 1 – Activates non-PBX forwarding

Some PBXs do not forward external callers to external destinations by default, since no non-system calling party numbers are allowed for forwarding. **UseTransferAni** activates in such cases the transfer option.

VarDwTimeout [REG_DWORD]

Default:	3 [Seconds]
Possible values:	<Time> [seconds]>

Time-out for the extension mode 'variable length'.

This value is e.g. of significance when the fax forward protocol is in use.

VoiceCallFwAllowed [REG_DWORD]

Default:	0
Possible values:	0 – No forwarding of a voice message via keyboard 1 – Forwarding of a voice message via keyboard

Defines whether the PBX allows to forward a voice mail via the keyboard (CorNet-NQ protocol).

If this registry value does not exist, the default value is used.

VoiceLicences [REG_DWORD]

Remark:	<i>TeleReg.</i> See VoiceLicences [REG_DWORD] .

VoiceResources [REG_DWORD]

Remark:	<i>TeleReg.</i> See VoiceResources [REG_DWORD] .

WaitForGeb [REG_SZ]

Default:	0x1
Possible values:	0 – Immediate end of communication 1 – Delayed end of communication
Remark:	Should always be set to 1, since the XPR server might otherwise not be able to correctly analyze the charge information.

Defines whether the ISDN APL waits for the billing information transmission by the service provider after the end of a communication relation, or ends the connection immediately.

WaitForIsdnMwiInd [REG_SZ]

Default:	1
Possible values:	0 – Does not expect MWI confirmation 1 – Expects MWI confirmation

Defines whether the XPR server expects a confirmation for an MWI transaction.

E.20.2.2 Blobs (Binary Large Objects)

Every registry entry administered by the TeleReg API may contain a reference to a Blob. Blobs are binary data ranges in which programmer-defined data may be stored.

This mechanism is currently not used by the ISDN APL. Blobs used can be found in the registry under the key:

`HKLM\Software\Wow6432Node\PP-COM\MRS\ISDNApi\Blobs`

E.20.2.3 Devices

A device corresponds to the physical device of an ISDN interface board. The device is composed of a defined number of logical communication channels. E.g. an S_0 interface consists of 2 logically separated channels or an S_{2M} interface consists of up to 30.

For each of these devices a consecutively numbered key n exists under the

`HKLM\Software\Wow6432Node\PP-COM\MRS\ISDNApi\Devices`

key. These contain respectively the following registry values that describe the properties of the individual physical interfaces.

AddDialOutLen [REG_DWORD]

Remark:	<i>TeleReg.</i> See AddDialOutLen [REG_DWORD] .

Blob [REG_DWORD]

Remark:	<i>TeleReg.</i> See Blob [REG_DWORD] .

Caps [REG_DWORD]

Remark:	<i>TeleReg.</i> See Caps [REG_DWORD] .

Channels [REG_DWORD]

Remark:	<i>TeleReg.</i> See Channels [REG_DWORD] .

Description [REG_SZ]

Remark:	<i>TeleReg.</i> See Description [REG_SZ] .

FaxG3 [REG_DWORD]

Remark:	<i>TeleReg.</i> See FaxG3 [REG_DWORD] .

Handle [REG_DWORD]

Remark:	<i>TeleReg.</i> See Handle [REG_DWORD] .

Lines [REG_DWORD]

Remark:	<i>TeleReg.</i> See Lines [REG_DWORD] .

Name [REG_SZ]

Remark:	<i>TeleReg.</i> See Name [REG_DWORD] .

PrefixedANI [REG_DWORD]

Remark:	<i>TeleReg.</i> See PrefixedAni [REG_DWORD] .

Private [REG_MULTI_SZ]

Default:	<Empty string>
Possible values:	<Initialization entry per line>
Remark:	<i>TeleReg.</i>

Defines ISDN APL-specific configuration data. A specific entry in the form <Label>=<Value> is performed per line. <Label> determines the name of the setting and <Value> the required content of the respective setting.

Example:

AutoDialNb1=NVS:VOICE/47

DebugItk=1

The following entries are possible for the ISDN APL:

- **AutoDialNb<n>:**
Error correction for certain PBX units. Defines a time in seconds after which the dummy number specified here is dialed by the relevant ISDN board.
After an undefined period of time, some older PBX units revert to a mode, where as master, do not convey this information back to the ISDN card. So they always report 'busy' for all lines. Via this hard-wired selection of the PBX this state is terminated.
<n> is a number from 1 to 4 so that four numbers may be entered.
Example: AutoDialNb1=NVS:VOICE/47
- **BlindTransViaDeflect:**
Not all signaling protocols support the 'Blind Transfer' features. If it is to be used just the same, it must be performed via 'Deflect'.
If the 'Blind Transfer' feature is to be installed for PBX system protocols other than Cornet N and Cornet NQ, this parameter must be forwarded with the value **1**.
- **CheckFacility:**
You can set this value to **1** if you require the 'Redirecting Number' feature in combination with a Hicom-300E PBX. For this PBX, 'Redirected Numbers' are added to the 'CAPI Connect-Indication' message in the field **Additional Info > Facility data array**. A variety of information is available for the ISDN APL from the **Facility data array** in a coded ANS1 package. A CAPI trace should be run from the XPR monitor to ensure that this information is available before this function is activated.
For more information on the topic "Redirecting Numbers" see also [Section 10.1.5, "Redirecting Numbers", on page 551](#).
- **DebugItk:**
Special internal debugging switch for ITK ISDN cards (**1**). Connects a D-channel monitor.
- **DirectLine:**
This value must be set to **1** for mixed ISDN card operation, for PBX and ISDN cards that are connected directly to the exchange. Otherwise the value **0** must be initialized.
- **Infos:**
Information given here is taken from the ISDN network. Possible parameters are: **GEB** (Billing information), **DTMF** (Tone recognition), **DW** and **DISPLAY**.
- **TransferViaDeflect:**
Not all signaling protocols support the 'Transfer' feature. If it is to be used just the same, it must be performed via 'Deflect'.
If the TransferViaDeflect parameter is set to **1**, 'Transfer' is performed via 'Deflect'.

- **NoHoldForECT:**
This value is always automatically correctly set subject to the D-channel protocol. Manual configuration is **not** required.
Depending on the D-channel protocol, various features are possible with explicit call transfer.
With QSIG ECMA v2 and Cornet-NQ (value=1) the caller remains in *Connected* state while a second connection is established for the call transfer. This enables e.g. the vogue script to play individual Music on Hold (MoH) during the time required for setting up the connection.
With all other D-channel protocols (value=0) the caller is set to Hold while a second connection is established for the call transfer. In this way the caller automatically hears the MoH of the PBX.
- **Srv:**
All CAPI services that are supported by the card.
Several services are preset by default. Normally a service only needs to be deactivated, if a card cannot handle it. However, this is an error of the board.

PrivateMode [REG_DWORD]

Default:	0
Remark:	<i>TeleReg.</i> Must not be modified.

Is only used by the quality assurance to adjust the internal value **PrivProfile** for the validation of new ISDN boards.

State [REG_DWORD]

Remark:	<i>TeleReg.</i> See State [REG_DWORD] .

Type [REG_DWORD]

Remark:	<i>TeleReg.</i> See Type [REG_DWORD] .

E.20.2.4 Trunk Groups

A trunk group describes the summary of several ² logical, bidirectional communication channels of a single device. Only channels of a coherent section can be summed up to one trunk group.

Each single trunk group is assigned one of the configured protocols.

For each trunk group a consecutively numbered key *m* exists under the

HKLM\Software\Wow6432Node\PP-COM\MRS\ISDNApi\Devices\n

key of the associated device. In this key you find the following values that define all properties of the relevant trunk group.

BaudRate [REG_DWORD]

Remark:	TeleReg. See BaudRate [REG_DWORD] .

Blob [REG_DWORD]

Remark:	TeleReg. See Blob [REG_DWORD] .

BoundExtensions [REG_SZ]

Default:	–
Possible values:	0 – Extension of this station is not assigned to the trunk group 1 – Extension of this station is assigned to the trunk group

Defines which extensions are assigned to the considered trunk group.

The contained value consists of 64 digits the may adopt value **1** or **0** each. The position of **1** or **0** in the digit string specifies the number of the assigned or not assigned extension. The first digit describes the assignment of the first extension, the second digit the assignment of the second extension etc.

Example: 101100000000...

In this example the trunk groups 1, 3 and 4 are assigned to the considered trunk group.

BoundProtocols [REG_DWORD]

Remark:	TeleReg. See BoundProtocols1 [REG_DWORD] .

CalledNumberWithTrunkCode [REG_DWORD]

Default:	0
Possible values:	0 – PBX transfers tie line number 1 – PBX does not transfer tie line number

Defines whether the connected PBX transfers the tie line number together with a phone number to the XPR server.

2. In extreme cases such a trunk group can include only one communication channel.

CallingNumberNoExternalPrefix [REG_DWORD]

Default:	0
Possible values:	0 – PBX transfers external prefix with type <i>Unknown</i> 1 – PBX does not transfer external prefix with type <i>Unknown</i>

Defines whether the PBX transfers originator numbers of type *Unknown* without external prefix to the XPR server.

Cost [REG_DWORD]

Remark:	<i>TeleReg.</i> See Cost [REG_DWORD] .

EndChannel [REG_DWORD]

Remark:	<i>TeleReg.</i> See EndChannel [REG_DWORD] .

NumChannel [REG_DWORD]

Remark:	<i>TeleReg.</i> See NumChannels [REG_DWORD] .

OAD [REG_DWORD]

Remark:	<i>TeleReg.</i> See OAD [REG_DWORD] .

PermMask [REG_DWORD]

Remark:	<i>TeleReg.</i> See PermMask [REG_DWORD] .

StartChannel [REG_DWORD]

Remark:	<i>TeleReg.</i> See StartChannel [REG_DWORD] .

State [REG_DWORD]

Remark:	<i>TeleReg.</i> See State [REG_DWORD] .

E.20.2.5 Extension number ranges

Each phone number dialed in the XPR server must be within the range indicated here with its extension, so that the incoming call can be accepted by the respective APL.

If the board delivers an ISDN Service Indicator it will be checked against a list of applicable protocols.

The following general registry value is found under the

HKLM\Software\Wow6432Node\PP-COM\MRS\ISDNapl\Extensions
key.

EnableRegSZ [REG_DWORD]

Remark:	<i>TeleReg.</i> See EnableRegSz [REG_DWORD] .

For each supported service normally one extension number range must be configured. All configured ranges are numbered ascendingly and stored as a separate key with their respective number under the key

HKLM\Software\Wow6432Node\PP-COM\MRS\ISDNapl\Extensions
as a separate key. In each of these keys the following values are found.

Blob [REG_DWORD]

Remark:	<i>TeleReg.</i> See Blob [REG_DWORD] .

Description [REG_SZ]

Remark:	<i>TeleReg.</i> See Description [REG_DWORD] .

End [REG_SZ]

Remark:	<i>TeleReg.</i> See End [REG_SZ] .

MSN [REG_SZ]

Remark:	<i>TeleReg.</i> See MSN [REG_SZ] .

OAD [REG_DWORD]

Remark:	<i>TeleReg.</i> See OAD [REG_DWORD] .

Protocol [REG_DWORD]

Remark:	<i>TeleReg.</i> See Protocol [REG_DWORD] .

Start [REG_SZ]

Remark:	<i>TeleReg.</i> See Start [REG_SZ] .

State [REG_DWORD]

Remark:	<i>TeleReg.</i> See State [REG_DWORD] .

VarDigits [REG_DWORD]

Remark:	<i>TeleReg.</i> See VarDigits [REG_DWORD] .

E.20.2.6 Protocols

Protocols are services supported by the various APLs. For each installed protocol a consecutively numbered key n exists under the

HKLM\Software\Wow6432Node\PP-COM\MRS\ISDNapl\Protocols

a continuously numerated key n is found. This contains the following values.

Attributes [REG_MULTI_SZ]

Remark:	<i>TeleReg</i> . See Attributes [REG_MULTI_SZ] .

AttributesAllowed [REG_DWORD]

Remark:	<i>TeleReg</i> . See AttributesAllowed [REG_DWORD] .

Blob [REG_DWORD]

Remark:	<i>TeleReg</i> . See Blob [REG_DWORD] .

CapMask [REG_DWORD]

Remark:	<i>TeleReg</i> . See CapMask [REG_DWORD] .

CheckMailbox [REG_DWORD]

Remark:	<i>TeleReg</i> . See CheckMailbox [REG_DWORD] .

ContMsg [REG_SZ]

Remark:	<i>TeleReg</i> . See ContMsg [REG_SZ] .

Description [REG_SZ]

Remark:	<i>TeleReg</i> . See Description [REG_SZ] .

DispPerm [REG_DWORD]

Remark:	<i>TeleReg</i> . See DispPerm [REG_DWORD] .

DocReps [REG_SZ]

Remark:	<i>TeleReg</i> . See DocReps [REG_SZ] .

EditPerm [REG_DWORD]

Remark:	<i>TeleReg</i> . See EditPerm [REG_DWORD] .

EditPermGenerated [REG_DWORD]

Remark:	<i>TeleReg.</i> See EditPermGenerated [REG_DWORD] .

FaxG3Chain [REG_DWORD]

Remark:	<i>TeleReg.</i> See FaxG3Chain [REG_DWORD] .

FaxG3Resend [REG_DWORD]

Remark:	<i>TeleReg.</i> See EditPermGenerated [REG_DWORD] .

FaxG4FaxG3 [REG_DWORD]

Remark:	<i>TeleReg.</i> See FaxG4FaxG3 [REG_DWORD] .

FaxG4T70 [REG_DWORD]

Remark:	<i>TeleReg.</i> See FaxG4T70 [REG_DWORD] .

FaxID [REG_MULTI_SZ]

Remark:	<i>TeleReg.</i> See FaxId [REG_SZ] .

Formats [REG_MULTI_SZ]

Remark:	<i>TeleReg.</i> See Formats [REG_SZ] .

FormatsAllowed [REG_DWORD]

Remark:	<i>TeleReg.</i> See FormatsAllowed [REG_DWORDS] .

FriendlyName [REG_SZ]

Remark:	<i>TeleReg.</i> See FriendlyName [REG_SZ] .

Headline [REG_SZ]

Remark:	<i>TeleReg.</i> See Headline [REG_SZ] .

MultiMaster [REG_DWORD]

Remark:	<i>TeleReg.</i> See MultiMaster [REG_DWORD] .

Name [REG_SZ]

Remark:	<i>TeleReg.</i> See Table on page 1885.

ParamBlock [REG_SZ]

Remark:	TeleReg. See ParamBlock [REG_SZ] .

Private [REG_MULTI_SZ]

Default:	<Empty string>
Possible values:	<Initialization entry per line>

Defines APL-specific entries. Depending on the protocol one specific entry per line is used by the ISDN APL.

1. *Fax G3*:

- **CheckPageNumbers**
When set to **1** an OK report is only sent when the number of sent pages reported by the CAPI driver corresponds to the number of pages in the document. Otherwise it would be possible to receive an "OK (2 pages sent)" report for a four-page document.
- **DocChainIgnoreOrig**
Only documents with identical recipient and originator address are chained in the Fax G3 protocol document chaining when this value is set to **0**. **1** initiates a chaining if the recipient address is identical. The originator address is not observed then. In this case correct billing information specifically for the originators is not possible.
- **EvalNLCauseForSubject**
With **1**, the text "Transmission not completed" is added to the subject line if fax message receiving is terminated with another reason than "Normal".
- **InsertMidHI**
With **1**, the document message ID is inserted into the headline. If used, a maximum of 22 characters for the headline is allowed.
- **UseFaxIdAsOAD**
Calling Line Identification (CLI) would be used as the originator's OAD with inbound fax documents. If this field is empty while no CLI can be determined, the number in the fax ID will be used as CLI. When this value is set to **1** the fax ID will always be used as the CLI with inbound fax documents.

2. *Fax G4*:

- **RejectUnknown**
With **1**, fax messages that cannot be related to a recipient are dismissed as undeliverable.

3. *Fax Forward (Server / Transparent)*:

- **FfuAmt**
Only when the IntlDialMode is set to **0** an external line prefix for Fax Forward Reports can be configured here. Normally LinePrefix would be used.
- **FfuSendErrRep**
When set to **1** an error report will be sent to the transmitting device by the XPR server when an error occurs in Fax Forward mode.
- **FfuSendMidInId**
The value **1** transmits the message ID of the XPR server to the internal fax device for fax forward.
- **FfuSendOkRep**
When set to **1** an error report will be sent to the transmitting device by the XPR server when an error occurs in Fax Forward mode.
- **FfuSendRundRep**
When set to **1** a receipt report (with all recipients) will be sent to the transmitting device from the XPR server by successful transmission of a distribution list in Fax Forward mode.

4. *ISDN SMI:*

- **ShortHold**
Short-Hold timer in seconds for SMI connections (Client/Server or Server/Server) via ISDN.
After the number of seconds entered here the connection is abolished in case no transmission was performed. Exception: with an existing dialog the connection is only abolished after the dialog has been terminated. If the value is set to **0**, this mechanism remains principally deactivated. The connection is consistent then.
Default: **60** [seconds]

5. *ISDN SMS:*

- **DefaultId**
Defines a global originator ID for SMS messages sent via the ISDN APL and the UCP protocol.
The UCP protocol can transfer an originator ID. This ID is usually taken from the SMS XPR database field of the sending user. As alternative, a global originator ID can be defined in **DefaultId**.
Vodafone D2 uses UCP, whereas German Telekom uses TAP, which does not allow originator ID transmission.
- **Digest**
The contents of a SMS message can be supplemented and/or modified before transmission. This includes rerouted messages to be sent as SMS message. It is, for example, possible to add the send time to a message.

Examples of a digest definition:

{ORGNOME}:{SUBJECT,80}-{DIGEST,40}

The following variables are available for supplementing or modifying messages:

- { DATE }
Defines the current date.
- { DIGEST [, <Max>] }
Long messages to be sent can be shortened according to the Digest Algorithm. In doing so the attempt is made to remove non-information elements (such as blank lines or salutation phrases) from the text.
The maximum length of the digest can be defined by the <Max> parameter. If the message text is longer, it is cut after <Max> characters and supplemented with '...' at the end.
- { FORMAT }
Defines the format of the original message (e.g. voice, fax or e-mail). This information is particularly interesting with message rerouting.
- { ORGNOME [, <Max>] }
Defines a legible version of the originator address. If e.g. an originator is contained in the speed dialing database, the actual originator name may be contained here instead of his/her phone number.
The maximum length of the address can be defined by the <Max> parameter. If the originator address is longer, it is cut after <Max> characters and supplemented with '...' at the end.
- { ORGNODE }
Defines the service type of the original message. This information is particularly interesting with message rerouting.
- { ORGUSER }
Defines the original originator address. This information is particularly interesting with message rerouting.
- { RECNAME [, <Max>] }
Defines a legible version of the recipient address. The maximum length of the legible recipient name can be specified by the optional entry <Max>. If the recipient address is longer, it is cut after <Max> characters and supplemented with '...' at the end.
- { RECNODE }
Defines which service has originally received the message. This information is particularly interesting with message rerouting.
- { RECUSER }
Defines the original recipient address. This information is particularly interesting with message rerouting.

- {SUBJECT[, <Max>] }
Defines the subject of the original message. This information is particularly interesting with message rerouting.
The maxim length of the subject information can be defined by the <Max> parameter. If the original subject is longer, it is cut after <Max> characters and supplemented with '...' at the end.
- {TIME}
Defines the current time.

6. Voice

- FileToPlay
Default announcement file for incoming calls.
- RecordTime
Maximum recording time for incoming calls in seconds.
Default: 120 [seconds]
- RemoteRecord
During an outbound call the remote recording mode is activated (**1**) or ignored (**0**).
- StorePath
Indication of the path in which the conversations recorded in the RemoteRecord mode are stored.

PrivateMode [REG_DWORD]

Remark:	<i>TeleReg.</i> Not used by the ISDN APL.

ScriptName [REG_SZ]

Remark:	<i>TeleReg.</i> See ScriptName [REG_SZ] .

SI [REG_MULTI_SZ]

Remark:	<i>TeleReg.</i> See SI [REG_SZ] .

State [REG_DWORD]

Remark:	<i>TeleReg.</i> See State [REG_DWORD] .

Type [REG_DWORD]

Remark:	<i>TeleReg.</i> See Type [REG_DWORD] .

E.20.2.7 Voice and Fax-on-Demand Systems

You find the values for installed VFS scripts under the following key:

HKLM\Software\Wow6432Node\PP-COM\MRS\IsdnApl\Vfs

AclAddress [REG_SZ]

Default:	NVS:HICOMDLG/VFS
Possible values:	<logical NVS address>

NVS address of the CTI APL line to the Hicom 300.

AclDelayMessage [REG_DWORD]

Default:	400 [Milliseconds]
Possible values:	<Time> [Milliseconds]

All display texts are collected and sent to the CTI APL after *n* milliseconds. Netload is reduced when numerous texts must be simultaneously displayed.

AclInternLen [REG_DWORD]

Default:	<Empty string>
Possible values:	<Phone number length>
Remark:	In connection with AclInternMax [REG_DWORD] .

Together with [AclInternMax \[REG_DWORD\]](#) a phone number length range is determined. **AclInternLen** defines the bottom limit of this phone number range.

If the XPR server is called and the length of the caller ID is within the range between **AclInternLen** to **AclInternLenMax**, the ACL functions would be used and the display text shown on the callers telephone.

Thus sending display texts to an external caller is avoided.

AclInternMax [REG_DWORD]

Default:	<Empty string>
Possible values:	<Phone number length>
Remark:	In connection with AclInternLen [REG_DWORD] .

Together with [AclInternLen \[REG_DWORD\]](#) a phone number length range is determined. **AclInternMax** defines the upper margin of this phone number range.

If the XPR server is called and the length of the caller ID is within the range between **AclInternLen** to **AclInternLenMax**, the ACL functions would be used and the display text shown on the callers telephone.

Thus sending display texts to an external caller is avoided.

AclUse [REG_DWORD]

Default:	0
Possible values:	0 – Deactivates ACL control function of VFS 1 – Activates ACL control function of VFS

If the Hicom APL is running as a part of the XPR server, the ACL control functions of VFS can be switched on when the value of **1** is set. These functions can be used by VFS scripts to e.g. display messages on the Hicom telephones.

DisplayColumns [REG_DWORD]

Default:	24
Possible values:	<Display Column Number>

Number of columns in the Hicom telephone display. This entry is required when text from an ACL function is to be sent to the Hicom telephone display.

DisplayRows [REG_DWORD]

Default:	2
Possible values:	<Display Line Number>

Number of lines in the Hicom telephone display. This entry is required when text from an ACL function is to be sent to the Hicom telephone display.

ErrDetect [REG_DWORD]

Remark:	Not used at the moment.

Log<n> [REG_SZ]

Default:	<Empty string>
Possible values:	<Line with structure as described below>

An individual log file can be written for every VFS script. To enable this, this entry is created with content

Prg<x>,<log-dir>,<log-intervall>,<headline>

.

- <n>
Defines a sequential number that exclusively serves for differentiating the various log entries in the registry.
- <x>
corresponds to the registry entry **Prg<x>**, whereas allocation of the log files to specific scripts is given.
- <log-dir>
Defines the directory in which the log files are stored.
- <log-intervall>
Defines the interval at which new log files are created.
Allowable are:

 <x>D: Specifying all <x> days in a new log file
 <x>M: Specifying all <x> months in a new log file
 <x>h: Specifying all <x> hours in a new log file
 <x>M: Specifying all <x> minutes in a new log file
- <headline>
Defines an arbitrary string which is written in the headline of the log file.

The contents of the log file is controlled by the script. Specific entries in log files can be used by the script for which the file was created.

LogName<n> [REG_SZ]

Default:	<Empty string>
Possible values:	<Logical Program Name>
Remark:	In connection with <i>Prg<n></i> [REG_SZ].

For each of the VFS scripts listed under **Prg<n>** you can create an entry **LogName<n>**, with the index <n> having to be identical in each case. The content of **LogName<n>** is a logical program name under which the script can be addressed.

Subsequently the script *Prg5* can be addressed e.g. with the address
 NVS : <LogName5>/4711.

PeakDuration [REG_DWORD]

Default:	5 [1/60 seconds]
Possible values:	<Time:> [1/60 seconds]
Remark:	Requires calling the voice recording feature VocRec() in the VFS script in the mode VOC_RECMODE_CHECKFIRSTPEEK. In connection with PeakLevel [REG_DWORD] .

Defines that a voice recording starts only, when anything other than silence is recognized (the so-called “First Peak”). The two values [PeakDuration \[REG_DWORD\]](#) and [PeakLevel \[REG_DWORD\]](#) serve for this.

The value in **PeakDuration** indicates in approximately 1/60 second units how long the incoming audio signal must be above **PeakLevel** so that recording is started. So the sensibility of the signal recognition can be adjusted.

Recognition becomes more sensitive when the value for **PeakDuration** is decreased.

PeakLevel [REG_DWORD]

Default:	32
Possible values:	<Level>
Remark:	Requires calling the voice recording feature VocRec() in the VFS script in the mode VOC_RECMODE_CHECKFIRSTPEEK. In connection with PeakDuration [REG_DWORD] .

Defines that a voice recording starts only, when anything other than silence is recognized (the so-called “First Peak”). The two values [PeakDuration \[REG_DWORD\]](#) and [PeakLevel \[REG_DWORD\]](#) serve for this.

This value indicates which level the incoming audio signal must reach in order to start recording. So the sensibility of the signal recognition can be adjusted.

Recognition becomes more sensitive when the value for **PeakLevel** is decreased.

Prg<n> [REG_SZ]

Default:	-
Possible values:	Up to 16 entries in the form Prg<n>

Each of these registry keys defines a VFS script. Up to 16 VFS scripts (registry keys) can be defined.

Each entry is in the form: <Script name> <Parameter>

- *Script name*: File name of the script
- *Parameter*: Optional parameters for the respective script

Example: mck.c

SilentTime [REG_DWORD]

Default:	20 [1/10 seconds]
Possible values:	<Time> [1/10 seconds]
Remark:	Requires calling the voice recording feature VocRec() in the VFS script in the mode VOC_RECMODE_CHECKSILENT.

Time of silence in approx. 1/10 seconds after which recording is automatically terminated.

SoftFaxFilter [REG_DWORD]

Default:	0
Possible values:	0 – Deactivates the software fax device detection 1 – Activates the software fax device detection

Defines whether software fax device detection is activated in the XPR server.

This option normally does not need not be activated for ISDN boards, since the detection is performed by the ISDN boards.

Stat<n> [REG_DWORD]

Default:	–
Possible values:	See description
Remark:	In connection with <i>Prg<n></i> [REG_SZ].

Analog to the individual log files, a VFS script can store individual statistics in files. A **Stat<n>** entry of the format

Prg<x>, <dir>, <stat-time>, <headline>, <stat-class>

is created in the registry for this purpose.

- <n>:
Defines a sequential number exclusively used for differentiating the various statistical entries in the registry.
- <x>:
Corresponds to the number of the registry key *Prg<x>*, whereby allocation of the statistical files to specific scripts is given.
- <dir>:
Defines the directory where statistical files are stored. The statistical file is an ASCII text file.
- <stat-time>:
Defines the time in the format *hh:mm* (*Hour:Minutes*) at which statistics are regularly created. This statistics generation should occur at night.

- `<headline>`:
Defines an arbitrary string that appears in the header of the statistics file.
- `<stat-class>`:
Defines an arbitrary string used for representing the statistical class.

(Principally a counter is found in the Correlation database for statistical classes. The counter is increased by 1 for every call of the function **IncStatCnt()** in the VFS script. The statistical function of the VFS script reads the database entry once a day and creates a statistical file corresponding to the given class.)

The statistic file contains entries in the form: *StatKey<\t>Counter<\n>*.

UseSpr [REG_DWORD]

Default:	1
Possible values:	0 – Deactivates speech recognition 1 – Activates speech recognition

Defines whether speech recognition is activated in the XPR server or not.

XmrTopic [REG_DWORD]

Default:	1
Possible values:	0 – VFS topic range is not displayed 1 – VFS topic range is displayed

Defines whether or not the VFS topic range of the ISDN APL is displayed in the XPR monitor.

E.20.3 IP APL Registry Keys

This section describes the IP APL registry values. Only the registry entries available in addition to the TeleReg entries are depicted in detail. The registry entries of the TeleReg API are correspondingly marked and described in [Section E.20.1, “Registry Keys of the TeleReg”, on page 1860](#).

The information is structured in the following manner:

- [General Entries](#)
- [Blobs \(Binary Large Objects\)](#)
- [Devices](#)
- [Trunk Groups](#)
- [Extension number ranges](#)
- [FAX G3 Support](#)
- [Protocols](#)
- [Voice and Fax-on-Demand Systems](#)

E.20.3.1 General Entries

The following general registry values are found under the key:

HKLM\Software\Wow6432Node\PP-COM\MRS\IpAp1

AdjustIncFaxLevel [REG_DWORD]

Default:	0
Possible values:	0: Adjust Incoming Faxlevel is not enabled 1: Adjust Incoming Faxlevel is enabled

AdjustOutgFaxLevel [REG_DWORD]

Default:	0
Possible values:	0: Adjust Outgoing Faxlevel is not enabled 1: Adjust Outgoing Faxlevel is enabled

AplIndex [REG_DWORD]

Default:	<APL index>
Possible values:	<APL index>

Defines the logical index of an IP APL that unambiguously designates each IP APL of an XPR installation. The APL index corresponds to the system index of an XPR node. The system index of the kernel node is *0*, the system index of the first satellite *1* etc.

The XPR addresses of the logical lines also derive from the APL index.

Example: NVS:FAXG3.I1.0101

The '1' that follows the denominator 'I' describes the APL index plus 1. In our example we thus deal with the IP APL of the XPR node with the system index *0* – thus a kernel node APL.

The APL index can e.g. be used to logically summarize the IP APLs of several XPR satellites of a location. For this, the APL indices of the respective APLs must simply be set to the same value in the registry.

Example:

We assume the presence of two XPR satellites with the system indices 3 and 4 in one location. The APL indices of the IP APLs then also read 3 and 4 by default. Derived from this, the associated fax lines of the IP APLs on these satellites have the denominators *NVS:FAXG3.I4.0101* or

NVS:FAXG3.I5.0101.

If the registry value **AplIndex** is set to 3 on both XPR satellites, the fax lines on both satellites will be labeled *NVS:FAXG3.I4.0101* and can thus be addressed together via Routing Rules.

BuiltInDtmf [REG_DWORD]

Remark:	<i>Not used by the IP APL at the moment.</i>

Checked<n> [REG_DWORD]

Remark:	<i>TeleReg. See Checked<n> [REG_DWORD].</i>

CLIMode [REG_DWORD]

Remark:	<i>Not used by the IP APL at the moment.</i>

ConvRecProtocol [REG_SZ]

Default:	–
Possible values:	<Protocol name>

In case of an Alcatel OXE R8/R9 with SIP support there is a special button for recording telephone conversation. When you push this button, a second connection as conference with Ergo is usually set up. You cannot configure this number, which always addresses the external voicemail system.

If, however, this key is pushed, a special parameter is transferred. At the parameter's transfer the IP APL checks whether a protocol is entered here. If so, this protocol is addressed instead of the voicemail number.

Just for this case you can configure the Conversation Recorder as protocol with the **Recordonly** parameter. The recording button at the Alcatel OXE R8/R9 will then work.

Cost [REG_DWORD]

Remark:	<i>Not used by the IP APL at the moment.</i>

DefaultCli [REG_SZ]

Remark:	<i>Not used by the IP APL at the moment.</i>

DestNumberPlan [REG_DWORD]

Remark:	<i>Not used by the IP APL at the moment.</i>

DestNumberType [REG_DWORD]

Remark:	<i>Not used by the IP APL at the moment.</i>

DlgFlags [REG_DWORD]

Remark:	Must not be modified.

Defines which registers are displayed in the configuration dialog of the APL.

EnableCDRHeader [REG_DWORD]

Default:	0
Possible values:	0 – Deactivate the X-Siemens CDR Header for billing 1 – Activate the X-Siemens CDR Header for billing
Remark:	If you want to change the described default behavior, you need to manually create this value in the registry first.

Defines whether the X-Siemens CDR Header is transmitted to the connected PBX for billing.

If the X-Siemens CDR Header is active, the IP APL uses this header for outgoing SIP-INVITE messages. The IP APL determines the information transmitted in the header by the **CostInfo** field of the XPR user database in the following way:

- By the **CostInfo** field defined for the relevant user.
- By the **CostInfo** field defined for the user group of the relevant user if the **CostInfo** field has not been filled in for the relevant user.
- By the **CostInfo** field defined for the tenant of relevant user if the **CostInfo** field has been filled in neither for the relevant user nor for the relevant user group.

- If the **CostInfo** field has been filled in neither for the user nor user group or tenant, the X-Siemens CDR Header is used to transfer the phone number from the FROM field of the associated SIP header. For OpenScape Voice, the normalized phone number without leading + character is thereby used.

EndingSilence [REG_DWORD]

Default:	0
Possible values:	0 – Cut DTMF tone from the RTP stream. 1 – Replace DTMF tone in the RTP stream with silence.

In G.729A there is the implemented PLC (Pack Loss Concealment) feature, which cannot be disabled. This feature ensures that the last packs are taken and the attempt is made, to interpolate the lost pack from these. A recognized DTMF tone is usually simply cut out and with G.729A this leads to an unwanted result by the PLC. By replacing the DTMF pack with silence, no packs are lost from the G.729A view and the PLC does not become active.

FakeOriginator [REG_DWORD]

Default:	0
Possible values:	0 – Originator number and destination number may be identical 1 – In case of identity, the originator number is replaced with * characters

With some PBXs problems occur if originator and destination number are identical. If this value is set, the identical originator number is replaced with the * character.

FaxLicences [REG_DWORD]

Remark:	<i>Not used by the IP APL at the moment.</i>

FaxResources [REG_DWORD]

Remark:	<i>Not used by the IP APL at the moment.</i>

LineLicences [REG_DWORD]

Remark:	<i>Not used by the IP APL at the moment.</i>

LineResources [REG_DWORD]

Remark:	<i>Not used by the IP APL at the moment.</i>

MaxAlertTime [REG_DWORD]

Default:	60 [Seconds]
Possible values:	<Time> [Seconds]

Defines a time after which each connection request is terminated that has not been accommodated until then.

MaxConnectTime [REG_DWORD]

Default:	60 [minutes]
Possible values:	<Time> [minutes]

Defines a time after which each connection still active is terminated.

NumberTypeMode [REG_DWORD]

Remark:	<i>Not used by the IP APL at the moment.</i>

OrigNumberPlan [REG_DWORD]

Remark:	<i>Not used by the IP APL at the moment.</i>

OrigNumberType [REG_DWORD]

Remark:	<i>Not used by the IP APL at the moment.</i>

PhonemailUserDependantRouting [REG_DWORD]

Default:	1
Possible values:	0 – Inactive. 1 – Use <code>PMROUTPREFIX</code> as prefix.

So that with PhoneMail user outcalls can be sent via different gateways depending on the user, you can write a dial prefix in the `PMROUTPREFIX` database field and activate it here.

PhoneNrSilenceLength [REG_DWORD]

Default:	200 [Milliseconds]
Possible values:	<Time> [Milliseconds]

Defines the pause length between single digits with announcing phone numbers to a user.

QueryBilling [REG_DWORD]

Remark:	<i>Not used by the IP APL at the moment.</i>

RoutingAccessLevel [REG_DWORD]

Default:	0
Possible values:	0- 127

You can set value “Routing Access Authorization” in the ISDN drivers of Dialogic. If, for example, you are connected to a HiPath 4000 via the IP APL, you can set this value here. This may be necessary for enabling the XPR server to phone via a trunk line. In such a case, set this value to 127.

SSL_TLsv1_Enable [REG_DWORD]

Default:	0
Possible values:	0: TLS 1.0 protocol disabled 1: TLS 1.0 protocol enabled

to full security both SSL_CBC_Enable and SSL_TLsv1_Enable must be set to 0.

By default TLSv1.2 is enabled.

SSL_TLsv1_1_Enable [REG_DWORD]

Default:	0
Possible values:	0: TLS 1.1 protocol disabled 1: TLS 1.1 protocol enabled

Used to disable TLS 1.1 on WebAp
This configuration does not affect outgoing connections.

By default TLSv1.2 is enabled.

SupportedDevices [REG_MULTI_SZ]

Remark:	<i>Not used by the IP APL at the moment.</i>

TransBreak [REG_DWORD]

Remark:	<i>Not used by the IP APL at the moment.</i>

TransMax [REG_DWORD]

Remark:	<i>Not used by the IP APL at the moment.</i>

UseCtiMonitorPoint [REG_DWORD]

Default:	0
Possible values:	0 – No monitor point is set on the APL 1 – A monitor point is set on the APL

To administer Call Attached Data (CAD) correctly, the CTI APL must be informed when a call status changes in the IP APL. To this, the CTI APL must set a monitor point on the IP APL.

If this registry value is set to **1**, such a monitor point will be configured.

UserDependantRouting [REG_DWORD]

Default:	1
Possible values:	0 – Inactive. 1 – Use FAXROUTPREFIX as prefix.

So that fax messages can be sent via different gateways depending on the sending user, you can write a dial prefix in the FAXROUTPREFIX database field and activate it here.

UseLastDiversion [REG_DWORD]

Default:	0
Possible values:	0 – Use the first diversion number. 1 – Use the last diversion number.

A new registry key needs to be added in the IpApl for allowing the last diversion number to be provided to TUI scripts in concatenated call forwarding scenarios.

VoiceLicences [REG_DWORD]

Remark:	<i>Not used by the IP APL at the moment.</i>

VoiceRecFormat [REG_DWORD]

Default:	0xffffffff
Possible values:	0x02000000 (33554432) – A-law 8Khz Mono 0x10000000 (268435456) – μ -law 8Khz Mono 0xffffffff (4294967295) – PCM 8Khz Mono
Remark:	If you want to change the described default behavior, you need to manually create this value in the registry first.

Defines the codec that the IP APL uses for voice recordings. Cf. [Section 10.1.7.2, “IP APL Memory Requirements”, on page 558.](#)

VoiceResources [REG_DWORD]

Remark:	<i>Not used by the IP APL at the moment.</i>

WaitForGeb [REG_SZ]

Remark:	<i>Not used by the IP APL at the moment.</i>

WaitForIsdnMwiInd [REG_DWORD]

Remark:	<i>Not used by the IP APL at the moment.</i>

E.20.3.2 Blobs (Binary Large Objects)

Every registry entry administered by the TeleReg API may contain a reference to a Blob. Blobs are binary data ranges in which programmer-defined data may be stored.

This mechanism is currently not used by the IP APL. Blobs used can be found in the registry under the key:

`HKLM\Software\Wow6432Node\PP-COM\MRS\IpApl\Blobs`

E.20.3.3 Devices

In case of the IP APL a device corresponds e.g. to a TAPI driver that is installed on the XPR server system. For each of these devices a consecutively numbered key *n* exists under the

`HKLM\Software\Wow6432Node\PP-COM\MRS\IpApl\Devices`

key. These contain respectively the following registry values that describe the properties of the individual physical interfaces.

AddDialOutLen [REG_DWORD]

Remark:	<i>TeleReg.</i> See AddDialOutLen [REG_DWORD] .

Blob [REG_DWORD]

Remark:	<i>TeleReg.</i> See Blob [REG_DWORD] .

Caps [REG_DWORD]

Remark:	<i>TeleReg.</i> See Caps [REG_DWORD] .

Channels [REG_DWORD]

Remark:	<i>TeleReg.</i> See Channels [REG_DWORD] .

Description [REG_SZ]

Remark:	<i>TeleReg.</i> See Description [REG_SZ] .

FaxG3 [REG_DWORD]

Remark:	<i>TeleReg.</i> See FaxG3 [REG_DWORD] .

Handle [REG_DWORD]

Remark:	<i>TeleReg.</i> See Handle [REG_DWORD] .

Lines [REG_DWORD]

Remark:	<i>TeleReg.</i> See Lines [REG_DWORD] .

Name [REG_SZ]

Remark:	<i>TeleReg.</i> See Name [REG_DWORD] .

PrefixedANI [REG_DWORD]

Remark:	<i>TeleReg.</i> See PrefixedAni [REG_DWORD] .

Private [REG_MULTI_SZ]

Default:	<Empty string>
Possible values:	<Initialization entry per line>
Remark:	<i>TeleReg.</i>

Defines IP APL-specific configuration data. A specific entry of the format *<Label> = <Value>* is performed per line with *<Label>* determining the respective setting name *and* *<Value>* the desired content of the respective setting.

Example: GK=10.1.35.15

The IP APL provides parameters for the following devices:

- [SIP device](#)

- [H.323-/CorNet-IP device](#)
- [Cisco IP PBX Service Provider](#)

1. SIP device

- **CLUSTERGW1**=<IP address>:<port number>
CLUSTERGW2=<IP address>:<port number> etc to
CLUSTERGWn=<IP address>:<port number>

The IP APL can be connected with several SIP gateways of an SIP cluster for redundancy. The **CLUSTERGW** parameters define the connection data of the different gateways that can be used by the IP APL.

By default, the IP APL uses the gateway that is configured via the XPR monitor to send SIP signals and MWI messages. (This gateway should also be defined with one of the **CLUSTERGW** parameters). If this connection fails, it uses the connection data of the first **CLUSTERGW** parameter. If this connection fails also, the next parameter is used etc. When the last **CLUSTERGW** parameter is reached, the IP APL starts again with the first parameter of the list. The **CLUSTERCNT** and **CLUSTERTIMESENS** parameters define when the IP APL considers a connection to an SIP gateway failed. After a reboot the IP APL always uses the gateway deployed last. (See also [Section 10.3.15, "IP APL at an SIP Gateway Cluster"](#), on page 591.)

- **CLUSTERCNT**=<whole number>
 To determine whether a connection to an SIP gateway failed, the IP APL uses so-called failure windows. If the IP APL detects at least one SIP or MWI connection error in such a failure window, the communication within this failure window is considered failed. **CLUSTERCNT** defines after how many failure windows with failed communication the IP APL considers the communication failed and uses the next SIP gateway. Every successful connection resets the current number of failure windows with failed communication to 0. If value **1** is configured for **CLUSTERCNT**, the IP APL uses the next SIP gateway immediately after the first connection error.

Default: 1

- **CLUSTERTIMESENS**=<time [milliseconds]>
 The IP APL uses so-called failure windows to determine whether the connection to an SIP gateway has failed. **CLUSTERTIMESENS** defines how long each failure window lasts. The IP APL starts the first failure window with the first connection error. Based on this connection error the communication within the first failure window is considered failed. If value **1** has been configured for **CLUSTERCNT**, the IP APL uses the next SIP gateway

immediately after the first connection error and the setting of **CLUSTERTIMESENS** is irrelevant.

Default: **60000** [milliseconds]

- **FAX_CNG_TONE=<0, 1>**
Specifies whether the IP APL sends inband the CNG fax tone to the called subscriber for outgoing T.38 fax messages.
0 – Deactivates the CNG fax tone for outgoing T.38 fax messages
1 – Activates the CNG fax tone for outgoing T.38 fax messages
Default: **1**
- **FAX_CED_TONE=<0, 1>**
Specifies whether the IP APL sends inband the CED fax tone to the calling subscriber for incoming T.38 fax messages.
0 – Deactivates the CED fax tone for incoming T.38 fax messages
1 – Activates the CED fax tone for incoming T.38 fax messages
Default: **1**
- **G711FAXREINVITE=<0, 1>**
Defines whether the IP APL tries to handle inbound fax messages using G.711 in case of a set G.729 codec, which does not allow fax.
0 – Fax not possible with G.729. Call is terminated.
1 – Attempt is made to switch the call to G.711.
Default: **0**
- **HOLDFORBLINDTRANSFER=<0, 1>**
If music-on-hold is to be played to a user via an XPR script, the XPR server must not place such calls in the HOLD connection state in case of a forwarding. In this case the caller would otherwise hear the PBX waiting music.
The **HOLDFORBLINDTRANSFER** parameter specifies whether the XPR server places calls in the HOLD state in case of a blind transfer. The performed setting is valid for all XPR scripts.
0 – Deactivates the HOLD state in case of a forwarding (blind)
1 – Activates the HOLD state in case of a forwarding (blind)
Default: **1**
- **HOLDFORSUPTRANSFER=<0, 1>**
If music-on-hold is to be played to a user via an XPR script, the XPR server must not place such calls in the HOLD connection state in case of a forwarding. In this case the caller would otherwise hear the PBX waiting music.
The **HOLDFORSUPTRANSFER** parameter specifies whether the XPR server places calls in the HOLD state in case of a supervised transfer.
If the setting is **0**, it is valid for all XPR scripts.
If the setting is **1**, it is valid for all XPR scripts except Vogue. For Vogue the setting in the **HOLDFORVOGUETRANSFER** parameter is evaluated in this case.

- 0** – Deactivates the HOLD state in case of a forwarding (supervised)
- 1** – Activates the HOLD state in case of a forwarding (supervised)

Default: 1

- **HOLDFORVOGUETRANSFER=<0, 1>**

If music-on-hold is to be played to a user via a script, the XPR server must not place such calls in the HOLD connection state in case of a forwarding. In this case the caller would otherwise hear the PBX waiting music.

The **HOLDFORSUPTRANSFER** parameter specifies whether the Vogue script places calls in the HOLD state in case of a forwarding.

- 0** – Deactivates the HOLD state in case of a forwarding (Vogue)

- 1** – Activates the HOLD state in case of a forwarding (Vogue)

Default: 1

- **KEEPMEDIA=<0, 1>**

If **KEEPMEDIA** is set to 1, the audio media line that is not supported will be present with communication port for that stream set to 0.

Default: 0

- **LISTEN=<IP address>**

The IP APL can be instantiated in an XPR server several times. This requires every IP APL to use a unique combination of IP address and port number.

The IP address of an IP APL is stored in the **LISTEN** parameter.

- **LOOPDETECTION =<0, 1>**

Unintentional loops may occur with SIP connections. As a result the IP APL uses a connection-loop detection based on the RTP addresses (SIP-loop detection). In case of SIP connections via a gateway please also heed value **LOOPDETECTIONFROMTO**.

LOOPDETECTION controls the SIP Loop Detection in the IP APL.

- 0** – Disables the SIP Loop Detection via the RTP address

- 1** – Activates the SIP Loop Detection via the RTP address

Default: 1

- **LOOPDETECTIONFROMTO =<0, 1>**

If incoming SIP connections reach the XPR server via a gateway, undesired connection loops may be created if only the RTP address of the caller is used for loop recognition. Reason: The gateway establishes an independent SIP connection to the XPR server. The original RTP originator address is then not recognizable anymore. Therefore, the IP APL uses a connection loop recognition based on the SIP header information **FROM** and **TO** (SIP loop detection). This recognition rules out the described connection loops.

LOOPDETECTIONFROMTO controls the SIP Loop Detection in the IP APL.

- 0** – Disables the SIP Loop Detection via **FROM** and **TO**

- 1** – Activates the SIP Loop Detection via **FROM** and **TO**

Default: 1

- **MWI_RFC**=<0, 1>
Defines which format the IP APL uses for MWI notifications.
0 – *Format*: “Messages-Waiting:yes\r\nVoice-Message: 1/0\r\n”
1 – *Format*: “Messages-Waiting:yes\r\n\r\n”
Default: **0**
At an Alcatel PBX of version 7.x value **1** must be set.
- **SPIS**=0
When selecting TLS as transport protocol, SIP-S is usually deployed as signaling protocol. This setting changes the signaling protocol to SIP in this case.
- **T38_IN_TIMER**=<100 ... 20000 [milliseconds]>
Specifies the time after which the IP APL automatically switches to T.38, if in case of an incoming fax transmission it has not received an SIP-REINVITE message until then.
Default: **8000** [milliseconds]
- **T38_OUT_TIMER**=<100 ... 20000 [milliseconds]>
Specifies the time after which the IP APL automatically switches to T.38, if in case of an outgoing fax transmission it has not received an SIP-REINVITE message until then.
Default: **10000** [milliseconds]
- **USE480** =<0, 1>
By enabling it, when one IpApl is not able to accept calls (e.g. when there is a restart pending) it will answer 480 - Temporarily Unavailable instead of 603 – Decline. PBX then knows it can overflow the call to the other IpApl (endpoint) as it is just a temporary issue with that specific endpoint.
Default: **0**
- **WAITFIRSTLEGCOMPLETION**=<0, 1>
Two calls, simultaneously initiated by the IP APL, are usually performed for a call transfer. Some PBXs such as those by Alcatel take relatively long time for this process and the call transfer is then not executed properly. In such cases you can set this value to 1, so that a period of five seconds passes between initiating the first and second call.
Default: **0**

2. H.323-/CorNet-IP device

- **ACCESSNUMBERS**=<*List of all configured access numbers*>
If the IP APL is to be used in the environment with a PBX IP Media Gateway of the manufacturer *Intel*, this parameter defines a list of all access numbers of the Access Modes configured in the XPR server. The single phone numbers are separated by a comma.
This parameter must be forwarded if several access modes are used, but no Called ID is transmitted to the XPR server.

Example: ACCESSNUMBERS=901,902,903

- **BC_FAXG3**=<0, 1>

“Speech” is reported as *Bearer Capability* default setting (0). This may lead to a disconnection caused e. g. by a message “Incompatible Destination” enabled by the “Echo Cancellation” then possible at the provider. If you set value 1 here, “3.1kHz Audio” is used as *Bearer Capability*. This value is default set to 1 for HiPath 3000.

- **CALLEDID**=<*Called ID*>

For testing purposes the IP APL can manipulate the Called ID information. This parameter defines which phone number is assigned to the Called ID. If this parameter value is empty, this mechanism is deactivated.

Example: CALLEDID=2750

- **CALLERID**=<*Caller ID*>

For testing purposes the IP APL can manipulate the Caller ID information. This parameter defines which phone number is assigned to the Caller ID. If this parameter value is empty, this mechanism is deactivated.

Example: CALLERID=2200

- **DMCREJECT**=<0, 1>

With H.323, a DMCDDataExchange.inv request can be used in case of fax calls, for example. XPR normally ignores such requests, which virtually all PBXs interpret as “is not supported”. The HiPath 4000 requires an active “reject”.

0 – Ignore the DMCDDataExchange.inv request

1 – Answer the DMCDDataExchange.inv request

Default: **0**

- **EFC**=<0, 1>

Controls the use of Extended Fast Connect (EFC) for the telephone services: Call Transfer, Single Step Call Transfer.

0 – Deactivates the use of EFC

1 – Activates the use of EFC

Default: **0**

- **FAX_CNG_TONE**=<0, 1>

Specifies whether the IP APL sends inband the CNG fax tone to the called subscriber for outgoing T.38 fax messages.

0 – Deactivates the CNG fax tone for outgoing T.38 fax messages

1 – Activates the CNG fax tone for outgoing T.38 fax messages

Default: **1**

- **FAX_CED_TONE**=<0, 1>

Specifies whether the IP APL sends inband the CED fax tone to the calling subscriber for incoming T.38 fax messages.

- 0** – Deactivates the CED fax tone for incoming T.38 fax messages
- 1** – Activates the CED fax tone for incoming T.38 fax messages

Default: 0

- **G729ASUPPORT=<0, 1>**

Defines whether the G.729AB codec normally used for H.323 is reduced to annex A of the codec standard. In combination with the HiPath 4000 and some gateways, occasionally poor voice quality could thus be corrected.

0 – Standard G.729AB support

1 – Exclusive G.729A support

Example: G729ASUPPORT=1

- **GK=<IP address>**

If the IP APL is to communicate with an H.323 gatekeeper, this parameter defines the IP address via which this gatekeeper can be reached. For a correct function a functional routing between the XPR server and the respective IP host is required.

Example: GK=10.1.35.15

- **GKE164=<E.164 address>**

If an H.323 gatekeeper is used on the basis of E.164 addresses (ISDN phone numbers), this parameter defines the E.164 address via which the XPR server logs on to the gatekeeper. When the gatekeeper then receives communication requests for the respective phone number, these are transmitted to the XPR server.

Example: GKE164=901

- **GKNAME=<H.323 name>**

If an H.323 gatekeeper is used on the basis of H.323 names, this parameter defines the name with which the XPR server logs on to the gatekeeper. When the gatekeeper then receives communication requests for the respective phone number, these are transmitted to the XPR server.

Example: GKNAME=XPR100

- **GW=<IP address>**

If the IP APL is to communicate with an H.323 gatekeeper, this parameter defines the IP address via which this gatekeeper can be reached. For correct operation a functional routing between the XPR server and the respective IP host is required.

Example: GW=10.1.35.15

- **GWTYPE=<Gateway type>**

If the IP APL is to communicate with a PBX IP Media Gateway of the manufacturer *Intel*, this parameter must be defined as follows:

GWTYPE=INTEL

- **H323TRACE**=< *storage location and logging file name*>**Attention: Activating the logging may significantly affect the XPR server system performance. Therefore only use it if it is actually required for troubleshooting.**

Activates the H.323 logging. The file specified here in the possibly indicated directory path is created/used as log file.

If only a file name without path indication is entered, the file is created/used in the folder `SYSTEM32`. If a directory path is defined, this must already exist, since the IP APL itself does not create new directory structures. Logging is deactivated by transmitting an empty string.

Example: `H323TRACE=D:\h323trace.txt`

- **LISTEN**=<IP address>
The IP APL can be instantiated in an XPR server several times. This requires each IP APL to use an individual IP address.
The IP address of an IP APL is stored in the **LISTEN** parameter.
- **MWIEXTCUTOFFLEN**=<*Digit number*>
If the IP APL is to be used in one environment with the PBX IP Media Gateway of the manufacturer *Intel*, a number of digits can be ignored in the MWI address (MWI phone number) that is forwarded to the IP APL.
This parameter defines how many digits are to be cut off at the beginning of the transmitted MWI phone number.
Example: `MWIEXTCUTOFFLEN=6`
- **NORMALIZEMWIEXT**=<0, 1>
Defines whether normalized phone numbers are used for addressing MWI messages.
0 – Non-normalized phone numbers are used.
1 – Normalized phone numbers are used.
Default: **0**
Example: `NORMALIZEMWIEXT=1`
- **NPL**=<0, 1, 3, 4, 8, 9, 15>
Specifies which phone number plan the IP APL transfers to the PBX in case of outgoing communication.
This parameter is evaluated by the IP APL in the following cases:
when setting up an outgoing call, when setting up a supervised transfer, when sending an MWI message.
0 – nplUnknown
1 – nplISDN
3 – nplData
4 – nplTelex
8 – nplNational
9 – nplPrivate

15 – nplReserved

Default: 0

Example: TON=8

- **REDIRCUTOFFLEN=<Digit number>**

If the IP APL is to be used in one environment with the PBX IP Media Gateway of the manufacturer *Intel*, a number of digits of the redirecting number transferred to the IP APL can be ignored.

This parameter defines how many digits are to be cut off at the beginning of the transmitted redirecting number.

Example: REDIRCUTOFFLEN=6

- **SCRIPTFAXDETECTION=<0, 1>**

The HG module of the HiPath 3000 cannot manage the load when changing from a Voice application such as Vogue to Fax.

Subsequently, the HiPath 3000 will be rebooted by its watchdog. To avoid this scenario, you can suppress this behavior here.

0 – Allow change to Fax.

1 – Terminate the call when changing to Fax.

Default: 0

- **T38_DISABLE_EFC=<0, 1>**

Fax with T.38 is normally always executed without EFC. With the corresponding messages, EFC is mostly automatically disabled. The HiPath 3000 expects an explicit deactivation before the T.38 protocol messages. You can enforce this behavior here by setting this parameter to 1.

0 – Use EFC if required

1 – Disable EFC before the T.38 protocol

Default: 0

- **TON=<0, 1, 2, 3, 4, 6, 7>**

Specifies which phone number type (Type-of-Number) the IP APL transfers to the PBX in case of outgoing communication.

This parameter is evaluated by the IP APL in the following cases: when setting up an outgoing call, when setting up a supervised transfer, when sending an MWI message.

0 – tonUnknown

1 – tonInternational

2 – tonNational

3 – tonNetwork

4 – tonSubscriber

6 – tonAbbreviated

7 – tonReserved

Default: 0

Example: TON=1

3. Cisco IP PBX Service Provider

- **CTIPORT**=<Name portion of the of the CTI ports>
Defines a string for the name portion of CTI ports. Only those ports possessing this name part are opened after the start of the IP APL.
Example: CTIPORT=XPR opens e.g. the port XPR001, but not VOIP021.
- <List of CTI ports>=<Access phone number>
For applying an access mode (Direct Access, Control Access etc.) to the voice mailbox of a user, two phone numbers must be transmitted to the IP APL: the Redirecting ID and the Called ID. Each logical CTI Port of the Cisco CallManager can solely process one call at a time. Therefore the access to the access mode is defined as CTI Route Point in the CallManager (cf. installation manual *XPRand Cisco CallManager*). This CTI route point distributes incoming calls for the voice mail system to the assigned CTI ports.
If an incoming call is logically terminated by a CTI port, this call receives the calling number of the corresponding CTI port as CalledID. The original entry is overwritten. However, this fact is problematic for the voice scripts of the XPR server.
For this reason the thus modified CalledID is reset to the calling number of the original CTI route point by the IP APL at this stage. Resetting is performed on the basis of translation rules that need to be defined manually.

Example: 100-115,120,130-145=200
resets the Called IDs transmitted to the IP APL with the entry 114 to 200.

(Valid notations for *List of CTI Ports*> are:
' , ' (**comma**) – for enumerations of single phone numbers
' - ' (**hyphen**) – for serial phone number ranges
Combinations are also possible, e.g.:
170,172,175-179=300.

PrivateMode [REG_DWORD]

Default:	0
Remark:	<i>TeleReg.</i> Must not be modified.

Is only used by the quality assurance to adjust the internal value **PrivProfile** for the validation of new ISDN boards.

State [REG_DWORD]

Remark:	<i>TeleReg</i> . See <i>State</i> [REG_DWORD].

Type [REG_DWORD]

Remark:	<i>TeleReg</i> . See <i>Type</i> [REG_DWORD].

E.20.3.4 Trunk Groups

A trunk group describes the summary of several ³ logical, bidirectional communication channels of a single device. Only channels of a coherent section can be summed up to one trunk group.

Each single trunk group is assigned one of the configured protocols.

For each trunk group a consecutively numbered key *m* exists under the

HKLM\Software\Wow6432Node\PP-COM\MRS\IpApl\Devices\n

key of the associated device. In this key you find the following values that define all properties of the relevant trunk group.

BaudRate [REG_DWORD]

Remark:	<i>TeleReg</i> . See <i>BaudRate</i> [REG_DWORD].

Blob [REG_DWORD]

Remark:	<i>TeleReg</i> . See <i>Blob</i> [REG_DWORD].

BoundExtensions [REG_SZ]

Default:	–
Possible values:	0 – Extension of this station is not assigned to the trunk group 1 – Extension of this station is assigned to the trunk group

Defines which extensions are assigned to the relevant trunk group.

The contained value consists of 64 digits the may adopt value **1** or **0** each. The position of **1** or **0** in the digit string specifies the number of the assigned or not assigned extension. The first digit describes the assignment of the first extension, the second digit the assignment of the second extension etc.

Example: 101100000000...

In this example the trunk groups 1, 3 and 4 are assigned to the relevant trunk group.

3. In extreme cases such a trunk group can include only one communication channel.

BoundProtocols [REG_DWORD]

Remark:	<i>TeleReg.</i> See BoundProtocols1 [REG_DWORD] .

CalledNumberWithTrunkCode [REG_DWORD]

Default:	0
Possible values:	0 – PBX transfers tie line number 1 – PBX does not transfer tie line number

Defines whether the connected PBX transfers the tie line number together with a phone number to the XPR server.

CallingNumberNoExternalPrefix [REG_DWORD]

Default:	0
Possible values:	0 – PBX transfers external prefix with type <i>Unknown</i> 1 – PBX does not transfer external prefix with type <i>Unknown</i>

Defines whether the PBX transfers originator numbers of type *Unknown* without external prefix to the XPR server.

Cost [REG_DWORD]

Remark:	<i>TeleReg.</i> See Cost [REG_DWORD] .

EndChannel [REG_DWORD]

Remark:	<i>TeleReg.</i> See EndChannel [REG_DWORD] .

NumChannel [REG_DWORD]

Remark:	<i>TeleReg.</i> See NumChannels [REG_DWORD] .

OAD [REG_DWORD]

Remark:	<i>TeleReg.</i> See OAD [REG_DWORD] .

PermMask [REG_DWORD]

Remark:	<i>TeleReg.</i> See PermMask [REG_DWORD] .

StartChannel [REG_DWORD]

Remark:	<i>TeleReg.</i> See StartChannel [REG_DWORD] .

State [REG_DWORD]

Remark:	<i>TeleReg.</i> See State [REG_DWORD] .

E.20.3.5 Extension number ranges

Each phone number dialed in the XPR server must be within the range indicated here with its extension, so that the incoming call can be accepted by the IP APL.

The find the following registry value under the key:

HKLM\Software\Wow6432Node\PP-COM\MRS\IpApl\Extensions

EnableRegSZ [REG_DWORD]

Remark:	<i>TeleReg.</i> See EnableRegSz [REG_DWORD] .

For each supported service normally one extension number range must be configured. All configured ranges are numbered ascendingly and stored as a separate key with their respective number under the key

HKLM\Software\Wow6432Node\PP-COM\MRS\IpApl\Extensions

as a separate key. In each of these keys the following values are found.

Blob [REG_DWORD]

Remark:	<i>TeleReg.</i> See Blob [REG_DWORD] .

Description [REG_SZ]

Remark:	<i>TeleReg.</i> See Description [REG_DWORD] .

End [REG_SZ]

Remark:	<i>TeleReg.</i> See End [REG_SZ] .

MSN [REG_SZ]

Remark:	<i>TeleReg.</i> See MSN [REG_SZ] .

OAD [REG_DWORD]

Remark:	<i>TeleReg.</i> See OAD [REG_DWORD] .

Protocol [REG_DWORD]

Remark:	<i>TeleReg.</i> See Protocol [REG_DWORD] .

Start [REG_SZ]

Remark:	<i>TeleReg.</i> See Start [REG_SZ] .

State [REG_DWORD]

Remark:	<i>TeleReg.</i> See <i>State</i> [REG_DWORD].

VarDigits [REG_DWORD]

Remark:	<i>TeleReg.</i> See <i>VarDigits</i> [REG_DWORD].

E.20.3.6 FAX G3 Support

You find the following registry values for supporting Fax G3 of the IP APL under the key:

HKLM\Software\Wow6432Node\PP-COM\MRS\IpApl\FaxG3_Configuration

FaxG3_AltConfigActive [REG_DWORD]

Default:	0
Possible values:	0 – AltConfig is not enabled. 1 – AltConfig is enabled.

When FaxG3_AltConfigActive is enabled (set to 1) then for each fax call ipapl will try to match the caller information. If it succeeds it will use the settings found in the respective line of **FaxG3_AltConfigValuesByCaller**. If no match is found then ipapl will try to match the ip address of the connecting device and use the settings from the respective entry of **FaxG3_AltConfigValuesByIP**. If no entry is found, default settings will be used

FaxG3_AltConfigValuesByCaller [REG_MULTI_SZ]

Each line must have the format:

caller,echo suppression,adjust incoming fax level,adjust outgoing fax level

e.g.

+554133416000,20,1,1

Echo suppression settings should be between 0-50 ms. Higher values won't work properly.

NOTE: Will be used only when **FaxG3_AltConfigActive** is enabled (set to 1)

NOTE: The character '*' is supported in order to define an extension range for **FaxG3_AltConfigValuesByCaller**, e.g. +4989700714*.

FaxG3_AltConfigValuesByIP [REG_MULTI_SZ]

Each line must have the following format:

ip address,echo suppression,adjust incoming fax level,adjust outgoing fax level
e.g.
10.10.98.4,50,1,1

NOTE: Will be used only when **FaxG3_AltConfigActive** is enabled (set to 1)

FaxG3_CheckNumberOfPages [REG_DWORD]

Default:	0
Possible values:	0 – Use message of the protocol stack. 1 – Additional check of the received number of pages.

Setting this value to 1 compares the number of pages reported by the protocol stack with the number of pages actually contained in the received TIFF file. If these values differ, status “Transmission not completed (x page(s) received)” is reported instead of “OK (x page(s) received)”.

FaxG3_CommetrexLogging [REG_DWORD]

Default:	0
Possible values:	0 – Deactivates logging of the T.38 protocol layer 1 – Activates logging of the T.38 protocol layer
Remark:	If more than 4 fax messages are processed in parallel by the XPR server, the T.38 logging must be disabled.

IMPORTANT:

Activating the T.38 logging can have serious negative effects on the efficiency of the XPR server.

The T.38 protocol layer of the IP APL possesses an independent logging.

FaxG3_CommetrexLogging defines, whether or not this logging is active.

If the T.38 logging is active, a log file is generated for *each* fax message that has a *minimum* size of 5MB. This size grows *disproportionately* with the volume of the corresponding fax message.

The log files are stored in the folder created under [FaxG3_CommetrexPath \[REG_SZ\]](#) under the file name `trm<xxx>.log`, with `<xxx>` representing a continuous number.

FaxG3_CommetrexPath [REG_SZ]

Default:	<code><XPR Install>\log\Commetrex</code>
Possible values:	<code><local path></code>

Path definition for logging you can activate under [FaxG3_CommetrexLogging \[REG_DWORD\]](#).

FaxG3_EchoSuppression [REG_DWORD]

Default:	0
Possible values:	<Milliseconds>

This parameter sets the *Echo Suppression Period* attribute of the Commetrex stack. It effects the *Echo Suppression* to be active during tenfold of the specified time in milliseconds. If problems occur during fax transmission, experimenting with a changed value is an option. In case of Cisco Callmanager for example, a setting of 10ms led to a successful transmission.

FaxG3_ForceConversion [REG_DWORD]

Default:	0
Possible values:	0 – Leave document unchanged 1 – Scale width to 1728 points

XPR does not support the A3 format. You therefore receive such a fax document in the binary format, which the MTA cannot convert to TIFF. When you set this value to 1, binary files are converted to the size A4 and can then be further processed by the MTA.

FaxG3_ICLLogging [REG_DWORD]

Default:	1
Possible values:	0 – No image logging 1 – Activates image logging

Activates logging of special image data during fax transmission. Should only be activated upon special request by developers.

FaxG3_Timezone [REG_DWORD]

Default:	0
Possible values:	0 – Server time will be used 1 – Sets time of fax according to user's timezone

Uses the user's timezone to set sending time of a fax. Should be set to 1 in order to activate.

NOTE: If there is a TIMEZONE configured (via WebAssistant) for the user or for the group of the user that is sending the fax message, the configured timezone will be used to specify the date and time in the header of the fax instead of the server timezone.

FaxG3_IncEncodingType [REG_DWORD]

Remark:	Must not be modified.

FaxG3_IncErrCorrMode [REG_DWORD]

Default:	1
Possible values:	0 – Deactivates ECM in case of T.38 1 – Activates ECM in case of T.38

FaxG3_IncErrCorrNrData [REG_DWORD]

Remark:	Must not be modified.

FaxG3_IncErrCorrNrSignal [REG_DWORD]

Remark:	Must not be modified.

FaxG3_IncErrCorrType [REG_DWORD]

Remark:	Must not be modified.

FaxG3_IncModemType [REG_DWORD]

Remark:	Must not be modified.

FaxG3_MaxRxSpeed [REG_DWORD]

Remark:	Must not be modified.

FaxG3_MaxTxSpeed [REG_DWORD]

Remark:	Must not be modified.

FaxG3_OutErrCorrMode [REG_DWORD]

Default:	0
Possible values:	0 – Deactivates ECM in case of T.38 1 – Activates ECM in case of T.38

FaxG3_OutgEncodingType [REG_DWORD]

Remark:	Must not be modified.

FaxG3_OutgErrCorrNrData [REG_DWORD]

Remark:	Must not be modified.

Faxg3_OutgErrCorrNrSignal [REG_DWORD]

Default:	0
Possible values:	0 – Deactivates frame repetition for T.38 signaling 1 – Activates frame repeat for T.38 signaling
Remark:	Must not be modified.

For error correction, the T.38 protocol transmits with each T.38 frame the two previously sent T.38 frames. With frame 100, T.38 thus sends, for example, also the frames 98 and 99.

This frame repetition may lead to problems: namely for the first and second T.38 frame. These frames contain the -1 and 0. Frames, which, in fact, do not exist, so that they may not be correctly processed by the T.38 protocol stack on the recipient side.

Because of this potential problem, **Faxg3_OutgErrCorrNrSignal** disables the frame repetition for T.38 signaling frames in the T.38 protocol stack of the IP APL by default. Disabling the repetition for signaling frames is sufficient, because the first two T.38 frames are always signaling frames. The transmission of dataframes remains untouched by this setting.

FaxG3_OutgErrCorrType [REG_DWORD]

Remark:	Must not be modified.

FaxG3_OutgModemType [REG_DWORD]

Remark:	Must not be modified.

FaxG3_PartialReception [REG_DWORD]

Default:	1
Possible values:	0 – Deactivates partial FaxG3 reception 1 – Activates partial FaxG3 reception

NOTE: When deactivated, the customer is able to receive up to 60 min. fax transmissions.

If activated, the sender may re-transmit the end of the fax until the end.

Faxg3_RetransmissionActive [REG_DWORD]

Default:	1
Possible values:	0 – Disables repetitive sending of fax pages 1 – Activates repetitive sending of fax pages

Some fax devices send an RTP or RTN (ReTrain Negative) after having received a fax page correctly, thus demanding this page again and again. You can use this switch to change the behavior in such a way that the receiving station's demand for sending a page repetitively is ignored. Use this switch only after a corresponding GVS request and on trial.

FaxG3_StartTimestamp [REG_DWORD]

Default:	0
Possible values:	0 – Time stamp when received completely 1 – Time stamp at the transmission start

If you set this value to 1, the time stamp for receiving a fax message is set to the transmission start. The time stamp that marks the end of the transmission is set as default.

FaxG3_T38ParamNegotiation [REG_DWORD]

Default:	0
Possible values:	0 – Do not update fax parameter. 1 – Update fax parameter.

The Commetrex Library is not updated along with some parameters negotiated at runtime by T.38 SDP. You can activate this update here for the following parameters:

- MaxBitRate
- Version
- MaxBuffer
- FillBitRemoval
- TranscodingMMR
- TranscodingJBIG
- FaxsimileRateManagement
- RateManagement
- ErrorControlType

Faxg3_TCFOffset [REG_DWORD]

Default:	–
Possible values:	<Milliseconds>

Defines the time of the first TCF package transmission. According to the specification in milliseconds, the package is sent earlier than intended by the Commetrex Stack. ITU recommendation V.17 determines this TCF package to be sent within 1393 ms. When communicating with an analog fax device, the Commetrex Stack sent the package some milliseconds later, so that no connection was set up. Change this value only upon the GVS's request when it recognizes problems after an analysis.

FaxG3_UsePreferredT38 [REG_DWORD]

Remark:	Must not be modified.

E.20.3.7 Protocols

Protocols are a service supported by the IP APL. For each installed protocol a consecutively numbered key n exists under the

HKLM\Software\Wow6432Node\PP-COM\MRS\IpApl\Protocols

again a consistently numbered key n exists. This contains the following values.

Attributes [REG_MULTI_SZ]

Remark:	<i>TeleReg.</i> See <i>Attributes</i> [REG_MULTI_SZ].

AttributesAllowed [REG_DWORD]

Remark:	<i>TeleReg.</i> See <i>AttributesAllowed</i> [REG_DWORD].

Blob [REG_DWORD]

Remark:	<i>TeleReg.</i> See <i>Blob</i> [REG_DWORD].

CapMask [REG_DWORD]

Remark:	<i>TeleReg.</i> See <i>CapMask</i> [REG_DWORD].

CheckMailbox [REG_DWORD]

Remark:	<i>TeleReg.</i> See <i>CheckMailbox</i> [REG_DWORD].

ContMsg [REG_SZ]

Remark:	<i>TeleReg.</i> See <i>ContMsg</i> [REG_SZ].

Description [REG_SZ]

Remark:	<i>TeleReg.</i> See <i>Description</i> [REG_SZ].

DispPerm [REG_DWORD]

Remark:	<i>TeleReg.</i> See <i>DispPerm</i> [REG_DWORD].

DocReps [REG_SZ]

Remark:	<i>TeleReg.</i> See <i>DocReps</i> [REG_SZ].

EditPerm [REG_DWORD]

Remark:	<i>TeleReg.</i> See <i>EditPerm</i> [REG_DWORD].

EditPermGenerated [REG_DWORD]

Remark:	<i>TeleReg.</i> See <i>EditPermGenerated</i> [REG_DWORD].

FaxG3Chain [REG_DWORD]

Remark:	<i>TeleReg. See FaxG3Chain [REG_DWORD].</i>

FaxG3Resend [REG_DWORD]

Remark:	<i>TeleReg. See FaxG3Resend [REG_DWORD].</i>

FaxG4FaxG3 [REG_DWORD]

Remark:	<i>Not used by the IP APL at the moment.</i>

FaxG4T70 [REG_DWORD]

Remark:	<i>Not used by the IP APL at the moment.</i>

FaxID [REG_MULTI_SZ]

Remark:	<i>TeleReg. See FaxId [REG_SZ].</i>

Formats [REG_MULTI_SZ]

Remark:	<i>TeleReg. See Formats [REG_SZ].</i>

FormatsAllowed [REG_DWORD]

Remark:	<i>TeleReg. See FormatsAllowed [REG_DWORDS].</i>

FriendlyName [REG_SZ]

Remark:	<i>TeleReg. See FriendlyName [REG_SZ].</i>

Headline [REG_SZ]

Remark:	<i>TeleReg. See Headline [REG_SZ].</i>

MultiMaster [REG_DWORD]

Remark:	<i>TeleReg. See MultiMaster [REG_DWORD].</i>

Name [REG_SZ]

Remark:	<i>TeleReg. See Name [REG_SZ].</i>

ParamBlock [REG_SZ]

Remark:	<i>TeleReg. See ParamBlock [REG_SZ].</i>

Private [REG_MULTI_SZ]

Default:	<Empty string>
Possible values:	<Initialization entry per line>

Defines APL-specific entries. Depending on the protocol, one specific entry per line is made for the IP APL.

1. *Fax G3*:

- **CheckPageNumbers**
When set to **1** an OK report is only sent when the number of sent pages reported by the CAPI driver corresponds to the number of pages in the document. Otherwise it would be possible to receive an “OK (2 pages sent)” report for a four-page document.
- **InsertMidHI**
With **1**, the document message ID is inserted into the headline. If used, a maximum of 22 characters for the headline is allowed.
- **UseFaxIdAsOAD**
Calling Line Identification (CLI) would be used as the originator’s OAD with inbound fax documents. If this field is empty while no CLI can be determined, the number in the fax ID will be used as CLI. When this value is set to **1** the fax ID will always be used as the CLI with inbound fax documents.

PrivateMode [REG_DWORD]

Remark:	<i>Not used by the IP APL at the moment.</i>

ScriptName [REG_SZ]

Remark:	<i>TeleReg. See ScriptName [REG_SZ].</i>

SI [REG_MULTI_SZ]

Remark:	<i>TeleReg. See SI [REG_SZ].</i>

State [REG_DWORD]

Remark:	<i>TeleReg. See State [REG_DWORD].</i>

Type [REG_DWORD]

Remark:	<i>TeleReg. See Type [REG_DWORD].</i>

UseOrigFax [REG_DWORD]

Default:	0
Possible values:	0 – Default algorithm for fax originator ID of the IP APL 1 – Always use the FAXG3 field 2 – Use the same logic as Fax G3 via ISDN APL

The default algorithm for the fax originator ID in the IP APL takes the first existing database field in the following sequence:

- User ID (if it consists of digits only)
- Costinfo
- FAXG3

- FAXG3-ID
- Fax G3 protocol server settings

In case of 1, the content of the FAXG3 field is always used. In case of 2, the same logic as with Fax G3 via the ISDN APL is used. The first existing database field is taken as fax originator ID in the following sequence:

- Costinfo
- FAXG3
- FAXG3-ID
- Fax G3 protocol server settings

E.20.3.8 Voice and Fax-on-Demand Systems

You find the values for installed VFS scripts under the following key:

HKLM\Software\Wow6432Node\PP-COM\MRS\IpApl\Vfs

AcIAddress [REG_SZ]

Remark:	<i>Not used by the IP APL at the moment.</i>

AcIDelayMessage [REG_DWORD]

Remark:	<i>Not used by the IP APL at the moment.</i>

AcIInternLen [REG_DWORD]

Remark:	<i>Not used by the IP APL at the moment.</i>

AcIInternMax [REG_DWORD]

Remark:	<i>Not used by the IP APL at the moment.</i>

AcIUse [REG_DWORD]

Remark:	<i>Not used by the IP APL at the moment.</i>

DisplayColumns [REG_DWORD]

Remark:	<i>Not used by the IP APL at the moment.</i>

DisplayRows [REG_DWORD]

Remark:	<i>Not used by the IP APL at the moment.</i>

ErrDetect [REG_DWORD]

Remark:	<i>Not used by the IP APL at the moment.</i>

Log<n> [REG_SZ]

Remark:	<i>Not used by the IP APL at the moment.</i>

LogName<n> [REG_SZ]

Remark:	<i>Not used by the IP APL at the moment.</i>

PeakDuration [REG_DWORD]

Remark:	<i>Not used by the IP APL at the moment.</i>

PeakLevel [REG_DWORD]

Remark:	<i>Not used by the IP APL at the moment.</i>

Prg<n> [REG_SZ]

Remark:	<i>Not used by the IP APL at the moment.</i>

SilentTime [REG_DWORD]

Remark:	<i>Not used by the IP APL at the moment.</i>

SoftFaxFilter [REG_DWORD]

Remark:	<i>Not used by the IP APL at the moment.</i>

Stat<n> [REG_DWORD]

Remark:	<i>Not used by the IP APL at the moment.</i>

UseSpr [REG_DWORD]

Remark:	<i>Not used by the IP APL at the moment.</i>

XmrTopic [REG_DWORD]

Remark:	<i>Not used by the IP APL at the moment.</i>

E.21 Entries of the V.24 APL

The following values can be found in the key V24Ap1.

ContIntFaxStr [REG_SZ]

Default:	Continuation of an interrupted message
Possible values:	<String>

This one line message is affixed to fax transmission continuations.

DefFaxRecipient [REG_SZ]

Default:	POSTMASTER
Possible values:	<User ID>

Recipient for incoming fax messages. Since extensions are not possible for fax modems connected to analog lines, it is not possible to assign the incoming fax messages to a user.

FaxConnTimeInJrn [REG_DWORD]

Default:	0
Possible values:	0 or 1

Accumulated connection times for fax document transmissions are listed in the journal (1). No connection times are listed in the journal (0).

Headline [REG_SZ]

Default:	<Empty>
Possible values:	<String>

Default fax G3 headline. A maximum of 32 characters in length is allowed.

InsertMidHI [REG_DWORD]

Default:	0
Possible values:	0 or 1

Document message ID is inserted into the headline. If used, a maximum of 22 characters for the headline is allowed.

InstalledDrivers [REG_MULTI_SZ]

Example:	cpvpico.sm creatix.sm elink324.sm elsa.sm null.sm usr_cou.sm zyxel.sm

List of installed script files for modem triggering. This entry cannot be modified since it is reinitialized with each V.24 APL reboot based on the driver scripts available in the *<XPR Install>\res\sm* directory.

InstalledProtocols [REG_MULTI_SZ]

Example:	SMI Transport;NVS:MODEM;1 FaxG3;NVS:FAXG3;1 FaxG3 Poll;NVS:FAXG3REV;1 GSM,cit_basic.sm;NVS:CIT_BASIC;1

List of installed protocols for modem triggering. This entry cannot be altered. By each new start of the V.24 APL the list is reinitialized with reference to the available protocol scripts in *<XPR Install>\res\sm* as well as the protocols *SMI Transport* (server coupling), *Fax G3* (receipt, transmission, and fax-on-demand), and *Fax G3 Poll* (fax polling).

OriginatorID [REG_SZ]

Example:	+49 2404 9876543
Possible values:	T.30-conform <String>

Default fax G3 ID. This ID must correspond to T.30 standards which allows only digits, spaces, and + for the ID.

E.21.1 Device Settings

Under the key `V24Ap1\Devices` for each installed serial interface a key with the name of the interface exists, i.e. normally `COM1`, `COM2`, `COM3`, ... In each of these keys the following values can be found.

AreaCodeEscape [REG_SZ]

Example:	0

National prefix. This number is set preceding the area code of the recipient when a domestic number is dialed. If this entry is not set the V.24 APL uses the default value in `MRS Globals\Location\AreaCodeEscape`.

BaudRate [REG_DWORD]

Example:	19200

Serial port baud rate.

CanBePolled [REG_DWORD]

Default:	0
Possible values:	0 or 1

Fax-on-demand is supported by the modem (1).

CanVoice [REG_DWORD]

Default:	0
Possible values:	0 or 1

This Value is currently non-functional.

CountryCodeEscape [REG_SZ]

Example:	00

International prefix. This number is set before the country code of the recipient when an international number is dialed. If this entry is not set the V.24 APL uses the default value in `MRS Globals\Location\CountryCodeEscape`.

ExternalLinePrefix [REG_SZ]

Example:	0

External Line. If this entry is not set the V.24 APL uses the default value in `MRS Globals\Location\ ExternalLinePrefix`.

FaxPollFile [REG_SZ]

Example:	default.fax
Possible values:	<File name>

The file entered here is sent for incoming fax-on-demand.

LineName [REG_SZ]

Example:	Creatix COM3
Possible values:	<String>

Line name in the XPR Monitor.

LocPrefixExtensions [REG_MULTI_SZ]

Default:	<Empty>

A list with phone numbers or partial phone numbers not modified with the normalization. Normally, all phone numbers are normalized to an international phone number. Example: In Germany the number 0240412345 would be normalized to 49240412345.

With corporate networks it is possible that dialing numbers such as 9992<Extension> exist. You can enter the prefix 9992 here so that all numbers beginning with this prefix will not be normalized.

Example:

9992
0111
444

All numbers that begin with 9992, 0111 or 444 will not be normalized.

This entry is only useful at this point if deviations from the global settings are to be configured for the V.24 APL under MRS
Globals\Location\LocPrefixExtensions.

PhoneNum [REG_SZ]

Example:	49-1234-5678-90
Possible values:	<Phone Number>

Telephone number of the modem. International prefixes, area codes, PBX number, and the extension of the modem are to be separated with a hyphen.

Protocols REG_MULTI_SZ

Protocol bindings to the modem. Under the key V24Ap1\Protocols all NVS addresses that are supported by this device and listed here are itemized as value.

ShortholdTime [REG_DWORD]

Default:	60
Possible values:	0 or <seconds>

Wait time in seconds after which an existing SMI connection over the V.24 APL is disconnected due to inactivity. If the Value is 0, no connection would be automatically disconnected.

SMFile [REG_SZ]

Example:	creatix.sm

Script file that contains the triggering and answer evaluation of the modem respectively of the serially addressed device. This is one of the device drivers listed in [InstalledDrivers \[REG_MULTI_SZ\]](#).

TouchTone [REG_DWORD]

Default:	1
Possible values:	0 – Pulse dialing 1 – DTMF dialing

Differentiation between pulse and tone (DTMF) dialing.

E.21.2 Protocols

Under the key `V24Apl\Protocols` all protocols connected to a device are listed via their NVS address and the associating protocol. As Value is the logical address given, which defines the device and the address to which the protocol is bound. The following protocols are available:

Protocol	Description
SMITR	Client/Server-Coupling over a SMI Transport.
FAXG3	Fax G3 Send/Receive/Fax-on-Demand Server.
FAXG3REV	Fax G3 Poll from a Fax-on-Demand Server.
GSM,[<i>Script-File</i>]	A General State Machine (GSM) script connection. The following GSM script language protocols are included: - cit_basic.sm This protocol allows setting an MWI signal via a Hicom PBX. - citmd110.sm This protocol allows setting of an MWI signal over an Ericsson MD 110 PBX.

Various parameters can be additionally appended to the protocols FAXG3 and FAXG3REV and separated by a semicolon. When possible, changes should only be made to repeat strategies.

reps=	Repeat Strategy. This parameter defines how often and at which interval delivery attempts are to be made by the router. Delivery attempts are successively executed, whereby the first parameter is the number delivery attempts to be made and the second parameter the time interval in seconds between delivery attempts. Up to five different dialing intervals can be indicated. Default: reps=3-60,2-120,2-300
attr=	A comma-separated list of line attributes. • IN – Line designated for inbound traffic only (in reference to the server). • OUT – Line designated for outbound traffic only. • SF – Line allowed Store-and-Forward operations. • DLG – Line allowed Dialog operations. • COST – Cost acquisition over this logical line is enabled in an outward direction only. Ensuing transmission costs will be stored in the Cost database. • SMITR – This line is designated as a SMI Transport. • LOCAL – Lines with this attribute will not be exported to systems connected by a Remote System Link. • PRIV – Lines with this attribute require a privilege check.
speed=	Transmission rate for the router. The usage of this attribute is similar to that of cost= so that a preference to lines can be assigned.
cost=	Through the use of this parameter preferences can be assigned to logical lines used by the router. The greater the value of cost, the more often the router uses this line (-100 < cost < 100).
frm=	This comma-separated list specifies valid document and file formats for this logical line. Since only FG3 is recognized by the V.24 APL, changing this parameter is of no value.

Example: FaxG3; reps=1-60, 2-120, 3-300

E.21.3 Protocol Settings

Under the key `HKLM\Software\Wow6432Node\PP-COM\MRS\V24Apl\Protocols` for each protocol that stores parameters in the registry a key with the protocol name exists.

Under the Key `cit_basic` the following Values are found.

CIT_Off [REG_SZ]

Default:	##8

This string is used together with the telephone number to turn off the MWI signal in the Hicom telephone system.

CIT_On [REG_SZ]

Default:	##7

This string is used together with the telephone number to activate the MWI signal in the Hicom telephone system.

E.22 Entries of the VM2TXT APL

The following values can be found in key `Vm2TxtApl`.

carootcert [REG_SZ]

Maps the configuration option **Certificate authority root certificate** in the registry. See [Section 31.2, “Configuring the VM2TXT APL”](#), on page 1496.

clientcert [REG_SZ]

Maps the configuration option **Client certificate** in the registry. See [Section 31.2, “Configuring the VM2TXT APL”](#), on page 1496.

libverbosemode [REG_DWORD]

Maps the configuration option **Enable HTTP library debug log** in the registry. See [Section 31.2, “Configuring the VM2TXT APL”](#), on page 1496.

libverbosemodedir [REG_SZ]

Default:	–
Possible values:	<Path>

Optional path for the log file activated under **Enable HTTP library debug log** if you wish to create this file in another directory.

IMPORTANT: A path different from the defaulted one must be previously created. If the path does not exist, no log data will be written.

maxAudioLength [REG_DWORD]

Default:	60
Possible values:	Seconds

Maximum length of a voicemail to be converted and sent to the conversion server. If a voicemail exceeds this length, a correspondingly shortened voicemail is used for conversion.

maxSimultaneousRequests [REG_DWORD]

Default:	30
Possible values:	10-1000 simultaneous requests

Maximum number of simultaneous requests to the conversion server. Any further requests are put in a waiting loop and processed delayed.

proxyaddress [REG_SZ]

Maps the configuration option **Address** in the registry. See [Section 31.2, “Configuring the VM2TXT APL”](#), on page 1496.

proxyport [REG_DWORD]

Maps the configuration option **Port** in the registry. See [Section 31.2, “Configuring the VM2TXT APL”](#), on page 1496.

recognitiontimeout [REG_DWORD]

Default:	3
Possible values:	<i>1-10 minutes</i>

Maximum waiting time allowed for a vendor conversion.

vendoraddress [REG_SZ]

Maps the configuration option **Vendor URL** in the registry. See [Section 31.2, “Configuring the VM2TXT APL”](#), on page 1496.

E.23 Entries of the Web APL

The following values can be found in the key `WEBAPL`.

AuthIncoming [REG_DWORD]

Default:	1
Possible values:	0 – No privilege check. 1 – Check originator privileges.

If messages come in via the Web APL, the originator privileges can be checked.

BindAddress [REG_SZ]

Maps the configuration option **Bind Address** in the registry. See [Section 13.2.1, “HTTP Tab”, on page 924](#).

CGI_IncludePath [REG_SZ]

Represents the configuration option **Include path** in the registry. See [Section 13.2.2, “CGI Tab”, on page 926](#).

DisablePUT [REG_DWORD]

Default:	1
Possible values:	0 – PUT method supported. 1 – PUT method not supported.

Via the PUT method you can upload any files to the XPR server. This is a security risk even if only compiled E-scripts in the form of vo-files would be executed.

EnglishLanguageForNetAdmin [REG_DWORD]

Default:	0
Possible values:	0 – Use set system language. 1 – Use English.

Via this value you can set the network administrator language in the Web Assistant to English.

HTTP_DefaultHTML [REG_SZ]

Represents the configuration option **Default HTML page** in the registry. See [Section 13.2.3, “HTML Tab”, on page 937](#).

HTTP_Enable [REG_DWORD]

Default:	0
Possible values:	0 – Protocol HTTP is disabled. 1 – Protocol HTTP is enabled.

The HTTP protocol is disabled by default for security reasons. To activate it, you need to switch it on here.

HTTP_KeyTimeout [REG_DWORD]

Maps the configuration option **Key lifetime** in the registry. See [Section 13.2.1, “HTTP Tab”, on page 924](#).

HTTP_MaxThreads [REG_DWORD]

Maps the configuration option **nThreads** in the registry. See [Section 13.2.1, “HTTP Tab”, on page 924](#).

HTTP_Port [REG_DWORD]

Maps the configuration option **HTTP Port** in the registry. See [Section 13.2.1, “HTTP Tab”, on page 924](#).

HTTP_RootTab [REG_MULTI_SZ]

Represents the configuration option **Root table** in the registry. See [Section 13.2.3, “HTML Tab”, on page 937](#).

HTTP_Timeout [REG_DWORD]

Maps the configuration option **Time-out of connection** in the registry. See [Section 13.2.1, “HTTP Tab”, on page 924](#).

HTTPS_Port [REG_DWORD]

Represents the configuration option **HTTPS port** in the registry. See [Section 13.2.4, “SSL Tab”, on page 939](#).

IgnoreSmtplibCheck [REG_DWORD]

Default:	0
Possible values:	0 – Check SMTP APL presence for e-mail notifications. 1 – Do not check SMTP APL presence for e-mail notifications.

MWI notifications for e-mails cannot be configured if no SMTP APL has been installed. You can disable the check for the APL's presence here.

IsPINResetOld [REG_DWORD]

Default:	0
Possible values:	0 – PIN may only be modified with specifying the password 1 – PIN may only be modified with specifying the PIN

If a user has forgotten his/her PIN for accessing the TUI, he/she can log on to the Web Assistant with his/her password and change his/her PIN without stating the current one. In this case, however, he/she still needs to know his/her password.

In scenarios where users also log on to the Web Assistant only via their mailbox number and PIN, further validation is desired. In such scenarios you can therefore set this value to 1. Thereafter the user will be prompted to specify the currently valid PIN if he/she wants to enter a new one.

LogicalLineClass [REG_SZ]

Default:	<System index>
Possible values:	<String>

Each Web APL logs in its logical trunks in the form `NVS : <Protocol> . <Class>`. The `<Class>` corresponds to the computer's system index where the Web APL is running. So several Web APLs could be installed in a distributed system and these could be distinguished from the trunks logged in at the MTA via the `<Class>`. Via this registry parameter an own `<Class>` for the trunks of this Web APL can be declared. If you would like to install the Web APL several times on a computer, you had to enter something different here in order to be able to distinguish.

LoginMethod [REG_DWORD]

Maps the configuration option **Authentication method** in the registry. See [Section 13.2.2, "CGI Tab", on page 926](#).

ProhibitDirectories [REG_MULTI_SZ]

Default:	<Empty>
Possible values:	<Prohibited Directory>

One directory may be entered per line. `<Prohibited Directory>` must begin with a `\` and, depending on the queried URL and the Root directory configured in [HTTP_RootTab \[REG_MULTI_SZ\]](#) for this URL, is to be considered relative to this directory.

Each access to one of the directories entered here is then answered with the message `404 - Not found`.

ProtectedDirectories [REG_MULTI_SZ]

Default:	<Empty>
Possible values:	<Protected Directory> : <Dialog Display>

One password protected directory can be entered per line.

<Prohibited Directory> must begin with a \ and, depending on the queried URL and the Root directory configured in [HTTP_RootTab \[REG_MULTI_SZ\]](#) for this URL, is to be considered relative to this directory.

<Dialog Display> is a normal text displayed in the password query dialog by the Web Browser.

If you call one of the directories entered here in your Web browser, you need to enter your user ID and associated password.

RefererCheck [REG_DWORD]

Default:	1
Possible values:	0 – Referer Header check disabled. 1 – Referer Header check active.

Checking the Referer HTTP Header is a measure against Cross-Site Request Forgery (CSRF) attacks. However, depending on the network configuration, this header may not be available, so that this check is impossible. In this case you must disable the check here.

SSL_CBC_Enable [REG_DWORD]

Default:	0
Possible values:	0: Ciphers with CBC mode are disabled 1: Ciphers with CBC mode are enabled

to full security both SSL_CBC_Enable and SSL_TLSv1_Enable must be set to 0.

SSL_CertificateFile [REG_SZ]

Maps the configuration option **Certificate file** in the registry. See [Section 13.2.4, “SSL Tab”, on page 939](#).

SSL_DHE_Disable [REG_DWORD]

Default:	0
Possible values:	0 – Use DHE key. 1 – Do not use DHE key.

For the time being, keys with DHE (Ephemeral Diffie Hellman a.k.a Perfect Forward Secrecy) cannot be decrypted by man-in-the-middle software. If you want to use software that decrypts and inspects the SLL traffic between web server and client, it must be able to decrypt SSL traffic. Therefore you need to switch off DHE use here.

SSL_Enable [REG_DWORD]

Maps the configuration option **Enable Secure Sockets** in the registry. See [Section 13.2.4, “SSL Tab”, on page 939](#).

SSL_PassPhrase [REG_SZ]

Represents the configuration option **Passphrase for private key** in the registry. See [Section 13.2.4, “SSL Tab”, on page 939](#).

SSL_PrivateKeyFile [REG_SZ]

Maps the configuration option **Private key file** in the registry. See [Section 13.2.4, “SSL Tab”, on page 939](#).

SSL_TLSv1_Enable [REG_DWORD]

Default:	0
Possible values:	0: TLS 1.0 protocol disabled 1: TLS 1.0 protocol enabled

to full security both SSL_CBC_Enable and SSL_TLSv1_Enable must be set to 0.

By default TLSv1.2 is enabled.

SSL_TLSv1_1_Enable [REG_DWORD]

Default:	0
Possible values:	0: TLS 1.1 protocol disabled 1: TLS 1.1 protocol enabled

Used to disable TLS 1.1 on WebApI

This configuration does not affect outgoing connections.

By default TLSv1.2 is enabled.

SSL_TrustedCaFile [REG_SZ]

Represents the configuration option **Trusted CA file** in the registry. See [Section 13.2.4, “SSL Tab”, on page 939](#).

UseTiffFormat [REG_DWORD]

Default:	0
Possible values:	0 – JPEG 1 – TIFF 2 – TIFF and JPEG 3 – PNG

Fax messages displayed on a web browser are converted into the format entered here beforehand. With setting 2 the Web Assistant will display a link to the TIFF file as well as the single pages as JPEG files. You will thus gain a first impression of the fax and be able to view the original copy via the TIFF. The PNG format offers a better quality than JPEG.

WebAssistVersion [REG_SZ]

Example:	v6755
Possible values:	<String>

Contains the version number of the Web Assistant that is read out of the WebAdmin.vo module during the installation and then entered here. If this value is not set, the Web APL assumes an older Web Assistant version.

WebCL_Enable [REG_DWORD]

Maps the **HTTP Client** configuration option in the registry. See [Section 13.2.5, “HTTP Client Tab”, on page 941](#).

WebCL_IncludePath [REG_SZ]

Represents the configuration option **Include path** in the registry. See [Section 13.2.5, “HTTP Client Tab”, on page 941](#).

WebCL_nThreads [REG_DWORD]

Maps the **Number of threads** configuration option in the registry. See [Section 13.2.5, “HTTP Client Tab”, on page 941](#).

WebCL_Script [REG_SZ]

Maps the **Script path** configuration option in the registry. See [Section 13.2.5, “HTTP Client Tab”, on page 941](#).

WebCL_Stacksize [REG_DWORD]

Default:	16384
Possible values:	<Number of bytes>

Stack size of the script operated by HTTP client. See [Section 13.2.5, “HTTP Client Tab”, on page 941](#).

WebCL_Timeout [REG_DWORD]

Maps the **Time out** configuration option in the registry. See [Section 13.2.5, “HTTP Client Tab”, on page 941](#).

WebCookieKey [REG_SZ]

Default:	<random number>

This random number is required to set the cookie for the simplified login. This simplified login is only possible with the Web Message Access, if the administrator gives his/her permission and the user explicitly activates it for himself/herself. After a once-only login an encrypted cookie is written on the system of the user. The cookie is valid for two weeks. As long as the cookie is valid, the user can log on for the Web Message Access from this system without any further authentication.

If you delete or modify this value here, all cookies assigned so far become immediately invalid.

E.23.1 Protocols

Under the key `WEBAPL\CGI_Protocols` a key with the protocol name can be found for each configured protocol, containing the following entries each:

CGI_Script [REG_SZ]

Represents the configuration option **Name** in the registry. See [Section 13.2.2, “CGI Tab”, on page 926](#).

CGI_ScriptParams [REG_MULTI_SZ]

Represents the configuration option **Parameter** in the registry. See [Section 13.2.2, “CGI Tab”, on page 926](#).

Enable [REG_DWORD]

Represents the configuration option **Enable Protocol** in the registry. See [Section 13.2.2, “CGI Tab”, on page 926](#).

IsDefault [REG_SZ]

Represents the configuration option **Default protocol** in the registry. See [Section 13.2.2, “CGI Tab”, on page 926](#).

VM_StackSize [REG_DWORD]

Possible values:	<Number of bytes>

Size of stacks for the virtual machine. The virtual machine executes the E-Script object codes. This is normally preset by the respective E script.

E.24 Entries of the XML APL

The following values are found in the key `XmlApl`.

Delay [REG_DWORD]

Default:	–
Possible values:	<Milliseconds> > 0

If a value is specified here, a corresponding break is taken after each event the XML APL sends to a client.

IntervalCheckTimeout [REG_DWORD]

Default:	–
Possible values:	<Milliseconds> > 0

A value greater than zero specifies the interval used for checking the overflow of the ICI event registrations. The default value for this interval is two hours. The XML APL thus checks the flow of such registrations every two hours.

IntervalGenerateTimeout [REG_DWORD]

Default:	–
Possible values:	<Milliseconds> > 0

The validity of a client's registration for ICI events is defaulted here. The default for this value is 12 hours. The XML APL would thus notify the client after 12 hours about the registration having expired. The client then needs to register again for receiving ICI events.

messageChanged_Skip [REG_SZ]

Default:	–
Possible values:	String that represents a portion of an ICI messageChanged event string.

If this value is set, ICI events that feature the string specified here are ignored and not sent to a client. This value thus enables suppressing specific types of events.

phoneCallChanged_Skip [REG_SZ]

Default:	–
Possible values:	String that represents a portion of an ICI phoneCallChanged event string.

If this value is set, ICI events that feature the string specified here are ignored and not sent to a client. This value thus enables suppressing specific types of events.

userChanged_Skip [REG_DWORD]

Default:	–
Possible values:	String that represents a portion of an ICI userChanged event string.

If this value is set, ICI events that feature the string specified here are ignored and not sent to a client. This value thus enables suppressing specific types of events.

E.25 Service Providers (MSP) Entries

E.25.1 Applets

For each installed application there is in the `HKLM\SOFTWARE\CYCOS AG\MSP\Applets` key a value with the internal name of the application, which holds the setup path of this application. Furthermore, this key contains the following values.

NOTE:

On a 64-bit operating system you find the values in key `HKLM\Software\Wow6432Node\Cycos AG\MSP\Applets`.

ProfileEditing [REG_DWORD]

Default:	Value does not exist.
Possible values:	0 – User profile must not be edited.

If this value exists and is set to 0, none of the users may edit his/her user profile. No new profiles can be created either. The existing profile can then only be used for logging on or off. This can also be set for each user individually. See [ProfileEditing \[REG_DWORD\]](#).

E.25.2 Database

The following values are specified in the key `HKLM\SOFTWARE\CYCOSAG\MSP\Database`.

NOTE:

On a 64-bit operating system you find the values in key `HKLM\Software\Wow6432Node\Cycos AG\MSP\Database`.

Directory [REG_SZ]

Example:	C:\Documents and Settings\All Users\Application Data\Cycos\Service Provider\Database\
Possible values:	<Path>

Directory in which the local database is stored.

Enabled [REG_DWORD]

Default:	1
Possible values:	0 – Local database is not used. 1 – Local database is used.

Specifies whether the database can or should be used. If, for example, only an applet is to be used that does not need the database, this value can be set to 0.

IMPORTANT:

Operation without database is to be considered an experiment!

MinDiskFree [REG_SZ]

Default:	100,50
Possible values:	20...4000, 10...4000

The minimum of required free disk space in megabyte on the drive specified by [Directory \[REG_SZ\]](#). As soon as this space falls short, the logged-in applications are notified so that they can issue a warning. As soon as the second value falls short, all logged-in applications receive an error message and are automatically logged off.

E.25.3 Server

The values in the key `HKLM\SOFTWARE\Cycos AG\MSP\ server` are used for internal administration by the service provider. The keys and values available here should never be modified. They are not documented here either, since they vary from system to system and are subject to change without prior notice.

NOTE:

On a 64-bit operating system you find the values in key `HKLM\Software\Wow6432Node\Cycos AG\MSP\Server`.

E.25.4 Service Provider

The following values are specified in the key
HKLM\SOFTWARE\CYCOSAG\MSP\ServiceProvider.

NOTE:

On a 64-bit operating system you find the values in key
HKLM\Software\Wow6432Node\Cycos AG\MSP\Service Provider.

ConfigDLL [REG_SZ]

Example:	C:\WINDOWS\system32\MspCfg.cpl

Path and file name of the service provider configuration DLL. This path is not used by the MSP itself but by applets. These require this value to start the GUI-based login and configuration of the MSP.

FileLogging [REG_DWORD]

Default:	0
Possible values:	0 – Do not use protocol file. 1 – Use protocol file.

Activates the protocol file set under [LogFile \[REG_SZ\]](#). This protocol method is used by the MSPTSP only. The MSP itself uses the protocol method configurable under [Section 32.14, “Logging Tool for Clients”, on page 1558](#).

Inbound [REG_SZ]

Example:	C:\Documents and Settings\All Users\ Application Data\Cycos\Service Provider\Inbound\

Path under which the MSP stores documents and temporary files.

LogFile [REG_SZ]

Example:	C:\Program Files\Common Files\Cycos\ Service Provider\msp.run.log

Path and file name for the protocol file that can be activated under [FileLogging \[REG_DWORD\]](#). This file is used by the MSPTSP only. The MSP itself uses the protocol method configurable under [Section 32.14, “Logging Tool for Clients”, on page 1558](#).

MinDiskFree [REG_SZ]

Default:	100,50
Possible values:	20...4000, 10...4000

The minimum of required free disk space in megabyte on the drive specified by [Inbound \[REG_SZ\]](#). As soon as this space falls short, the logged-in applications are notified so that they can issue a warning. As soon as the second value falls short, all logged-in applications receive an error message and are automatically logged off.

Module [REG_SZ]

Example:	C:\Program Files\Common Files\Cycos\Service Provider\MspSvc.exe

Path to the service provider program. Is used by the first applet. It starts the MSP, if the provider is not running already.

NetworkLoginOnly [REG_DWORD]

Default:	0
Possible values:	0 – No Novell Network support 1 – Novell Network support active

If this value is set to 1, the Novell Network user account is used in user profiles instead of the Windows user account.

OdsLogging [REG_DWORD]

Default:	0
Possible values:	0 – No debug output via the OutputDebugString function. 1 – Debug output via the OutputDebugString function.

Activates special debug outputs via the OutputDebugString function. Using them also requires an appropriate tool like, for example, DebugView by <http://www.sysinternals.com>.

ProductFlavor [REG_SZ]

Example:	XPR

This value is written during the setup of a client application and contains the short name of the installed version. To find this value, a client application searches HKCU\SOFTWARE\Cycos AG\MSP\ServiceProvider and HKLM\SOFTWARE\Cycos AG\MSP\ServiceProvider or, on a 64-bit operating system, HKLM\SOFTWARE\Wow6432Node\Cycos AG\MSP\ServiceProvider consecutively via the MSPAPI.

If this value is available in neither of the two registry sections, MRS is delivered as product name to the client application.

Service [REG_DWORD]

Example:	1
Possible values:	0 or value not available – MSP installed as program. 1 – MSP installed as Windows service.

By this value an applet knows whether the MSP is installed as program or service. This value is only generated by `MSPSVC.EXE` and should never be modified.

Tunnel [REG_SZ]

Example:	C:\Program Files\Common Files\Cycos\ Service Provider\stunnel.exe

Path and file name of the STunnel application. This application is installed along with the MSP setup. Via STunnel you can establish a connection to the XPR server secured by SSL. See [UseEncryption \[REG_DWORD\]](#).

UseEncryption [REG_DWORD]

Default:	Value not available
Possible values:	1 – Connection to the XPR server secured via SSL.

Upon the TCP/IP APL installation the STunnel program is set up with a certificate. If you activate this value here and set the [NatClient \[REG_DWORD\]](#) value to 1 in addition, a connection secured by SSL to the TCP/IP APL of the server is used.

The default does not set this encryption, so that the server can first be upgraded to the current version and subsequently all old clients still work. You can then set the two registry values in the course of the clients update.

Furthermore, the load of upgraded systems should be watched, since via STunnel active delivery can no longer be performed by a connection setup from the server to the client. In conjunction with the [NatClient \[REG_DWORD\]](#) value the connection is not closed down any more and continuously loads the server.

UserProfiles [REG_MULTI_SZ]

Possible values:	<Name of the profile>,,<XPR SERVER>,

Optional default of a user profile for all users. This profile normally uses the Windows user account of the logged in user. Via [NetwareLoginOnly \[REG_DWORD\]](#) you can use the Novell Netware user account for logging on to the XPR server instead of the Windows user account.

E.25.5 Transport

The following values are specified in the key

HKLM\SOFTWARE\CYCOSAG\MSP\Transport\NVS:TCPIP.

NOTE:

On a 64-bit operating system you find the values in key

HKLM\Software\Wow6432Node

\Cycos AG\MSP\Transport\NVS:TCPIP.

ServerCache [REG_MULTI_SZ]

Example:	INHOUSE@NVS:TCPIP/mrs.sample.com:8944
Possible values:	<Server name>@NVS:<Protocol>/<Network address>

Contains a list of all XPR servers found during the installation. The sequence of the entries determines the protocol bindings for each server. There is one entry per line with the above syntax. As <protocol>, TCPIP is exclusively supported.

E.25.6 TCP/IP-Transport

The following values are specified in the key
HKLM\SOFTWARE\CYCOSAG\MSP\Transport.

NOTE:

On a 64-bit operating system you find the values in key
HKLM\Software\Wow6432Node\Cycos AG\MSP\Transport.

AplBrowseTimeout [REG_DWORD]

Default:	4
Possible values:	Seconds

The MSP tries automatically to find all XPR servers in the network. Here you can specify a period in seconds, after which the search process is abandoned, if no further server has reported within this period. This value should not be smaller than 4 seconds.

BindAddress [REG_SZ]

Default:	0.0.0.0
Possible values:	<IP address>

In a system with several IP addresses you can specify the IP address here via which the communication with the XPR server is handled.

MspListenPort [REG_DWORD]

Default:	8968
Possible values:	<IP Port>

Number of the TCP/IP port on which the MSP is contacted by the TCP/IP APL. This is used, for example, for active delivery where the client does not regularly check for new messages itself. Instead, the XPR server tries to reach the MSP at the familiar IP address and to deliver new messages immediately.

NatClient [REG_DWORD]

Default:	0
Possible values:	0 – Use local IP address. 1 – ###.###.###.### as IP address.

If the MSP is behind an NAT firewall, it transfers ###.###.###.### as local IP address to the TCP/IP APL. If the TCP/IP APL receives an address of this type, it replaces this address with the one delivered by the NAT firewall. The

clients set this address at the XPR server exclusively as return address for monitoring requests. This type of address replacement only works if the NAT firewall replaces each private IP address with a unique public IP address.

UseNameServer [REG_DWORD]

Example:	1
Possible values:	0 – Use IP addresses. 1 – Use Fully-Qualified-Domain-Names (FQDN).

Depending on the local configuration of the network stack the MSP either works with IP addresses or with FQDN.

VerifyShorthand [REG_DWORD]

Default:	0
Possible values:	0 – Always assume shorthand by server. 1 – Check shorthand by server.

The XPR server closes a TCP connection after some time, if no data are exchanged. This closing down is called shorthand. If the shorthand check is set here, the MSP sends a “ping” by UDP to the XPR server after cancellation of the connection. If the TCP/IP APL replies, the connection was set up by the shorthand time-out. If the reply fails to appear, the MSP assumes that the XPR server respectively the TCP/IP APL were shut down and the server cannot be reached any more. In this case a corresponding notification is sent to the applets. However, the check does not work all the time. This is, for example, the case if a Network Address Translation (NAT) is between MSP and server. The ping packet may also simply not arrive. This is in the UDP's nature, as the U stands for Unreliable.

No check is default set, so that the MSP always assumes a regular shorthand.

E.25.7 User-dependent Entries

The following values are specified in the key `HKCU\SOFTWARE\CYCOSAG\MSP`. Such entries are not created by the MSP itself but by the applets. From the MSP's point of view, the MSP configuration module is an applet as well.

DefaultProfile [REG_SZ]

Name of the default user profile set in the MSP configuration module. See also [UserProfiles \[REG_MULTI_SZ\]](#).

HiddenServers [REG_MULTI_SZ]

List of the XPR servers that in the MSP configuration module are hidden from the list of displayed XPR servers by means of the **Hide** button.

NetwareLoginOnly [REG_DWORD]

Default:	0
Possible values:	0 – No Novell Netware support 1 – Novell Netware support active

If this value is set to 1, the Novell Netware user account is used in user profiles instead of the Windows user account.

ProfileEditing [REG_DWORD]

Default:	Value does not exist.
Possible values:	0 – User profile must not be edited.

If this value exists and is set to 0, the user may neither edit his/her user profile nor define new profiles. The existing profile can then only be used for logging on or off. This can also be set for all users globally. See [ProfileEditing \[REG_DWORD\]](#).

UserProfiles [REG_MULTI_SZ]

Possible values:	<i><Name of the profile>,[USER ID],<XPR SERVER>,[Encrypted password]</i>

List of all user profiles created via the configuration module. If no *User ID* has been specified, the logged in Windows user account is used. In this case no password is required. When using an XPR *user ID*, the password that is then stored here encrypted may optionally be specified as well. Without this specification the password is queried with each login to the XPR server. If this value does not exist, a global user profile is searched for under [UserProfiles \[REG_MULTI_SZ\]](#).

Via [NetwareLoginOnly \[REG_DWORD\]](#) you can use the Novell Netware user account for logging on to the XPR server instead of the Windows user account. This can also be set individually for the respective user via the [NetwareLoginOnly \[REG_DWORD\]](#) value.

F Open Source and other licensed Software

XPR uses the Open Source or otherwise licensed products listed in the following. For using them legally, specific conditions must be met. For this reason, you find, among other things, references to the availability of modified sources and licenses.

- **7-Zip**
The Backup-and-Restore tool uses 7-Zip. 7-Zip is under the GNU LGPL. You find more information about 7-Zip under <http://www.7-zip.org>.
- **ActiveXperts SMS and MMS Toolkit**
OpenScape Xpressions V7 contains a network communication component licensed from ActiveXperts Software B.V. This component may only be used as part of and in connection with OpenScape Xpressions V7.
- **Apache ActiveMQ 4.1.1, Apache Commons, Apache XML RPC, Apache Jakarta Commons, log4cxx 0.97, log4j 1.2.14, log4net 1.2.9.0, OpenJPA 0.9.7, Tomcat 6.0.10**
Copyright 2001-2008 The Apache Software Foundation
This product includes software developed by
The Apache Software Foundation (<http://www.apache.org/>).
- **Apache Geronimo**
See [Section F.1, “Apache Geronimo”](#), on page 2007.
- **Apache Jakarta JCS 1.3**
Copyright 2001-2007 The Apache Software Foundation.
Portions Copyright (c) Xerox Corporation 1998-2001.
- **Boost 1.33.1, SOCI 2.2.0**
This software is used for creating the binary code, parts are included.
- **Business Intelligence and Reporting Tools (BIRT)**
BIRT is under the Eclipse Public License - v 1.0 (<http://www.eclipse.org/legal/epl-v10.html>). You find more information about BIRT under <http://www.eclipse.org/birt/phoenix/>.
- **Boost 1.33.1**
This software is only passed on in the binary code.
- **crypto++ 5.2.1**
Copyright (c) 1995-2006 by Wei Dai. Portions Copyright 1998 Brian Gladman.
- **cURLpp 0.5.2**
See [Section F.3, “cURLpp Copyright and Permission Notice”](#), on page 2022.
- **CxImage**
Copyright (C) 2001 - 2004, Davide Pizzolato

- Eclipse Equinox 3.3
Copyright (c) The Eclipse Foundation
Source code is available at <http://download.eclipse.org/eclipse/equinox/>

The Cycos AG herewith offers the provision of a machine readable version of the entire modified source code. The costs that may be incurred, for example, the costs for a blank CD, are invoiced without surcharge.

Please send your request to relbuilder@cycos.com.
- Eclipse GEF 3.3
Copyright (c) The Eclipse Foundation
Source code is available at <http://www.eclipse.org/gef/downloads/>

The Cycos AG herewith offers the provision of a machine readable version of the entire modified source code. The costs that may be incurred, for example, the costs for a blank CD, are invoiced without surcharge.

Please send your request to relbuilder@cycos.com.
- Eclipse RCP 3.3
Copyright (c) The Eclipse Foundation
Source code is available at <http://download.eclipse.org/eclipse/download/>

The Cycos AG herewith offers the provision of a machine readable version of the entire modified source code. The costs that may be incurred, for example, the costs for a blank CD, are invoiced without surcharge.

Please send your request to relbuilder@cycos.com.
- Fast Infoset 1.0
This product includes software developed by the Fast Infoset Project (<http://fi.dev.java.net>)
Copyright (c) 2005-2008 Sun Microsystems Inc.
- fax2pdf 0.1.3
This product contains a modified version of fax2pdf 0.1.3, which, in turn, is published under the license GNU GPL.

The Cycos AG herewith offers the provision of a machine readable version of the entire modified source code. The costs that may be incurred, for example, the costs for a blank CD, are invoiced without surcharge.

Please send your request to relbuilder@cycos.com.
- Google Web Toolkit GWT 1.4.60
See [Section F.4, "Google Web Toolkit GWT 1.4.60", on page 2022](#).
- GPL Ghostscript 8.50
This product contains an unmodified version of GPL Ghostscript 8.50.

The Cycos AG herewith offers the provision of a machine readable version of the entire modified source code upon request. The costs that may be incurred, for example, the costs for a blank CD, are invoiced without surcharge.

Please send your request to relbuilder@cycos.com.

- GraphicsMagick
See [Section F.5, “GraphicsMagick”, on page 2023](#).
- iCal4j 1.0 beta3
See [Section F.6, “iCal4j 1.0 beta3”, on page 2026](#).
- Jain Sip/Sdp implementation by NIST V 1.2
See [Section F.7, “Jain Sip/Sdp implementation by NIST V 1.2”, on page 2027](#).
- Java Architecture for XML Binding (JAXB API)
developed by Sun Microsystems (<http://www.sun.com/>)
License: COMMON DEVELOPMENT AND DISTRIBUTION LICENSE
(CDDL) Version 1.0 (<http://www.sun.com/cddl/cddl.html>)
Source code is available from <https://jaxb2-sources.dev.java.net/>
- jpeg 6b
This software is based in part on the work of the Independent JPEG Group.
- K-XML 2.3
See [Section F.8, “K-XML 2.3”, on page 2027](#).
- libcurl 7.15.1
See [Section F.9, “libcurl Copyright and Permission Notice”, on page 2028](#).
- libpng 1.2.8
Copyright (C) 2004, 2006 Glenn Randers-Pehrson
- libtiff 3.8.0
See [Section F.10, “libTIFF Copyright and Permission Notice”, on page 2028](#).
- OpenSSL
See [Section F.12, “OpenSSL License”, on page 2029](#).
- PostgreSQL 8.2 & PostgreSQL 8.2 JDBC Drivers
See [Section F.13, “PostgreSQL 8.2 & PostgreSQL 8.2 JDBC Drivers”, on page 2031](#).
- Rhino 1.6
This product includes software developed by
The Mozilla Foundation (<http://www.mozilla.org/>).
License: Mozilla Public License v. 1.1
<http://www.mozilla.org/MPL/MPL-1.1.txt>
Source code availability: <http://www.mozilla.org/rhino/>
- SNMP4J 1.7.5
See [Section F.14, “SNMP4J 1.7.5”, on page 2032](#).
- SoundTouch 1.2.1
This product contains an unmodified version of SoundTouch 1.2.1.

The Cycos AG herewith offers the provision of a machine readable version of the entire modified source code upon request. The costs that may be incurred, for example, the costs for a blank CD, are invoiced without surcharge.

Please send your request to relbuilder@cycos.com.

- Spring Framework
This product includes software developed by the Spring Framework Project (<http://www.springframework.org>).
- Stunnel
Stunnel is found under the GNU GPL. You receive more information about Stunnel under <http://www.stunnel.org>.
- Sun Java Streaming XML Parser 1.0.1
Sun Java Runtime Environment 5
Sun Java Runtime Environment 6

This product includes software developed by Sun Microsystems, Inc., under the Sun Binary Code License Agreement (<http://www.java.com/en/download/license.jsp>)
- Sun XACML implementation 1.2
See [Section F.15, “Sun XACML implementation 1.2”](#), on page 2032.
- tinyXML 2.4.3
This product includes software developed by Lee Thomason (www.grinninglizard.com) and others (www.sourceforge.net/projects/tinyxml).
- WiX
This compiler is used for MSI installation packets. Some of the displayed dialogs contain results of the WiX Localization Projects. The WiX source code is found under <http://wix.sourceforge.net>. The current status of the WiX localization project is found under <http://www.tramontana.co.hu/wix/loc/index.php>.
- Xerces-C 2.7.0
See [Section F.2, “Apache License”](#), on page 2018 and [Section F.16, “Xerces-C”](#), on page 2033.
- zlib
Copyright (C) 1995-2005 Jean-loup Gailly and Mark Adler

NOTE:

The license conditions of some Open Source components listed in the following exclusively refer to the respectively mentioned components. The XPR server itself with all its components is **not** specified under one of these licenses.

F.1 Apache Geronimo

```

=====
== NOTICE file corresponding to section 4(d) of the Apache License, ==
== Version 2.0, in this case for the Apache Geronimo distribution. ==
=====

Apache Geronimo

Copyright 2003-2008 The Apache Software Foundation

This product includes software developed by

The Apache Software Foundation (http://www.apache.org/).

=====
== Apache Geronimo Dojo Notice ==
=====

Portions of the Geronimo Dojo plugins were developed by the Dojo Foundation.

Copyright (c) 2005-2008, The Dojo Foundation

All rights reserved.

=====
== Apache Geronimo Web Console Notice ==
=====

Portions of the Web Console were originally developed by International Business
Machines Corporation and are licensed to the Apache Software Foundation under
the "Software Grant and Corporate Contribution License Agreement", informally
known as the "IBM Console CLA".

Portions of the Web Console were developed by the Apache Pluto community.

Apache Pluto Project

Copyright 2003-2008 The Apache Software Foundation.

=====
== Apache Geronimo OpenEJB Notice ==
=====

Portions of the Geronimo OpenEJB and Corba plugins were developed by the Apache
OpenEJB community.

Apache OpenEJB Project

Copyright 1999-2007 The Apache Software Foundation

=====
== Bouncy Castle Notice ==
=====

This product includes software (the ASN1 codec implementation in geronimo-cryp-
to) developed by the Bouncy Castle project. (http://www.bouncycastle.org/)

Copyright (c) 2000-2005

The Legion Of The Bouncy Castle (http://www.bouncycastle.org)

=====
== Apache Geronimo Webservices Builder Notices ==
=====

For soap_encoding_1_1.xsd -

```


W3C SOFTWARE NOTICE AND LICENSE

Copyright © 1994-2002 World Wide Web Consortium, (Massachusetts Institute of Technology, Institut National de Recherche en Informatique et en Automatique, Keio University). All Rights Reserved. <http://www.w3.org/Consortium/Legal/>

This W3C work (including software, documents, or other related items) is being provided by the copyright holders under the following license. By obtaining, using and/or copying this work, you (the licensee) agree that you have read, understood, and will comply with the following terms and conditions:

Permission to use, copy, modify, and distribute this software and its documentation, with or without modification, for any purpose and without fee or royalty is hereby granted, provided that you include the following on ALL copies of the software and documentation or portions thereof, including modifications, that you make:

1. The full text of this NOTICE in a location viewable to users of the redistributed or derivative work.
2. Any pre-existing intellectual property disclaimers, notices, or terms and conditions. If none exist, a short notice of the following form (hypertext is preferred, text is permitted) should be used within the body of any redistributed or derivative code: "Copyright © [date-of-software] World Wide Web Consortium, (Massachusetts Institute of Technology, Institut National de Recherche en Informatique et en Automatique, Keio University). All Rights Reserved. <http://www.w3.org/Consortium/Legal/>"
3. Notice of any changes or modifications to the W3C files, including the date changes were made. (We recommend you provide URIs to the location from which the code is derived.)

THIS SOFTWARE AND DOCUMENTATION IS PROVIDED "AS IS," AND COPYRIGHT HOLDERS MAKE NO REPRESENTATIONS OR WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO, WARRANTIES OF MERCHANTABILITY OR FITNESS FOR ANY PARTICULAR PURPOSE OR THAT THE USE OF THE SOFTWARE OR DOCUMENTATION WILL NOT INFRINGE ANY THIRD PARTY PATENTS, COPYRIGHTS, TRADEMARKS OR OTHER RIGHTS.

COPYRIGHT HOLDERS WILL NOT BE LIABLE FOR ANY DIRECT, INDIRECT, SPECIAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF ANY USE OF THE SOFTWARE OR DOCUMENTATION.

The name and trademarks of copyright holders may NOT be used in advertising or publicity pertaining to the software without specific, written prior permission. Title to copyright in this software and any associated documentation will at all times remain with copyright holders.

For wsdl.xsd -

Copyright 2001-2003 International Business Machines Corporation, Microsoft Corporation. All rights reserved.

```
#####
## APACHE GERONIMO DEPENDENCIES                                     ##
#####
```

A binary distribution of Apache Geronimo, or an Apache Geronimo server which is built from source, includes a number of dependent packages with separate copyright notices and license terms. The following notices apply to these dependencies.

```
=====
==  ANNOGEN Notice                                              ==
=====
```

This product includes software developed by the Annogen project

(<http://annogen.codehaus.org/>)

This software consists of voluntary contributions made by many individuals on behalf of the Apache Software Foundation and was originally based on software copyright (c) 2000-2004 BEA Systems Inc., <<http://www.bea.com/>>. For more information on the Apache Software Foundation, please see <<http://www.apache.org/>>.

```
=====
==  Apache ActiveMQ Notice                               ==
=====
```

Copyright 2005-2007 The Apache Software Foundation

This product includes software developed by

The Apache Software Foundation (<http://www.apache.org/>).

```
=====
==  Apache Ant Notice                                   ==
=====
```

Apache Ant

Copyright 1999-2006 The Apache Software Foundation

This product includes software developed by

The Apache Software Foundation (<http://www.apache.org/>).

This product includes also software developed by :

- the W3C consortium (<http://www.w3c.org/>) ,
- the SAX project (<http://www.saxproject.org/>)

The <sync> task is based on code Copyright (c) 2002, Landmark Graphics Corp that has been kindly donated to the Apache Software Foundation.

```
=====
==  Apache Axiom Notice                               ==
=====
```

This product includes software developed by

The Apache Software Foundation (<http://www.apache.org/>).

Portions Copyright 2006 International Business Machines Corp.

```
=====
==  Apache Commons BeanUtils Notice                   ==
=====
```

This product includes software developed by

The Apache Software Foundation (<http://www.apache.org/>).

Portions Copyright 2006 International Business Machines Corp.

```
=====
==  Apache Commons BeanUtils                           ==
=====
```

Copyright (c) 1999-2003 The Apache Software Foundation. All rights reserved.

```
=====
==  Apache Commons CLI Notice                         ==
=====
```

This product includes software developed by

The Apache Software Foundation (<http://www.apache.org/>).

Open Source and other licensed Software

Copyright (c) 1999-2001 The Apache Software Foundation. All rights reserved.

```
=====
==  Apache Commons Lang Notice                               ==
=====
```

This product includes software developed by

The Apache Software Foundation (<http://www.apache.org/>).

Copyright (c) 2002-2003 The Apache Software Foundation. All rights reserved.

```
=====
==  Apache Commons XML Resolver                               ==
=====
```

This product includes software developed by

The Apache Software Foundation (<http://www.apache.org/>).

Copyright (c) 2001-2003 The Apache Software Foundation. All rights reserved.

```
=====
==  Apache CXF                                                ==
=====
```

Apache CXF

Copyright 2006-2007 Apache Software Foundation

This product includes software developed at

Apache Software Foundation (<http://www.apache.org/>).

This product includes/uses software, Web Services Metadata 2.0 (http://geronimo.apache.org/specs/geronimo-ws-metadata_2.0_spec), developed by Apache Software Foundation (<http://www.apache.org>)

License: The Apache Software License, Version 2.0 (<http://www.apache.org/licenses/LICENSE-2.0.txt>)

This product includes/uses software, AOP alliance (<http://aopalliance.sourceforge.net>)

License: Public Domain

This product includes/uses software, Logging ([http://jakarta.apache.org/commons/\\${pom.artifactId.substring\(8\)}/](http://jakarta.apache.org/commons/${pom.artifactId.substring(8)}/)), developed by The Apache Software Foundation (<http://jakarta.apache.org>)

License: The Apache Software License, Version 2.0 (/LICENSE.txt)

This product includes/uses software, Woodstox (<http://woodstox.codehaus.org>), developed by Codehaus (<http://www.codehaus.org/>)

License: The Apache Software License, Version 2.0 (<http://www.apache.org/licenses/LICENSE-2.0.txt>)

This product includes/uses software, Activation 1.1 (http://geronimo.apache.org/specs/geronimo-activation_1.1_spec), developed by Apache Software Foundation (<http://www.apache.org>)

License: The Apache Software License, Version 2.0 (<http://www.apache.org/licenses/LICENSE-2.0.txt>)

This product includes/uses software, Spring Framework: Core (<http://www.springframework.org>), developed by Spring Framework (<http://www.springframework.org/>)

License: The Apache Software License, Version 2.0 (<http://www.apache.org/licenses/LICENSE-2.0.txt>)

This product includes/uses software, Lang ([http://jakarta.apache.org/commons/\\${pom.artifactId.substring\(8\)}/](http://jakarta.apache.org/commons/${pom.artifactId.substring(8)}/)), developed by The Apache Software Foundation (<http://jakarta.apache.org>)

License: The Apache Software License, Version 2.0 ([/LICENSE.txt](#))

This product includes/uses software, StAX API (<http://stax.codehaus.org/>)

License: The Apache Software License, Version 2.0 (<http://www.apache.org/licenses/LICENSE-2.0.txt>)

This product includes/uses software, WSDL4J (<http://sf.net/projects/wsdl4j>)

License: CPL (<http://www.opensource.org/licenses/cpl1.0.txt>)

This product includes/uses software, Neethi, developed by The Apache Software Foundation (<http://www.apache.org/>)

License: The Apache Software License, Version 2.0 (<http://www.apache.org/licenses/LICENSE-2.0.txt>)

This product includes/uses software, Java Architecture for XML Binding (JAXB API), developed by Sun Microsystems (<http://www.sun.com/>)

License: COMMON DEVELOPMENT AND DISTRIBUTION LICENSE (CDDL) Version 1.0 (<http://www.sun.com/cddl/cddl.html>)

This product includes/uses software, XmlSchema (<http://ws.apache.org/commons/XmlSchema>), developed by Apache Software Foundation (<http://www.apache.org/>)

License: The Apache Software License, Version 2.0 (<http://www.apache.org/licenses/LICENSE-2.0.txt>)

This product includes/uses software, XML Commons Resolver Component (<http://xml.apache.org/commons/components/resolver/>), developed by Apache Software Foundation (<http://www.apache.org/>)

License: The Apache Software License, Version 2.0 (<http://www.apache.org/licenses/LICENSE-2.0.txt>)

This product includes/uses software, Apache CXF Common Utilities (<http://cwiki.apache.org/CXF>), developed by Apache Software Foundation (<http://www.apache.org/>)

License: The Apache Software License, Version 2.0 (<http://www.apache.org/licenses/LICENSE-2.0.txt>)

This product includes/uses software, Spring Framework: Beans (<http://www.springframework.org>), developed by Spring Framework (<http://www.springframework.org/>)

License: The Apache Software License, Version 2.0 (<http://www.apache.org/licenses/LICENSE-2.0.txt>)

This product includes/uses software, Annotation 1.0 (http://geronimo.apache.org/specs/geronimo-annotation_1.0_spec), developed by Apache Software Foundation (<http://www.apache.org>)

License: The Apache Software License, Version 2.0 (<http://www.apache.org/licenses/LICENSE-2.0.txt>)

This product includes/uses software, Apache CXF Common Schemas (<http://cwiki.apache.org/CXF/cxf-common-schemas>), developed by Apache Software Foundation (<http://www.apache.org/>)

License: The Apache Software License, Version 2.0 (<http://www.apache.org/licenses/LICENSE-2.0.txt>)

Open Source and other licensed Software

This product includes/uses software, Spring Framework: Context (<http://www.springframework.org>), developed by Spring Framework (<http://www.springframework.org/>)

License: The Apache Software License, Version 2.0 (<http://www.apache.org/licenses/LICENSE-2.0.txt>)

```
=====
==  Apache Derby Notice                               ==
=====
```

Apache Derby

Copyright 2004-2006 The Apache Software Foundation

This product includes software developed by

The Apache Software Foundation (<http://www.apache.org/>).

Portions of Derby were originally developed by International Business Machines Corporation and are licensed to the Apache Software Foundation under the "Software Grant and Corporate Contribution License Agreement", informally known as the "Derby CLA".

The following copyright notice(s) were affixed to portions of the code with which this file is now or was at one time distributed and are placed here unaltered.

(C) Copyright 1997,2004 International Business Machines Corporation.
All rights reserved.

(C) Copyright IBM Corp. 2003.

The portion of the functionTests under 'nist' was originally developed by the National Institute of Standards and Technology (NIST), an agency of the United States Department of Commerce, and adapted by International Business Machines Corporation in accordance with the NIST Software Acknowledgment and Redistribution document at http://www.itl.nist.gov/div897/ctg/sql_form.htm

```
=====
==  Apache Geronimo Gshell Notice                       ==
=====
```

Apache Geronimo

Copyright 2007 The Apache Software Foundation

```
=====
==  Apache MyFaces Notice                               ==
=====
```

This software includes Sun's web-facesconfig.dtd files (see <http://java.sun.com/dtd/>).

```
=====
==  Apache OpenEJB Notice                               ==
=====
```

Apache OpenEJB

Copyright 1999-2008 The Apache OpenEJB development community

```
=====
==  Apache OpenJPA Notice                               ==
=====
```

This product includes software developed by

The Apache Software Foundation (<http://www.apache.org/>).

COPYRIGHT NOTICES

* OpenJPA includes software developed by the SERP project

Copyright (c) 2002-2006, A. Abram White. All rights reserved.

* OpenJPA is bundled with the binaries from the JPA specification, by Sun Microsystems and licensed under the CDDL 1.0. The source code is available at: <https://glassfish.dev.java.net/source/browse/glassfish/>

== Apache Pluto ==

This product includes software developed by the Apache Software Foundation (<http://www.apache.org/>).

Copyright 2003-2008 The Apache Software Foundation.

== Apache Scout ==

This product includes software developed by the Apache Software Foundation (<http://www.apache.org/>).

Copyright 2001-2004 The Apache Software Foundation.

== Apache Tomcat Notice ==

Java compilation software for JSP pages is provided by Eclipse, which is open source software. The original software and related information is available at <http://www.eclipse.org>.

== Apache WS Commons Notice ==

This product includes software developed by

The Apache Software Foundation (<http://www.apache.org/>).

Portions Copyright 2006 International Business Machines Corp.

== Apache XmlBeans Notice ==

This product includes software developed by

The Apache Software Foundation (<http://www.apache.org/>).

Portions of this software were originally based on the following:

- software copyright (c) 2000-2003, BEA Systems, <<http://www.bea.com/>>.

Aside from contributions to the Apache XMLBeans project, this software also includes:

- one or more source files from the Apache Xerces-J and Apache Axis products, Copyright (c) 1999-2003 Apache Software Foundation
- W3C XML Schema documents Copyright 2001-2003 (c) World Wide Web Consortium (Massachusetts Institute of Technology, European Research Consortium for Informatics and Mathematics, Keio University)

Open Source and other licensed Software

- resolver.jar from Apache Xml Commons project,
Copyright (c) 2001-2003 Apache Software Foundation
- Piccolo XML Parser for Java from <http://piccolo.sourceforge.net/>,
Copyright 2002 Yuval Oren under the terms of the Apache Software License 2.0
- JSR-173 Streaming API for XML from
<http://sourceforge.net/projects/xmlpullparser/>,
Copyright 2005 BEA under the terms of the Apache Software License 2.0

=====
== Apache Yoko Notice ==
=====

Apache Yoko Project

Copyright 1999-2006 The Apache Software Foundation

This product includes software developed at

The Apache Software Foundation (<http://www.apache.org/>).

ORB Portions of this software were developed at IONA Technologies.

Object Management Group (OMG) classes used by the orb. The original classes are available from www.org.omg.

The RMI over IIOP implementation were developed at Trifork Technologies.

=====
== ASM Notice ==
=====

Copyright (c) 2000-2005 INRIA, France Telecom

All rights reserved.

=====
== AspectJ Notice ==
=====

This product includes software developed by

the Eclipse Foundation (<http://www.eclipse.org/>).

AspectJ source code can be obtained from the AspectJ web site

<http://www.eclipse.org/aspectj/>

=====
== Backport Util Concurrent Notice ==
=====

The backport-util-concurrent software has been released to the public domain, as explained at: <http://creativecommons.org/licenses/publicdomain>.

Acknowledgements: backport-util-concurrent is based in large part on the public domain sources from:

- 1) JSR166,
- 2) package `dl.util.concurrent`,
- 3) Doug Lea's "collections" package.

=====
== Castor Notice ==
=====

Copyright 2004-2005 Werner Guttman

This product includes software developed by the Exolab project.

(<http://www.exolab.org/>)

Copyright 1999-2004 (C) Intalio Inc., and others. All Rights Reserved..

```
=====
== Dojo Notice                                     ==
=====
```

Copyright (c) 2004-2006, The Dojo Foundation, All Rights Reserved

```
=====
== Howl Notice                                     ==
=====
```

Copyright (c) 2004, Bull S.A.

All rights reserved.

```
=====
== jaxen Notice                                     ==
=====
```

This product includes software developed by the jaxen project

(<http://jaxen.org/>).

Copyright 2003-2006 The Werken Company. All rights reserved.

```
=====
== JDBM Notice                                     ==
=====
```

This product includes software developed by the JDBM Project

(<http://jdbm.sourceforge.net/>).

Copyright 2000 (C) Cees de Groot. All rights reserved.

Contributions are Copyright (C) 2000 by their associated contributors.

```
=====
== JDOM Notice                                     ==
=====
```

This product includes software developed by the JDOM Project

(<http://www.jdom.org/>).

Copyright (C) 2000-2004 Jason Hunter & Brett McLaughlin.

All rights reserved.

```
=====
== Jetty Notice                                     ==
=====
```

```
=====
Jetty Web Container
```

```
Copyright 1995-2006 Mort Bay Consulting Pty Ltd
=====
```

This product includes software developed at The Apache Software Foundation

(<http://www.apache.org/>).

The UnixCrypt.java code ~Implements the one way cryptography used by Unix systems for simple password protection. Copyright 1996 Aki Yoshida, modified April 2001 by Iris Van den Broeke, Daniel Deville.

Open Source and other licensed Software

The default JSP implementation is provided by the Glassfish JSP engine from project Glassfish <http://glassfish.dev.java.net>. Copyright 2005 Sun Microsystems, Inc. and portions Copyright Apache Software Foundation.

Some portions of the code are Copyright:

2006 Tim Venum

1999 Jason Gilbert.

```
=====
==  JLine Notice                               ==
=====
```

Copyright (c) 2002-2006, Marc Prud'hommeaux <mwpl@cornell.edu>

All rights reserved.

```
=====
==  SAAJ Notice                               ==
=====
```

```
=====
==  OGNL Notice                               ==
=====
```

This product includes software developed by the OpenSymphony Group

(<http://www.opensymphony.com/>).

Copyright (c) 2001-2004 The OpenSymphony Group. All rights reserved.

```
=====
==  Plexus Notice                               ==
=====
```

This product includes software developed by the Plexus project

(<http://plexus.codehaus.org/>)

The source code for the Plexus project can be downloaded from:

<http://plexus.codehaus.org/source-repository.html>

```
=====
==  Serp Notice                               ==
=====
```

Copyright (c) 2002, A. Abram White

All rights reserved.

```
=====
==  SL4J Notice                               ==
=====
```

Copyright (c) 2004-2005 SLF4J.ORG

Copyright (c) 2004-2005 QOS.ch

All rights reserved.

```
=====
==  Sun CDDL Notice                           ==
=====
```

This product includes software developed for the JAXB Reference Implementation project. (<https://jaxb.dev.java.net/>)

This product includes software developed for Java API for XML Web Services project (JAX-WS) (<https://jax-ws.dev.java.net/>)

This product includes software developed for the Java Server Pages Tag Library project (<https://jstl.dev.java.net/>)

This product includes software developed for SOAP with Attachments API for Java (SAAJ). The software is available from the GlassFish project (<https://saaaj.dev.java.net/>)

```
=====
==  WADI Notice                               ==
=====
```

This product includes software developed by the WADI project (<http://wadi.codehaus.org/>)

```
=====
==  Spring Notice                             ==
=====
```

This product also includes software developed by Spring Framework Project (<http://www.springframework.org>)

This product includes software developed by the Apache Software Foundation (<http://www.apache.org>).

This product also includes software developed by Clinton Begin (<http://www.ibatis.com>).

The end-user documentation included with a redistribution, if any, must include the following acknowledgement:

"This product includes software developed by the Spring Framework Project (<http://www.springframework.org>)."

Alternately, this acknowledgement may appear in the software itself, if and wherever such third-party acknowledgements normally appear.

The names "Spring" and "Spring Framework" must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact rod.johnson@interface21.com or juergen.hoeller@interface21.com.

```
=====
==  W3C DOM Notice                             ==
=====
```

Copyright (c) 2000 World Wide Web Consortium, (Massachusetts Institute of Technology, Institut National de Recherche en Informatique et en Automatique, Keio University). All rights reserved.

The DOM bindings are published under the W3C Software Copyright Notice and License. The software license requires "Notice of any changes or modifications to the W3C files, including the date changes were made." Consequently, modified versions of the DOM bindings must document that they do not conform to the W3C standard; in the case of the IDL binding, the pragma prefix can no longer be 'w3c.org'; in the case of the Java binding, the package names can no longer be in the 'org.w3c' package.

Note: The original version of the W3C Software Copyright Notice and License could be found at

<http://www.w3.org/Consortium/Legal/copyright-software-19980720>

Copyright (c) 1994-2000 World Wide Web Consortium, (Massachusetts Institute of Technology, Institut National de Recherche en Informatique et en Automatique, Keio University). All Rights Reserved. <http://www.w3.org/Consortium/Legal/>

Open Source and other licensed Software

```
=====
==  Woodstox Notice                               ==
=====

This product currently only contains code developed by authors of specific com-
ponents, as identified by the source code files.

Since product implements StAX API, it has dependencies to StAX API classes.

For additional credits (generally to people who reported problems) see CREDITS
file.

=====
==  W3C Software Notice                             ==
=====

Copyright (c) 1994-2002 World Wide Web Consortium, (Massachusetts Institute of
Technology, Institut National de Recherche en Informatique et en Automatique,
Keio University). All Rights Reserved. http://www.w3.org/Consortium/Legal/

=====
==  WSDL4J Notice                                   ==
=====

The Program includes all or portions of the following software which is subject
to the Common Public License ("CPL Code"). This software consists of voluntary
contributions made by many individuals on behalf of the WSDL4J project.

You may download the source version of the WSDL4J component at

http://sourceforge.net/projects/wsdl4j

=====
==  XPP3 Notice                                     ==
=====

This product includes software developed by the Indiana University Extreme! Lab
(http://www.extreme.indiana.edu/).

Copyright (c) 2002 Extreme! Lab, Indiana University. All rights reserved.

=====
==  XStream Notice                                 ==
=====

Copyright (c) 2003-2006, Joe Walnes

All rights reserved.
```

F.2 Apache License

Version 2.0, January 2004
<http://www.apache.org/licenses/>

TERMS AND CONDITIONS FOR USE, REPRODUCTION, AND DISTRIBUTION

1. Definitions.

"License" shall mean the terms and conditions for use, reproduction, and distribution as defined by Sections 1 through 9 of this document.

"Licensor" shall mean the copyright owner or entity authorized by the copyright owner that is granting the License.

"Legal Entity" shall mean the union of the acting entity and all other entities that control, are controlled by, or are under common control with that entity. For the purposes of this definition, "control" means (i) the power, direct or indirect, to cause the direction or management of such entity, whether by contract or otherwise, or (ii) ownership of fifty percent (50%) or more of the outstanding shares, or (iii) beneficial ownership of such entity.

"You" (or "Your") shall mean an individual or Legal Entity exercising permissions granted by this License.

"Source" form shall mean the preferred form for making modifications, including but not limited to software source code, documentation source, and configuration files.

"Object" form shall mean any form resulting from mechanical transformation or translation of a Source form, including but not limited to compiled object code, generated documentation, and conversions to other media types.

"Work" shall mean the work of authorship, whether in Source or Object form, made available under the License, as indicated by a copyright notice that is included in or attached to the work (an example is provided in the Appendix below).

"Derivative Works" shall mean any work, whether in Source or Object form, that is based on (or derived from) the Work and for which the editorial revisions, annotations, elaborations, or other modifications represent, as a whole, an original work of authorship. For the purposes of this License, Derivative Works shall not include works that remain separable from, or merely link (or bind by name) to the interfaces of, the Work and Derivative Works thereof.

"Contribution" shall mean any work of authorship, including the original version of the Work and any modifications or additions to that Work or Derivative Works thereof, that is intentionally submitted to Licensor for inclusion in the Work by the copyright owner or by an individual or Legal Entity authorized to submit on behalf of the copyright owner. For the purposes of this definition, "submitted" means any form of electronic, verbal, or written communication sent to the Licensor or its representatives, including but not limited to communication on electronic mailing lists, source code control systems, and issue tracking systems that are managed by, or on behalf of, the Licensor for the purpose of discussing and improving the Work, but excluding communication that is conspicuously marked or otherwise designated in writing by the copyright owner as "Not a Contribution."

"Contributor" shall mean Licensor and any individual or Legal Entity on behalf of whom a Contribution has been received by Licensor and subsequently incorporated within the Work.

2. Grant of Copyright License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable copyright license to reproduce, prepare Derivative Works of, publicly display, publicly perform, sublicense, and distribute the Work and such Derivative Works in Source or Object form.
3. Grant of Patent License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable (except as stated in this section) patent license to make, have made,

use, offer to sell, sell, import, and otherwise transfer the Work, where such license applies only to those patent claims licensable by such Contributor that are necessarily infringed by their Contribution(s) alone or by combination of their Contribution(s) with the Work to which such Contribution(s) was submitted. If You institute patent litigation against any entity (including a cross-claim or counterclaim in a lawsuit) alleging that the Work or a Contribution incorporated within the Work constitutes direct or contributory patent infringement, then any patent licenses granted to You under this License for that Work shall terminate as of the date such litigation is filed.

4. Redistribution. You may reproduce and distribute copies of the Work or Derivative Works thereof in any medium, with or without modifications, and in Source or Object form, provided that You meet the following conditions:
 - (a) You must give any other recipients of the Work or Derivative Works a copy of this License; and
 - (b) You must cause any modified files to carry prominent notices stating that You changed the files; and
 - (c) You must retain, in the Source form of any Derivative Works that You distribute, all copyright, patent, trademark, and attribution notices from the Source form of the Work, excluding those notices that do not pertain to any part of the Derivative Works; and
 - (d) If the Work includes a "NOTICE" text file as part of its distribution, then any Derivative Works that You distribute must include a readable copy of the attribution notices contained within such NOTICE file, excluding those notices that do not pertain to any part of the Derivative Works, in at least one of the following places: within a NOTICE text file distributed as part of the Derivative Works; within the Source form or documentation, if provided along with the Derivative Works; or, within a display generated by the Derivative Works, if and wherever such third-party notices normally appear. The contents of the NOTICE file are for informational purposes only and do not modify the License. You may add Your own attribution notices within Derivative Works that You distribute, alongside or as an addendum to the NOTICE text from the Work, provided that such additional attribution notices cannot be construed as modifying the License.

You may add Your own copyright statement to Your modifications and may provide additional or different license terms and conditions for use, reproduction, or distribution of Your modifications, or for any such Derivative Works as a whole, provided Your use, reproduction, and distribution of the Work otherwise complies with the conditions stated in this License.

5. Submission of Contributions. Unless You explicitly state otherwise, any Contribution intentionally submitted for inclusion in the Work by You to the Licensor shall be under the terms and conditions of this License, without any additional terms or conditions. Notwithstanding the above, nothing herein shall supersede or modify the terms of any separate license agreement you may have executed with Licensor regarding such Contributions.
6. Trademarks. This License does not grant permission to use the trade

names, trademarks, service marks, or product names of the Licensor, except as required for reasonable and customary use in describing the origin of the Work and reproducing the content of the NOTICE file.

7. Disclaimer of Warranty. Unless required by applicable law or agreed to in writing, Licensor provides the Work (and each Contributor provides its Contributions) on an "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied, including, without limitation, any warranties or conditions of TITLE, NON-INFRINGEMENT, MERCHANTABILITY, or FITNESS FOR A PARTICULAR PURPOSE. You are solely responsible for determining the appropriateness of using or redistributing the Work and assume any risks associated with Your exercise of permissions under this License.
8. Limitation of Liability. In no event and under no legal theory, whether in tort (including negligence), contract, or otherwise, unless required by applicable law (such as deliberate and grossly negligent acts) or agreed to in writing, shall any Contributor be liable to You for damages, including any direct, indirect, special, incidental, or consequential damages of any character arising as a result of this License or out of the use or inability to use the Work (including but not limited to damages for loss of goodwill, work stoppage, computer failure or malfunction, or any and all other commercial damages or losses), even if such Contributor has been advised of the possibility of such damages.
9. Accepting Warranty or Additional Liability. While redistributing the Work or Derivative Works thereof, You may choose to offer, and charge a fee for, acceptance of support, warranty, indemnity, or other liability obligations and/or rights consistent with this License. However, in accepting such obligations, You may act only on Your own behalf and on Your sole responsibility, not on behalf of any other Contributor, and only if You agree to indemnify, defend, and hold each Contributor harmless for any liability incurred by, or claims asserted against, such Contributor by reason of your accepting any such warranty or additional liability.

END OF TERMS AND CONDITIONS

APPENDIX: How to apply the Apache License to your work.

To apply the Apache License to your work, attach the following boilerplate notice, with the fields enclosed by brackets "[]" replaced with your own identifying information. (Don't include the brackets!) The text should be enclosed in the appropriate comment syntax for the file format. We also recommend that a file or class name and description of purpose be included on the same "printed page" as the copyright notice for easier identification within third-party archives.

Copyright [yyyy] [name of copyright owner]

Licensed under the Apache License, Version 2.0 (the "License");
you may not use this file except in compliance with the License.
You may obtain a copy of the License at

<http://www.apache.org/licenses/LICENSE-2.0>

Unless required by applicable law or agreed to in writing, software distributed under the License is distributed on an "AS IS" BASIS,

WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied.
See the License for the specific language governing permissions and
limitations under the License.

F.3 cURLpp Copyright and Permission Notice

Copyright (c) 2002-2006, Jean-Philippe Barrette-LaPierre

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

F.4 Google Web Toolkit GWT 1.4.60

Copyright (c) Google, Inc. 2008. All rights reserved. Visit Google Code (<http://code.google.com/webtoolkit/>).

This product includes software developed by:

- The Apache Software Foundation (<http://www.apache.org/>).
 - Tomcat (<http://tomcat.apache.org/>) with modifications
License: Apache License v. 2.0 (see above)
Source code availability: <http://tomcat.apache.org> modifications are at [org/apache/tomcat](http://org.apache/tomcat) within gwt-dev.jar
 - Tapestry (<http://tapestry.apache.org/>)
- The Eclipse Foundation (<http://www.eclipse.org/>).
 - Java Development Tools (<http://www.eclipse.org/jdt/>)
License: Eclipse Public License v. 1.0
<http://www.eclipse.org/legal/epl-v10.html>
Source code availability: <http://archive.eclipse.org/eclipse/downloads/drops/R-3.3.1-200709211145/download.php?dropFile=eclipse-JDT-SDK-3.3.1.zip>
 - Standard Widget Toolkit (<http://www.eclipse.org/swt/>) with modifications
License: Eclipse Public License v. 1.0
<http://www.eclipse.org/legal/epl-v10.html>
Source code availability:
Linux: <http://download.eclipse.org/eclipse/downloads/drops/>

- R-3.2.1-200609210945/download.php?dropFile=swt-3.2.1-gtk-linux-x86.zip
- Windows: <http://download.eclipse.org/eclipse/downloads/drops/R-3.2.1-200609210945/download.php?dropFile=swt-3.2.1-win32-win32-x86.zip>
- The Mozilla Foundation (<http://www.mozilla.org/>).
- Rhino (<http://www.mozilla.org/rhino/>) with modifications
 - License: Mozilla Public License v. 1.1 <http://www.mozilla.org/MPL/MPL-1.1.txt>
 - Source code availability: com/google/gwt/dev/js/rhino/ within gwt-dev.jar
- The OpenQA Project (<http://openqa.org/>)
- Selenium-RC (<http://selenium-rc.openqa.org/>)
- The WebKit Open Source Project (<http://www.webkit.org>)

F.5 GraphicsMagick

This product includes GraphicsMagick software distributed by the GraphicsMagick Group.

The licences which components of this software fall under are as follows.

In November 2002, the GraphicsMagick Group created GraphicsMagick from ImageMagick Studio's ImageMagick and applied this license:

Copyright (C) 2002 GraphicsMagick Group, an organization dedicated to making software imaging solutions freely available.

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files ("GraphicsMagick"), to deal in GraphicsMagick without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of GraphicsMagick, and to permit persons to whom GraphicsMagick is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of GraphicsMagick.

The software is provided "as is", without warranty of any kind, express or implied, including but not limited to the warranties of merchantability, fitness for a particular purpose and noninfringement. In no event shall GraphicsMagick Group be liable for any claim, damages or other liability, whether in an action of contract, tort or otherwise, arising from, out of or in connection with GraphicsMagick or the use or other dealings in GraphicsMagick.

Except as contained in this notice, the name of the GraphicsMagick Group shall not be used in advertising or otherwise to promote the sale, use or other dealings in GraphicsMagick without prior written authorization from the GraphicsMagick Group.

In August 1999, ImageMagick Studio assumed the responsibility for the development of ImageMagick and applied a new license:

Copyright (C) 2002 ImageMagick Studio, a non-profit organization dedicated to making software imaging solutions freely available.

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files ("ImageMagick"), to deal in ImageMagick without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of ImageMagick, and to permit persons to whom the ImageMagick is furnished to do so, subject to the following conditions:

Open Source and other licensed Software

The above copyright notice and this permission notice shall be included in all copies or substantial portions of ImageMagick.

The software is provided "as is", without warranty of any kind, express or implied, including but not limited to the warranties of merchantability, fitness for a particular purpose and noninfringement. In no event shall ImageMagick Studio be liable for any claim, damages or other liability, whether in an action of contract, tort or otherwise, arising from, out of or in connection with ImageMagick or the use or other dealings in ImageMagick.

Except as contained in this notice, the name of the ImageMagick Studio shall not be used in advertising or otherwise to promote the sale, use or other dealings in ImageMagick without prior written authorization from the ImageMagick Studio.

From 1991 to August 1999, ImageMagick was developed and distributed by E. I. du Pont de Nemours and Company:

Copyright 1999 E. I. du Pont de Nemours and Company

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files ("ImageMagick"), to deal in ImageMagick without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of ImageMagick, and to permit persons to whom the ImageMagick is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of ImageMagick.

The software is provided "as is", without warranty of any kind, express or implied, including but not limited to the warranties of merchantability, fitness for a particular purpose and noninfringement. In no event shall E. I. du Pont de Nemours and Company be liable for any claim, damages or other liability, whether in an action of contract, tort or otherwise, arising from, out of or in connection with ImageMagick or the use or other dealings in ImageMagick.

Except as contained in this notice, the name of the E. I. du Pont de Nemours and Company shall not be used in advertising or otherwise to promote the sale, use or other dealings in ImageMagick without prior written authorization from the E. I. du Pont de Nemours and Company.

This copyright is limited to some code (for locating an installed Ghostscript under Windows) in the file magick/nt_base.c which was incorporated from the gsview package:

Copyright (C) 2000-2002, Ghostgum Software Pty Ltd. All rights reserved.

Permission is hereby granted, free of charge, to any person obtaining a copy of this file ("Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of this Software, and to permit persons to whom this file is furnished to do so, subject to the following conditions:

This Software is distributed with NO WARRANTY OF ANY KIND. No author or distributor accepts any responsibility for the consequences of using it, or for whether it serves any particular purpose or works at all, unless he or she says so in writing.

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

The GraphicsMagick Base64Decode() and Base64Encode() functions are based on source code obtained from OpenSSH. This source code is distributed under the following license:

Copyright (c) 2000 Markus Friedl. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

THIS SOFTWARE IS PROVIDED BY THE AUTHOR ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Many of the pattern images in coders/logo.c are derived from XFig, which is distributed under the following license:

FIG : Facility for Interactive Generation of figures

Copyright (c) 1985-1988 by Supoj Sutanthavibul

Parts Copyright (c) 1989-2000 by Brian V. Smith

Parts Copyright (c) 1991 by Paul King

Any party obtaining a copy of these files is granted, free of charge, a full and unrestricted irrevocable, world-wide, paid up, royalty-free, nonexclusive right and license to deal in this software and documentation files (the "Software"), including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons who receive copies from any such party to do so, with the only requirement being that this copyright notice remain intact.

The documentation for the composition operators is copied from the rlecomp manual page, which is authored by Rod Bogart and John W. Peterson. Rlecomp is part of the Utah Raster Toolkit distributed by the University of Michigan and the University of Utah. The copyright for this manual page is as follows:

Copyright (c) 1986, University of Utah

This software is copyrighted as noted below. It may be freely copied, modified, and redistributed, provided that the copyright notice is preserved on all copies.

There is no warranty or other guarantee of fitness for this software, it is provided solely "as is". Bug reports or fixes may be sent to the author, who may or may not act on them as he desires.

You may not include this software in a program or other software product without supplying the source, or without informing the end-user that the source is available for no extra charge.

If you modify this software, you should include a notice giving the name of the person performing the modification, the date of modification, and the reason for such modification.

The source code comprising swab.c is originally derived from libtiff which has the following license:

Copyright (c) 1988-1997 Sam Leffler

Copyright (c) 1991-1997 Silicon Graphics, Inc.

Open Source and other licensed Software

Permission to use, copy, modify, distribute, and sell this software and its documentation for any purpose is hereby granted without fee, provided that (i) the above copyright notices and this permission notice appear in all copies of the software and related documentation, and (ii) the names of Sam Leffler and Silicon Graphics may not be used in any advertising or publicity relating to the software without the specific, prior written permission of Sam Leffler and Silicon Graphics.

THE SOFTWARE IS PROVIDED "AS-IS" AND WITHOUT WARRANTY OF ANY KIND, EXPRESS, IMPLIED OR OTHERWISE, INCLUDING WITHOUT LIMITATION, ANY WARRANTY OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

IN NO EVENT SHALL SAM LEFFLER OR SILICON GRAPHICS BE LIABLE FOR ANY SPECIAL, INCIDENTAL, INDIRECT OR CONSEQUENTIAL DAMAGES OF ANY KIND, OR ANY DAMAGES WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER OR NOT ADVISED OF THE POSSIBILITY OF DAMAGE, AND ON ANY THEORY OF LIABILITY, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

The C++ API known as "Magick++", and which resides in the Magick++ directory, is distributed under the following license:

Copyright 1999 - 2003 Bob Friesenhahn <bfriesen@simple.dallas.tx.us>

Permission is hereby granted, free of charge, to any person obtaining a copy of the source files and associated documentation files ("Magick++"), to deal in Magick++ without restriction, including without limitation of the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of Magick++, and to permit persons to whom the Magick++ is furnished to do so, subject to the following conditions:

This copyright notice shall be included in all copies or substantial portions of Magick++. The copyright to Magick++ is retained by its author and shall not be subsumed or replaced by any other copyright.

The software is provided "as is", without warranty of any kind, express or implied, including but not limited to the warranties of merchantability, fitness for a particular purpose and noninfringement. In no event shall Bob Friesenhahn be liable for any claim, damages or other liability, whether in an action of contract, tort or otherwise, arising from, out of or in connection with Magick++ or the use or other dealings in Magick++.

GraphicsMagick makes use of third-party "delegate" libraries to support certain optional features. These libraries bear their own copyrights and licenses, which may be more or less restrictive than the GraphicsMagick license. For convenience, when GraphicsMagick is bundled with (or compiled with) "delegate" libraries, a copy of the licenses for these libraries is provided in a "licenses" directory.

Copyright (C) 2002 - 2008 GraphicsMagick Group

F.6 iCal4j 1.0 beta3

=====
iCal4j - License
=====

Copyright (c) 2007, Ben Fortuna

All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

- o Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
- o Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
- o Neither the name of Ben Fortuna nor the names of any other contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT OWNER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

F.7 Jain Sip/Sdp implementation by NIST V 1.2

Conditions Of Use

This software was developed by employees of the National Institute of Standards and Technology (NIST), and others.

This software has been contributed to the public domain.

Pursuant to title 15 United States Code Section 105, works of NIST employees are not subject to copyright protection in the United States and are considered to be in the public domain. As a result, a formal license is not needed to use this software.

This software is provided "AS IS." NIST MAKES NO WARRANTY OF ANY KIND, EXPRESS, IMPLIED OR STATUTORY, INCLUDING, WITHOUT LIMITATION, THE IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, NON-INFRINGEMENT AND DATA ACCURACY. NIST does not warrant or make any representations regarding the use of the software or the results thereof, including but not limited to the correctness, accuracy, reliability or usefulness of this software.

F.8 K-XML 2.3

Copyright (c) 2002,2003, Stefan Haustein, Oberhausen, Rhld., Germany

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/

or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

The software is provided "as is", without warranty of any kind, express or implied, including but not limited to the warranties of merchantability, fitness for a particular purpose and noninfringement. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

F.9 libcurl Copyright and Permission Notice

COPYRIGHT AND PERMISSION NOTICE

Copyright (c) 1996 - 2006, Daniel Stenberg, <daniel@haxx.se>.

All rights reserved.

Permission to use, copy, modify, and distribute this software for any purpose with or without fee is hereby granted, provided that the above copyright notice and this permission notice appear in all copies.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OF THIRD PARTY RIGHTS. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

Except as contained in this notice, the name of a copyright holder shall not be used in advertising or otherwise to promote the sale, use or other dealings in this Software without prior written authorization of the copyright holder.

F.10 libTIFF Copyright and Permission Notice

Copyright (c) 1988-1997 Sam Leffler
Copyright (c) 1991-1997 Silicon Graphics, Inc.

Permission to use, copy, modify, distribute, and sell this software and its documentation for any purpose is hereby granted without fee, provided that (i) the above copyright notices and this permission notice appear in all copies of the software and related documentation, and (ii) the names of Sam Leffler and Silicon Graphics may not be used in any advertising or publicity relating to the software without the specific, prior written permission of Sam Leffler and Silicon Graphics.

THE SOFTWARE IS PROVIDED "AS-IS" AND WITHOUT WARRANTY OF ANY KIND, EXPRESS, IMPLIED OR OTHERWISE, INCLUDING WITHOUT LIMITATION, ANY WARRANTY OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

IN NO EVENT SHALL SAM LEFFLER OR SILICON GRAPHICS BE LIABLE FOR ANY SPECIAL, INCIDENTAL, INDIRECT OR CONSEQUENTIAL DAMAGES OF ANY KIND,

OR ANY DAMAGES WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER OR NOT ADVISED OF THE POSSIBILITY OF DAMAGE, AND ON ANY THEORY OF LIABILITY, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

F.11 log4net Notice

```

**
** NOTICE file corresponding to the section 4 (d) of the Apache License,
** Version 2.0, in this case for the Apache log4net distribution.
**
This product includes software developed by
The Apache Software Foundation (http://www.apache.org/)

Please read the LICENSE files present in the root directory of this
distribution.

The names "log4net" and "Apache Software Foundation" must not be used to
endorse or promote products derived from this software without prior
written permission. For written permission, please contact
apache@apache.org.

```

F.12 OpenSSL License

LICENSE ISSUES
=====

The OpenSSL toolkit stays under a dual license, i.e. both the conditions of the OpenSSL License and the original SSLeay license apply to the toolkit. See below for the actual license texts. Actually both licenses are BSD-style Open Source licenses. In case of any license issues related to OpenSSL please contact openssl-core@openssl.org.
OpenSSL License

```

/* =====
 * Copyright (c) 1998-2005 The OpenSSL Project. All rights reserved.
 *
 * Redistribution and use in source and binary forms, with or without
 * modification, are permitted provided that the following conditions
 * are met:
 *
 * 1. Redistributions of source code must retain the above copyright
 *    notice, this list of conditions and the following disclaimer.
 *
 * 2. Redistributions in binary form must reproduce the above copyright
 *    notice, this list of conditions and the following disclaimer in
 *    the documentation and/or other materials provided with the
 *    distribution.
 *
 * 3. All advertising materials mentioning features or use of this
 *    software must display the following acknowledgment:
 *    "This product includes software developed by the OpenSSL Project
 *    for use in the OpenSSL Toolkit. (http://www.openssl.org/)"
 *
 * 4. The names "OpenSSL Toolkit" and "OpenSSL Project" must not be used to

```

Open Source and other licensed Software

```
* endorse or promote products derived from this software without
* prior written permission. For written permission, please contact
* openssl-core@openssl.org.
*
* 5. Products derived from this software may not be called "OpenSSL"
* nor may "OpenSSL" appear in their names without prior written
* permission of the OpenSSL Project.
*
* 6. Redistributions of any form whatsoever must retain the following
* acknowledgment:
* "This product includes software developed by the OpenSSL Project
* for use in the OpenSSL Toolkit (http://www.openssl.org/)"
*
* THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT ``AS IS'' AND ANY
* EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE
* IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR
* PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OpenSSL PROJECT OR
* ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL,
* SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT
* NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES;
* LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION)
* HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT,
* STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE)
* ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED
* OF THE POSSIBILITY OF SUCH DAMAGE.
* =====
*
* This product includes cryptographic software written by Eric Young
* (eay@cryptsoft.com). This product includes software written by Tim
* Hudson (tjh@cryptsoft.com).
*
*/

Original SSLeay License
-----

/* Copyright (C) 1995-1998 Eric Young (eay@cryptsoft.com)
 * All rights reserved.
 *
 * This package is an SSL implementation written
 * by Eric Young (eay@cryptsoft.com).
 * The implementation was written so as to conform with Netscapes SSL.
 *
 * This library is free for commercial and non-commercial use as long as
 * the following conditions are aheared to. The following conditions
 * apply to all code found in this distribution, be it the RC4, RSA,
 * lhash, DES, etc., code; not just the SSL code. The SSL documentation
 * included with this distribution is covered by the same copyright terms
 * except that the holder is Tim Hudson (tjh@cryptsoft.com).
 *
 * Copyright remains Eric Young's, and as such any Copyright notices in
 * the code are not to be removed.
 * If this package is used in a product, Eric Young should be given attribution
 * as the author of the parts of the library used.
 * This can be in the form of a textual message at program startup or
 * in documentation (online or textual) provided with the package.
 *
 * Redistribution and use in source and binary forms, with or without
 * modification, are permitted provided that the following conditions
 * are met:
 * 1. Redistributions of source code must retain the copyright
 * notice, this list of conditions and the following disclaimer.
```

```

* 2. Redistributions in binary form must reproduce the above copyright
*   notice, this list of conditions and the following disclaimer in the
*   documentation and/or other materials provided with the distribution.
* 3. All advertising materials mentioning features or use of this software
*   must display the following acknowledgement:
*   "This product includes cryptographic software written by
*    Eric Young (eay@cryptsoft.com)"
*   The word 'cryptographic' can be left out if the routines from the library
*   being used are not cryptographic related :-).
* 4. If you include any Windows specific code (or a derivative thereof) from
*   the apps directory (application code) you must include an acknowledgement:
*   "This product includes software written by Tim Hudson (tjh@cryptsoft.com)"
*
* THIS SOFTWARE IS PROVIDED BY ERIC YOUNG ``AS IS'' AND
* ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE
* IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE
* ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE
* FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL
* DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS
* OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION)
* HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT
* LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY
* OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF
* SUCH DAMAGE.
*
* The license and distribution terms for any publicly available version or
* derivative of this code cannot be changed. i.e. this code cannot simply be
* copied and put under another distribution license
* [including the GNU Public License.]
*/

```

F.13 PostgreSQL 8.2 & PostgreSQL 8.2 JDBC Drivers

PostgreSQL Database Management System
(formerly known as Postgres, then as Postgres95)

Portions Copyright (c) 1996-2005, The PostgreSQL Global Development Group

Portions Copyright (c) 1994, The Regents of the University of California

Permission to use, copy, modify, and distribute this software and its documentation for any purpose, without fee, and without a written agreement is hereby granted, provided that the above copyright notice and this paragraph and the following two paragraphs appear in all copies.

IN NO EVENT SHALL THE UNIVERSITY OF CALIFORNIA BE LIABLE TO ANY PARTY FOR DIRECT, INDIRECT, SPECIAL, INCIDENTAL, OR CONSEQUENTIAL DAMAGES, INCLUDING LOST PROFITS, ARISING OUT OF THE USE OF THIS SOFTWARE AND ITS DOCUMENTATION, EVEN IF THE UNIVERSITY OF CALIFORNIA HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

THE UNIVERSITY OF CALIFORNIA SPECIFICALLY DISCLAIMS ANY WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE SOFTWARE PROVIDED HEREUNDER IS ON AN "AS IS" BASIS, AND THE UNIVERSITY OF CALIFORNIA HAS NO OBLIGATIONS TO PROVIDE MAINTENANCE, SUPPORT, UPDATES, ENHANCEMENTS, OR MODIFICATIONS.

F.14 SNMP4J 1.7.5

```
=====
== NOTICE file corresponding to the section 4 d of ==
== the Apache License, Version 2.0, ==
== in this case for the SNMP4J distribution. ==
=====
```

This product includes software developed by

SNMP4J.org (<http://www.snmp4j.org/>).

Please read the different LICENSE files present in the root directory of this distribution.

The names "SNMP4J" and "Apache Software Foundation" must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact info@snmp4j.org (SNMP4J) or apache@apache.org.

F.15 Sun XACML implementation 1.2

Copyright 2003 Sun Microsystems, Inc. All Rights Reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistribution of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistribution in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

Neither the name of Sun Microsystems, Inc. or the names of contributors may be used to endorse or promote products derived from this software without specific prior written permission.

This software is provided "AS IS," without a warranty of any kind. ALL EXPRESS OR IMPLIED CONDITIONS, REPRESENTATIONS AND WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT, ARE HEREBY EXCLUDED. SUN MICROSYSTEMS, INC. ("SUN") AND ITS LICENSORS SHALL NOT BE LIABLE FOR ANY DAMAGES SUFFERED BY LICENSEE AS A RESULT OF USING, MODIFYING OR DISTRIBUTING THIS SOFTWARE OR ITS DERIVATIVES. IN NO EVENT WILL SUN OR ITS LICENSORS BE LIABLE FOR ANY LOST REVENUE, PROFIT OR DATA, OR FOR DIRECT, INDIRECT, SPECIAL, CONSEQUENTIAL, INCIDENTAL OR PUNITIVE DAMAGES, HOWEVER CAUSED AND REGARDLESS OF THE THEORY OF LIABILITY, ARISING OUT OF THE USE OF OR INABILITY TO USE THIS SOFTWARE, EVEN IF SUN HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

You acknowledge that this software is not designed or intended for use in the design, construction, operation or maintenance of any nuclear facility.

F.16 Xerces-C

```
=====
== NOTICE file corresponding to section 4(d) of the Apache License, ==
== Version 2.0, in this case for the Apache Xerces distribution.      ==
=====
```

This product includes software developed by
The Apache Software Foundation (<http://www.apache.org/>).

Portions of this software were originally based on the following:
- software copyright (c) 1999, IBM Corporation., <http://www.ibm.com>.

Index

A

- Access protocol layer *see* APL
- Active alert, monitor 178
- Active alerts 193
- Active directory 1130
 - interface (DSI) 1129
- addressing 73
- AdjustIncFaxLevel 1939
- AdjustOutgFaxLevel 1939
- Advanced settings, IP APL
 - Device tab 842
- Advanced settings, ISDN APL
 - Device tab 827
 - Outbound tab 834
 - Resources tab 832
- AllowDotInName 1624
- AllowHypherInName 1624
- Alternative receivers 1577
- AMIS 123
 - configuration 750, 751
- APL
 - overview 66
 - server structure 61
- Application converter 1592, 1648
- ASR server 763
- Attribute mapping 1122
- Attributes (configuration tab)
 - fax G3 710
 - fax G3 polling *see* Fax G3
 - fax G4, *see* fax G3
 - fax-fax converter, *see* Fax G3
 - Hicom MWI, *see* Fax G3
 - MWI message waiting, *see* Fax G3
 - PlayWave, *see* Fax G3
 - SMI, *see* Fax G3
 - voice, *see* Fax G3
- Automatic carbon copies, routing rules, MTA 200
- Automatic cleanup, automatic maintenance, MTA 186
- Automatic fax tone recognition 654
- Automatic maintenance, MTA 185
- Automatic rerouting, routing rules, MTA 201

B

- Batch condition 354
- batch expressions 367
- Batch rule 360
- Bind Address 924

- Bindings
 - V.24 APL 1226
- Broadcast 881
- Buffering when busy 1571

C

- CAD 559
- Call attached data 559
- Call Transfer Settings (tab)
 - voicemail 819
- Call type checker 341, 370
- Callback access
 - PhoneMail 643
 - VMS 682
- CallerGuide
 - announcements 773
 - configuration 767
 - Customer tab 772
 - General tab 767
 - Name Dialing tab 770
 - Options tab 768
 - defining name pronunciation 774
 - excluding users 776
 - installation 764, 765
 - tracking phone numbers 773
- Carbon copy 1577
- CGI script 941
- Change default profile 154
- Changing NCO settings 432
- Cheap tariff 1577
- CITFILE 203, 1044
- CLASS 73
- ComAssistant 961
- ComAssistantSSLMode 961
- Communications 81
- Components
 - installing 78
 - starting 78
 - stopping 79
 - uninstalling 79
- Compression, automatic maintenance, MTA 188
- CON_APL StartDelay 1713
- Conditions
 - NCO 370
- Configuration
 - AMIS 750
 - CTI computer telephony integration 757

- Ergo 617
 - Evo 594
 - Fax G3 polling 715
 - Fax G3 post-dialing 711
 - fax-on-demand 719
 - Hicom MWI 738
 - IP APL 837
 - message waiting indication 739
 - pager 742
 - SIM transport 734
 - SMS 748
 - VMS 678
 - Vogue 760
 - voice 735
 - voicemail networking 750
 - voicemail VMS 678
 - Configuration service 65
 - Configuring a logging monitor 171
 - Configuring Line Monitors 173
 - Connect points 343
 - Conversion 1590
 - Conversion rules 357
 - Copies 1577
 - CorNet IP 568
 - Corporate network 418
 - rules 366, 420
 - Cost-effective transmissions 1577
 - Creating SIP certificate 801
 - Crystal Report XI 1282
 - Crystal Reports XI
 - Example 1288
 - CTI 1047
 - CTI computer telephony integration
 - configuration 757
 - CTI Light 759
 - Customer (configuration tab)
 - fax-on-demand server 727
 - Customer (parameter tab)
 - Ergo configuration 628
 - Evo configuration 612
 - VMS configuration 691
 - Customer Settings (tab)
 - voicemail 823
- D**
- Data protection and data security 59
 - Database
 - address book synchronization 64
 - call charge database 64
 - cTree 64
 - journal database 64
 - kernel component 61
 - user database 64
 - Database fields 1576
 - Databases 1331
 - ADO 1367
 - Basics 1365
 - call charges 1334
 - CodeBase 1366
 - CORREL 1332
 - JobInfo 1341
 - JobRecipient 1341
 - JOURNAL 1335
 - DbTool 1510
 - introduction and function 1510
 - Demilitarized zone (DMZ) 160
 - Department printer settings (PrintAPL) 1211
 - Device
 - general 785
 - Devices (tab)
 - advanced settings, IP APL 842
 - advanced settings, ISDN APL 827
 - Devices, V24APL 1224
 - Direct access
 - PhoneMail 643
 - VMS 682
 - Directory services 1129
 - Distribution lists 881
 - broadcast call 697
 - central distribution list 697
 - private distribution lists 698
 - DMZ (demilitarized zone) 160
 - Document info, PrintAPL 1213
 - Document routing strategy, MTA 200
 - Documents (configuration tab)
 - fax-on-demand server 726
 - DTMF 694
- E**
- EmailForOff365 1765
 - encoding
 - payload 565, 588
 - signaling 565
 - SIP signaling 586
 - Ending telematics APLs 'softly' 877
 - Ergo
 - adjusting the routing rules 637
 - configuration 617
 - language settings 626
 - parameter tab Customer 628
 - parameter tab General 618
 - parameter tab Menu 622
 - parameter tab Options 620
 - parameter tab Prompts 623

- parameter tab Special 625
- parameter tab Test 636
- text-to-speech 598, 620
- Event signaling 1573
- Event viewer 1581
- Evo
 - adjusting the routing rules 616
 - configuration 594
 - installation 595
 - language settings 603
 - parameter tab Customer 612
 - parameter tab General 597
 - parameter tab Menu 599
 - parameter tab Name Dialing 605
 - parameter tab Options 598
 - parameter tab Prompts 600
 - parameter tab Special 602
 - parameter tab Speech Recognition 608
 - parameter tab Test 615
- Export
 - NCO 375
- ExportMrsUsers 1396
- ExportNCOLocation 1401
- Extended message reporter service 61, 64
- Extensions
 - general 785
- Extensions (tab)
 - settings, IP APL 842
 - settings, ISDN APL 824
- External prefix 64

F

- Fax
 - G.711 578
 - T.38 576
- Fax access
 - PhoneMail 643
- Fax conversion, MTA 211
- Fax delivery at favorable tariffs 1577
- Fax forward
 - private parameters 1929
- Fax G3
 - configuration tab Attributes 710
 - configuration tab Fax G3 706
 - configuration tab Formats 709
 - configuration tab General 704
 - configuration tab Identification 705
 - configuration tab Private 708, 718, 749
 - configuration tab Repeat Strategy 707
 - private parameters 1929, 1968
- Fax G3 (configuration tab)
 - fax G3 706

- Fax G3 polling
 - configuration 715
 - configuration tab Attributes *see* Fax G3
 - configuration tab Formats *see* Fax G3
 - configuration tab General *see* Fax G3
 - configuration tab Private *see* Fax G3
 - configuration tab Repeat Strategy *see* Fax G3
- Fax G3 post-dialing
 - configuration 711
- Fax G4
 - configuration tab Attributes *see* Fax G3
 - configuration tab Fax G4 717
 - configuration tab Formats *see* Fax G3
 - configuration tab General *see* Fax G3
 - configuration tab Identification 717
 - configuration tab Repeat Strategy *see* Fax G3
 - private parameters 1929
- Fax G4 (configuration tab)
 - fax G4 717
- Fax tone recognition 654
- Fax-fax converter
 - configuration tab Attributes *see* Fax G3
 - configuration tab Formats *see* Fax G3
 - configuration tab General *see* Fax G3
 - configuration tab Private 730
 - configuration tab Repeat Strategy *see* Fax G3
 - server 729
 - transparent 728
- FaxG3_AltConfigActive 1960
- FaxG3_AltConfigValuesByCaller 1960
- FaxG3_AltConfigValuesByIP 1960
- Fax-on-demand
 - configuration 719
- Fax-on-demand server
 - administration 722
 - configuration tab customer 727
 - configuration tab Documents 726
 - configuration tab General 725
 - configuration tab Supervisor 727
 - direct fax polling (reverse polling) 720
 - storing documents 722
- Fax-over-IP 564, 565, 576, 578
- Fax-over-IP (T.38) 567
- Features
 - D-channel protocols 555
 - Ergo 555
 - PhoneMail 557
 - VMS 556
- FG3PD 711
- File interface
 - file interface APL to host 1425

- General
 - File Interface APL 1421
- File Interface APL (FIAPL) 1421
- FiSym 1435
- Flexrouting 659
- FOD
 - Direct Fax-on-demand by telephone 720
- FoIP (T.38) 567
- Format conversions 1590
- Formats (configuration tab)
 - fax G3 709
 - fax G3 polling *see* Fax G3
 - fax G4, *see* fax G3
 - fax-fax converter, *see* Fax G3
 - Hicom MWI, *see* Fax G3
 - MWI message waiting, *see* Fax G3
 - PlayWave, *see* Fax G3
 - SML, *see* Fax G3
 - voice, *see* Fax G3
- Forward access
 - PhoneMail 643
- G**
 - G.711 565
 - General (configuration tab)
 - MWI message waiting, *see* Fax G3
 - General (configuration tab)
 - fax G3 704
 - fax G3 polling *see* Fax G3
 - fax G4, *see* fax G3
 - fax-fax converter, *see* Fax G3
 - fax-on-demand server 725
 - Hicom MWI, *see* Fax G3
 - PlayWave, *see* Fax G3
 - SML, *see* Fax G3
 - voice, *see* Fax G3
 - General (parameter tab)
 - Ergo configuration 618
 - General (tab)
 - Evo configuration 597
 - Geographic node separation (OpenScape Voice) 1082
 - Global journal, MTA 207
 - Global LDAP settings 1153
 - gnu ghostscript 1590
 - Greeting
 - Company greeting 130
 - Duration of announcement 130
 - Guest access
 - PhoneMail 643
 - VMS 682

H

- H.323 567
 - gatekeeper 567
 - gateway 567
 - Multipoint Control Unit (MCU) 567
 - terminal 567
- Hicom message waiting indication
 - configuration tab Private 740
- Hicom MWI
 - configuration 738
 - configuration tab Attributes *see* Fax G3
 - configuration tab Formats *see* Fax G3
 - configuration tab General *see* Fax G3
 - configuration tab Private 738
- Hicom TCS 1571
- HiPath 4000 1943
- HiPath User Management 1169
- HPM APL 1169

I

- ICI interface 1442
- Identification (configuration tab)
 - fax G3 705
 - fax G4 717
- Identification
 - V24APL 1222
- IMAP4 897
- Import
 - NCO 375
- Infostor 61, 64
- InfoTool 1529
- Installation
 - Evo 595
 - NCO 384
- Interface tools 69
- Internet standard RFC 1823 1129
- IP APL 837
 - configuration 837
 - H.323 564
 - Memory for voice messages 558
 - quality of Service 581
 - structure 564
 - TAPI 564
 - Wave interface 564
- ISDNAPL 804
 - communication Devices 827
 - Memory for voice messages 558
 - protocols 805
 - scripts 806, 839
 - SMS (TAP Protocol) 748

J

Java timezone 92

K

Key management
 MIKEY 585
 PKI 582

L

Language settings

 Ergo 626
 Evo 603
 PhoneMail 664
 VMS 696
 Vogue 762

LDAP

 advantages 1121
 authentication type 1137
 configuration file 1135
 DSI (active directory interface) 1129
 editing attributes 1144
 function 1122
 function model 1127
 general considerations 1121
 information model 1124
 LDAP APL installation 1132
 LDAP APL settings 1134
 monitoring the LDAP APL 1161
 naming model 1125
 querying DS attributes 1137
 RFCs 1163
 Search tab 1138
 security model 1128
 test connection 1137

Lear tool 1617

LicSvcTimeout 1627

Line control 1578

Line monitor, monitor 175

Local database (cache) 151

Localization rules 341

Location

 NCO 340, 350, 783

Location codes 350

Location prefixes 351

Locations (tab)

 settings, IP APL 873
 settings, ISDN APL 831

Log information 64

Logging monitor, configuration 171

Logging monitor, monitor 176

Logging profile 179

Logical lines, MTA 209

M

Main log file, monitor 177

Managing

 user data 1169

Maximum duration of name recording 130

Maximum duration of voice message 130

Maximum number of private distribution lists 131

MaxRetries 269

Media Server

 settings conference portal
 language 1465

Memory for voice messages 558

 IP APL 558

 ISDNAPL 558

Menu (parameter tab)

 Ergo configuration 622

 Evo configuration 599

Message copies 1577

Message transfer agent 61, 63, 185

Message waiting indication
 configuration 739

Messaging Settings (tab)

 voicemail 812, 813, 816, 821

Microsoft Office 1592

MIKEY 585

Modules Window, Monitor 175

Monitor 167

Monitor options, default layout 175

Monitor, active alert 178

Monitor, line monitor 175

Monitor, logging monitor 176

Monitor, main log file 177

Monitor, modules window 175

MSDE

 password 1280

MSP

 user profiles 153

MSP (service provider) 151

MTA 61

 advanced settings

 remote system links 206

 send voice as CIT message 203

 user quotas 205

 automatic maintenance

 active alerts 193

 automatic cleanup 186

 compression 188

 general 185

 jobs 190

 remove database entries and documents 187

 removing documents 188

- watchdog 192
- document routing strategy 200
- global journal 207
- logical lines 209
- message transfer agent 185
- routing rules 200
- routing rules, autom. carbon copies 200
- routing rules, automatic rerouting 201
- text-to-speech 210
- Multimedia internet keying 585
- MWI message waiting
 - configuration tab Attributes *see* Fax G3
 - configuration tab Formats *see* Fax G3
 - configuration tab General *see* Fax G3

N

- Name areas 372
- Name Dialing (parameter tab)
 - Evo configuration 605
- Name locator 61, 65
- NameLoc 61
- NAT (network address translation) 160
- NCO 331, 340
 - batch condition 354
 - batch expressions 367
 - batch rule 360
 - call type checker 341, 370
 - clients 347
 - conditions 353, 370
 - connect points 343, 347
 - conversion rules 357
 - corporate network 418
 - elements 337
 - export 375
 - import 375
 - installation 384
 - localization rules 341
 - location 340, 350, 783
 - location codes 350
 - location prefixes 351
 - name areas 372
 - NCO clients 342
 - NCO configuration 387
 - NCOAdmin 387
 - negating condition 354
 - normalization rules 341
 - normalized phone number format 345
 - number length condition 355
 - number range condition 354
 - phone numbers 350
 - postprocessing rules 357
 - prefixes 350

- preprocessing rules 357
- range lists 376
- reference 435
- regular expression condition 355
- regular expression rule 363
- rules 366, 420
- service-specific NCO clients 342, 347
- set of conditions 356
- set of rules 365
- technological concepts 336
- User-specific NCO clients 343, 348
- variable condition 356
- variables 343, 372

NCO client

- service-specific 342, 347
- user-specific 343, 348

NCO clients 342

- NCO clients and connect points 347

NCO configuration 387

NCO elements 337

NCO location information

- database structure 1403
- database tables 1404
- NCO_LOCATION 1404

NCO variable

- AcceptOldNormNumber 520

- AddExternalPrefix 520

Build-In

- NumberInput 496

- NumberResult 497

Client CTI APL

- AdditionalOutPrefix 499

- AdditionalPrefix 499

- AllowedNumberCharacters 499

- TypeOfNumber 500

- UseTypeInternational 500

Client ISC PhoneMail

- DstPrefix 501

- SrcPrefix 501

Client SAP

- AddressType 502

- LocalizeInternalNumbers 502

client Telematic APLs

- CalledNumberWithTrunkCode 503

- CallingNumberNoExtPrefix 503, 504

- DirectLine 503

- HP8000 504

- SkipCalledNumberDigits 504

- SkipRedirectingDigits 504, 505

- TypeOfNumber 506

- UseTypeInternational 506

client XML APL

- XMLMinInternationalLength 507
- XMLMinNationalLength 507
- XMLUserDialsExternalPrefix 507
- CNConversion 508
- CNDestLocation.CountryCode 513
- CNDestLocation.ExternalPrefix 513
- CNDestLocation.InternationalPrefix 514
- CNDestLocation.Name 514
- CNDestLocation.RangeCode 515
- CNDestLocation.TrunkCode 515
- CNDestPublicID 508
- CNOrgLocation.AreaCode 510, 513
- CNOrgLocation.CountryCode 510
- CNOrgLocation.ExtensionCode 510, 513
- CNOrgLocation.ExternalPrefix 510
- CNOrgLocation.InternationalPrefix 511
- CNOrgLocation.MaxExtensionLength 511, 514
- CNOrgLocation.Name 511
- CNOrgLocation.RangeCode 512
- CNOrgLocation.SubscriberCode 512, 515
- CNOrgLocation.TrunkCode 512
- CNOrgLocationID 509
- CNOrgToDestPrefix 509
- DialAlwaysArea 520
- EnablePostDialing 521
- GUISeparator 521
- GUIUserDialsExtPrefix 521
- location
 - AreaCode 516
 - CountryCode 516
 - ExtensionCode 516
 - ExternalPrefix 516
 - InternationalPrefix 517, 518
 - Location.DialAlwaysArea 517
 - Location.HasRange 517
 - Location.IsCorporateNetworkSite 517
 - Location.MaxExtensionLength 517
 - Location.Name 518
 - Location.PrivateNumbers 518
 - RangeCode 518
 - SubscriberCode 518
 - TrunkCode 519
 - TrunkPrefix 519
- MaxExtensionLength 521
- PurposeOfNumber 522
- TUIUserDialsExtPrefix 523
- UIDialAlwaysArea 523
- NCOAdmin 339, 387
- Negating condition 354
- Network address translation (NAT) 160
- Night tariff 1577
- NL interface 565
- NODE 73
- Node separation (OpenScape Voice) 1082
- Normalization rules 341
- Normalized phone number format 345
- NOT_APL_StartDelay 1794
- Notification 698
- Notification APL 67, 1033
- Novell eDirectory 1131
- nThreads 924
- Number conversion object 331
- number conversion object 331, 340
- Number conversion prepare 432
- Number length condition 355
- Number of failed login attempts 131
- Number range condition 354
- O**
- Octel Migrator Tool 1540
- One number service 1478
- OpenScape voice cluster 590
- OpenScape voice layer 3 cluster 590
- OpenScape-Voice geo-separated 590
- Options (parameter tab)
 - Ergo configuration 620
 - Evo configuration 598
- Outbound (tab)
 - advanced settings, ISDN APL 834
- OutCallHoldAllowed 1910
- P**
- Pager
 - configuration 742
 - pager sets 746
 - script parameters 747
 - wizard 744
- Parameter tab Recording
 - VMS configuration 685
- Password
 - MSDE 1280
- Phone number handling 333
- Phone numbers
 - NCO 350
- PhoneMail
 - callback access 643
 - company-internal messages 674
 - company-specific greetings 664
 - configuration 638
 - default allocation shortcuts 669
 - direct access 643
 - fax access 643
 - forward access 643
 - guest access 643

- guest mailbox 675
 - language settings 664
 - menu adjustment 665
 - MenuConfig.ini 666
 - out-of-office greetings 673
 - repeat strategy user-outcall 669
 - transfer access 643
 - universal access 643
 - user outcall 669
 - with VMS in parallel 638, 678
- PhoneMail and VMS in parallel 699
- PinToProcessor 1713
- PKI 582
- PlayWave
 - configuration tab Attributes *see* Fax G3
 - configuration tab Formats *see* Fax G3
 - configuration tab General *see* Fax G3
 - private parameters 1886
- POP3 897
- Postmaster account 643
- Postprocessing rules 357
- Postscript 1590
- Prefix addressing 324
- Prefixes
 - NCO 350
- Preprocessing rules 357
- PrintAPL
 - document info 1213
 - fax mode, Print APL 1212
 - General (Department Printer Settings) 1211
 - number of copies 1212
 - telex banner 1212
- Private (configuration tab)
 - fax G3 708, 718, 749
 - fax G3 polling *see* Fax G3
 - fax-fax converter 730
 - Hicom MWI 738
 - MWI message waiting 740
- Private parameters
 - Fax forward 1929
 - Fax G3 1929, 1968
 - Fax G4 1929
 - PlayWave 1886
 - SMI 1930
 - SMS 1930
 - voice 1932
- Privilege inheritance 81
- Privileges 118
 - ACD Monitor Privilege 124
 - ACD Supervisor Privilege 124
 - Additional Recording Info privilege 123
 - Advanced USER 125
 - AMIS privilege 123
 - Answering Options Menu privilege 119
 - Automatic Playback Menu privilege 119
 - Call Forwarding Menu privilege 119
 - Cell Phone Number Menu privilege 120
 - Change Language Menu privilege 120
 - Change Password Menu privilege 120
 - Change Referral Extension Menu privilege 121
 - Client Beta-Tester 125
 - Company announcement file enabled 123
 - ConnectToInfoboxOfUser is prompted 122
 - Distribution List Menu privilege 120
 - Document Chain Query 128
 - e-Mail dialog 118
 - e-Mail privilege 123
 - External Archive Query 125
 - FAX G3 Poll privilege 124
 - FAX G3 privilege 124
 - FAX G4 privilege 124
 - Fax Logo- and Coverpage-Editor 125
 - Faxtone Recognition Menu privilege 120
 - File Group Access 123
 - File Owner Access 123
 - Global Alias Editor 127
 - Global Distribution List Editor 126
 - Global Distribution List Send privilege 127
 - Guest Mailbox Privilege 120
 - Help Desk Privilege 126
 - Hide Voice Conference 119
 - Hide Web Conference 119
 - Internal Call privilege 126
 - Internal Fax privilege 119
 - International Call privilege 126
 - International Fax privilege 119
 - Internet Mail privilege 124
 - ISDN Service Remote Access 126
 - Local Call privilege 125
 - Local Fax privilege 119
 - Local File Access 126
 - Login via Phone possible with PIN from all devices 126
 - Long prompts available 123
 - Mailbox Options Menu privilege 120
 - Mailbox Stand-In Menu privilege 120
 - Messagetype Menu privilege 121
 - National Call privilege 126
 - National Fax privilege 119
 - No obligation to change password after first login 122
 - No obligation to record name after first login 122
 - Paging privilege 124
 - Pickup call 125

- Playback Options Menu privilege 121
- Private Query 126
- Prompt Level Menu privilege 121
- Query Result Document View 128
- Receive Broadcast privilege 123
- Receive Dictates privilege 118
- Recording Menu privilege 121
- Restricted ACD Supervisor Privilege 124
- Send Broadcast privilege 123, 124
- Send Dictates privilege 123
- Send enterprise broadcast message privilege 124
- Sequence Menu privilege 121
- Server File Access 127
- Server Query 126
- SERVICE privilege 127
- Set Notifications Menu privilege 121
- Short Message privilege 124
- Short Recording Start Info privilege 123
- Special Delivery Options privilege 127
- SUPERVISOR privilege 82, 127
- Telex dialog 118
- Telex privilege 124
- Tenant Supervisor privilege 128
- Transfer Menu privilege 121
- Trusted Domain privilege 125
- Trusted transfer mode 121
- TTS Capabilities privilege 128
- Use Programmable Short Cuts Menu privilege 122
- USER privilege 128
- View other users remote phone numbers 128
- VMS Administrator privilege 128
- Voice dialog 119
- Voice privilege 124
- Voicemail transcript 128
- VoiceMailSystem is prompted 123
- Volume Menu privilege 122
- Web Assistant 128
- Web Mail Access 128
- Xpressions Folder Menu privilege 122
- Prompts (parameter tab)
 - Ergo configuration 623
 - Evo configuration 600
- Protocol
 - general 782
- Protocols
 - settings, ISDN APL 805
- Protocols (tab)
 - settings, IP APL 838
 - settings, ISDN APL 838
- Protocols of the server 593
- public key infrastructure 582

Q

- QDC 856, 872
- QoS
 - quality of Service 581
- QoS data control 856, 872

R

- Range lists 376
- Recording Settings (tab)
 - voicemail 815
- Redirecting numbers 551
 - cascaded forwarding 552
 - function test 553
 - known problems 554
 - support 553
- Redundant connection to OpenScape Voice with
 - geographic node separation 1082
- Reference
 - NCO 435
- Reg IP SSL_TLSv1_Enable 1944
- Reg Web SSL_TLSv1_1_Enable 1631, 1944, 1987
- Reg Web SSL_TLSv1_Enable 1631, 1987
- Registry key
 - DocumentationMode 1623
- Registry key (ABC APL)
 - Address 1709
 - AdjustedNotAplSettings 1709
 - DisplayNameEmail 1709
 - DisplayNameFax 1709
 - DisplayNameSMS 1709
 - DisplayNameVoice 1709
 - LogicalLineClass 1709
 - LogicalLineNode 1710
 - MinUpdateInterval 1710
 - MrsNodeName 1710
 - Port 1710
- Registry key (Client Logging)
 - LogActive 1558
 - LogFilter 1559
 - LogPath 1559
- Registry key (CMP Usage Tracking)
 - PATHNAME 1706
 - ProductId 1706
- Registry key (Con APL)
 - BindAddress 1711
 - CertificateDirectory 1711
 - Http_Port 1711
 - ListenerTimeout 1711
 - MaxClientsThreads 1711
 - MaxNumDocsRequest 1712
 - MaxServerThreads 1712
 - Verbosity 1712

- VoiceMailsOnly 1712
- Registry key (CSTA APL)
 - BindAddress 1717
 - ComfortTransferApplication 1717
 - DeflectTimeout 1717
 - LogMask 1717
 - ParkingDevice 1718
 - ParkingLoop 1718
 - PortList 1718
 - SendSnapshot 1718
- Registry key (CTI APL)
 - ACL_AccessListCheck 1720
 - ACL_AccessProtoList 1720
 - AllowedNumberChars 1728
 - AssociatedNormPublic 1728
 - AutoLearnerTimeout 1729
 - AutoReconnectAfterConsultation 1729
 - BindAddress 1730
 - BindAddress2 1730
 - BlindConferenceDelayTime 1731
 - CallId 1731
 - CallTransferDelay 1732
 - Capabilities 1732
 - CAPI2032.DLL 1733
 - CAPI_ControllerIndex 1732
 - CAPI_ControllerNr 1732
 - CheckACLAccessForAllLocation 1720
 - CheckComputerNameField 1721
 - CheckMonitorLimit 1721
 - CheckMonitorTimer 1721
 - CheckTimeValue 1733
 - CIT-Beep 1733
 - CIT-Display 1734
 - CIT-LED 1734
 - CIT-RefreshTime 1735
 - CitSF 1735
 - CitSFAddr 1736
 - CstaDll 1736
 - CSTAVersion 1736
 - CtiTeleActive 1736
 - DBFieldForMWI 1737
 - DontLocalize 1737
 - DontLocalizeInternal 1737
 - DontSendDead 1737
 - ExtPrefix 1738
 - FirstLoadDelay 1738
 - FirstPlayMessageDevice 1738
 - GetPhoneFrom 1722
 - GrantsPrivilegeToWatcher 1722
 - HicomAplCompatible 1723
 - HostName 1739
 - HostName2 1739
 - IgnoreCallType 1723
 - IsBChannel 1739
 - LastPlayMessageDevice 1740
 - License 1741
 - LicKey 1741
 - LineSleep 1741
 - LinkMaster 1742
 - LoadBackupDelay 1742
 - LocalLine 1742
 - Login_Delaytime 1743
 - LoginID 1743
 - Logout_Delaytime 1743
 - LogUID_Tree 1723
 - MaxLoadBackup 1744
 - MaxMonitor 1723
 - MaxMonRange 1745
 - ModifyLocation 1724
 - MonDelay 1745
 - MonitorLimit 1745
 - MonitorTimeout 1746
 - MPCallCause 1746
 - MulapPrefix 1747
 - MultiPBXAutoLearnMode 1724
 - MultiPBXAutoLearnModeWithoutLocation 1724
 - MwiRefreshAllLinks 1725
 - NetType 1747
 - NodeNumber 1747
 - NoSpeaker 1747
 - NotSupported_Device 1748
 - Number_of_TAPI-Links 1748
 - NumMaxConnections 1748
 - NumMaxMonitors 1748
 - NumMaxTrans 1749
 - NumMaxXmrLines 1749
 - PabxManufacturer 1749
 - PabxModel 1750
 - Password 1750
 - PbxRelease 1750
 - PhoneNumber 1751
 - PhoneSetStatus 1751
 - PlayMessage_withIndex 1751
 - Port 1751
 - Port2 1751
 - PrivateProfile 1752
 - RepeatPhysMonitor 1752
 - SendDelayTime 1753
 - ServerID 1753
 - StatCtiCall 1725
 - StatCtiEvents 1725
 - StatDevEvents 1725
 - StdTransTimeout 1753
 - Supported_Device 1753

- TransBreak 1726
- TransferringDeviceClearTime 1758
- TransMax 1726
- TRType 1753
- TrunkLineEnd 1754
- TrunkLineStart 1754
- TryOpenUnknownLines 1754
- UniqueCallId 1726
- UseAcidDnis 1754
- UseAcidProxy 1755
- UseACSE 1755
- UseFieldForPhone 1727
- UseOldTSAPIStack 1727
- UsePbxUID 1755
- UseXXX_XXX 1727
- Wait_of_ISDN_Send_receipt 1756
- WatchdogTimeout 1756
- WithCallCenter 1756
- XmrLogMask 1756
- Registry key (DB APL)
 - ADOCCommandTimeOut 1759
 - ADOConnectionTimeOut 1759
 - GarbageConnectionTimeOut 1759
 - MaxConnectionCount 1759
 - MaxThreadPoolCount 1759
 - RDBASyncRequestTimeOut 1759
 - ThreadPoolTimeOut 1760
- Registry key (FI APL)
 - BodyDelay 1761
 - CheckPrivileges 1761
 - EnableIncoming 1762
 - EnableReports 1762
 - HdrInDir 1762
 - HdrOutDir 1762
 - HdrPattern 1762
 - IncFaxFormat 1762
 - IncFileSuffix 1762
 - MaxAddressCount 1761
 - MaxPerPoll 1762
 - PollRate 1762
 - PrivData 1762
 - Protocols 1761
 - RemoveHeader 1762
 - RepFileSuffix 1763
 - ResPath 1761
 - SendFormats 1763
 - TxtInDir 1763
 - TxtOutDir 1763
- Registry key (Global)
 - AccessCode 1652
 - AddMimeExtensions 1635
 - AllowPartialConversion 1635
 - AlwaysDefaultLanguage 1635
 - AreaCode 1652
 - AreaCodeEscape 1652
 - AsrShareGrammars 1624
 - AutodetectPostscript 1635
 - AutoUpdate 1624
 - AutoUpdateNoAdmin 1625
 - AutoUpdateNotification 1625
 - BackupDirectory 1625
 - BinToExt 1636
 - CertificateDirectory 1625
 - CheckForDateConsistencyOnStart 1625
 - CheckTIFF 1636
 - ClusterConfigurationActive 1626
 - ConverterFont 1636
 - Country 1652
 - CountryCode 1652
 - CountryCodeEscape 1653
 - CoverDir 1636
 - DarkeningLevel 1637
 - DateFormat 1653
 - DateFormatLong 1653
 - DcxViewerLowResPatch 1637
 - DDESleep 1637
 - DefaultLanguage 1638
 - DisableGS 1637, 1638
 - EMailFaxWidth 1638
 - ExternalLinePrefix 1653
 - FastAsyncKernelShutdown 1626
 - FaxG3Resolution 1638
 - FaxG4Resolution 1639
 - FaxMonitorLogfile 1639
 - FixTif2Fax 1639
 - FolderDirectory 1626
 - fontHeight 1639
 - fontType 1639
 - fontWeight 1639
 - GhostsriptPath 1640
 - GSPaperSize 1640
 - InfoStorRecordIDs 1626
 - Language 1627
 - LicSvcAddress 1627
 - LocalSystemList 1627
 - LocPrefixExtensions 1654
 - LogoGroup 1640
 - margin_b 1640
 - margin_l 1640
 - margin_r 1641
 - margin_t 1641
 - MaxFirstPagePrintTime 1641
 - MaxPopupDialogs 1642
 - MaxWaitForNTShutdown 1628

- MonitorDirectory 1628
- MSClusterNodes 1628
- NCODirectory 1628
- NetworkAliveCheck 1629
- NetworkTryReconnect 1629
- NoGlobalFaxFormServices 1642
- NonInteractiveServices 1629
- NTShutdownFixActive 1630
- PartialConversionServices 1642
- PcmIsEurope 1642
- PcmIsWave 1643
- PostscriptToBinary 1643
- PreloadedVoices<n> 1643
- PrintTextfileWithProgram 1643
- SapiVoices<n> 1644
- SecurityIdentifier 1630
- ServiceStartDelay 1631
- StartPrintingTimeout 1644
- StatisticsClasses 1632
- System type 1633
- SystemName 1632
- SystemShutDelay 1632
- TiffToExternalConverter 1644
- TiffToExternalExtension 1645
- TimeFormat 1654
- TimeFormatLong 1655
- TransportFormats 1633
- UnnecessaryToPrint 1645
- UseForTextToFaxA4 1645
- UseG4ResolutionForExtension 1646
- UseLHTTS 1646
- UserDirectory 1633
- UseTiffToExternalView 1646
- WaveCodec 1647
- WaveFormat 1647
- WebumKey 1634
- Registry key (HPM APL)
 - AddressUpdated 1766
 - AttributeMapping 1765
 - GivenNameMandatoryBug 1765
 - PropertiesUrl 1765
 - ResourceField 1765
 - TcpIpPort 1765
 - UseHttps 1766
 - UserNotifications 1766
 - ValidateExpr 1766
- Registry key (InfoStor)
 - Administrator 1696
 - CompactDatabases 1694
 - DatabaseDirectory 1695
 - InvalidateKeys 1695
 - JournalLayout 1695
 - MaintenanceDelay 1695
 - MaxLockTime 1695, 1696
 - Postmaster 1696
- Registry key (IP APL)
 - AclAddress (Vfs) 1969
 - AclDelayMessage (Vfs) 1969
 - AclInternLen (Vfs) 1969
 - AclInternMax (Vfs) 1969
 - AclUse (Vfs) 1969
 - AddDialOutLen (Devices) 1947
 - AplIndex (APL) 1940
 - Attributes (Protocols) 1966
 - AttributesAllowed (Protocols) 1966
 - BaudRate (Trunk Groups) 1957
 - Blob (Devices) 1947
 - Blob (Extensions) 1959
 - Blob (Protocols) 1966
 - Blob (Trunk Groups) 1957
 - BoundExtensions (Trunk groups) 1957
 - BoundProtocols (Trunk Groups) 1958
 - BuiltInDtmf (APL) 1940
 - CalledNumberWithTrunkCode (Trunk Groups) 1958
 - CallingNumberNoExternalPrefix (Trunk Groups) 1958
 - CapMask (Protocols) 1966
 - Caps (Devices) 1947
 - Channels (Devices) 1947
 - Checked<n> (APL) 1940
 - CheckMailbox (Protocols) 1966
 - CliMode (APL) 1940
 - ContMsg (Protocols) 1966
 - ConvRecProtocol (APL) 1940
 - Cost (APL) 1941
 - Cost (Trunk Groups) 1958
 - DefaultCli (APL) 1941
 - Description (Devices) 1947
 - Description (Extensions) 1959
 - Description (Protocols) 1966
 - DestNumberPlan (APL) 1941
 - DestNumberType (APL) 1941
 - DisplayColumns (Vfs) 1969
 - DisplayRows (Vfs) 1969
 - DispPerm (Protocols) 1966
 - DlgFlags (APL) 1941
 - DocReps (Protocols) 1966
 - EditPerm (Protocols) 1966
 - EditPermGenerated (Protocols) 1966
 - EnableCDRHeader (APL) 1941
 - EnableRegSz (Extensions) 1959
 - End (Extensions) 1959
 - EndChannel (Trunk Groups) 1958

EndingSilence (APL) 1942
 ErrDetect (Vfs) 1970
 FakeOriginator (APL) 1942
 FaxG3 (Devices) 1947
 FaxG3Chain (Protocols) 1967
 FaxG3_CheckNumberOfPages (FAX) 1961
 FaxG3_CommetrexLogging (FAX) 1961
 FaxG3_CommetrexPath (FAX) 1961
 FaxG3_EchoSuppression (FAX) 1962
 FaxG3_ForceConversion (FAX) 1962
 FaxG3_ICLLLogging (FAX) 1962
 FaxG3_IncEncodingType (FAX) 1963
 FaxG3_IncErrCorrNrData (FAX) 1963
 FaxG3_IncErrCorrNrSigna (FAX) 1963
 FaxG3_IncErrCorrType (FAX) 1963
 FaxG3_OutgErrCorrNrData (FAX) 1963
 Faxg3_OutgErrCorrNrSignal 1963
 FaxG3_OutgErrCorrType (FAX) 1964
 FaxG3_OutgModemType (FAX) 1964
 FaxG3Resend (Protocols) 1967
 Faxg3_RetransmissionActive 1964
 FaxG3_StartTimestamp (FAX) 1965
 FaxG3_T38ParamNegotiation 1965
 Faxg3_TCFOffset 1965
 FaxG3_UsePreferredT38 (FAX) 1965
 FaxG4FaxG3 (Protocols) 1967
 FaxG4T70 (Protocols) 1967
 FaxID (Protocols) 1967
 FaxLicences (APL) 1942
 FaxResources (APL) 1942
 Formats (Protocols) 1967
 FormatsAllowed (Protocols) 1967
 FriendlyName (Protocols) 1967
 Handle (Devices) 1947
 Headline (Protocols) 1967
 IncErrCorrMode (FAX) 1963
 IncKodemType (FAX) 1963
 LineLicences (APL) 1942
 LineResources (APL) 1942
 Lines (Devices) 1947
 Log<n> (Vfs) 1970
 LogName<n> (Vfs) 1970
 MaxAlertTime (APL) 1942
 MaxConnectTime (APL) 1943
 MaxRxSpeed (FAX) 1963
 MaxTxSpeed (FAX) 1963
 MSN (Extensions) 1959
 MultiMaster (Protocols) 1967
 Name (Devices) 1947
 Name (Protocols) 1967
 NumberTypeMode (APL) 1943
 NumChannel (Trunk Groups) 1958
 OAD (Extensions) 1959
 OAD (Trunk Groups) 1958
 OrigNumberPlan (APL) 1943
 OrigNumberType (APL) 1943
 OutErrCorrMode (FAX) 1963
 OutgEncodingType (FAX) 1963
 ParamBlock (Protocols) 1967
 PeakDuration (VFS) 1970
 PeakLevel (VFS) 1970
 PermMask (Trunk Groups) 1958
 PhoneNrSilenceLength (APL) 1943
 PrefixedAni (Devices) 1947
 Prg<n> (Vfs) 1970
 Private (Devices) 1947
 Private (Protocols) 1967
 PrivateMode (Devices) 1956
 PrivateMode (Protocols) 1968
 Protocol (Extensions) 1959
 QueryBilling (APL) 1943
 RoutingAccessLevel (APL) 1943
 ScriptName (Protocols) 1968
 SI (Protocols) 1968
 SilentTime (Vfs) 1970
 SoftFaxFilter (Vfs) 1970
 Start (Extensions) 1959
 StartChannel (Trunk Groups) 1958
 Stat<n> (Vfs) 1970
 State (Devices) 1957
 State (Extensions) 1960
 State (Protocols) 1968
 State (Trunk Groups) 1958
 SupportedDevices (APL) 1944
 TransBreak (APL) 1944
 TransMax (APL) 1944
 Type (Devices) 1957
 Type (Protocols) 1968
 UseCtiMonitorPoint (APL) 1944
 UseOrigFax (protocols) 1968
 UseSpr (Vfs) 1970
 VarDigits (Extensions) 1960
 VoiceLicences (APL) 1945
 VoiceRecFormat (APL) 1945
 VoiceResources (APL) 1946
 WaitForGeb (APL) 1946
 WaitForIsdnMwilnd (APL) 1946
 XmrTopic (Vfs) 1970
 Registry key (ISDN APL)
 AclAddress (Vfs) 1933
 AclDelayMessage (Vfs) 1933
 AclInternLen (Vfs) 1933
 AclInternMax (Vfs) 1934
 AclUse (Vfs) 1934

AddDialOutLen (Devices) 1920
 ALawCoding (APL) 1889
 AlcatelDiscKey (APL) 1889
 AplIndex (APL) 1889
 Attributes (Protocols) 1927
 AttributesAllowed (Protocols) 1927
 BaudRate (Trunk Groups) 1923
 Blob (Devices) 1920
 Blob (Extensions) 1925
 Blob (Protocols) 1927
 Blob (Trunk Groups) 1923
 BoundExtensions (Trunk groups) 1923
 BoundProtocols (Trunk Groups) 1923
 BuildInDtmf (APL) 1890
 CalledNumberWithTrunkCode (Trunk Groups) 1923
 CallingNumberNoExternalPrefix (Trunk Groups) 1924
 CapMask (Protocols) 1927
 Caps (Devices) 1920
 CfExplicit (APL) 1890, 1891
 CfgCompress (APL) 1892
 Channels (Devices) 1920
 Checked<n> (APL) 1892
 CheckEiconStatus (APL) 1892
 CheckMailbox (Protocols) 1927
 CliMode (APL) 1892
 ContMsg (Protocols) 1927
 Cost (APL) 1892
 Cost (Trunk Groups) 1924
 CtiLayerActive (APL) 1893
 CtiSwitchMode (APL) 1893
 CtiSwitchType (APL) 1893
 CtiTimeout (APL) 1893
 DatusLeast (APL) 1894
 DefaultCli (APL) 1894
 Description (Devices) 1920
 Description (Extensions) 1925
 Description (Protocols) 1927
 DestNumberPlan (APL) 1894
 DestNumberType (APL) 1894
 DialInfoTimeout (APL) 1894
 DialMode (APL) 1894
 DialPlan (APL) 1895
 DirectStationSelect (APL) 1895
 DisableEiconLevelDelimiter (APL) 1895
 DisableL1DownOnMonitor (APL) 1895
 DisplayColums (Vfs) 1934
 DisplayRows (Vfs) 1934
 DispPerm (Protocols) 1927
 DiversionCtrlParty (APL) 1896
 DlgFlags (APL) 1896
 DM (APL) 1896, 1941
 DO (APL) 1896
 DocReps (Protocols) 1927
 DT (APL) 1897
 DtmfPeriods (APL) 1897
 ECT (APL) 1897
 EditPerm (Protocols) 1927
 EditPermGenerated (Protocols) 1928
 EnableChangePartnerEvt (APL) 1898
 EnableRegSz (Extensions) 1925
 End (Extensions) 1925
 EndChannel (Trunk Groups) 1924
 EricssonUseCCN (APL) 1898
 ErrDetect (Vfs) 1935
 FakeOriginator (APL) 1899
 FakeOriginatorPrefix (APL) 1899
 FaxCallFwAllowed (APL) 1899
 FaxG3 (Devices) 1920
 FaxG3Chain (Protocols) 1928
 FaxG3CheckStationID (APL) 1900
 FaxG3Resend (Protocols) 1928
 FaxG4FaxG3 (Protocols) 1928
 FaxG4T70 (Protocols) 1928
 FaxID (Protocols) 1928
 FaxLicences (APL) 1901
 FaxResources (APL) 1901
 FilterSMSDialString (APL) 1901
 Formats (Protocols) 1928
 FormatsAllowed (Protocols) 1928
 FriendlyName (Protocols) 1928
 G3ErrorHandle (APL) 1901
 G4ReplyNcpi (APL) 1901
 G4UseIso8208 (APL) 1902
 Handle (Devices) 1920
 Headline (Protocols) 1928
 IgnoreMwiOffResponse 1902
 IgnoreOADType (APL) 1902
 IgnoreUnknownDiscCauses (APL) 1903
 IncReject (APL) 1903
 IntlDialmode (APL) 1903
 LineLicences (APL) 1903
 LineMonitorBytesRefreshSec (APL) 1903
 LineResources (APL) 1904
 Lines (Devices) 1920
 LocalizeNumberForRcc (APL) 1904
 LocPrefixExtensions (APL) 1904
 Log<n> (Vfs) 1935
 LogName<n> (Vfs) 1935
 MaxConnectTime (APL) 1904
 MaxG3Speed (APL) 1905
 MaxLengthForAreaOad (APL) 1905
 MaxRedirLength (APL) 1906

MaxSuppServiceCnt (APL) 1906
 MinLengthForExternalOad (APL) 1906
 MinRedirectedLen (APL) 1907
 MSN (Extensions) 1925
 MultiMaster (Protocols) 1928
 MwiListSize (APL) 1907
 Name (Devices) 1920
 Name (Protocols) 1928
 NoInboundNormalize (APL) 1907
 NormTransAni (APL) 1907
 NotDecrRptCntCodes (APL) 1908
 NotRepeatCodes (APL) 1908
 NumberTypeMode (APL) 1909
 NumChannel (Trunk Groups) 1924
 OAD (Extensions) 1925
 OAD (Trunk Groups) 1924
 OadIndicator (APL) 1909
 OadLicStyle (APL) 1909
 OldCostInfo (APL) 1910
 OldStyleConnInd (APL) 1910
 OrigNumberPlan (APL) 1910
 OrigNumberType (APL) 1910
 ParamBlock (Protocols) 1929
 PeakDuration (VFS) 1936
 PeakLevel (VFS) 1936
 PermMask (Trunk Groups) 1924
 PhoneNrSilenceLength (APL) 1911
 PrefixedAni (Devices) 1920
 Prg<n> (Vfs) 1936
 PrioClass (APL) 1911
 PrioThread (APL) 1912
 Private (Devices) 1920
 Private (Protocols) 1929
 PrivateMode (Devices) 1922
 PrivateMode (Protocols) 1932
 Protocol (Extensions) 1926
 QueryBilling (APL) 1912
 ReportVoiceOKAfterConn (APL) 1912
 Restart (APL) 1912
 Rout1 (APL) 1913
 ScriptName (Protocols) 1932
 ShowSecretNumber (APL) 1913
 SI (Protocols) 1932
 SilentTime (Vfs) 1937
 SimulResDw (APL) 1913
 SkipRedirectingDigits (APL) 1913
 SmiShortHold (APL) 1913
 SmsProviderList (APL) 1914
 SoftFaxFilter (Vfs) 1937
 SSCTAbortable (APL) 1915
 Start (Extensions) 1926
 StartChannel (Trunk Groups) 1924
 Stat<n> (Vfs) 1937
 State (Devices) 1922
 State (Extensions) 1926
 State (Protocols) 1932
 State (Trunk Groups) 1924
 StdCharging (APL) 1915
 SupportedDevices (APL) 1915
 TakeOriginalType (APL) 1915
 TransBreak (APL) 1916
 TransMax (APL) 1916
 Type (Devices) 1922
 Type (Protocols) 1932
 UseCallPartySubAddress (APL) 1916
 UseCapiDII (APL) 1916
 UseCtiMonitorPoint (APL) 1917
 UserUserSupported (APL) 1917
 UseSameCardForEct (APL) 1917
 UseSecondCallingPartyNumber (APL) 1917
 UseSpr (Vfs) 1938
 UseTransferAni (APL) 1918
 VarDigits (Extensions) 1926
 VarDwTimeout (APL) 1918
 VoiceCallFwAllowed (APL) 1918
 VoiceLicences (APL) 1918
 VoiceResources (APL) 1918
 WaitForGeb (APL) 1918
 WaitForIsdnMwilnd (APL) 1919
 XmrTopic (Vfs) 1938
 Registry key (LDAP APL)
 AttributeMap 1768
 BindDomain 1768
 BINDMethod 1768
 BindPassWord 1768
 BindUserName 1768
 CreateDsEntries 1768
 CreateMrsEntries 1769
 DefaultMRSValues 1769
 DeleteDsEntries 1769
 DeleteMrsEntries 1769
 DiscardGarbageBlobs 1767
 DS-Attributes 1769
 DS-AttributesSize 1769
 DS-Type 1770
 Enable 1770
 E-ScriptName 1770
 HostName 1770
 MRS-NonDeleteAtts 1767
 MRS-NonSyncAtts 1767
 Polling interval 1770
 PollSchedule 1770
 PortNumber 1771
 ResPath 1767

- SaveDsUSN 1771
- SaveMrsUpdateId 1771
- SearchFolders 1771
- SearchPageSize 1771
- SearchTimeOut 1771
- UseSSL 1772
- WriteToDs 1772
- WriteToMrs 1772
- Registry key (Lear APL)
 - Block 1773
 - Count 1773
 - Filename 1773
 - Freq 1773
 - originator 1773
 - PMF properties 1773
 - recipient 1773
 - SetPmfProps 1774
 - StatMsgRec 1774
 - StatMsgSend 1774
 - StatRepFail 1774
 - StatRepOk 1774
 - StatRepRec 1774
 - StatRepSend 1774
 - TransBlock 1774
 - TransCmd 1774
 - TransCount 1775
 - TransPeriod 1775
 - TransRec 1775
 - Type 1775
- Registry key (license service)
 - InstalledProduct 1650
 - k1 1650
 - k3 1650
 - SiemensProductId 1650
 - SiemensProductVersion 1650
- Registry key (LPR APL)
 - AplVersion 1777
 - BindAddress 1777
 - MaxPrintChannels 1777
 - MaxQueueSize 1777
 - PrinterType 1777
 - Repeats_1 1778, 1779
 - RepeatTime_1 1778
 - RepeatTime_2 1778, 1779
 - SleepTimeAfterPrint 1777
 - TCP-Log 1778
- Registry key (Mail APL)
 - AllowRecursiveAwake 260, 1781
 - AutoAwake 1781
 - BeginTag 1788
 - CTIJOURNAL 1781
 - CtiJournalAllCalls 1781
 - CtiJrnLoadDelay 1782
 - CtiLogBlackList 1782
 - CtiLogUnknown 1782
 - DatabasePollRate 260, 1782
 - DateFormat 1788
 - DateSeparator 1789
 - DbBackend 1782
 - DefaultAwakeAge 1783
 - DistribDefaultsSets 1783
 - DistribLinePathlist 1783
 - DistribLineProtocols 1784
 - DoAddressBookConsistencyCheck 1784
 - EndTag 1789
 - EnterDeflectCallinCtiJournal 1784
 - Fax 1789
 - FaxStationery 1789
 - FromName 1789
 - FromUid 1789
 - KeepFirstCallee 1785
 - MaxAwake 260, 1785
 - NewCtiJournal 1785
 - PhoneField 1786
 - PreserveDocument 1789
 - PrioHigh 1790
 - PrioKey 1790
 - PrioLow 1790
 - PrioNormal 1790
 - PrioUrgent 1790
 - RefreshCtiMonitor 1786
 - ResetCITonRead 1786
 - SendDate 1790
 - SendTime 1790
 - SepTag 1791
 - SMS 1791
 - Smtip 1791
 - Style 1791
 - Subject 1791
 - SupportEC 1786
 - ToName 1791
 - TumBackend 1787
 - TumQueueSize 1787
 - TumSingleSession 1787
 - TumWorkerThreads 1787
 - UseAlcatelTwinDevice 1787
 - UseRecipientForNdr 1788
 - VanityNumber 1788
- Registry key (MSP)
 - AplBrowseTimeout 1999
 - BindAddress 1999
 - ConfigDLL 1995
 - DefaultProfile 2000
 - Directory 1993

- Enabled 1994
- FileLogging 1995
- HiddenServers 2000
- Inbound 1995
- LogFile 1995
- MinDiskFree 1994, 1996
- Modules 1996
- MspListenPort 1999
- NatClient 1999
- NetwareLoginOnly 1996, 2001
- OdsLogging 1996
- ProductFlavor 1996
- ProfileEditing 1993, 2001
- ServerCache 1998
- SERVICE 1997
- Tunnel 1997
- UseEncryption 1997
- UserNameServer 2000
- UserProfiles 1997, 2001
- VerifyShorthold 2000
- Registry key (MTA)
 - AccountingDatabase 1656
 - AddSendJournalToQuota 1656
 - AutoBiDirectionalLinks 1684
 - AutolearnAllfromProperty 1656
 - AutolearnOIDfromProperty 1657
 - AutolearnSetPreferred 1657
 - Awake 1688
 - AwakeCustomBackup 1688
 - AwakeType 1688
 - BroadcastSlowDown 1657
 - CacheActive 1683
 - Capabilities 1657
 - CarbonCopy 1688
 - CarbonCopyCustomBackup 1688
 - CarbonCopyType 1688
 - CarbonMode 1688
 - CarbonModeBackup 1689
 - CheckCredit 1658
 - CheckQuotas 1658
 - Cipher 1680
 - CitActive 1677
 - CitCacheActive 1677
 - CitCacheActiveForNoCitOff 1677
 - CitCounter 1677
 - CitMessage 1677
 - CitMessageFile 1677
 - CitMessageMode 1678
 - CitUserBasedMessage 1678
 - CitUserIsOriginator 1678
 - ClassMangling 1658
 - CompressionType 1659
 - CSEncryption 1680
 - DataPath 1680
 - DefaultListSet 1675
 - DocumentLifeTimeCompress 1659
 - DocumentLifeTimeDeleted 1659
 - DocumentLifeTimeEmail 1659
 - DocumentLifeTimeInbound 1660
 - DocumentLifeTimeRead 1660
 - DocumentLifeTimeService 1660
 - DocumentLifeTimeUnread 1660
 - DocumentLifeTimeUserdefined 1660
 - DocumentLiveTime 1659
 - EarlyOwnerRecipient 1661
 - EMailSecurityLevel 1684
 - ExportDbFields 1680
 - ExportProtocols 1680
 - File Systems 1661
 - ForceAuthentication 1684
 - ForceLowerAddresses 1661
 - ForceUpperAddresses 1661
 - GlobalLink 1684
 - HeartBeat 1680
 - HeartbeatApls 270, 1662
 - HeartbeatErrFails 271, 1662
 - HeartbeatExtHandler 271, 1662
 - HeartbeatInterval 270, 1662
 - HeartbeatRestartFails 271, 1662
 - HeartbeatWaitTime 270, 1662
 - HeartbeatWarnFails 270, 1662
 - HideCitMessages 1678
 - IgnoreOriginatorInGroup 1663
 - ImportedFields 1685
 - IntRout 1663
 - LineCacheVersion 1683
 - LinkenheilSlowDown 1663
 - LinkList 1685
 - LogicalLines 1683
 - LogReportPeriodicity 1675
 - LowerCaseAddresses 1663
 - MaintenanceActive 1663
 - MaintenanceBackupTemp 1664
 - MaintenanceDontTouch 1664
 - MaintenanceLastStart 1664
 - MaintenanceLastUpdateId 1664
 - MaintenanceMonitorDateTime 1664
 - MaintenanceMonitorYear 1665
 - MaintenanceScript 1665
 - MaxCarbonCopy 1689
 - MaxHopCount 1665
 - MaximumCacheTime 1678
 - MaximumReplicationRecordsPerTransaction 1686
 - MaxLockTime 1665

MaxPreConvRules 1689
 MaxPrivateRules 1665
 MaxReRouteRules 1689
 MaxRouteTargets 1665
 MinimumBusyTime 1666
 MinimumRejectTime 1666
 MinimumRepeatTime 1666
 MinimumTimeBetweenReports 1675
 MonitorDiskUsageAlerts 1666
 MonitorMemoryUsageAlerts 1666
 MultiAddresses 1667
 NoCitOffSignal 1679
 NoNdrOnGlobalList 1667
 NoOwnerOnNOPREFERRED 1667
 NotImportedFields 1686
 OptimizeQueueSize 1667
 OrgAddress 1681
 OtherTimeout 1691
 PredictiveConversion 1689
 PreferredTransactionAddresses 1667
 PrivilegeDnoServices 1668
 Privileges 1690
 Profiles 1681
 ProhibitDoubleHop 1668
 ProxyOpenDelay 1668
 ProxyRetryDelay 1669
 PubKey 1681
 QueueThresh 1669
 RecursiveDistributionLists 1669
 RecursivReRoute 235, 1669
 RemoteLocalServices 1686
 RemoveFromCapaList 1669
 RemovePropertiesOnCarbonCopy 1670
 RemovePropertiesOnResend 1670
 RepeatStandardDeviation 1670
 ReplPollTime 1681
 ReportEncapsulation 1687
 ReportList 1675
 Rerouting 1689, 1690
 ReroutingCustomBackup 1690
 ReRouteLevel 235, 1670
 RouteHeuristic 1670
 RoutingType 1690
 RouteOpt 1670
 RouteStrat 1671
 SmtPMessageSize 1681
 StateTimeout 1671
 SystemStartDelay 1671
 TransactionSlowdown 1671
 UnsecureSMI 1671
 UseOldConnectServerFormat 1682
 UseOriginalDocOnRoute 1671

UserRemovalExtension 1672
 UseTrustedDomains 1687
 VerifyDocumentDeliveryToApl 1672
 VirusCheck 1672
 VirusCheckFileFormats 1672
 WebTimeout 1691
 WriteLoginStat 1673
 Registry key (NOT APL)
 InitialProcMode 1793
 MaxBackendConnections 1793
 MaxScheduleTimeout 1793
 MemoryMapCPURelease 1793
 MinimumJobDistance 1793
 MWIForEmail 1794
 MWIForFax 1794
 MWIForVoice 1794
 MWIStringFormat 1794
 PendingJobQueueSize 1794
 ResetMwi 1794
 SignalAnyChange 1794
 TaRepTimeout 1795
 TextStringFormat 1795
 TransactionRepetitions 1795
 TransactionTimeout 1795
 Verbose 1795
 VoiceProtocols 1795
 WebumActive 1795
 WebumConfidential 1795
 WebumOriginator 1795
 WebumStringFormat 1795
 Registry key (Presence APL)
 CalendarRefreshMinutes 1797
 DefaultPrivileges 1797
 OverwriteDefaultPrivileges 1798
 RtcPassword 1798
 RtcServerName 1798
 RtcSingInName 1798
 RtcSingUserName 1798
 Registry key (Print APL)
 Address 1800, 1801
 BadPrinterCreateDC 1799
 DeviceName 1801
 DocInfoLine1 1800
 DocInfoLine2 1800
 DocInfoLine3 1800
 DocInfoLine4 1800
 DocOverlapFooter 1800
 DocPrintInfo 1800
 EMailAddresses 1799
 FaxPrintMode 1800
 Formats 1800
 IsDefault 1801

- LineName 1801
- NovellNetworkPrinter 1801
- NumberOfCopies 1800
- RetryOnError 1799
- TelexBanner 1801
- UseDefaults 1802
- Registry key (Report APL)
 - Access mode 1803
 - BackupDirectory 1810
 - BackupSettings 1811
 - BIRT_RUNTIME 1805
 - Comment 1821
 - CompressDbSettings 1811
 - ConnectionString 1803
 - Count 1820
 - CR Export Destination 1814
 - CR Export Format 1814
 - CR Export Mode 1814
 - CR Layout 1815
 - CRDOTNET 1803
 - Data Sources 1821
 - DataBaseDirectory 1811
 - DB Data Sources 1815
 - DB Export Destination 1815
 - DB Export Hidden 1815
 - DB Export only 1815
 - DB Time Select Fixed Offset 1816
 - DB Time Select from 1816
 - DB Time Select Mode 1817
 - DB Time Select Range 1817
 - DB Time Select to 1817
 - DbStatDir 1804
 - Description 1817
 - EnableNewStyleDbExport 1810
 - EnableOldStyleDbExport 1810
 - Error Handling 1817
 - Export interval 1806
 - ExportIVRStatistics 1804
 - ExportMrsUsers 1808
 - ExportNCOLocation 1808
 - ID 1818
 - JID 1813
 - Job List 1813
 - Last Result 1818
 - Location 1820
 - Name 1818, 1821
 - Recipients 1818
 - Repeat Custom Days 1818
 - Repeat Custom Hours 1818
 - Repeat Custom Minutes 1819
 - Repeat Mode 1819
 - SlowDownCorrel 1809
 - SlowDownGeb 1809
 - SlowDownJournal 1809
 - Start Now 1819
 - Start Time 1819
 - status 1819
 - Time Selections 1809
 - TimerThreadRunTime 1806
 - TimerThreadSleepTime 1806
 - TriggerThreadSleepTime 1806
 - UpdateDbSettings 1811
 - Use Foreign Exports 1812
 - WatchdogStateSave 1807
- Registry key (services)
 - Access Protocol Layers 1692
 - Kernel 1693
 - MaxRetries 269, 1693
 - Recover-<Computername>-<Service> 269, 1693
 - Recover-<Service> 269, 1693
 - Recover-Kernel 269, 1693
 - WatchdogActive 1693
 - WatchdogRestartSystemDelay 268, 1693
 - WatchdogRetryDelay 268, 1693
- Registry key (SMS IP APL)
 - Adapter 1825
 - Address 1825
 - BindAddress 1825
 - BlackList 1825
 - BulkSenders 1826
 - CaseSensitiveSearch 1826
 - COST 1827
 - DailyLimit 1827
 - DBInField 1827
 - DBOutField 1827
 - DefaultOriginator 1827
 - DefaultRecipient 1827
 - Enabled 1827
 - ForcedIdentification 1827
 - FromAddressNPI 1828
 - FromAddressTON 1828
 - GsmDeviceCheckRate 1828
 - GSMInitString 1828
 - Identity 1828
 - InternalData 1829
 - KeepAliveTimer 1829
 - LimLeft 1829
 - LimRight 1829
 - LogFile 1829
 - LongSmsMode 1829
 - MailNotificationFlags 1829
 - MailReports 1830
 - MapperTable 1830
 - MaxRestartAttempts 1830

- MessageStorage 1830
- MidMapperSize 1830
- NotificationFlags 1830
- PollRate 1830
- PrefetchBuffering 1823
- Protocol 1831
- ReconnectInterval 1831
- RepeatStrategy 1823
- ReportsStorage 1831
- RequestNotifications 1831
- RetryInterval 1831
- SendSubjectOnly 1831
- SendTimeout 1831
- SerBaudRate 1832
- ServerTimeout 1832
- Service Center 1832
- SessionPassword 1832
- SmsCenter 1832
- SmsDigest 1832
- SmsDontDeleteMessages 1832
- SmsLogsRecipient 1832
- SmsOriginatorPropertyName 1824
- SmsPrefix 1832
- SmsSuffix 1832
- SmsValidityTime 1824
- SourceRouting 1833
- System type 1835
- SystemAddressRange 1833
- SystemCharSet 1833
- SystemDestinationNPI 1833
- SystemDestinationTON 1834
- SystemMode 1834
- SystemSourceAddress 1834
- SystemSourceNPI 1834
- SystemSourceTON 1835
- SystemThroughput 1835
- ToAddressNPI 1835
- ToAddressTON 1835
- UseDecimalIdForReports 1836
- WindowSize 1836
- Registry key (SMTP APL)
 - AuthIncoming 1837
 - BindAddress 1837
 - BuildCC 1837
 - DefaultSapUsers 1837
 - DocReps 1837
 - DontRelay 1838
 - HostName 1838
 - Imap4_BindAddress 1838
 - Imap4_Enable 1839
 - Imap4_IgnoreCopy 1839
 - Imap4_JEntriesPerFetch 1839
 - Imap4_MaxLogins 1839
 - Imap4_MaxMailboxes 1839
 - Imap4_maxPerlp 1839
 - Imap4_nThreads 1839
 - Imap4_Outbox 1840
 - Imap4_Port 1840
 - Imap4_PortSSL 1840
 - Imap4_PreLoginTimeout 1840
 - Imap4_Timeout 1840
 - Imap4_Trash 1840
 - LeaveMsgOnServer 1853
 - LogicalLineClass 1841
 - MxCacheMaxAge 1841
 - MxCacheMaxEntries 1841
 - MxCacheNumFailSkip 1842
 - Netmap 1842
 - NoVpimSubject 1842
 - PhoneBookEntry 1853
 - PMI_NoDBLookup 1842
 - PMI_NotifyPostmaster 1842
 - PollEveryNMinutes 1853
 - Pop3_BindAddress 1842
 - Pop3Delete 1843
 - Pop3_Enable 1843
 - Pop3FlgRead 1844
 - Pop3Formats 1844
 - Pop3MaxMsgs 1844
 - Pop3_maxPerlp 1843
 - Pop3MaxSize 1844
 - Pop3NonStdTo 1844
 - Pop3_nThreads 1843
 - Pop3PollType 1845
 - Pop3_Port 1843
 - Pop3_PortSSL 1843
 - Pop3_Timeout 1843
 - RasPassword 1853
 - Receive_AllowRelay 1845
 - Receive_AutoLearn 1845
 - Receive_BindAddress 1845
 - Receive_CheckUserExist 1845
 - ReceivedForDepth 1848
 - Receive_Enable 1846
 - Receive_EnableVRFY 1846
 - Receive_ESMTP_Capabilities 1846
 - Receive_LocalHosts 1846
 - Receive_MaxNotAuthAttempts 1847
 - Receive_maxPerlp 1847
 - Receive_MaxSize 1847
 - Receive_nThreads 1847
 - Receive_Port 1847
 - Receive_Separator 1847
 - Receive_Timeout 1848

- Receive_UseFrom 1848
- ReducedLineName 1848
- RelayAllowedSecs 1849
- RelayHost 1849
- ReportReps 1849
- SAP_Enable 1849
- Send_AuthMethods 1850
- SendFormats 1850
- Send_MaxOut 1850
- Send_Ras 1850
- Send_RequireSSL 1850
- SendTest_Data 1850
- SendTimeout 1851
- SSL_CertificateFile 1851
- SSL_Enable 1851
- SSL_PassPhrase 1851
- SSL_PrivateKeyFile 1851
- SSL_TrustedCaFile 1851
- SSL_VerifyClientCert 1852
- SSL_VerifyServerCert 1852
- TimeSched 1853
- UseBindAddress 1852
- UseReceivedFor 1852
- VPIM_Enable 1852
- WaitDisconnect 1854
- Registry key (TCP/IP APL)
 - BindAddress 1857
 - HighWaterThreshold 1855
 - IoPort 1857
 - LowWaterThreshold 1855
 - Netmap 1855
 - ShortholdTime 1855
 - ShowSubLineInfo 1856
 - SmiQueueSize 1855
 - TunPort 1857
- Registry key (TeleReg)
 - AddDialOutLen (Devices) 1866
 - Attributes (Protocols) 1878
 - AttributesAllowed (Protocols) 1880
 - BaudRate (Trunk Groups) 1870
 - Blob (Devices) 1866
 - Blob (Extensions) 1874
 - Blob (Protocols) 1880
 - Blob (Trunk Groups) 1870
 - BoundProtocols (Trunk Groups) 1870
 - BoundProtocols1 (trunk group) 1871
 - BoundProtocols2 (trunk group) 1871
 - BoundProtocols3 (trunk group) 1871
 - BuiltInDtmf (APL) 1860
 - CapMask (Protocols) 1880
 - Caps (Devices) 1867
 - CfgCompress (APL) 1860
 - Channels (Devices) 1867
 - Checked<n> (APL) 1861
 - CheckMailbox (Protocols) 1881
 - CheckName<n> (APL) 1861
 - CliMode (APL) 1862
 - ContMsg (Protocols) 1881
 - Cost (APL) 1862
 - Cost (Trunk Groups) 1871
 - Description (Devices) 1867
 - Description (Extensions) 1875
 - Description (Protocols) 1881
 - DestNumberPlan (APL) 1862
 - DestNumberType (APL) 1863
 - DispPerm (Protocols) 1881
 - DocReps (Protocols) 1882
 - EditPerm (Protocols) 1882
 - EditPermGenerated (Protocols) 1883
 - EnableRegSz (Extensions) 1874
 - End (Extensions) 1875
 - EndChannel (Trunk Groups) 1871
 - FaxG3 (Devices) 1867
 - FaxG3Chain (Protocols) 1883
 - FaxG3Resend (Protocols) 1883
 - FaxG4FaxG3 (Protocols) 1883
 - FaxG4T70 (Protocols) 1884
 - FaxID (Protocols) 1884
 - FaxLicences (APL) 1863
 - FaxResources (APL) 1863
 - Formats (Protocols) 1884
 - FormatsAllowed (Protocols) 1885
 - FriendlyName (Protocols) 1885
 - Handle (Devices) 1868
 - Headline (Protocols) 1885
 - LineLicences (APL) 1863
 - LineResources (APL) 1864
 - Lines (Devices) 1868
 - MSN (Extensions) 1875
 - MultiMaster (Protocols) 1885
 - Name (Devices) 1868
 - Name (Protocols) 1885
 - NeedConference (Protokolle) 1886
 - NumChannels (Trunk Groups) 1871
 - OAD (Extensions) 1875
 - OAD (Trunk Groups) 1872
 - OrigNumberPlan (APL) 1864
 - OrigtNumberType (APL) 1864
 - ParamBlock (Protocols) 1886
 - PermMask (Trunk Groups) 1872
 - PhonemailUserDependantRouting (APL) 1943
 - PrefixedAni (Devices) 1868
 - Private (Devices) 1868
 - Private (Protocols) 1886

- PrivateMode (Devices) 1869
- PrivateMode (Protocols) 1886
- QueryBilling (APL) 1864
- ScriptName (Protocols) 1886
- SI (Protocols) 1887
- StartChannel (Trunk Groups) 1872
- State (Devices) 1869
- State (Extensions) 1877
- State (Protocols) 1887
- State (Trunk Groups) 1872
- SupportedDevices (APL) 1865
- Type (Protocols) 1888
- UserDependantRouting (APL) 1945
- VarDigits (Extensions) 1877
- VoiceLicences (APL) 1865
- VoiceResources (APL) 1865

Registry key (V.24 APL)

- AreaCodeEscape 1975
- Baudrate 1975
- CanBePolled 1975
- CanVoice 1975
- CIT_Off 1979
- CIT_On 1979
- ContIntFaxStr 1973
- CountryCodeEscape 1975
- DefFaxRecipient 1973
- ExternalLinePrefix 1975
- FaxConnTimeInJrn 1973
- FaxPollFile 1976
- Headline 1973
- InsertMidHI 1973
- InstalledDrivers 1974
- InstalledProtocols 1974
- LineName 1976
- LocPrefixExtensions 1976
- OriginatorID 1974
- PhoneNum 1976
- Protocols 1976
- ShorthandTime 1977
- SMFile 1977
- TouchTone 1977

Registry key (VM2TXT APL)

- carootcert 1981
- clientcert 1981
- libverbosemode 1981
- libverbosemodedir 1981
- maxAudioLength 1981
- maxSimultaneousRequests 1981
- proxyaddress 1981
- proxyport 1982
- recognitiontimeout 1982
- vendoraddress 1982

Registry key (Web APL)

- AuthIncoming 1983
- BindAddress 1983
- CGI_IncludePath 1983
- CGI_Script 1989
- CGI_ScriptParams 1989
- Delay 1991
- DisablePUT 1983
- Enable 1989
- EnglishLanguageForNetAdmin 1983
- HTTP_DefaultHTML 1983
- HTTP_Enable 1984
- HTTP_KeyTimeout 1984
- HTTP_MaxThreads 1984
- HTTP_Port 1984
- HTTP_RootTab 1984
- HTTPS_Port 1984
- HTTP_Timeout 1984
- IgnoreSmtptCheck 1984
- IntervalCheckTimeout 1991
- IntervalGenerateTimeout 1991
- IsDefault 1989
- IsPINResetOld 1985
- LogicalLineClass 1985
- messageChanged_Skip 1991
- phoneCallChanged_Skip 1991
- ProhibitDirectories 1985
- ProtectedDirectories 1986
- RefererCheck 1986
- SSL_CertificateFile 1986
- SSL_DHE_Disable 1986
- SSL_Enable 1987
- SSL_PassPhrase 1987
- SSL_PrivateKeyFile 1987
- SSL_TrustedCaFile 1987
- userChanged_Skip 1992
- UseTiffFormat 1988
- VM_StackSize 1989
- WebAssistVersion 1988
- WebCL_Enable 1988
- WebCL_IncludePath 1988
- WebCL_nThreads 1988
- WebCL_Script 1988
- WebCL_Stacksize 1988
- WebCL_Timeout 1988
- WebCookieKey 1989

Registry key (XMR)

- AutoReportFilter 1697
- DiagAddress 1697
- DiagFilter 1697
- DiagNeName 1697
- DiagNodeId 1697

- DiagPassword 1698
- DiagPath 1698
- DiagPeriod 1698
- DiagUser 1698
- FlushAfterWrite 1698
- LogFileFilter 1698
- LogFilePath 1699
- LogServer 1699
- MaxLines 1699
- ModuleCache 1699
- SnmPMode 1700, 1703
- REG_SMTP_SSL_TLSv1_Enable 1851
- Reg_SMTP_SSL_TLSv1_1_Enable 1851
- Regular expression condition 355
- Regular expression rule 363
- Regular expressions 367
- Remote desktop connection 183
- Remote system link 195, 734
- Remote system links, settings, MTA 206
- Remove database entries/documents, MTA 187
- Remove documents, automatic maintenance, MTA 188
- Repeat Strategy (configuration tab)
 - fax G3 707
 - fax G3 polling *see* Fax G3
 - fax G4, *see* fax G3
 - fax-fax converter, *see* Fax G3
 - SMI, *see* Fax G3
 - voice, *see* Fax G3
- Report APL 1241
 - configuration 1254
 - Provider tab 1256
 - connection to SQL database 1280
- Report Schedule APL 1241
 - configuration 1261
 - export 1265
 - extension 1269
 - layouts 1273
 - parameters 1278
 - recipient 1264
 - reports 1261
 - times 1263
- Reporting
 - activating a layout 1321
 - compressed databases 1366
 - default reports 1343
 - introduction 1246
 - jobs 1251
 - layout files
 - AccessbyHour 1356
 - ADObService_e.rpt 1348
 - ADObUser_e.rpt 1349

- ADODemo.rpt 1345
- ADOFaxReport.rpt 1347
- ADOSTdGeb.rpt/StdGeb.rptdesign 1346
- BillingInformation 1361
- CallActivity 1351
- CallLength 1353
- InvalidAccessAttempts 1364
- Outcalling 1363
- SubscriberAccessActivity 1359
- SubscriberAccessInactivity 1360
- SubscriberMessageActivity 1358
- SubscriberMessageInactivity 1359
- layouts 1251
- MSDE 1242, 1365
- raw data 1379
- report creation 1247, 1279
- resource file 1252
- SQL Server 2005 Express Edition 1242, 1365
- Resources (tab)
 - advanced settings, ISDN APL 832
- RFC 2833 565
- Routing Access Authorization 1943
- Routing rules, MTA 200
- RTP
 - transmitting DTMF/fax tones 579

S

- SAPROUTEAPL 184
- Saving monitor layouts 174
- Secure realtime transport protocol 588
- Secure Socket Layer (SSL) 939
- Send voice as CIT message, MTA 203
- Server
 - starting 75
 - stopping 75
- Server structure 61
- Service control manager 75
- Service provider (MSP) 151, 159
 - configuration 153
- Set of conditions 356
- Set of rules 365
- Settings, IP APL
 - Extensions tab 842
 - Locations tab 873
 - Protocols tab 838
 - Voice mail tab 841
- Settings, ISDN APL
 - Extensions tab 824
 - Locations tab 831
 - Protocols tab 838
 - Voice mail tab 811
- Several IP APLs 565

- Shutdown 75
 - SIP 569
 - MIKEY 585
 - quality of Service 581
 - SIP gateway cluster 591
 - SMI
 - configuration tab Attributes *see* Fax G3
 - configuration tab Formats *see* Fax G3
 - configuration tab General *see* Fax G3
 - configuration tab Repeat Strategy *see* Fax G3
 - private parameters 1930
 - SMI transport
 - configuration 734
 - SMS
 - configuration 748
 - configuration tab General *see* Fax G3
 - configuration tab Repeat Strategy *see* Fax G3
 - Global-Values
 - MaxLicenses 1823
 - private parameters 1930
 - SMTP 897
 - SMTP after POP 913, 1849
 - SMTP APL
 - repeat dialing strategy
 - reports 1849
 - SN network
 - admin. access 301
 - configuration 320
 - configuration management 311, 318
 - location profile 302
 - network profile 310
 - security mechanisms 329
 - SMTP relay host 328
 - structure 299
 - user addressing 324
 - SOAP 1441
 - Software structure 62
 - Special (parameter tab)
 - Ergo configuration 625
 - Evo configuration 602
 - Speech Recognition (ASR) 620
 - Speech Recognition (parameter tab)
 - Evo configuration 608
 - S RTP 565, 588
 - MIKEY 585
 - SSL 586
 - SSL coding 939
 - Standards
 - CTI APL 1115
 - Telematics APLs 878
 - Start mode 75
 - Store & forward interface 151
 - Supervisor (configuration tab)
 - fax-on-demand server 727
 - Surveillance terminal 64
 - System
 - addressing 73
 - administration tools 69
 - architecture 70
 - general considerations 41
 - process structure 71
 - server 73
 - software structure 62
 - structure 61
 - System (parameter tab)
 - VMS configuration 684
 - System networking 299
 - SystemVersionInfo 1555
- ## T
- T.38 564, 565, 576
 - TAPI 566
 - Target network 73
 - TCP/IP ports 284
 - TCS 1571
 - TDD terminal 106
 - Technological concepts
 - NCO 336
 - Telematics APL 525
 - Telematics service
 - configuration example 787
 - general configuration 786
 - Telephone password
 - Minimum number of digits 130
 - Number of warning days before expiry 130
 - Telex banner 1212
 - Test (parameter tab)
 - Ergo configuration 636
 - Evo configuration 615
 - Text-to-speech 598, 620
 - 645, 684, 1590
 - Text-to-speech, MTA 210
 - Tiff2Pdfa 1644
 - Time-triggered fax transmission 1577
 - TLS 565, 586
 - Tone transmission (RFC 2833) 565
 - Transactions interface 152
 - Transfer access
 - PhoneMail 643
 - Transmitting DTMF/fax tones 579
 - Transport layer security 586
 - Truncate 1836
 - Trunk groups
 - general 785

Trusted transfer mode 532

TSL

PKI 582

U

UID, update ID 1153

Universal access

PhoneMail 643

Universal access (VMS) 682

Update ID (UID) 1153

Update sequence number (USN) 1153

User data

adding a field 1575

managing 1169

User database fields

ADDR1 82

ADDR2 82

CIT 82

CITFILE 82

CITY 83

COMPANY 83

CONSRV 83

CONTACT-ID 83

CONUSER 83

COSTINFO 83

COSTINFO# 83

COUNTRY 83

CTIJOURNAL 83

DIVISION 83

E_LOGIN_WEB 83

EXCH 84

FAX-ACT-QUOTA 84

FAXG3 84

FAXG3# 84

FAXG3-HEADLINE 84

FAXG3-ID 85

FAXG4 85

FaxG4# 85

FAXG4-ID 85

FAX-MAX-PAGES 84

FAX-QUOTA 84

FAXROUTPREFIX 85

FAXSTATIONARY 85

GROUP 85

GSM 85

GSM# 86

HPMRES 86

ISDN-CLASS 86

KEYWORD 86

LANGUAGE_ID 86

LMACCOUNT 86

LN 86

MAILBOX 86

MAX_MONITOR 87

MAX_VOICE_MSG 87

NAME 87

NCO_GUI_CONN_PT 87

NCO_GUI_PREFIX 87

NCO_LOCATION 87

NCO_TUI_CONN_PT 87

NCO_TUI_PREFIX 87

NO_REPLICATION 87

OS_SPEECHENABLE 87

PAGER_01 87

PAGER_02 88

PAGER_03 88

PAGER_04 88

PAGERSET_01 88

PAGERSET_02 88

PAGERSET_03 88

PAGERSET_04 88

PASSWORD 88

PHONE 88

PHONE# 88

PIN 88

PMI-HOSTNAME 88

PMI-PASSWORD 89

PMI-SCHEDULE 89

PMI-USERNAME 89

PMROUTPREFIX 89

POP3_Timeout 89

POPFORMATS 89

PREFERRED 89

PRINTER 89

PRIVFAX 89

PRIVFAX# 89

PRIVILEGES 83, 90

PRIVTEL 90

PRIVTEL# 90

QUOTA 90

QUOTAUSED 90

REMARK 90

SAPSMTP 90

SEC_LANGUAGE_ID 90

SMS 90

SMS# 90

SMS-ACT-QUOTA 90

SMS-QUOTA 91

SMTP 91

STAND-IN 91

STATE 91

TCPIP 91

TIMEZONE 91

TZ 92

- USE_LAST_REDIR 92
- USER 92
- VM_ANNOUNCE_01 92
- VM_ANNOUNCE_02 92
- VM_ANNOUNCE_03 92
- VM_ANNOUNCE_04 92
- VM_ANNOUNCE_05 92
- VM_ANNOUNCE_06 92
- VM_ANNOUNCE_07 92
- VM_ANNOUNCE_08 92
- VM_ANNOUNCE_09 93
- VM_AUTH_CODES 93
- VM_DN_00 93
- VM_DN_01 93
- VM_DN_02 93
- VM_DN_03 93
- VM_DN_04 93
- VM_DN_05 93
- VM_DN_06 93
- VM_DN_07 93
- VM_DN_08 93
- VM_DN_09 93
- VM_FAX_EXT 93
- VM_FAX_INT 93
- VM_HI_DSP_NAM 93
- VM_HI_PIN 93
- VM_LAST_LOGIN 93
- VM_LOCK_SET 93
- VM_LOGIN_FAILED 93
- VM_MSG_COUNT 93
- VM_NAME 93
- VM_OUT_ANN_T 94
- VM_PIN_UPDATED 94
- VM_PRINTER 94
- VM_PROTOCOL 94
- VM_TIMEPROFILE 94
- VM_USER_OPTIONS 94
- VOICE 94
- VOICE# 94
- VPIM 94
- WARNING-LEVEL 94
- WEB_STARTPAGE 95
- ZIP 95
- User group 81
- User name 159
 - 131
- User outcall 669, 698, 1045
- User prompts (parameter tab)
 - VMS configuration 687, 689
- User quotas, settings, MTA 205
- USN, update sequence number 1153

V

- V.24 APL
 - bindings 1226
 - devices 1224
 - identification 1222
- Variable condition 356
- Variables
 - NCO 343, 372
- VMS 205
 - company specific greetings 696
 - company-specific greetings 696
 - configuration 678
 - database fields 697
 - distribution lists 697
 - language settings 696
 - notification user outcall 698
 - parameter 692
 - parameter tab Customer 691
 - parameter tab Recording 685
 - parameter tab System 684
 - parameter tab User prompts 687, 689
 - repeat strategy user-outcall 698
 - user outcall 698
- VMS and PhoneMail in parallel 699
- VMS parameters
 - cut end of recording 694
 - default PIN - suppress use 692
 - forward and backward jumps 693
 - impulse length of a signal 694
 - progress indicator during message playback 693
 - pulse length of a pause in speech 694
 - pulse level 694
 - suppress user prompts 693
- VOGUE
 - IVR Application 1409
 - IVR box 1411
 - statistical raw data 1407
- Vogue
 - behavior for offline mode 762
 - configuration 760
 - language settings 762
- Voice
 - configuration 735
 - configuration tab Attributes *see* Fax G3
 - configuration tab Formats *see* Fax G3
 - configuration tab General *see* Fax G3
 - configuration tab Repeat Strategy *see* Fax G3
 - private parameters 1932
- Voice mail (tab)
 - settings, IP APL 841
 - settings, ISDN APL 811

- Voice mail settings
 - Group specific 130
- voice quality 581
- Voicemail
 - Call Transfer Settings tab 819
 - Customer Settings tab 823
 - General Settings tab 812, 813, 816, 821
 - Recording Settings tab 815
- Voicemail networking
 - configuration 750
- Voicemail VMS
 - configuration 678
- VPIM 123, 897

W

- WALLAPL 184
- Watchdog, automatic maintenance, MTA 192
- Web message access 1039, 1042
- Web Server 923
- Web service 1440
- Web service server 1441
- Windows NT
 - resource kit 76
- WSDL 1440

X

- X.500 directory service 1121
- XML APL 1439
 - configuration 1446
 - ICI interface 1442
 - OpenScape connection 1445
 - SAP R/3 Connection 1444
 - SOAP 1441
 - structure 1439
 - web service server 1441
 - XPR interface 1442
- XMRSVC 61
- XPR interface 1442
- XprConfig 1427
- XpressionsFolder 1713

