



A MITEL
PRODUCT
GUIDE

OpenScape Xpressions

Server Installation

Installation Guide

10/2025

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

1 Introduction	15
1.1 Who should read this Manual?	16
1.2 General Notes for this Manual	16
1.2.1 Manual Structure	16
1.3 Required Tools	17
1.3.1 Manuals	17
1.4 Document Conventions	17
1.5 Acronym Directory	18
1.6 Data Protection and Data Security	20
2 Planning the Initial Installation	23
2.1 Checklist for preparing the XPR Server Installation	23
2.1.1 Hardware Environment at Installation Site	23
2.1.2 Checking the System Requirements for the Server PC	24
2.1.3 Checking Windows 64-bit Server Settings	29
2.1.4 Installing .NET Framework on Windows Server 2012 R2 and Windows Server 2016,2019 or 2022	32
2.1.5 Configuring the Firewall for Windows 2008 Server	33
2.1.6 Troubleshooting in Case of a Network Connection Breakdown	33
2.1.7 Language Settings for Non-Unicode Programs	34
2.2 Pre-installation Checklist	35
2.3 Choosing between a Central or Distributed XPR System	35
3 Generating Licenses	37
3.1 Licensing Routine	38
3.2 MAC address	39
3.3 Generating an Advanced Locking ID	39
3.4 Determining the MAC ID of the CLA Computer	40
3.5 Generating a License Key	41
3.5.1 Retrieving a License File	42
3.6 Rehost - shifting available Licenses to a new System	43
3.7 Activating Licenses in the CLA	44
4 XPR System Installation	47
4.1 Installation Basics	48
4.1.1 Text-to-Speech Engine Nuance Vocalizer for Networks 5	50
4.1.2 Installation via Remote Desktop Connection	51
4.1.3 Overview of the Installation Sequence	53
4.2 HiPath License Management (CLM)	55
4.2.1 How the CLM operates	55
4.2.2 Possible Scenarios for the CLM	56
4.2.3 Installing the CLM	57
4.2.4 Installing the CLA	61
4.2.5 Activating a License	65
4.3 Performing the Initial Installation	69
4.3.1 Notes for the Installation	69
4.3.2 Settings and Selection of the Components	70
4.3.3 Installing/Connecting the License Service	71
4.3.3.1 Installing the License Service on the local Computer	72
4.3.4 Specifying the Server Name	76

Contents

4.3.5	Selecting the Server Languages and the Default Language	77
4.3.6	Confirming the Release Notes	79
4.3.7	Selecting System Components	80
4.3.8	Selecting Client Components	81
4.3.9	Selecting External Software	83
4.3.10	Installing the Adobe Reader	85
4.3.11	Installation Type for Automatic Speech Recognition	85
4.3.12	Installing the Dialogic/Eicon Drivers for Communication Hardware	87
4.4	Installation of the Microsoft .NET Framework	89
4.5	Installing the XPR Server and Configuring the Services	90
4.5.1	Selecting Features	91
4.5.2	Summary of the Specifications and Settings	100
4.5.3	Selecting the Folder for the Database and the Document Folder	101
4.5.4	Assigning Service Accounts	102
4.5.5	Selecting the Default Speech-Encoding	103
4.5.6	Configuring the User Authentication	104
4.5.6.1	Login via the Windows User Account	106
4.5.6.2	Login via XPR Account	107
4.5.7	Configuring the XPR Server Components and Services	108
4.5.7.1	Configuring regional Connection Settings	109
4.5.7.2	Additional IP Addresses for the Web Conference Server	113
4.5.7.3	Connection APL	114
4.5.7.4	Installing the Smart Services Delivery Platform (SSDP)	115
4.5.7.5	Setup Wizard for the SMTP APL	121
4.5.7.6	Installing and Configuring the CTI APL	124
4.5.7.7	Setup Wizard for the LDAP APL	125
4.5.7.8	Installing the Exchange 2003 Gateway	125
4.5.7.9	Installing the Exchange 2007 Gateway	126
4.5.7.10	Installing the Lotus Notes Gateway	126
4.5.7.11	Installing the SAP R3 Components	126
4.5.7.12	Installing and Configuring the V.24 APL	126
4.5.8	Installing and Configuring the Web Conference Server	132
4.5.8.1	Installing the Web Conference Server	132
4.5.8.2	Configuring the Web Conference Server	136
4.5.8.3	Configuring several Web Conference Servers	138
4.5.9	Installing and Configuring Voice Conferences	141
4.5.9.1	Installing Voice Conferences	141
4.5.9.2	Configuring Voice Conferences	141
4.5.10	Installing the Java Runtime Environment	142
4.5.11	Creating the SSL Certificate	144
4.5.11.1	Configuring stunnel	145
4.5.12	Installing the Copssh	147
4.5.13	Installing the Language Packets	150
4.5.13.1	Installing Language Packets belatedly	150
4.5.14	Installing Client Applications	151
4.5.15	Installing the Application Builder	153
4.5.16	Installing the Add-On Components	154
4.5.16.1	Adobe Reader	154
4.5.16.2	Installing the HiPath CAP Fault Management	154
4.5.17	Completing the Component Installer	157
4.5.18	Checking Policies and Services	157
4.5.19	Checking Fax G3 Post-Dialing	159

4.5.20	161
4.5.21 Installing the Web Conference Server in a DMZ	162
4.5.22 Voice Conferences with SIP	165
4.6 Modifying, repairing or removing the XPR Installation	166
4.6.1 Running Xpressions Setup with OpenSSL files on Hotfix folder	167
4.6.1.1 Installing the SNMP feature	168
4.6.2 Stopping and starting the XPR Server	169
4.6.3 Modifying an existing Installation	169
4.6.4 Repairing an Installation	172
4.6.5 Removing the XPR System completely	175
5 Installing and Configuring the Driver Software	177
5.1 Installation and Configuration of the Sangoma Diva(R) ISDN Boards	177
5.1.1 Driver Installation under Windows Server 2008 (R2) / Windows 7 Prof.	178
5.2 Configuration of the Sangoma Diva(R) ISDN Boards	182
5.2.1 Configuration of the Sangoma Diva(R) Server BRI Board respectively 4BRI Board	182
5.2.2 Configuration of the Sangoma Diva(R) Server PRI Board	185
5.2.2.1 Restricting the Number of active Channels	188
5.2.3 Configuration of the Sangoma Diva(R) Server PRI Board V3.0 and higher for Voice Conferences	189
6 Setting up a Distributed XPR System	191
6.1 Overview	191
6.1.1 Hardware Requirements	192
6.2 Firewalls between the Computers of a distributed XPR Server	193
6.3 Configure User Account	194
6.3.1 Assign User Account	195
6.4 Local Status Dispatcher Server on Satellite Computers	196
6.5 Installation Routine	197
6.6 Installation Checklist	198
6.7 Installation on the Satellite Computer	200
6.7.1 Installation of a Text-to-Speech System on Satellite Nodes	203
6.7.2 EVO on Satellite Systems	203
6.8 Checking the XPR System	203
A Appendix	205
A.1 Installation under Windows 7 Professional	205
A.1.1 Configuring the Windows 7 Firewall	205
A.2 Using the Report APL with SQL Databases	207
A.2.1 Using Microsoft SQL Server 2012 Express	207
A.2.1.1 Installation	208
A.2.1.2 Configuring the Report APL	210
A.2.2 Using a Microsoft SQL Server	210
A.2.3 Microsoft SQL Server Memory Restriction	212
A.2.4 Switching from CodeBase to Microsoft SQL Server Express or Microsoft SQL Server	213
A.3 XPR in a virtual Environment	214
A.3.1 Distributing CPU Cores in the virtual Host System	217
A.3.1.1 Example of an XPR System in a virtual Environment using VMware	217
A.4 MAPI Fax Printer Driver	221
A.5 Installation and Configuration of the IppAssistant	222
A.5.1 Features	222
A.5.2 Requirements	222
A.5.3 Overview	223
A.5.4 Configuring the IppAssistant Script	224

Contents

A.5.5	Configuring an Extension for PlayWave	225
A.5.6	Manual Entries in the XPR Database	226
A.5.7	Determining the Normalization Prefix	227
B	Notes for Installing the Operating System	229
B.1	General Considerations	229
B.1.1	Preliminary Remark	229
B.1.2	BIOS Settings	229
B.1.3	Preparing the Hardware	230
B.1.3.1	Modem and SMS Transmitter	230
B.1.3.2	Establishing the LAN Connection	230
B.2	Installing Windows 7 Server Professional	230
B.2.1	Starting the Installation	230
B.2.2	Basics	230
B.2.3	Advanced Settings	232
B.3	Installing Windows Server 2008 R2	233
B.3.1	Starting the Installation	233
B.3.2	Basics	234
B.3.3	Advanced Settings	235
B.3.4	Optional Components	236
B.4	Installing Windows 2012/2016/2019/2022 Server	236
B.4.1	Starting the Installation	236
B.4.2	Basics	237
B.4.3	Advanced Settings	237
B.4.4	Optional Components	238
C	Configuring OpenScope Xpressions as Voice-only System	239
C.1	Preface	239
C.1.1	About this Chapter	239
C.1.2	Previous Knowledge	239
C.2	Installation Fundamentals	239
C.2.1	Hardware and Software - Minimum Requirements	239
C.2.2	XPR V7 Line Boards	239
C.2.3	Types of Integration/Protocols Supported	240
C.3	PBX Systems Supported	240
C.3.1	Connection Matrix for PBX Systems	241
C.3.2	Installation Overview	242
C.3.3	Performing the Checklist	243
C.4	BRI/PRI HiPath 4000/CorNet-NQ Installation	244
C.4.1	Pre-installation Checklist	244
C.4.2	Activate the License	245
C.4.3	Install the License Service	246
C.4.4	Server Name, Languages and Release Notes	247
C.4.5	Install the OpenScope Xpressions Software	250
C.4.6	Install the Dialogic DIVA Driver	253
C.4.7	Install the Xpressions Components	259
C.5	BRI/PRI/Eicon HiPath 3000/CorNet-N Installation	279
C.5.1	Pre-installation Checklist	279
C.5.2	Activate the License	280
C.5.3	Install the License Service	281
C.5.4	Server Name, Languages and Release Notes	282
C.5.5	Install the OpenScope Xpressions Software	285
C.5.6	Install the Dialogic DIVA Driver	288

C.5.7 Install the Xpressions Components	294
C.6 Hicom 300H/CorNet-T Installation	314
C.6.1 Pre-installation Checklist	314
C.6.2 Activate the License	315
C.6.3 Install the License Service	316
C.6.4 Server Name, Languages and Release Notes.	317
C.6.5 Install the OpenScape Xpressions Software	320
C.6.6 Install the Dialogic DIVA Driver	323
C.6.7 Install the Xpressions Components	328
C.7 PRI/Eicon Nortel Meridian QSIG Installation	348
C.7.1 Configuring the Nortel Meridian	348
C.7.2 Pre-installation Checklist	348
C.7.3 Activate the License	349
C.7.4 Install the License Service	350
C.7.5 Server Name, Languages and Release Notes.	351
C.7.6 Install the OpenScape Xpressions Software	354
C.7.7 Install the Dialogic DIVA Driver	357
C.7.8 Install the Xpressions Components	362
C.8 System Test and Troubleshooting.	383
C.8.1 Create Test Users	383
C.8.2 Testing the System	384
C.8.3 Troubleshooting Hints	385
C.8.3.1 Start-up Problems.	385
C.8.3.2 Cannot Access Xpressions.	386
C.8.3.3 TUI	386
C.8.3.4 MWI Light Indication	386
D PBX Connection Variants for OpenScape Xpressions	387
D.1 Connecting CorNet-N to Hicom 300/Hicom 300 E/H.	388
D.1.1 Introduction	388
D.1.2 Connecting Hicom 300.	388
D.1.2.1 Hardware/Software Requirements	389
D.1.2.2 OpenScape Xpressions Access Numbers	392
D.1.2.3 General Notes for the Configuration with S ₀ /S ₂ Connection	394
D.1.2.4 Integration Features through the Use of CorNet-N.	395
D.1.2.5 Configuration of the S ₀ /S ₂ Interfaces to OpenScape Xpressions.	395
D.1.2.6 Hicom 300 and Hicom 300-E/H Connection Differences	397
D.1.3 Configuring MWI and Remote Service Access	397
D.1.3.1 Message Waiting Indication	397
D.1.3.2 Remote Service Access	398
D.1.4 Configuring Hicom 300 Users and Services	398
D.1.4.1 General Aspects	398
D.1.4.2 Voice Messaging Aspects.	400
D.1.4.3 Fax Messaging Aspects	401
D.1.4.4 Aspects of e-mail Access via Telephone	406
D.1.5 Settings for special (Fax) Applications.	407
D.1.5.1 Fax-On-Demand Applications.	407
D.1.6 Appendix: Hicom 300 AMO Batch Examples.	407
D.2 Connecting HiPath 3000 (CorNet-N).	413
D.2.1 Introduction	413
D.2.2 Connecting to HiPath 3000	413
D.2.2.1 Hardware/Software Requirements	413

Contents

D.2.2.2	OpenScape Xpressions Access Numbers	413
D.2.2.3	Further Notes	415
D.2.2.4	Integration Features through the Use of CorNet-N	415
D.2.2.5	Configuring S ₀ Interfaces to OpenScape Xpressions	417
D.2.3	Configuring Message Waiting Indication and Remote Service Access	417
D.2.3.1	Message Waiting Indication	417
D.2.3.2	Remote Service Access	417
D.2.4	Configuring Participants	418
D.2.4.1	General Aspects	418
D.2.4.2	Voice Messaging Aspects	418
D.2.4.3	Aspects of e-mail Access via Telephone	418
D.2.5	Settings for special (Fax) Applications	419
D.2.5.1	Fax-On-Demand Applications	419
D.2.6	Examples	419
D.2.6.1	Example Configuration HiPath 3000	419
D.3	Connecting HiPath 3000 (CorNet-IP)	432
D.3.1	Configuration in the Manager E	433
D.3.2	Configuration in the HG1500	441
D.3.3	Configuration in the XPR Server	443
D.4	Connecting HiPath 4000 V6 and OpenScape 4000 V7 / V8	455
D.4.1	CorNet-IP	455
D.4.2	SIP	457
D.4.2.1	Start	465
D.4.2.2	Creating a Feature Profile	467
D.4.2.3	Creating a Subscriber	470
D.4.2.4	Endpoint Configuration	473
D.4.3	Configuration of the HiPath 8000 V3.0 via NMC and SMC	474
D.4.3.1	Configuration of the basic Voice Mail Number	476
D.4.3.2	Forwarding to OpenScape Xpressions for a HiPath 8000 V3.0 Subscriber	477
D.4.4	IP APL Configuration	478
D.4.4.1	Configuring the MWI Protocol	478
D.4.4.2	Activating the SIP Device	479
D.4.4.3	Settings in the Server Location	491
D.4.5	Setting up MWI on Optipoint 410/420/600 SIP Phones	493
D.4.5.1	Defining the Keypad for Voice Mail Messages	493
D.4.5.2	Definition of a Number to be dialed for a Keypad	493
D.4.6	Configuring the Alternate Feature with optiPoint 410/420	494
D.4.7	DTMF Digits on the XPR Server	495
D.4.8	T.38 Calls for HiPath 8000 V3.0	495
D.4.9	Differences between small Enterprise and big Network Solutions	495
D.5	Connecting OpenScape Voice V7 (SIP)	496
D.5.1	Configuring the OpenScape Voice V7	496
D.5.1.1	Requirements	496
D.5.1.2	CMP Login	498
D.5.1.3	Creating an Endpoint Profile	498
D.5.1.4	Creating an Endpoint	498
D.5.1.5	Creating a Destination	499
D.5.1.6	Creating a Prefix Access Code	500
D.5.1.7	Creating a Feature Profile	501
D.6	Connecting OpenScape Voice V8 (SIP)	502
D.7	Connecting OpenScape Voice V9 (SIP)	502
D.8	IPSec Configuration	503

D.8.1	Using IPSec	503
D.8.2	Configuring IPSec for CSTA Connections	504
D.8.2.1	Configuring OpenScape Voice for IPSec-based CSTA Connections	504
D.8.3	Configuring OpenScape Xpressions for IPSec-based CSTA Connections	507
D.9	Connecting an Alcatel OmniPCX Enterprise (OXE) via IP APL	508
D.9.1	Connection Concept	508
D.9.1.1	Alcatel OmniPCX Enterprise Configuration	510
D.9.1.2	IP APL Configuration	510
D.10	Connecting a Mitel 3300 ICP	515
D.10.1	Configuration of the Mitel 3300 ICP PBX	515
D.10.1.1	Configuring virtual Telephones	516
D.10.1.2	Hunt Group Configuration	518
D.10.1.3	Class of Service (COS) Assignment	520
D.10.2	XPR Configuration	524
D.10.2.1	Installation/Configuration of Mitel Tapi Service Provider (TSP) and MiAUDIO Server Edition	524
D.10.2.2	Mitel TSP configuration at a later Time	533
D.10.2.3	Activating Wave Drivers	533
D.10.2.4	Usage of the Mitel TSP with the IPAPL	533
D.10.3	Known Problems	534
D.10.4	MWI	534
D.10.4.1	MWI via IPAPL	534
E	Connecting OpenScape UC Application	535
E.1	Connecting OpenScape-Xpressions via Trusted Transfer Mode	535
E.1.1	Connecting OpenScape-Xpressions with the HiPath 4000 V6	535
E.1.1.1	Trusted Transfer Mode with the HiPath 4000	536
E.1.2	Trusted Transfer Mode Configuration	538
E.1.2.1	Requirements	538
E.1.2.2	Configuring the PhoneMail Script	538
E.1.2.3	Configuring OpenScape Users	543
E.1.2.4	Importing OpenScape Users in XPR	544
Index		547

History of Change

Date	Changes	Reason
03/2012	First draft	
05/2012	IPSec configuration added	
06/2012	Note for SSDP removed	
06/2012	Settings of the NOT APL for a special situation added.	CQ00215350
09/2012	Section 3.3 “Generating an Advanced Locking ID” added	CQ00209313
10/2012	Section A.3.1 “Distributing CPU Cores in the virtual Host System” added	CQ00228272
10/2012	Port 5000 is optional.	CQ00229160
10/2012	Parameter ClientUrlBase added in Section 4.5.8.2 “Configuring the Web Conference Server”	CQ00229348
02/2013	New note: In Microsoft Windows Server 2012, the Loopback Adapter is called <i>Microsoft KM-TEST Loopback Adapter</i> .	CQ00245129
04/2013	New note: A Microsoft hotfix is required with the installation of network drives.	
04/2013	Clarified that connections to HiPath 4000 use the CorNet-IP. Only the connection to the optional conference service occurs via SIP.	CQ00254403
05/2013	More information about the PGROOT password (see step 1 on page 114)	CQ00201017
05/2013	List of supported operating systems updated (see Section 2.1.2, “Checking the System Requirements for the Server PC”, on page 24)	FRN5992, FRN4909
2013-07-19	Section “Connecting HiPath 4000 V6 (CorNet-IP)” removed. Section “Connecting HiPath 4000 V6 R1” renamed to section “Connecting HiPath 4000 V6”.	
2013-07-19	Information added when to use CorNet-IP or SIP for HiPath 4000 (see Section D.4, “Connecting HiPath 4000 V6 and OpenScape 4000 V7 / V8”, on page 455)	
2013-07-19	A HiPath 4000 that has ISDN boards can be upgraded to V6 by adding a DSCXL-V2 board (see Section D.4.1, “CorNet-IP”, on page 455). A HiPath 4000 hardware without any ISDN boards, i.e. a purely server-based solution (VoIP switch), is supported as of HiPath 4000 V6 R0 (see Section D.4.2, “SIP”, on page 457).	
2013-10-04	Section 2.1.2, “Checking the System Requirements for the Server PC”, on page 24 : The support of Windows Server 2008 R2 has been changed to Windows Server 2008 R2 SP1. This applies to Windows clusters as well. Windows Server 2008 R2 SP1 Datacenter Edition is supported. This applies to Windows clusters as well. However, Windows Server 2008 Datacenter Edition is not supported.	
2013-10-04	Voice conferences are not supported anymore for ISDN PBXs with Dialogic/Eicon ISDN boards of the hardware version 3.0 or later (see Section 5.2.3, “Configuration of the Sangoma Diva(R) Server PRI Board V3.0 and higher for Voice Conferences”, on page 189).	
2013-10-04	No CPU core must be permanently assigned to a virtual computer during the migration by means of VMware vMotion (see Section A.3.1, “Distributing CPU Cores in the virtual Host System”, on page 217).	

History of Change

Date	Changes	Reason
2013-10-04	Install .NET Framework 3 on Windows Server 2012 (see Section 2.1.4, "Installing .NET Framework on Windows Server 2012 R2 and Windows Server 2016,2019 or 2022" , on page 32).	
2013-11-05	The name "Unify" has been introduced.	
2013-11-05	The .NET Framework version in Section 2.1.4, "Installing .NET Framework on Windows Server 2012 R2 and Windows Server 2016,2019 or 2022" , on page 32 has been updated.	
2014-01-06	The name "Unify" has been introduced in screenshots.	
2014-02-10	If the HiPath 8000 V3.0 standard certificate signed with the Standard-Root-Certificate-Authority of the HiPath 8000 V3.0 is already integrated in the IP APL, replace this certificate (see step 19 on page 488).	CQ00285679
2014-02-10	Section 6.4, "Local Status Dispatcher Server on Satellite Computers" , on page 196 added	CQ00276143
2014-02-10	R2 of Windows Server 2012 is supported (see Section 2.1.2, "Checking the System Requirements for the Server PC" , on page 24).	
2014-02-10	"Lotus Notes" has been replaced by "IBM Notes" for version 9 and higher.	
2014-02-10	VMware ESXi V5.5 is supported (see Section 2.1.2, "Checking the System Requirements for the Server PC" , on page 24 and Section 4.5.22, "Voice Conferences with SIP" , on page 165).	FRN7740
2014-02-13	The registry on the kernel computer must be changed in Section 6.4, "Local Status Dispatcher Server on Satellite Computers" , on page 196.	CQ00276143
2014-05-02	The <code>ThirdPartyServices</code> registry key may contain <code>pqsql-8.4</code> (see step 20 on page 171).	CQ00289455
2014-05-02	The installation steps for a connection to HiPath 4000 V6 are analog to the installation steps for a connection to OpenScape 4000 V7 (see Section D.4, "Connecting HiPath 4000 V6 and OpenScape 4000 V7 / V8" , on page 455).	
2014-05-02	If you use SIP in the IP APL and for voice conferences, two IP addresses are needed (see Section 4.5.22, "Voice Conferences with SIP" , on page 165).	CQ00295982
2014-05-26	OpenScape Voice V8 is supported (see Section D.6, "Connecting OpenScape Voice V8 (SIP)" , on page 502).	
2014-05-26	Refer to the service documentation <i>OpenScape Xpressions Release Notice</i> for details about the supported operating systems (see Section 2.1.2, "Checking the System Requirements for the Server PC" , on page 24).	
2014-06-16	Table 17 on page 215, "Virtual Machine configuration parameters" , and a hint for additional VMware configuration parameters have been added (see Section A.3, "XPR in a virtual Environment" , on page 214).	CQ00301593
2014-11-03	Refer to the <i>OpenScape Xpressions Release Notice</i> for a list of the supported operating systems and Dialogic/Eicon ISDN boards (see Section 2.1.2, "Checking the System Requirements for the Server PC" , on page 24 and Section 5.1, "Installation and Configuration of the Sangoma Diva(R) ISDN Boards" , on page 177).	
2014-11-03	Introduction of the <code>...\OpenScape\xprlicsvc</code> directory (see step 1 on page 72)	CQ00315239
2015-02-04	ADDED: prerequisites paragraph to Section 4.2.3 "Installing the CLM"	CQ00325503
2015-02-04	ADDED: path to Java Runtime Environment installation file to Section 4.5.10 "Installing the Java Runtime Environment"	CQ00325503
2015-02-05	REMOVED: image from Section 4.3.6 "Confirming the Release Notes"	CQ00325962

Date	Changes	Reason
2015-02-18	REMOVED Sections: D.4 Connecting HiPath 4000 V3.0 (CorNet-NQ) D.5 Connecting HiPath 4000 V3.0 (CorNet-IP) D.6 Connecting HiPath 4000 V4.0 (CorNet-IP) D.7 Connecting HiPath 4000 V5.0 (CorNet-IP) D.10 Connecting OpenScape Voice V3.1 (SIP)	CQ00326156 CQ00325964
2015-02-18	UPDATED: Section D.5 “Connecting OpenScape Voice V7 (SIP)” and Section D.6 “Connecting OpenScape Voice V8 (SIP)”	CQ00325964
2015-02-20	Removed paragraph on MTLS from Section D.5.1 “Configuring the OpenScape Voice V7” and on URI from Section D.5.1.6 “Creating a Prefix Access Code”	CQ00325964
2015-03-27	UPDATED: The “Prerequisites” paragraph in Section 4.2.3 “Installing the CLM” , and the “Note” in Section 4.5.10 “Installing the Java Runtime Environment”	CQ00327692
2015-09-10	ADDED: “Note Remote System Link is not compatible with [Crypt_Sec], it is designed to only work with [KRYPT].” To Section 4.1 “Installation Basics” , Section 4.3.4 “Specifying the Server Name” , Section 4.5.7.12 “Installing and Configuring the V.24 APL” , Section C.4.4 “Server Name, Languages and Release Notes” , Section C.5.4 “Server Name, Languages and Release Notes” , Section C.6.4 “Server Name, Languages and Release Notes” , Section C.7.5 “Server Name, Languages and Release Notes” ,	CQ00333644
2016-01-13	Removed: “If the HiPath 8000 V3.0 standard certificate signed with the Standard-Root-Certificate-Authority of the HiPath 8000 V3.0 is already integrated in the IP APL, remove this certificate. Create a new client client certificate and configure the described settings.” from Section D.5.4 IP APL Configuration Step 19 .	UCBE-4195
2016-07-13	Updated chapter 4.5.8.1 Installing the Web Conference Server and 4.5.21 Installing the Web Conference Server in a DMZ	UCBE-5284
2016-08-18	Replaced Windows Server 2003 with Windows Server 2008 throughout the document. Added chapter B 5 Installing Windows 2012 Server.	UCBE-7282
2017-03-28	Updated Section 2.1.2 Checking the System Requirements for the Server PC	UCBE-10723
2017-03-29	Updated Section D PBX Connection Variants for OpenScape Xpressions remove OpenScape Voice V3, V5 and V6 and add V9	review
2017-10-24	Remove Windows XP references	review
2018-05-18	Updated - Section 2.1.2 Checking the System Requirements for the Server PC - Section 2.1.3 Checking Windows 2008 64-bit Server Settings - Section 2.1.4 Installing .NET Framework on Windows Server - Section 2.1.6 Troubleshooting in Case of a Network Connection Breakdown - Appendix A.3 XPR in a virtual Environment with VMware - Appendix B.4.1 Starting the Installation - Appendix B.4.2 Basics - Appendix B.4.4 Optional Components	UCBE-15941
2018-05-24	Updated rename Section 2.1.3 Checking Windows 2008 64-bit Server Settings to 2.1.3 Checking Windows 64-bit Server Settings update Section 2.1.4 Installing .NET Framework on Windows Server	UCBE-15941 (reopened)
2018-09-17	Updated: Section 4.5.11.1 Configuring stunnel	UCBE-17176
2019-03-12	Added: 4.6.1 Running Xpressions Setup with OpenSSL files on Hotfix folder 4.6.1.1 Installing the SNMP feature	UCBE-18989

History of Change

Date	Changes	Reason
2019-04-07	Updated: 5. Installing and Configuring the Driver Software	UCBE-19214
2019-04-15	Updated” A.2 Using the Report APL with SQL Databases Added: A.2.3 Microsoft SQL Server Memory Restriction	UCBE-19467
2020-04-07	Updated: A.3 XPR in a virtual Environment with VMware	UCBE-23045
2025-03-10	Updated: A.3 XPR in a virtual Environment A.3.1 Distributing CPU Cores in the virtual Host System A.3.1.1 Example of an XPR System in a virtual Environment using VMware 3.1 Licensing Routine Removed the following sections: 4.5.20 Downloading the Web Conference Client 4.5.21 Installing the Web Conference Server in a DMZ Installing the web conference server Configuration in the XPR	DOCLOC-9345
2025-03-10	Updated: 2.1.2 Checking the System Requirements for the Server PC 2.1.3 Checking Windows 64-bit Server Settings 2.1.4 Installing .NET Framework on Windows Server 2012 R2, Windows Server 2016, 2019, 2022 or 2025 2.1.6 Troubleshooting in Case of a Network Connection Breakdown A.3 XPR in a virtual Environment B.4 Installing Windows 2012/2016/2019/2022/2025 Server B.4.2 Basics B.4.4 Optional Components	UCBE-38540

1 Introduction

The OpenScape Xpressions system (XPR) is a powerful Unified Communications system for improving internal and external corporate communication. OpenScape Xpressions bundles messages from a wide variety of sources via a uniform user interface and supports the user in exchanging voice, fax, and e-mail messages every day. In this way, the user can attend to calls, fax documents, e-mails, voice mails, and SMS messages via a standard interface and administer them in user-specific mailbox.

This mailbox can be accessed flexibly via telephone or PC. A user can thus check his XPR mailbox in the office, from home (e.g. as a tele worker), or when on the move (on business trips, customer visits, etc.).

People who mainly use a mobile phone can use the Short Message Service (SMS) to be informed when they have new messages, to send SMS messages to a mobile phone, to divert their mobile phone to OpenScape Xpressions and to access all voice, fax and e-mail messages.

Messages in the XPR system are accessed from PCs via IMAP4 clients, or else via the MS Exchange 200x, IBM/Lotus Notes or SAP/R3 e-mail systems available at the customer facility.

The XPR system combines the following services on one Windows server platform to one Unified Communications system.

- Voicemail
- Fax
- E-mail
- SMS
- CTI
- Voice conferences
- Web conferences
- Presence
- Chat

Information about the supported Windows server platforms can be found in the XPR Release Notes.

Thanks to its modular, scalable client/server architecture, this solution can be ideally configured to meet users' individual communication needs. Open standards, integration in existing data processing and telecommunications environments, universal access to messages via PC and telephone, secure access via ISDN and/or VoIP, LAN, and Intranet/Internet, and the available conversion options guarantee protection of your investment in the future.

Introduction

Who should read this Manual?

Services, user packages, data processing integration as well as software-only solutions or certified all-in systems can be implemented when required, thus creating a tailored solution for every requirement from the small entry-level variant right up to networked communication solutions.

NOTE: For information on client installations, please refer to the *OpenScape Xpressions Client Installations* manual.

1.1 Who should read this Manual?

This manual is intended for system administrators in charge of installing and configuring the XPR system. In order to understand the described functions and processes, the reader must have specialized knowledge in the following areas:

- Administration and configuration of the supported operating systems
- Network technology
- Installation and configuration of the XPR system. This knowledge can be obtained by participating in a Unify GmbH & Co. KG seminar.
- Configuration of the PBX used in connection with the XPR system.

1.2 General Notes for this Manual

1.2.1 Manual Structure

The manual is divided into the following topics:

- Introductory chapter with general notes on the product and on how to use the manual (current chapter).
- Information on setup preparation (starting from [Chapter 2](#))
- Installation of the XPR system (starting from [Chapter 4](#))
- Installation and configuration of the hardware drivers (starting from [Chapter 5](#))
- Installation of a distributed XPR system (starting from [Chapter 6](#))
- Information on how to create license keys (starting from [Chapter 3](#))
- Information on installation and configuration of optional XPR components (in [Appendix A](#))

- Information on the installation of the supported Windows operating systems (in [Appendix B](#))
- Installation of a voice-only XPR system (in [Appendix C](#))

1.3 Required Tools

1.3.1 Manuals

During the XPR installation and configuration the following Cycos manuals in electronic or printed format will be referred to:

- OpenScape XpressionsServer Installation (this manual)
- OpenScape XpressionsServer Administration
- OpenScape XpressionsCommunications
- OpenScape XpressionsWeb Assistant

1.4 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. 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: Signals information of high priority. 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**.

1.5 Acronym Directory

The following table lists in alphabetic sequence the most important acronyms used.

Acronyms	Description
APL	A ccess P rotocol L ayer
ASR	A utomatic S peech R ecognition
BRI	B asic R ate I nterface
CLA	C ustomer L icense A gent
CLC	C ustomer L icense C lient
CLM	C ustomer L icense M anagement
CLS	C entral L icense S erver
CRM	Customer Relationship Management
CSTA	Computer Supported Telecommunication Applications
CTI	Computer Telephony Integration
CMP	Common Management Platform
DTMF	Dual Tone Multi Frequency
ERP	Enterprise Resource Planning
GUI	G raphical U ser I nterface
HKLM	H KEY_ L OCAL_ M ACHINE
HTTP	H ypertext T ransfer P rotocol
IDE	I ntegrated D evice E lectronics
IMAP4	Internet Message Access Protocol
IP	I nternet P rotocol
IVR	I nteractive V oice R esponse
LDAP	Lightweight Directory Access Protocol
MWI	M essage W aiting I ndicator
POP3	Post Office Protocol
PRI	P rimary R ate I nterface
RPC	Remote Procedure Call
SCSI	S mall C omputer S ystem I nterface
SMS	S hort M essage S ervice
SMTP	S imple M ail T ransfer P rotocol
SOAP	S imple O bject A ccess P rotocol
SSDP	Smart Services Delivery Platform
TAPI	Telephony Application Programming Interfaces
TCP	T ransmission C ontrol P rotocol
TSP	Tapi Service Provider

Acronyms	Description
TTS	T ext T o S peech
UCC	Unified Communications and Collaboration
UM	U nified M essaging
VM	Virtual Machine
VMS	Voice Mail Server
VPIM	Voice Profile for Internet Mail
XML	E xtended M arkup L anguage
XPR	OpenScape Xpressions

1.6 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.

NOTE: 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 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 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 storage media, such as backup diskettes or log printouts. This applies to service calls as well as to storage and transport.
- Ensure that storage media which are no longer required are completely destroyed. Ensure that no sensitive documents are left unprotected.

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

Introduction

Data Protection and Data Security

2 Planning the Initial Installation

2.1 Checklist for preparing the XPR Server Installation

Step
1. Section 2.1.1, “Hardware Environment at Installation Site”, on page 23
2. Section 2.1.2, “Checking the System Requirements for the Server PC”, on page 24
3. Section 2.1.3, “Checking Windows 64-bit Server Settings”, on page 29
4. Section 2.2, “Pre-installation Checklist”, on page 35
5. Section 2.3, “Choosing between a Central or Distributed XPR System”, on page 35

2.1.1 Hardware Environment at Installation Site

IMPORTANT: The hardware used must have been tested and released by the producer of the operating system. For information about tested and released hardware, please refer to the following address:

<http://www.windowsservercatalog.com/default.aspx>

Before the actual startup begins, make sure that the required hardware environment is available on site. These are:

- Three main connections 220V (U.S.: 110 V), one for each PC and monitor, one in reserve e.g. for a protocol tester
- Wired LAN sockets and LAN wires
- In case of an ISDN connection: Wired S_0 -/ S_{2M} sockets with RJ45 jacks for the tie line

We recommend to check the S_0 -/ S_{2M} sockets with an appropriate protocol tester to prevent false wiring.

You find details on commissioning and assembling the communication system in the appropriate service manual.

2.1.2 Checking the System Requirements for the Server PC

The XPR system supports a wide range of different interface modules. The modules referred to in the following configurations are thus only intended as examples, in particular with regard to the slots required.

PC hardware/software (new installations)

For the XPR system the operating systems Windows Server 2008 R2 and Windows Server 2012 R2, Windows Server 2016, Windows Server 2019, Windows Server 2022 and Windows Server 2025 are recommended for new installations. The hardware used must have been tested and released by the producer of the operating system. Please also read the note in [Section 2.1.1, “Hardware Environment at Installation Site”, on page 23](#) on this.

The following minimum requirements should be met:

- **Processor**

- At least Intel Pentium 4 (or compatible) (Xeon processor or dual core system), at least 2 GHz
- Using T.38 Fax on more than two parallel lines requires a server with at least 2 GHz, at least 2 GB RAM and at least one dual core system
- For conference usage one additional core per 50 voice channels
- Using OpenScape Web Client requires a powerful processor depending on the number of users and sessions. The performance requirements per OpenScape Web Client user is approximately twice as high as for an optiClient 130 user.

- **Working memory**

- 2 GB (recommendation: 4 GB)
- in case of TTS usage
 - additional 100 MB per installed TTS voice of Nuance Vocalizer for Network 5 and
 - additional 2 MB per channelat least, however, 1 GB in addition
- in case of ASR usage 512 MB in addition
- in case of conference usage 2 GB in addition
- in case of OpenScape Web Client usage at least 1 GB in addition

- **Hard disks**

2 hard disks with at least 100 GB (IDE or SCSI) each.

- Be sure that the partition on which the XPR server software is installed has a minimum size of 10 GB. The target path must not contain any blanks (e. g. c:\SemensOs Xpressions\xpr)!
- **Second hard disk for data backup recommended**
- **USB slot** for installing the XPR from USB
- **LAN**

Ethernet 100 Base T or Gigabit

- The network board must be connected with the LAN to ensure trouble-free XPR server booting.
- The network board settings must correspond to those of the router/HUB.
- For physical machines a MS Loopback Adapter must be installed (cf. [Section 2.1.3, "Checking Windows 64-bit Server Settings", on page 29](#), point [Installing the Microsoft Loopback Adapter](#)).

IMPORTANT: The Loopback Adapter must not be installed on Virtual Machines (VM).

NOTE: In Microsoft Windows Server 2012 R2, Windows Server 2016, Windows Server 2019, Windows Server 2022 and Windows Server 2025, the Loopback Adapter is called *Microsoft KM-TEST Loopback Adapter*.

- If the web conference server is installed on the computer that also hosts the XPR server, the following requirements must have been complied with:
 - The computer must have two IP addresses or two DNS host entries that point to the same IP address.
 - Port 80 (TCP) and port 5000 (TCP) must be accessible.

IMPORTANT: Protocol IPv6 must be disabled.

IMPORTANT: When replacing the network board or modifying the configuration (hardware), the MAC-ID used must be checked as it may have changed and a new license file may have to be created. In this case, the old MAC ID is disabled and no further license files may be generated for this MAC ID. Likewise, the licenses for this MAC-ID can no longer be extended.

Planning the Initial Installation

Checklist for preparing the XPR Server Installation

- **Slots**

When using ISDN boards, PCI respectively PCIe slots are required depending on the boards to be deployed.

- **Operating systems**

Refer to the service documentation *OpenScape Xpressions Release Notice* for details about the supported operating systems.

IMPORTANT: Be sure that the partition on which the XPR server software is installed has a minimum size of 10 GB. The target path must not contain any blanks (e. g. c:\OpenScape Xpressions\xpr)!

IMPORTANT: The installation of an XPR system on substituted drives is not possible, since the setup program cannot create the required directory shares of the XPR system.

IMPORTANT: Installing the XPR system on a domain controller is not permitted.

IMPORTANT: You may not set up an XPR on a computer on which a ComAssistant is installed. In this context it is irrelevant whether or not the XPR is integrated in the ComAssistant.

Communication hardware when using an ISDN connection

To address the XPR system via the telephone user interface (TUI) and/or to be able to send and receive fax messages, you need at least one S₀ or S₂ board by Dialogic/Eicon for mounting in the server PC.

Dialogic/Eicon ISDN boards

IMPORTANT: At times, Dialogic uses different version numbers for the same board. For example, the hardware description features a specific version number for a board, but in the Dialogic Diva Configuration Manager you find another version number for the same board. The version numbers used for Dialogic ISDN boards in this XPR V7 guide are always the version numbers specified in the Dialogic Diva Configuration Manager!

Refer to the *OpenScape Xpressions Release Notice* for a list of the supported Dialogic/Eicon ISDN boards.

Mixed operation between different BRI or PRI cards as well as mixed operation of BRI and PRI cards on a server computer is not released.

IMPORTANT: Using more than 3 Dialogic/Eicon-4BRI boards in the CorNet-T context may lead to a faulty call forwarding connection. Please note the workaround in [Section C.6, "Hicom 300H/CorNet-T Installation", on page 314](#).

Minimum equipment of the client PCs

The client PC minimum equipment complies with the requirements of the desired operating system. Consult the documentation of this operating system on this subject.

NOTE: All client programs can also be executed on 64-bit operating systems. However, with the exception of the fax printer driver, they are not compiled in the 64-bit mode.

On a 64-bit operating system, client programs are typically not installed in folder `C:\Program Files\` but in folder `C:\Program Files (x86)\`.

The following client components have individual requirements that may deviate from those of the operating system:

- OpenScape Xpressions optiClient 130 (see *Client Installations* manual)
- Communications (see *Communications* manual)

2.1.3 Checking Windows 64-bit Server Settings

NOTE: The new security component User Account Control (UAC) with Windows Server 2008 demands editing some applications as administrator. Select the **Run as administrator** option in the context menu and start the application.

- **Computer Name**

IMPORTANT: The name of the computer on which the XPR is installed must not exceed 15 characters.

- **Partitioning**

In general we recommend to use the first of the two hard disks for setting up the operating system, the required Office applications and the XPR server. The second hard disk should be used for user data and mailboxes. So that the enhanced security mechanisms and the extensibility can be used, both hard disks must be formatted with the NTFS format.

- **Optimizing the physical memory**

Windows Server 2008 64-bit is normally optimized with maximum throughput as a file server. However, an XPR server requires considerably less memory for the disk cache. Select the **Balance** option under **Start > Settings > Control Panel > Network Connections > LAN > Properties > File and Printer Sharing for Microsoft Networks > Properties**.

- **Optimizing availability**

After an operating system crash, a file that contains debugging information is created from the paging file next time the system starts. If the size of this file is close to the size of the system's physical storage, almost all of the virtual memory is used for generating this file during system startup. This may result in some services of the XPR server not being able to start properly.

To resolve this problem, select **(none)** under **Start > Settings > Control Panel > System > Advanced > Startup and recovery > System Failure > Write Debug Information**.

Leave the remaining options unchanged. The **Automatically reboot** option forces an automatic restart if Windows crashes, thus considerably increasing the server's availability.

- **Russian or Turkish as XPR Server Default Language**

If *Russian* or *Turkish* is intended as default language for the XPR server, the language should correspondingly be set for non-Unicode programs in the operating system. This setting initializes the XPR server database with the correct code page (1251 for Russian respectively 1254 for Turkish) at the

installation, so that in many areas Cyrillic or Turkish characters are used. For the outputs in all other languages, code page 1252 is still used. Please read on this topic also [Section 2.1.7, “Language Settings for Non-Unicode Programs”, on page 34.](#)

The use of Russian or Turkish as default language for the XPR server has the following operational effects:

- a) When a client (for example Communications) that is set to another language logs on, special characters delivered from the database may not be correctly represented in the client, if its code page used does not contain this character or contains it in another position.
 - b) There is still the restriction that neither Cyrillic nor Turkish characters may be used for user IDs.
 - c) If a Turkish client logs on to a Russian server - or a Russian client logs on to a Turkish server - it is **not** possible to correctly represent data from the database, since none of the two code pages contains characters from the other code page.
 - d) Only if all servers use the same code page, they can be connected in a System Networking. For example, a Russian and a Turkish server **cannot** be connected.
- **Windows DHCP service**
Make sure that the Windows-individual DHCP service is terminated and not active.
 - **SMTP service**
It is essential to remove the Windows 2008 SMTP service because XPR features a proprietary SMTP link that may conflict with the Windows Server 2008 service. This is done under **Start Settings Control Panel Add/Remove Programs Add/Remove Windows Components Internet Information Service (IIS) Details Remove SMTP Service.**
 - **Internet information service (IIS)**
Both the IIS and the WEB APL use port 80. During the installation the IIS service is therefore set to startup type **Manual**.

IMPORTANT: In case of a reinstallation of a server operating system we recommend not to install the IIS, since the IIS, once it has been installed on the server, must not be uninstalled any more!

- **Network integration**
The LAN connection of the computer on which the XPR system is to be installed must be established **before** the XPR software setup, since otherwise the network services cannot be started by the operating system.

Planning the Initial Installation

Checklist for preparing the XPR Server Installation

- **Installing the Microsoft Loopback Adapter**

NOTE: In Microsoft Windows Server 2012 R2 , Windows Server 2016, Windows Server 2019, Windows Server 2022 and Windows Server 2025, the Loopback Adapter is called *Microsoft KM-TEST Loopback Adapter*.

The Microsoft Loopback Adapter is a driver providing a loopback device. Without this “adapter” an XPR server would immediately stop running if e.g. the network plug was removed, since in this case the whole internal communication of the XPR services would stop.

Therefore, the Microsoft Loopback Adapter driver should be installed on each XPR server. The installation is performed via **Start Settings Control Panel Hardware**.

If the setup is performed on a computer with two network boards (for example a network board and a Microsoft Loopback Adapter), Windows usually finds the Loopback address as first network device. Be sure to configure the network board as first network interface, since the first address is bound to the XPR components that require a local IP address.

- **DHCP client**

The **DHCP client** Windows service must be stopped and deactivated in the service manager.

- **Antivirus software**

To avoid installation errors, deactivate the antivirus software during the installation.

- **License logging**

The **license logging** Windows service must be stopped and deactivated in the service manager.

- **Connection to IBM/Lotus Notes**

To connect the XPR server to a IBM/Lotus Notes environment, a IBM/Lotus Notes client and corresponding access rights to IBM/Lotus Notes databases must be provided on the server **before** the installation of the XPR software (for detailed information please refer to the manual *OpenScape Xpressions IBM Notes Gateway*).

- **Connection to Exchange 2003**

You find information about the connection in the *OpenScape Xpressions Exchange Gateway* manual.

- **Connection to Exchange 2007**

You find information about the connection in the *OpenScape Xpressions Exchange Gateway* manual.

- **Connection to SAP/R3**

You find information about the connection in the *OpenScape Xpressions SAP Gateway* manual.

Deactivating DEP

If the Crystal Reports XI Developer Edition is used, the data execution prevention (DEP) must be disabled. If the processor supports DEP and DEP is active, Crystal Reports will be prevented to access memories. DEP was introduced with Service Pack 1.

How to deactivate DEP:

1. Deactivate all antivirus programs and spyware on your computer.
2. Click on **Start > Settings > Control Panel > System**.
3. Click the **Advanced** tab.
4. Click on the **Settings** button in the **Performance** section.
5. Click on the **Data Execution Prevention** tab.
6. Activate the radio button **Turn on DEP for all programs and services except those I select:**.
7. Click the **Add...** button.
8. Select the EXE file for the Crystal Reports XI Developer Edition, for example
C:\Program Files (x86)\Business Objects\Crystal Reports 11\crw32.exe.
9. Click the **Open** button.
10. Click on **OK**.
11. Click on **OK**.

2.1.4 Installing .NET Framework on Windows Server 2012 R2 and Windows Server 2016, 2019, 2022, 2025

If you use Windows Server 2012 R2 or Windows Server 2016, 2019, 2022 or 2025 .NET Framework 4 has been installed per default. Please, add the Windows feature .NET Framework 3.5 (via Server Manager/Add Roles and Features Wizard).

2.1.5 Configuring the Firewall for Windows 2008 Server

The architecture of Windows 2008 Server is designed in a way that you do not see the computer in the network when the firewall is inactive. You can evade this characteristic of Windows 2008 Server by configuring the default setting for the domain as follows:

- Inbound = blocking
- Outbound = allowing

To do this, the ports for inbound data traffic must be configured accordingly (see example).

Example:

IpAPL	SIP UDP	UDP	5060
IpAPL	SIP TCP	TCP	5060
IpAPL	SIP TLS	TCP	5061
VoiceConference	SIP UDP	UDP	5062
VoiceConference	SIP TCP	TCP	5062
VoiceConference	SIP TLS	TLS	5063
WebAPL		TCP	80
WebAPL	SSL	TCP	443
WebClient	SSL	TCP	8443
TcpAPL		TCP	8944

Table 1 Examples of Port Connections under Windows 2008 Server

2.1.6 Troubleshooting in Case of a Network Connection Breakdown

A network connection breakdown cannot be automatically trapped, so that such an error inevitably requires manual intervention. Using an MS Loopback Adapter increases the system stability significantly, though.

NOTE: In Microsoft Windows Server 2012 R2, Windows server 2016, Windows Server 2019, Windows Server 2022 and Windows Server 2025, the Loopback Adapter is called *Microsoft KM-TEST Loopback Adapter*.

If the active respectively licensed network card or the network cable fail owing to a defect, the APLs shut down automatically. Some services, inclusive the *XPR Administrator(mrs)* service, remain booted.

How to revive the system after a network connection breakdown:

1. Stop the *XPR Administrator(mrs)* service via the Windows service management. This service will stop all other booted services before it stops itself. Proceed as follows:
 1. Open the Windows service management via **Start > Administrative Tools > Services**.
 2. Find the entry **XPR Administrator(mrs)** and select it.
 3. Open the **Action** menu and select the **Stop** option.
2. Replace the defect network card respectively the defect cable and test the network functioning.
3. Start the *XPR Administrator(mrs)* service via the Windows service management. Proceed as follows:
 1. Open the Windows service management via **Start > Administrative Tools > Services**.
 2. Find the entry **XPR Administrator(mrs)** and select it.
 3. Open the **Action** menu and select the **Restart** option.

2.1.7 Language Settings for Non-Unicode Programs

IMPORTANT: The language setting modification requires a computer reboot to take effect. Make sure that no important applications are operated on the server, which are not available during the reboot. Consult the system administration on site about an ideal time for a computer reboot.

The setup medium of the operating system is required for changing the language setting.

This setting is important, if Turkish or Russian is to be used as XPR server default language. It enables in many areas the use of Russian or Turkish special characters. Please also heed the section [Russian or Turkish as XPR Server Default Language](#) on [page 29](#) on this.

How to perform the language settings for non-Unicode programs in the operating systems Windows Server 2008 and Windows 7 Professional:

1. Open the dialog **Regional and Language Options** via **Start > Control Panel > Regional and Language Options**.
2. Open the **Advanced** tab.

Planning the Initial Installation

Pre-installation Checklist

3. In the **Language for non-Unicode programs** section, select the option **Russian** or **Turkish** from the drop-down menu.
4. Click **OK**.
5. Insert the setup medium of your operating system when you are prompted to do so.

If the required data are already available on the system, you can use them. Click in the information dialog on **Yes** for this purpose.
6. Click on **Yes** to reboot the computer.

2.2 Pre-installation Checklist

Topic	Description
Information to be provided by the customer:	
IP settings	Address, gateway, DNS server, possibly the VoIP servers' addresses
Passwords	Local and Domain.
Fax document type	Which document types are sent by fax (suitable conversion software to be provided)?
Numbering plan	The numbering plan agreed with the customer must be available.
PC check before installing software:	
Hardware	Remove superfluous hardware from the server PC (for example sound cards).
Operating system (Configuration)	See Section 2.1.3, "Checking Windows 64-bit Server Settings"
LAN integration	Verify that the server PC is correctly integrated into the customer LAN.
Miscellaneous	Before the software installation, shut down all applications running in the background (for example antivirus programs). After the successful installation such applications can be rebooted.

Table 2 Pre-installation Checklist

2.3 Choosing between a Central or Distributed XPR System

Before the initial XPR installation you should already know whether to install a singular system (one that is based on a kernel computer) or a distributed system (with one or more satellite computers). Refer to [Chapter 6](#) for information on setting up a distributed system.

3 Generating Licenses

With the help of a license management, different software products are centrally licensed. This license management provides a user-friendly and efficient licensing procedure. It consists of the following components:

- Central License Server (CLS)
- Customer License Client (CLC)
- Customer License Agent (CLA)
- Customer License Management (CLM)

Central License Server (CLS)

Via the Central License Server you apply for license files that a license generator creates there. Licenses are applied for via the Internet. The license must be available at the time of the product installation. After the license has expired, the product is still fully operable for a specific period ("Grace Period", e.g. 30 days, depending on the product), but it cannot be rebooted. In addition, the license server administers the product licenses assigned to the license agents and their permanent link via the locking ID (= MAC address of the first IP interface of the computer on which the CLA runs) to the CLA.

Customer License Client (CLC)

The CLC represents the interface between the product and the CLA. Via the CLC the product can query at the CLA whether or not a valid license is available. The CLC is a DLL and an integral part of the product to be licensed and contained in the product's setup.

Customer License Agent (CLA)

The CLA's task is to save the received licenses and to provide them to OpenScape Xpressions. Via the integrated CLC, OpenScape Xpressions enquires whether or not the entered license is valid. The CLA checks the query and releases the software when the license is correct.

Customer License Management (CLM)

The CLM may be installed on the OpenScape Xpressions PC, on an administration PC together with the CLA, or on any PC in the network. The CLM accesses the license agent(s) via network. It has an interface to the CLS and to the CLA. It can thus be used to control various license management processes such as license activation, or displaying the current license distribution to single OpenScape Xpressions servers. The CLM is a web application. The connection to the CLS is established via the Internet.

3.1 Licensing Routine

Licensing follows this routine:

1. The customer places the order, which is registered, for example, via SAP.
2. The relevant order data are stored in the database of the CLS.
3. From the data, the CLS generates the authentication code and forwards it to you (e.g. by e-mail).
4. The hardware/software delivery is initiated.
5. You install the software incl. the license management.
6. Using the CLM you generate your licenses via the Internet at the CLS. To this you need the authentication code. The CLM then sends the authentication code and some customer-specific hardware data (locking ID) to the CLS.
7. Based on the authentication code and the customer-specific hardware data (locking ID = MAC address of an implemented network card), the CLS generates a license file and returns this file to your CLM. If you use a virtual environment, you need to use an Advanced Locking ID as locking ID. You can generate the Advanced Locking ID on the CLS.
8. The CLM transfers the license file to a selected CLA. Based on the locking ID the CLA checks whether the license file is valid for the hardware/software. The software is only released for usage if the locking ID of the hardware on which the CLA runs matches the locking ID in the license file. Otherwise the software will not be released.
9. Start OpenScape Xpressions. The CLC integrated there checks at the CLA whether the software has been released. After a successful check you can use the software.

3.2 MAC address

The MAC address is a world-unique identification number of a network board. This MAC address is used for encrypting the different licenses when generating the license file. If several network boards are implemented in one computer, the MAC address of the first network board found must be used. This licensing model ensures that the software can only run on the associated hardware.

Prerequisites for identifying the MAC ID

NOTE: The network card must definitely be physically connected to the hub since otherwise the MAC ID cannot be read out. In addition, the TAPI Service Provider must be installed and running.

Exchange or Failure of Network Boards

NOTE: When changing the network board or modifying the hardware configuration, check the MAC address used. If the address changes, a new license file must be created. In this case, the old MAC ID is disabled and no further license files may be generated for this MAC ID. An extension of the licenses is then not possible either, because the system to be expanded cannot be identified via the MAC address anymore.

3.3 Generating an Advanced Locking ID

To generate the **Advanced Locking ID** you need some network settings from the virtual computer you wish to use. You need the host name, the host IP address, the gateway IP address and the first DNS IP address.

1. Execute the following link to reach the CLS administration page: <https://www.central-license-server.com/AdminTool/pages/login.jsf>.
2. Enter your access data to access the web page.
3. Click on **CLS AddOns** in the navigation on the left and then on **Calculate Locking ID**.
4. Select the product for which you wish to generate the **Advanced Locking ID** from the drop-down list and click on **Select**.
5. Select **Virtual** from the next drop-down list and click on **Select**.

The information of your network settings is now required.

6. Edit all fields and click on **Calculate Locking ID**.

The generated locking ID is displayed.

Generating Licenses

Determining the MAC ID of the CLA Computer

7. Note down the locking ID for using it to create a license key at a later date.

3.4 Determining the MAC ID of the CLA Computer

To determine the MAC address, open a DOS shell and enter the command

```
ipconfig /all
```

. Among other things, the MAC address (physical address) will be displayed.

NOTE: The MAC ID is also used for customer identification and must definitely be archived at the customer facility because only via this MAC ID another retrieval is possible.

3.5 Generating a License Key

The license server must be used to generate a license key. Proceed as follows:

1. Invoke the license server's website with this URL:
<https://www.central-license-server.com/>
. The website is available in English, German and French.
2. Log in with your login name and the corresponding password. These are known to the regions. If by way of an exception this is not the case, please contact your product manager.
3. The page for generating an initial license is displayed. The following data must be available for generating an initial license:
 - **SD order number**
 - **Packing slip number** (enter this without the leading characters "CD")
 - **Network board MAC address**

NOTE: The SD order and packing slip numbers can be found on the packing slip. The packing slip is contained inside the packaging and is not to be confused with other documents such as the order verification slip, for example. If your system was delivered in several batches, then you should use the number of the packing slip on the OpenScape Xpressions base package.

4. Click **Generate and download license key**. Enter your data in the corresponding fields. Then click **Generate license key**.
The license file is generated and the license key details displayed.
5. Click the **Save License Key** button to locally store the license on your computer. The license is saved as text file with the suffix "lic" and can be imported later during the system software installation.

License generation is thus accomplished.

3.5.1 Retrieving a License File

If the locally saved license file gets lost, it can be retrieved from the license server and saved whenever required. Proceed as follows:

1. Log in at the license server and click the **Next** button next to **View used Licenses and Certificates** in the **Management of used Licenses** section.
2. Select a license and click the **View Details** button.
3. Click the **Save License Key** button.

3.6 Rehost - shifting available Licenses to a new System

This function enables shifting all licenses to a new system. The feature is always used when the hardware used (e.g. new network board, replacement of the computer) changes. In consequence of a hardware change the available licenses must be shifted to the new hardware.

In this process the license management system heeds rules that affect the license rehost and the number of licenses usable on a system. The result of this feature is the generation of a license key that is bound to the new hardware on the basis of the hardware's MAC address and made available for saving.

NOTE: The old MAC address is then barred and can no longer be used. This applies for all licensing types and procedures.

Proceed as follows:

1. After logging in click the **Next** button next to the **Rehost** entry in the **Management of Used Licenses** section.
2. Select the license to be shifted and click **Rehost**.
3. Enter the new hardware's MAC address in the **MAC Address** field and select the required languages. Then click on **Next**.

NOTE: Via the **Check** button you can verify the number of selected languages matching the license.

4. Check your entries, read the **legal note** and select the **I agree with the above terms.** field. Then click **Finish**.

The license key is generated.

5. Click the **License Key** button. The new key's details are displayed.
6. Click **Save License Key**.

The rehost process is now completed.

3.7 Activating Licenses in the CLA

In this section we assume that the license is available on a data carrier as XML file. If you want to generate a license, read the corresponding sections in the CLM online help.

NOTE: To generate licenses, you need the login data for the license server (CLS) and an authentication code.

How to transfer already available licenses to the CLA:

1. Start the CLM.
2. Synchronize the CLM with the desired CLA. Proceed as follows:
 - a) On the CLM interface click on the **Logon/Synchronize** button.
 - b) Click on the **Details >>** button.
 - c) If the license agent is not in status *synchronized*, make sure that the **Logon to local PC of the license agent** option is active.
 - d) Enter the user name and password in the **Name** and **Password** fields for a user account that belongs to the group of local administrators (for example *Administrator*) on the CLA computer. In case of removed CLAs this is mandatory, with a local CLA this is only required if you are logged in as license agent administrator.
 - e) Afterwards, click on **OK**.

3. Transfer the license to the CLA and activate it. Proceed as follows:

a) Click in the navigation section of the CLM interface on the **Contents** entry or on the **Contents Page** button at the top right margin. This button is always displayed when you are not on the contents page.

a) Click the **Activate License** button.

b) Select the **Install local license key on license agent (offline activation)** option.

Selecting one of the other two options makes the license server (CLS) request the license. To this you need the logon data for the license server (CLS) as well as the authentication code. You can obtain information about license generation on the license server and about how to further proceed via the **Help** button at the top right margin of the CLM interface.

c) Select the **License file** option.

d) Click the **Browse...** button and find the license file in the computer's file system respectively on the external data carrier on which it has been stored.

e) Click the **Activate** button.

f) Click on the **Open confirmation code for printing...** link, and subsequently click on the **Print** button in a second window.

The operating system's print dialog opens, in which you can select a printer and start printing via the **Print** button.

g) Close the second window via the **Close** button.

h) In the CLM click on **OK**.

i) The license is now active and can be used.

Generating Licenses

Activating Licenses in the CLA

4 XPR System Installation

This chapter takes you step by step through the **initial installation** of an XPR system. Use the following checklist (cf. [Section 2.2, “Pre-installation Checklist”, on page 35](#)) to ensure that the requirements to install XPR have been met.

NOTE: You find information about upgrading an XPR system in the service manual *OpenScape Xpressions Upgrade*.

Before starting an installation check in g-DMS if the current version of the Release Notice and the Release Notes are available. The following table reflects the product structure in the G-DMS / SWS (Software Supply Server) and the diagnostics structure in the ICTS (Case Tracking System)

Main category	Applications
Product family	OpenScape Xpressions
Product	OpenScape Xpressions
Product version	OpenScape Xpressions V7
Product code	P30152-P1526-A1-1

Table 3 Product Structure in the G-DMS / SWS

Product family	Applications
Product group	OpenScape Xpressions
Product type	OpenScape Xpressions
Product version	V7
SW version	V7 R1.1.0

Table 4 Diagnostics Structure in the ICTS

Installation checklist

Before you start the installation, you need to have executed the following steps:

- [Section 2.1, “Checklist for preparing the XPR Server Installation”, on page 23](#)
- [Section 2.1.2, “Checking the System Requirements for the Server PC”, on page 24](#)
- [Section 2.1.3, “Checking Windows 64-bit Server Settings”, on page 29](#)

4.1 Installation Basics

NOTE: The new security component User Account Control (UAC) with Windows Server 2008 demands editing some applications as administrator. Select the **Run as administrator** option in the context menu and start the application.

NOTE: Remote System Link is not compatible with [Crypt_Sec], it is designed to only work with [KRYPT].

The product installation does not only include the actual XPR server, but also components that are no primary XPR server elements. Such elements are installed as independent products. The product installation comprises among other things:

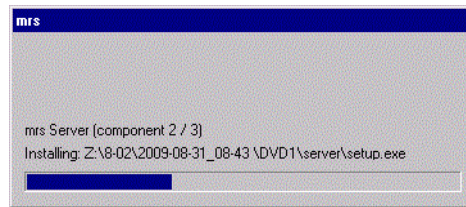
- further server components
- additional language packets (for example English, French, Spanish)
- client applications (e.g. Application Builder)
- drivers for ISDN hardware and the connection to a PBX
- components for text-to-speech
- Acrobat Reader for displaying the product documentation
- Automatic Speech Recognition (ASR)

The *OpenScape Xpressions server* component comprises so-called features. Each feature provides a specific functionality, such as a connection to Microsoft Exchange or CTI functionality, by means of an APL. The available licenses determine which features you can select.

NOTE: If you wish to start the installation from a network share, then please note <http://support.microsoft.com/kb/978869> and request the Microsoft hotfix if required.

When you connect the setup medium to the installation computer, a setup program starts in which you need to make some specifications and select the components to be installed. This program will be called **Wrapper** in the following.

After you have made all necessary specifications and selected the desired components, the Wrapper starts automatically and in succession the installation programs of the selected components. During this phase the following status dialog appears in the top left corner of the screen:

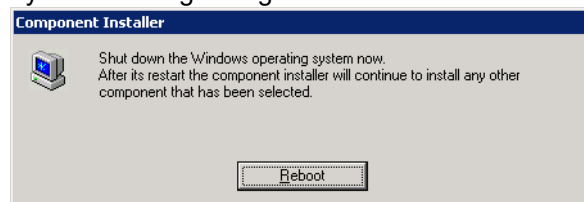


This dialog displays the following information:

- Number of components to be installed
- Number of components already installed
- Status of the entire installation

The number of components you can select in the Wrapper depends on the licenses you have purchased. Some of the component installation programs prompt you to make further entries by appropriate dialogs.

IMPORTANT: The computer may only be rebooted, if you are prompted to do so by the following dialog:



After the installation you have an operable but vastly unconfigured XPR system. During the installation only those components are configured that cannot work without an initial configuration. Among these components you find:

- SMTP APL
- Lotus Notes gateway
- LDAP APL
- Exchange Gateway

IMPORTANT: The XPR server must not be installed on the domain controller.

4.1.1 Text-to-Speech Engine Nuance Vocalizer for Networks 5

Contrary to the relevant XPR services, the text-to-speech engine *Nuance Vocalizer for Networks 5* operates under a different Windows account. This may lead to the following error message and the text-to-speech conversion fails:

Class not registered

To avoid this error, you need to adapt the following XPR services to that effect that they run under the same account as *Nuance Vocalizer for Networks 5*:

- XPR Administrator (MTA)
- all Telematic APLs (IP APL, ISDN APL, etc.)

Proceed as follows:

1. Open the Windows service management (for example via **Start > Administrative Tools > Services**)
2. Select the entry of the XPR MTA service and open its properties dialog (menu option **Action > Properties**).
3. Open the **Log On** tab, select the **This account:** option and enter the data of the administrator account in the corresponding fields.
4. Then click the **OK** button.

IMPORTANT: If you perform an installation via a remote desktop connection and want to set up text-to-speech (TTS), please heed the instructions in [Section 4.1.2, "Installation via Remote Desktop Connection"](#), on page 51.

NOTE: TTS and ASR have been released only for specific operating systems and on real hardware or on certain VMware ESXi versions (see service documentation *OpenScape Xpressions Release Notice*).

4.1.2 Installation via Remote Desktop Connection

IMPORTANT: If you perform an installation via a remote desktop connection, start the remote desktop connection by entering the

```
mstsc /v:<IP address> /console
```

or

```
mstsc c:xyz.rdp /console
```

or

```
mstsc /v:<IP address> /admin
```

or

```
mstsc c:xyz.rdp /admin
```

command in the command prompt. Replace hereby `c:\xyz.rdp` by path and file name of the corresponding file on your system. Use the `admin` parameter with Windows 7 and Windows Server 2008 and use the `console` parameter with all other operating systems. `<IP address>` is the IP address of the computer on which the XPR is to be set up. Connect the setup medium to the installation computer or link the remote desktop client share up with a drive letter.

Do not use **Start > Programs > Accessories > Communications > Remote Desktop Connection**, since then the XPR setup cannot be correctly performed to the end.

Otherwise, installing the Microsoft SQL Server 2005 Express is not possible.

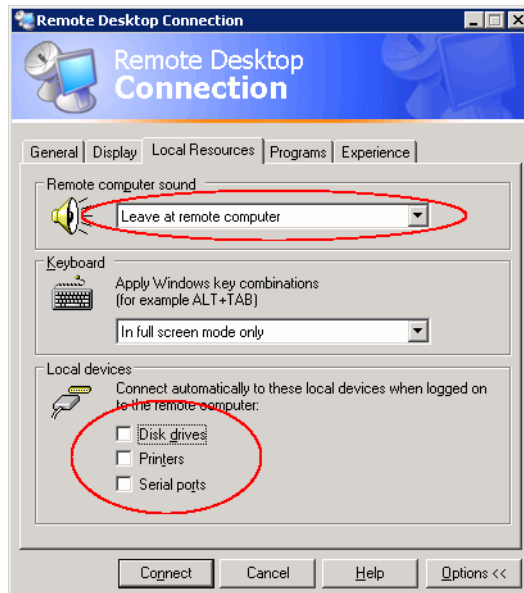
You find further information about the Microsoft SQL Server 2005 Express in the Report APL context in [Section A.2, "Using the Report APL with SQL Databases"](#), on page 207.

Installation is generally possible via a remote desktop connection. Using this method make sure that no local resources (drives, printers, serial interfaces) of the connecting computer are linked to the remote computer.

Otherwise you run the risk that printer drivers are installed on the connecting computer instead of on the remote computer and the attempt to convert documents on the remote computer fails. In this case the XPR monitor displays error messages as shown in the following example:

```
SmtplConversion E Could not open printer'Server Fax G3  
TurboBits Printer'
```

The following remote desktop connections settings avert this problem:



IMPORTANT: If you do not select the **Leave at remote computer** option in the **Remote computer sound** section of the above dialog, components may crash as soon as you establish a remote connection to the XPR server computer. We recommend to **always** use the parameters set here for a remote connection to the XPR server computer.

4.1.3 Overview of the Installation Sequence

The following list shows the installation sequence and refers to the corresponding text passages.

1. [Section 4.3.3, "Installing/Connecting the License Service", on page 71](#)
2. [Section 4.3.4, "Specifying the Server Name", on page 76](#)
3. [Section 4.3.5, "Selecting the Server Languages and the Default Language", on page 77](#)
4. [Section 4.3.6, "Confirming the Release Notes", on page 79](#)
5. [Section 4.3.7, "Selecting System Components", on page 80](#)
6. [Section 4.3.8, "Selecting Client Components", on page 81](#)
7. [Section 4.3.9, "Selecting External Software", on page 83](#)
8. [Section 4.3.10, "Installing the Adobe Reader", on page 85](#)
9. [Section 4.3.11, "Installation Type for Automatic Speech Recognition", on page 85](#)
10. [Section 4.3.12, "Installing the Dialogic/Eicon Drivers for Communication Hardware", on page 87](#)
11. [Section 4.5.1, "Selecting Features", on page 91](#)
12. [Section 4.5.2, "Summary of the Specifications and Settings", on page 100](#)
13. [Section 4.5.3, "Selecting the Folder for the Database and the Document Folder", on page 101](#)
14. [Section 4.5.5, "Selecting the Default Speech-Encoding", on page 103](#)
15. [Section 4.5.6, "Configuring the User Authentication", on page 104](#)
16. [Section 4.5.7, "Configuring the XPR Server Components and Services", on page 108](#)
17. [Section 4.5.7.1, "Configuring regional Connection Settings", on page 109](#)
18. [Section 4.5.7.2, "Additional IP Addresses for the Web Conference Server", on page 113](#)
19. [Section 4.5.7.3, "Connection APL", on page 114](#)
20. [Section 4.5.7.5, "Setup Wizard for the SMTP APL", on page 121](#)
21. [Section 4.5.7.6, "Installing and Configuring the CTI APL", on page 124](#)
22. [Section 4.5.7.8, "Installing the Exchange 2003 Gateway", on page 125](#)
23. [Section 4.5.7.10, "Installing the Lotus Notes Gateway", on page 126](#)

24. [Section 4.5.7.11, “Installing the SAP R3 Components”, on page 126](#)
25. [Section 4.5.7.12, “Installing and Configuring the V.24 APL”, on page 126](#)
26. [Section 4.5.7.12, “Installing and Configuring the V.24 APL”, on page 126](#)
27. [Section 4.5.8, “Installing and Configuring the Web Conference Server”, on page 132](#)
28. [Section 4.5.10, “Installing the Java Runtime Environment”, on page 142](#)
29. [Section 4.5.11, “Creating the SSL Certificate”, on page 144](#)
30. [Section 4.5.13, “Installing the Language Packets”, on page 150](#)
31. [Section 4.5.14, “Installing Client Applications”, on page 151](#)
32. [Section 4.5.15, “Installing the Application Builder”, on page 153](#)
33. [Section 4.5.16, “Installing the Add-On Components”, on page 154](#)
34. [Section 4.5.17, “Completing the Component Installer”, on page 157](#)

Modifying, repairing or removing the XPR installation

1. [Section 4.6.2, “Stopping and starting the XPR Server”, on page 169](#)
2. [Section 4.6.3, “Modifying an existing Installation”, on page 169](#)
3. [Section 4.6.4, “Repairing an Installation”, on page 172](#)
4. [Section 4.6.5, “Removing the XPR System completely”, on page 175](#)

4.2 HiPath License Management (CLM)

Using the CLM, licenses for products are centrally administered and provided in a network.

Before you can install OpenScape Xpressions server, the following requirements must be met:

- A CLM must be available in the network (cf. [Section 4.2.3, “Installing the CLM”, on page 57](#)).
- A HiPath Customer License Agent (CLA) must be installed (cf. [Section 4.2.4, “Installing the CLA”, on page 61](#)). The CLA can be installed on any computer in the network. Please heed the scenarios described in the following (cf. [Section 4.2.2, “Possible Scenarios for the CLM”, on page 56](#)).
- The licenses you have purchased must be activated via the CLM and transferred to the corresponding CLA. Please read the corresponding section in the CLM help on this.

4.2.1 How the CLM operates

The CLM operation mode is comprehensively explained in the product documentation, which you can open via the **Help** button in the CLM product interface. Here, we only provide a short outline:

1. The CLM and the XPR server are uninstalled
2. By means of the CLM and via the Internet you generate the required licenses at the Central License Server (CLS). To do this you need the authorization code and the MAC ID of the computer on which the CLA is installed (locking ID). The authorization code and the locking ID are sent by the CLM to the CLS.
3. With the help of the authorization code and your specific locking ID the CLS generates a license file and returns this file to your CLM. Thus the licenses are bound to the MAC ID of the computer on which the CLA has been installed. This affects the scenarios described further below.
4. Using the CLM the license file is transferred to the selected CLA. Based on the locking ID the latter checks whether the license file is valid for the XPR server. If the locking ID matches the one in the license file, the XPR server is released, otherwise the XPR server is not released.
5. The license service that communicates with the CLA using the CLC was automatically installed on the computer on which the XPR server is installed. The CLC is a function library (DLL = Dynamic Link Library), which provides functions required for communication between the license service and the CLA.

6. When the XPR server starts, the installed APLs query the license service for an available license. Using the CLC the license service transfers this request to the CLA. The CLA checks whether a license is available on the specific XPR server for the corresponding APL and answers accordingly. After a successful check the APL starts and may be used.

4.2.2 Possible Scenarios for the CLM

IMPORTANT: When you select your scenario make sure the licenses are always bound to the MAC ID of the computer on which the CLA is installed and operates.

Scenario 1:

The XPR server is installed on an individual computer. CLM and CLA are installed on other computers in the network. This can be considered the scenario most commonly used.

Scenario 2:

The XPR server and the CLA are installed on one computer. The CLM is installed on another computer in the network. In this case you need an individual license pack for each installed XPR server.

Scenario 3:

The XPR server, the CLM and the CLA are installed on the same computer.

4.2.3 Installing the CLM

Prerequisites:

CLM requires the installation of Java Runtime Environment. Complete installation of Java Runtime Environment as described in [Section 4.5.10, “Installing the Java Runtime Environment”](#)

How to install the CLM:

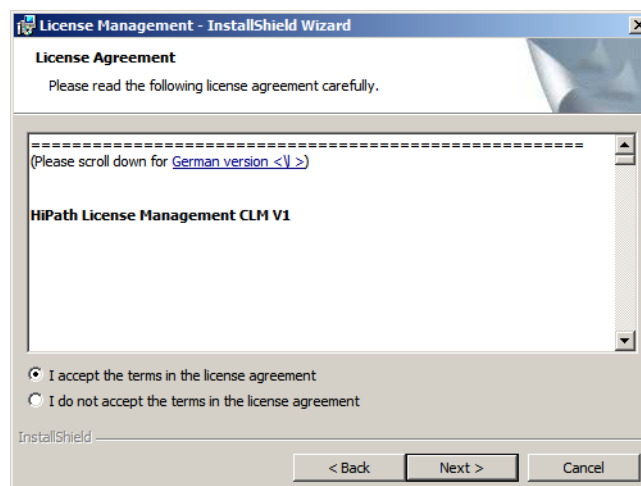
1. Start the `setup.exe` file from the `XpressionsInstall\Prerequisites\HLM\CLM` directory of the setup medium as administrator.

The setup is prepared and the following dialog opened:



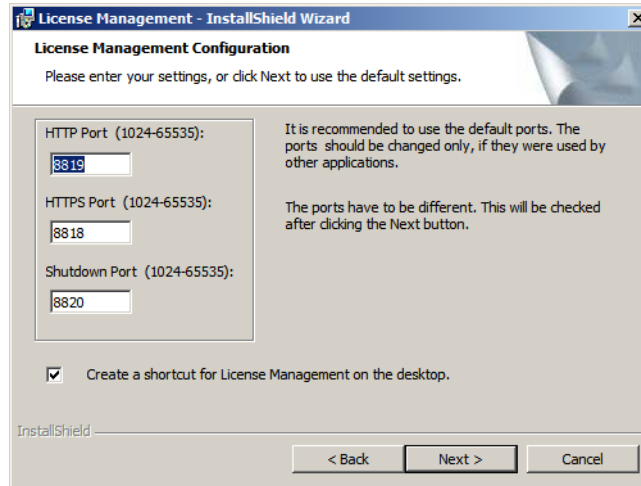
2. Click on **Next**.

Up comes this dialog:



3. Activate the radio button **I accept the terms of license agreement** and click on **Next**.

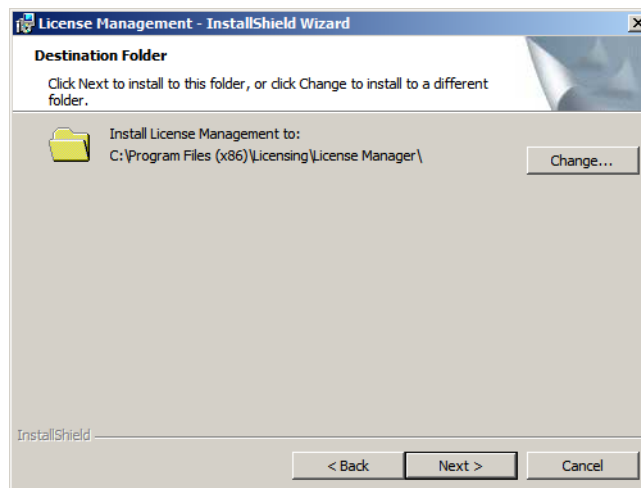
Up comes this dialog:



NOTE: We recommend to use the preset ports and not to modify them until port conflicts with other applications occur. Also verify that these ports are correspondingly released in a firewall that may exist in the network. In case of doubt please contact the network administrator.

4. Click on **Next**.

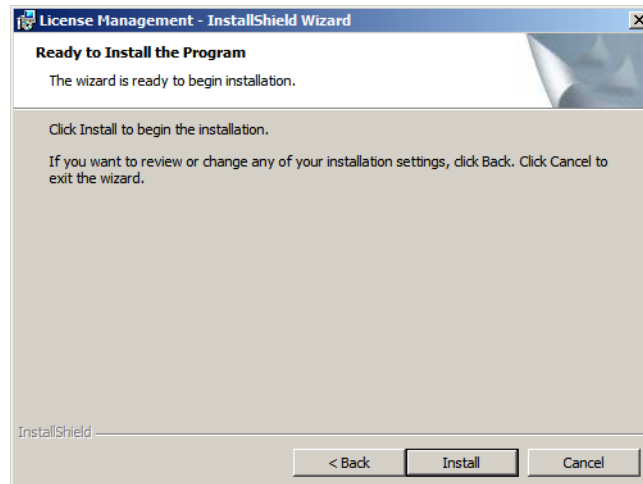
Up comes this dialog:



5. If you want to use the defaulted target folders, click on **Next**.

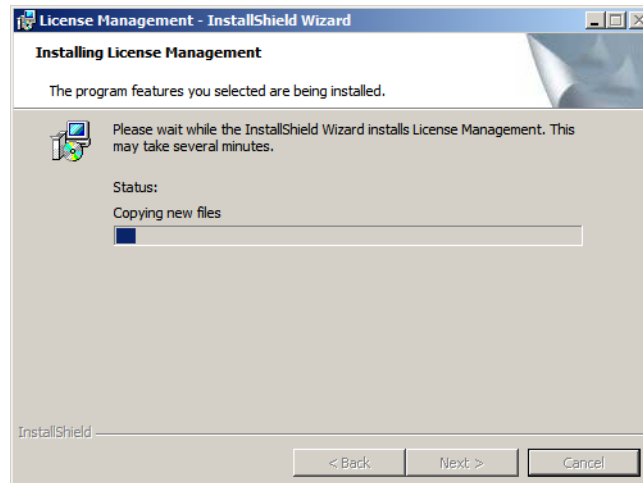
Via the **Change...** button you can specify another target folder for the installation. After you have changed the target folder, click in this dialog on **Next**.

Up comes this dialog:



6. Click the **Install** button.

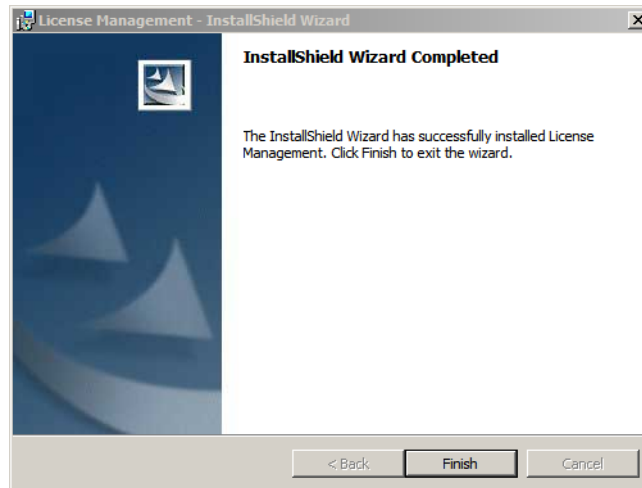
The installation starts and you can see the progress in the following dialog:



As soon as the installation process is complete, the following dialog appears:

XPR System Installation

HiPath License Management (CLM)



7. Click the **Finish** button to complete the installation.

The dialog closes and the CLM installation is complete.

After the CLM installation you find an icon on the desktop.



Further information about the CLM is available after the application's start via the **Help** button.

4.2.4 Installing the CLA

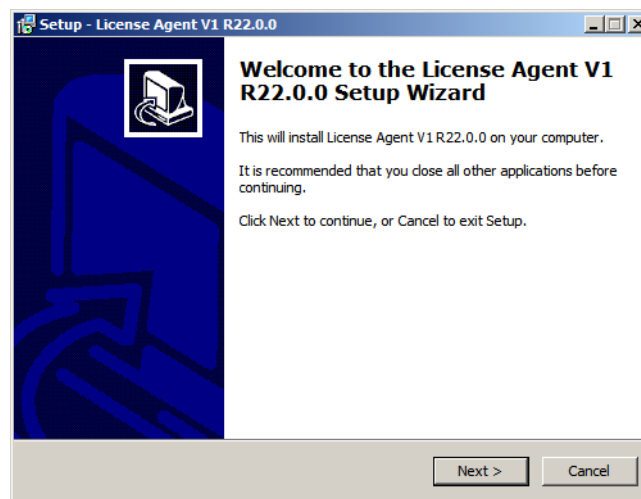
NOTE: If you want to install several XPR servers you need to install an individual CLA for each of these servers.

How to install a CLA:

1. Start the `setup.exe` file from the following directory of the `setup` medium:

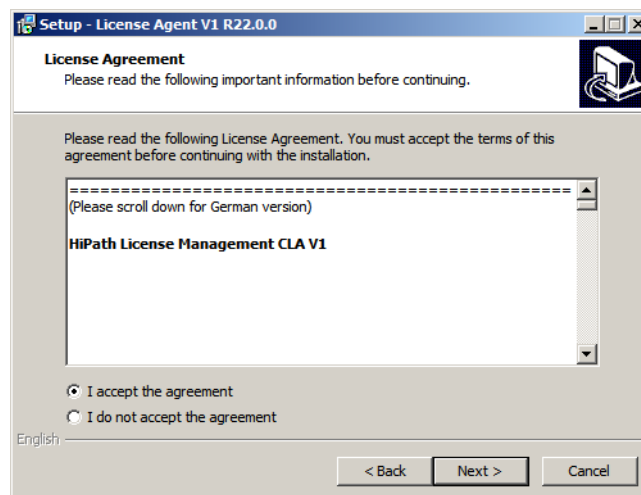
`XpressionsInstall\Prerequisites\HLM\CLA.`

The setup is prepared and the following dialog opened:



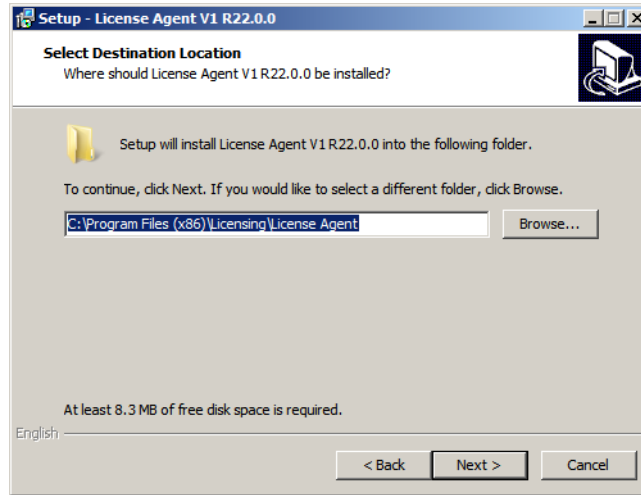
2. Click on **Next**.

Up comes this dialog:



3. Activate the radio button **I accept the agreement** and click on **Next**.

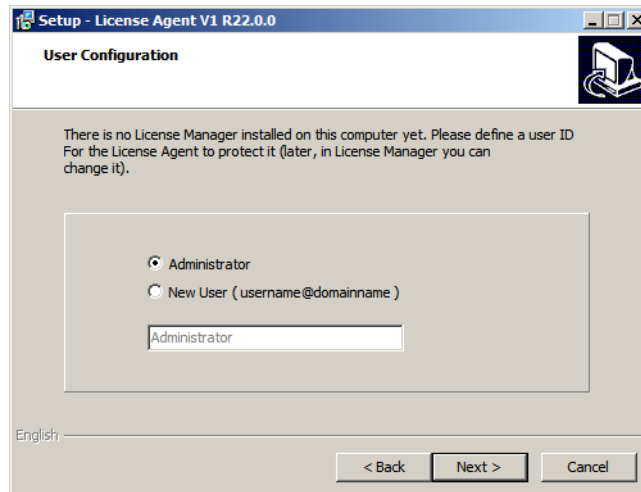
Up comes this dialog:



4. If you want to use the defaulted target folders, click on **Next**.

Via the **Browse...** button you can specify another target folder for the installation. Then, click on **Next** in this dialog.

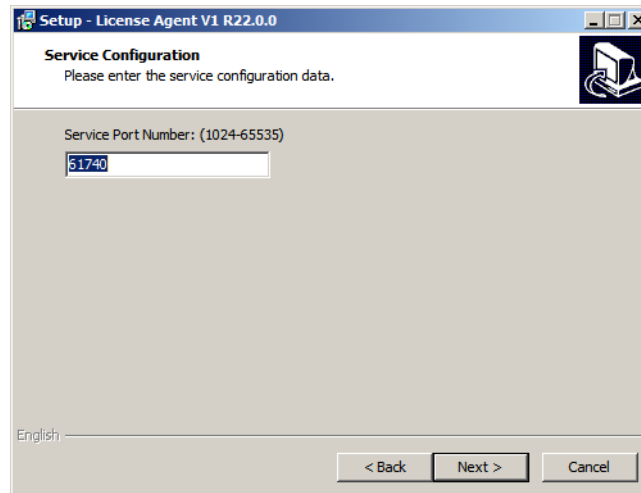
If a CLM is available on the computer on which you install the CLA, continue the installation with [step 6 on page 63](#). If no CLM is available on the computer, the following dialog opens:



5. Select the user under whose account the CLA is to run. If you select the **New User** option, the account under which you perform the installation must have the corresponding privileges on the computer or in the domain.

Click the **Continue** button.

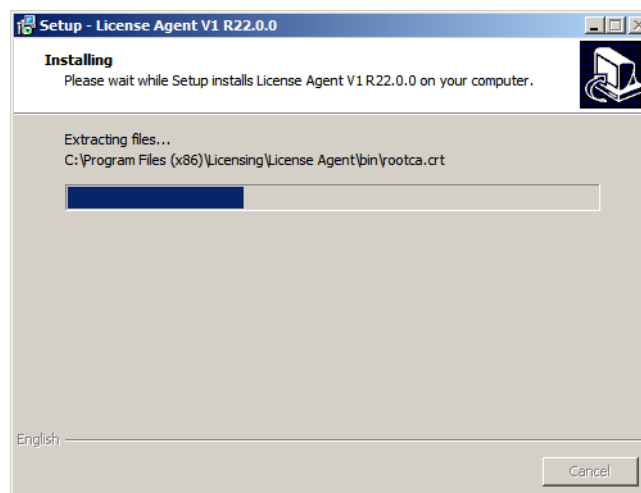
Up comes this dialog:



NOTE: If you change the entry in the **Service Port Number** field you need to enter this modified port number with the license service installation (cf. [Section 4.3.3.1, “Installing the License Service on the local Computer”](#), on [page 72](#), step 5 on [page 73](#)).

6. If you have not changed the ports during the CLM installation, you can copy the settings here. Click on **Next**.

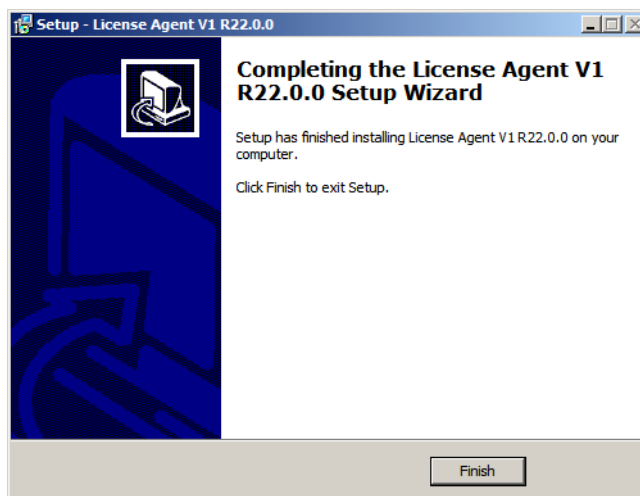
The installation starts and you can see the progress in the following dialog:



As soon as the installation process is complete, the following dialog appears:

XPR System Installation

HiPath License Management (CLM)



7. Click the **Finish** button to complete the installation.
The dialog closes and the CLA installation is complete.

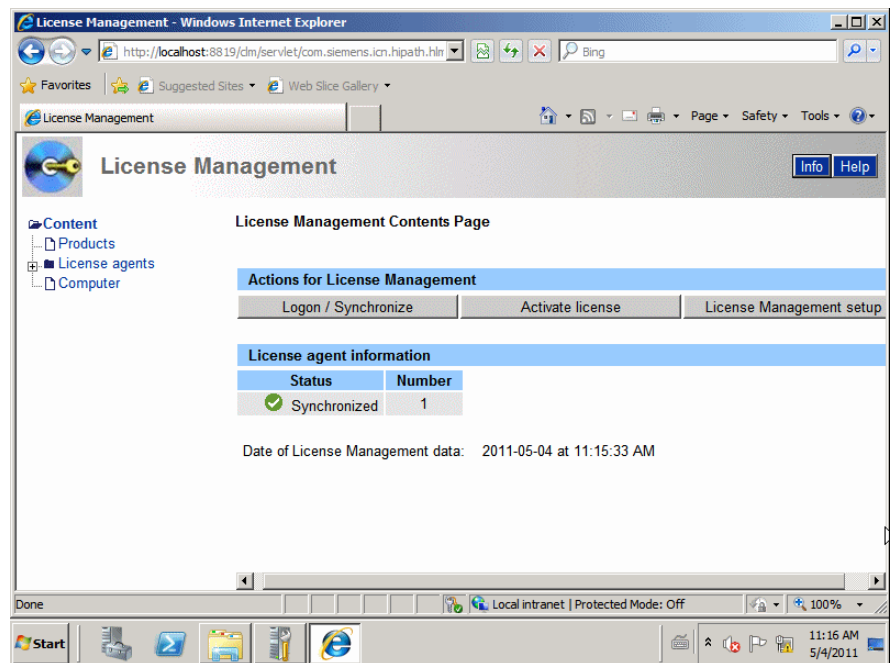
4.2.5 Activating a License

Activating a license means transferring the license file to a CLA so that this can provide the product with the necessary licenses.

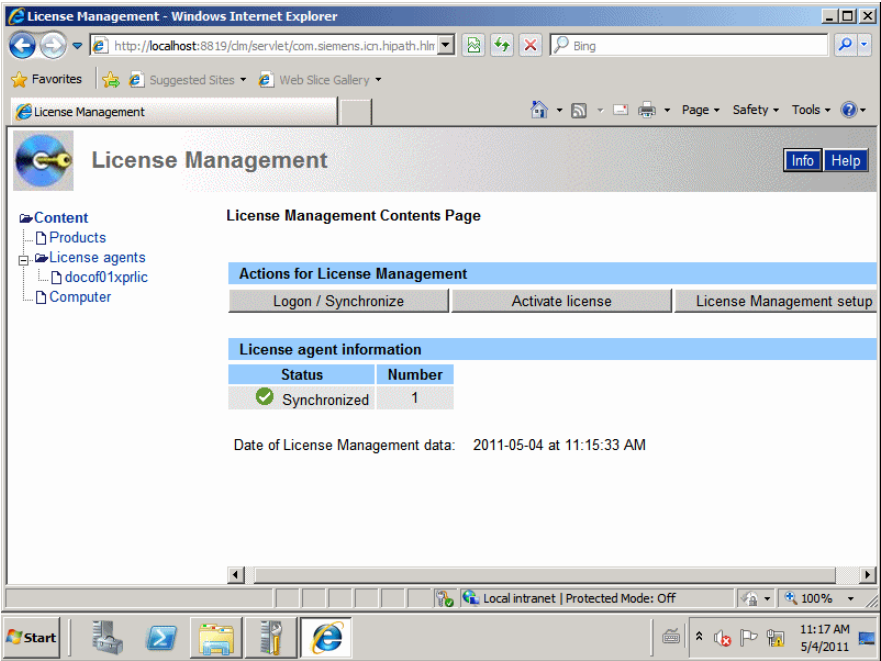
This section describes an example of how to activate licenses. Please obtain details from the operation instructions for the HiPath license management, which you can start via the **Help** button on the interface of the HiPath license management.

If you want to operate several XPR servers, you need to activate an individual license on an individual CLA for each of these servers.

1. Click on the desktop icon created in step 7 on page 60.

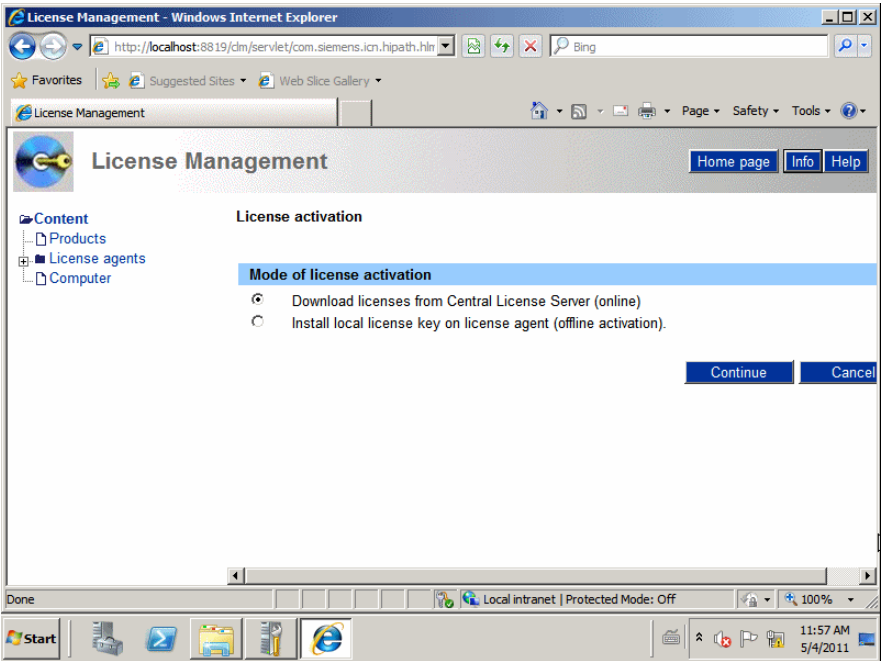


2. Expand the **License agents** entry.

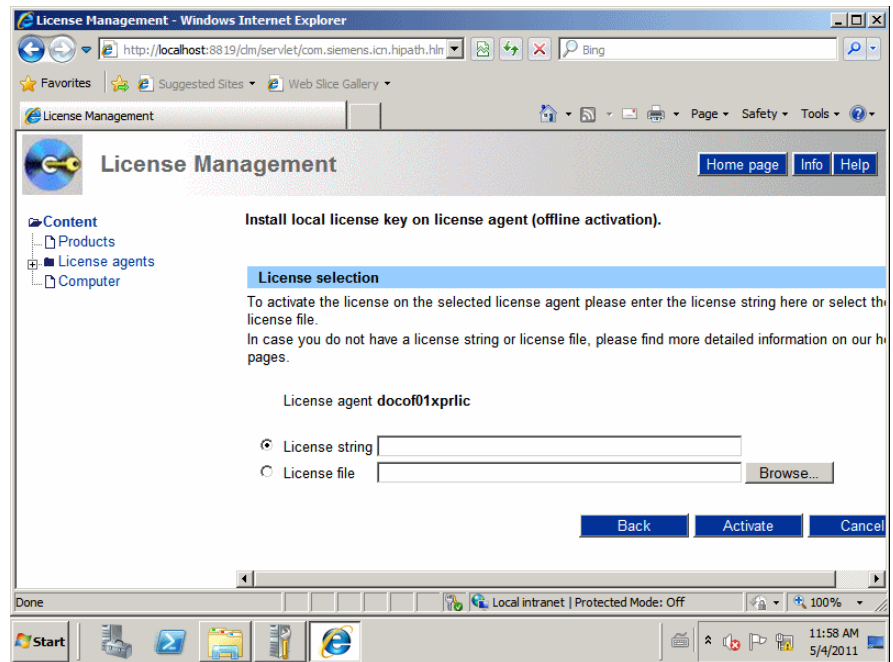


There is a subentry with the name of the computer the CLA is installed on.

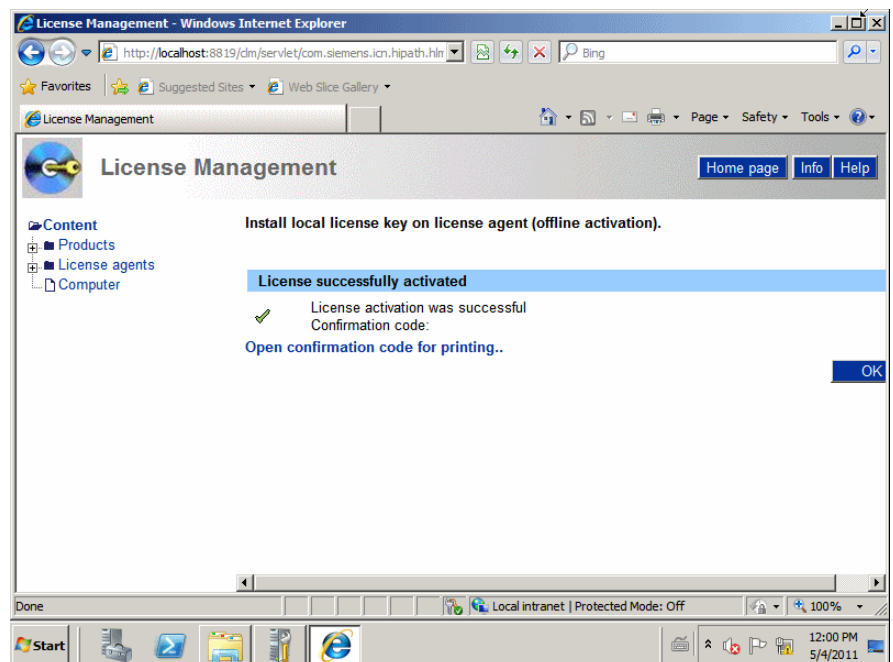
3. Click the **Activate license** button.



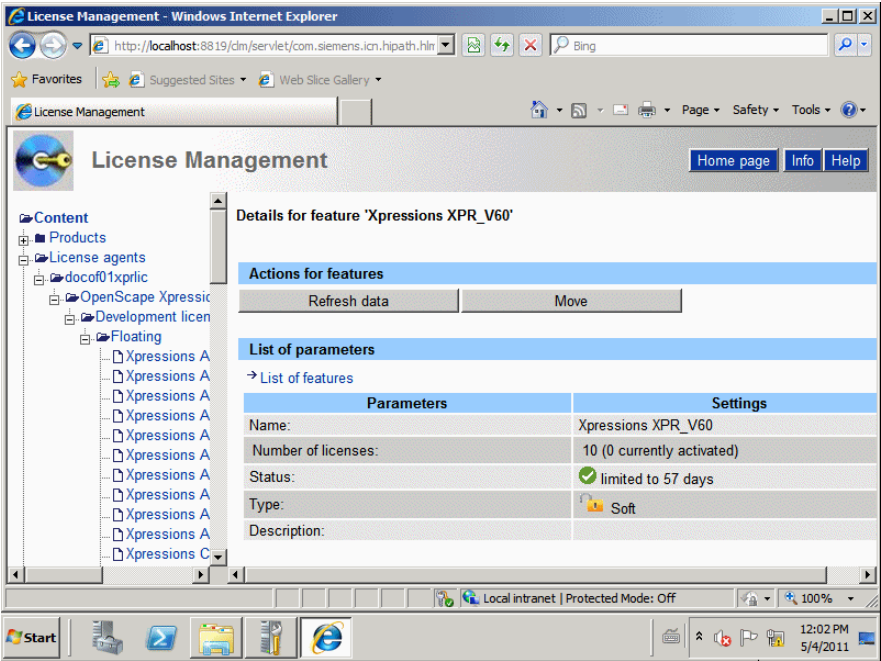
4. You see the offline activation. Click the radio button **Install local license key on license agent (offline activation)**.



5. Activate the radio button **License file**, click the **Browse...** button and select the license file (.lic file).



6. Expand the **License agents** entry to see the licensed features.



4.3 Performing the Initial Installation

This section describes the performance of the initial installation. The sequence of the numbered subsections ([Section 4.3.2, “Settings and Selection of the Components”, on page 70](#) to [Section 4.3.12, “Installing the Dialogic/Eicon Drivers for Communication Hardware”, on page 87](#)) reflects the actual installation process.

4.3.1 Notes for the Installation

Please heed the following notes for the installation:

- Before you begin with the installation, deactivate the antivirus software that has probably been started on the target computer.
- Make sure that a HiPath License Management is available in the network and install a HiPath License Agent before the XPR server installation. Please refer to [Section 4.2.3, “Installing the CLM”, on page 57](#) and [Section 4.2.4, “Installing the CLA”, on page 61](#). If several XPR servers are to be installed successively, one CLA and a separate license must be available for each XPR server.
- The installation sources are shipped on an installation medium. They comprise the XPR server software, drivers, AddOns, client setup programs and the language packages of the supported languages inclusive the text-to-speech (TTS) languages.
- If the target computer does not have an appropriate slot, you can start the installation from any connection shared in the network or from a regular network share.

Installation from a network share

1. First, copy the entire content of the installation medium to a directory on this network share.
 2. Then, start the `setup.exe` file in the `XpressionsInstall` directory on the network share to which you have copied the content of the setup medium.
- In this chapter we assume that no XPR components have yet been installed on the target computer.
 - You can perform a IBM/Lotus Notes integration even if the IBM/Lotus Notes path is not the default path. In this case the IBM/Lotus Notes path must be configured in one of the following two ways.
 - a) The path is entered in the `setup.ini` file of the XPR server setup directory. Example:

[Notes]<

```
NotesIniPath=C:\Program Files(x86)\MyOwnNotes\
```

- b) Path transfer in case of a silent optiClient 130 installation and direct MSI invocation. Example:

```
msiexec /i cyphone.msi  
NOTESINIPATHBYUSER="C:\Program Files(x86)\MyOwnNotes\"
```

NOTE: Please note that the path must be embedded in inverted commas.

In both cases this user-defined path is checked for containing a `notes.ini` file. If the user-defined path does not contain a `notes.ini` file, the path stored in the registry is taken.

optiClient 130 can be set up via this invocation with or without user interface. The installation without user interface requires the parameters `/qb` or `/qn` (see the *OpenScape Xpressions Client Installations* manual).

4.3.2 Settings and Selection of the Components

1. Insert the installation medium in the server computer. If the Autostart mode is active, the Wrapper starts automatically.

NOTE: If the Autostart mode is not active for accessing the installation medium, perform the `Setup.exe` program in the `XpressionsInstall` directory of the setup medium to start the installation. Select the **Run** command in the Windows **Start** menu. A dialog opens. Enter `x:\XpressionsInstall\Setup` in the **Open:** text field, with "x" representing the drive letter of the setup medium or of the installation medium connected via network. Confirm your input with **OK**.

2. The Wrapper checks whether the current **C+Redistributable** is already installed on the computer. The C+Redistributable enables executing programs that were compiled with the current VC compiler.

If the current C++ Redistributable has not been installed yet, all necessary setups (for example interim versions) are started, fully automatically executed and completed.

3. Subsequently the following welcome screen is displayed:



The welcome screen closes after a moment and the installation continues with the license service installation (cf. [Section 4.3.3, "Installing/Connecting the License Service"](#)).

4.3.3 Installing/Connecting the License Service

NOTE: If a license service is already installed, you start the installation with specifying the server name (cf. [Section 4.3.4, "Specifying the Server Name"](#), on [page 76](#)).

All licenses you have purchased are compiled in a file with the extension `*.xml` and obtained via the License Management (cf. [Chapter 3, "Generating Licenses"](#)).

IMPORTANT: After you have received the license file, save it on an external data carrier and protect it from unauthorized access or unintentional deletion.

By means of the license service the installed server components check whether a valid license is available.

Procedure when a CLA computer IP address has been changed

If the IP address of the computer on which the XPR server can reach the CLA changes, this new IP address has to be configured in the XPR server. The IP address of the CLA may, for instance, change, if the XPR server has been set up and configured in a test environment and is then moved to "real-life" environment, or if the CLA is installed on the same computer as the XPR server and this

XPR System Installation

Performing the Initial Installation

computer is assigned another IP address because of the move. In the event that the same CLA is used in the test and "real-life" environment, no adjustment is necessary.

Please proceed as follows to configure the new IP address of the CLA:

1. Open the following file in a text editor:

```
<XPR server directory>\OpenScape\xprlicsvc\HPXPR_V5.0.ccf
```

2. Overwrite the existing IP address in the first line of the file with the IP address of the computer the CLA is running on.

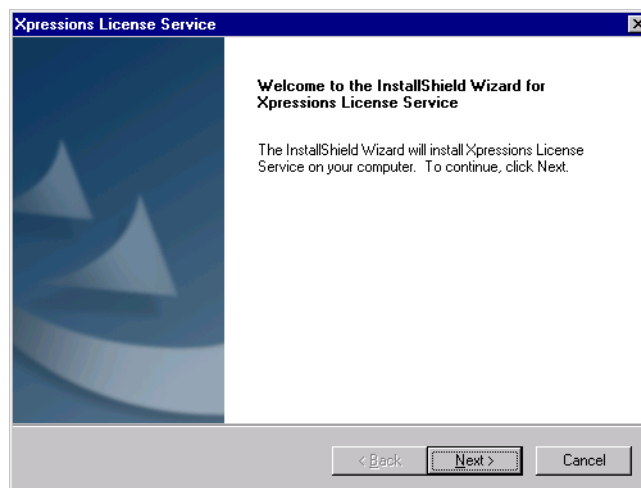
If the CLA in the "real-life" environment uses other ports in than the CLA in the test environment, change the second line respectively. In case of doubt please ask the network administrator for the port.

3. Save your changes and restart the license service on the XPR server computer. Proceed as follows:
 1. Open the Windows service management **Start > Administrative Tools > Services**.
 2. Click with the right mouse button on the entry **XPRLicense Service (licsvc)** and select in the context menu the **Restart** option.

4.3.3.1 Installing the License Service on the local Computer

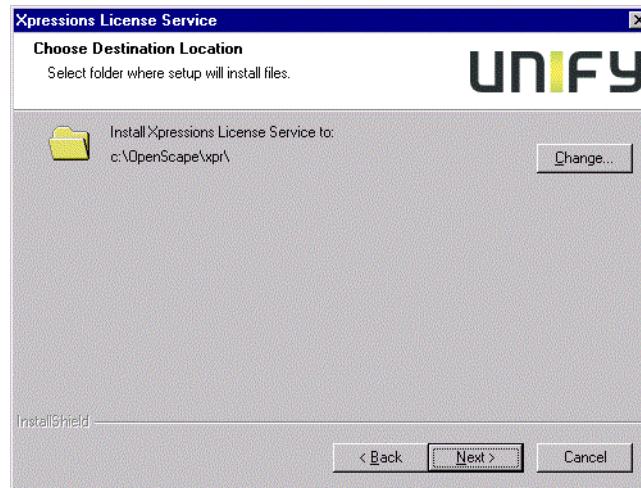
How to install the license service on the local computer:

1. Select the **New license service installation** option.
2. Click on **Next**. The license service installation routine starts and the following dialog opens:



3. Click on **Next**.

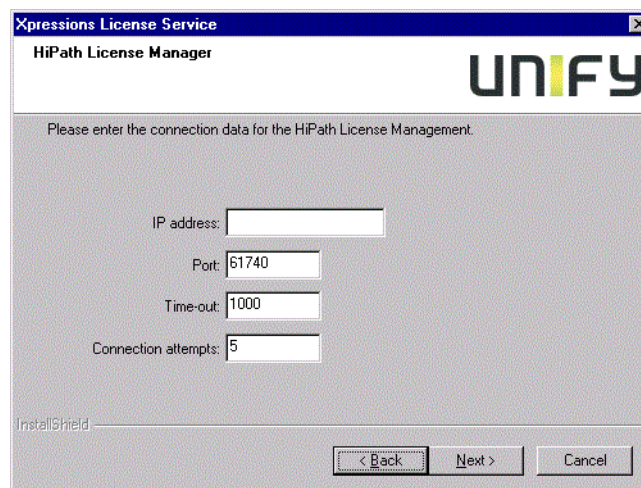
Up comes this dialog:



4. Accept the defaulted target path for the installation or click the **Change** button to specify another installation target path. Click the **Continue** button.

NOTE: We recommend to copy the default.

Up comes this dialog:



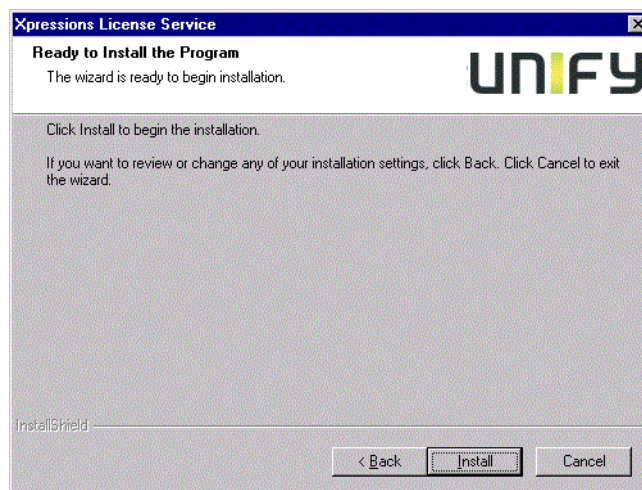
5. In the **IP address** field specify the IP address of the computer on which the CLA for this XPR server runs. Click the **Continue** button.

If you have not changed the ports during the CLM installation, you can copy the settings for the port here. The time-out in the **Time-out** field is specified in milliseconds.

Up comes this dialog:

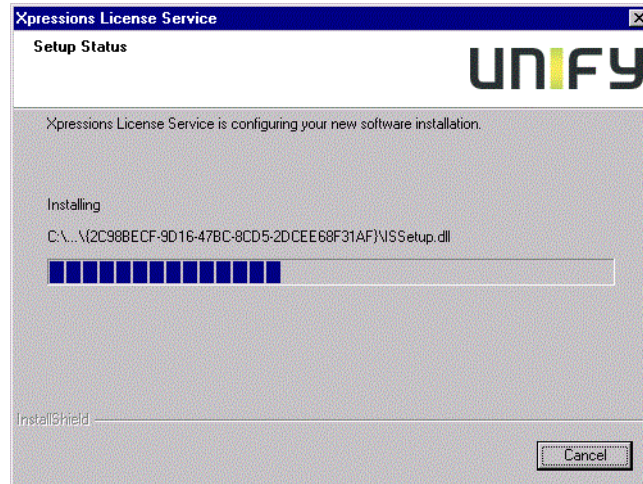
XPR System Installation

Performing the Initial Installation

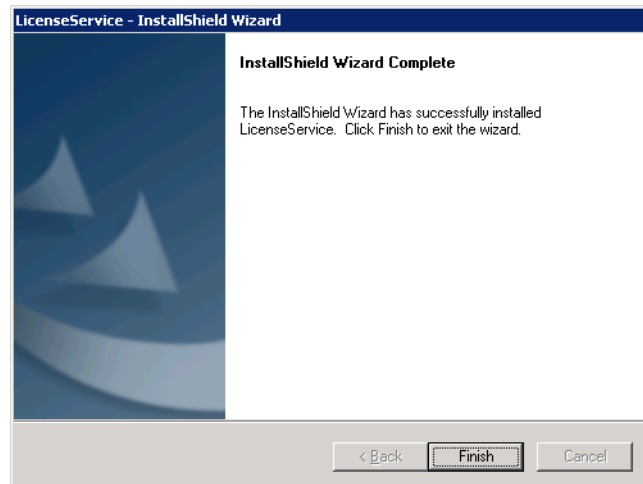


6. Click the **Install** button.

The license service installation starts. The installation progress is displayed in the following dialog:

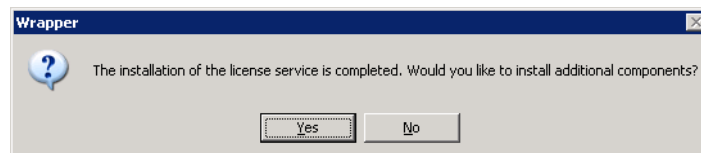


7. After the copying process has been completed, the following dialog opens:



8. Click on **Finish**.

Up comes this dialog:



9. Click **Yes**, if you want to install further components, such as the XPR server software.

Click **No**, if no further software is to be installed besides the license service.

Subsequently, the wrapper starts automatically.

The installation continues with entering the server name (cf. [Section 4.3.4](#), “Specifying the Server Name”).

4.3.4 Specifying the Server Name

NOTE: If the C++ Redistributable and the license service have already been installed, the installation of further components starts with this step.

When you select the server name, heed the following points:

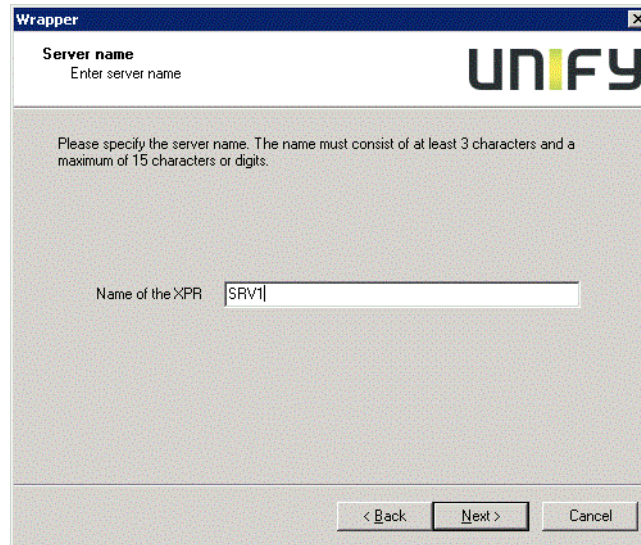
- the name you enter here **cannot be modified any more**.
- the name must not contain blanks, special characters such as ;, !, %, &, ... , or German umlauts (ä, ö, ü).

IMPORTANT: if a remote system link is used, the server name **must not** contain a hyphen (-)!

- you must not use names of logical XPR lines. For example: *PhoneMail*, *VMS*, *ERGO*, *COM*, *CON*, *FAXG3*, *FAXG4*, *MWI*, *FOD*, *PlayWave* and *SMTP* will not be accepted.
- The XPR server name must not exceed a length of 15 characters. If you want to connect the XPR server to another XPR server via a Remote System Link, then the XPR server name must not exceed a length of 11 characters.

NOTE: Remote System Link is not compatible with [Crypt_Sec], it is designed to only work with [KRYPT].

1. Up comes this dialog:



2. Enter the desired server name in the **Name of the XPR** field.
3. Click on **Next**.

The installation continues with the selection of the server languages that are to be installed (cf. [Section 4.3.5, “Selecting the Server Languages and the Default Language”](#)).

4.3.5 Selecting the Server Languages and the Default Language

If Russian or Turkish is intended to be the XPR server default language, the language setting for non-Unicode programs should be adjusted in the operating system before the installation. Please read section [Russian or Turkish as XPR Server Default Language](#) on page 29 as well as [Section 2.1.7, “Language Settings for Non-Unicode Programs”](#), on page 34 on this.

All languages supported for the XPR server are supplied in one language packet each. Each language packet contains the necessary files to provide, for example, the Web Assistant or the voice mail system in the corresponding language.

The following languages are available:

- German
- British English
- US-English
- French
- Italian

XPR System Installation

Performing the Initial Installation

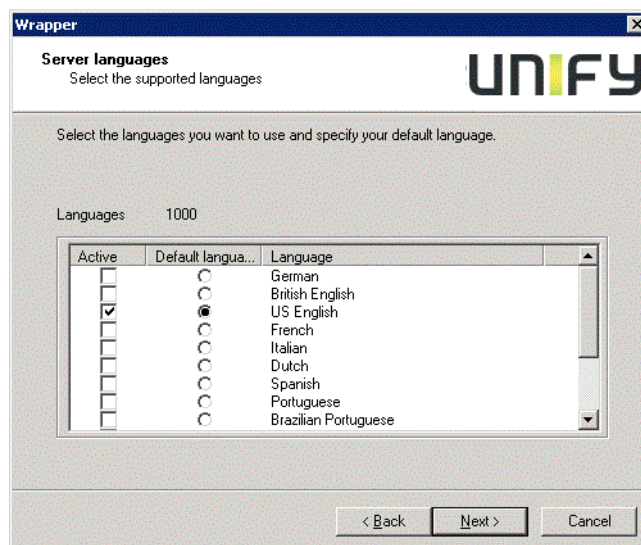
- Dutch
- Spanish
- Portuguese
- Brazilian Portuguese
- Russian
- Turkish
- Spanish (USA)
- Canadian French
- Slovenian
- Catalan

The dialog shows all available language packets. On top of the list you can see the number of purchased language licenses. One language license is valid for an arbitrary language.

The default language selected here is also the greeting default language of the voicemail systems **PhoneMail**, **VMS**, **Ergo**, and of the **Web Assistant**.

If further language packets are installed, the users can switch the Web Assistant as well as the TUI to one of these languages. When a new user logs on to the Web Assistant for the first time, the Web Assistant and the TUI interface feature the default language selected here.

1. Up comes this dialog:



2. In the **Active** column select the languages to be installed. Only select as many languages as licenses are available.

NOTE: You need to select at least one language in order to continue the installation.

3. In the **Default language** column select the language that the XPR server is to use as default.
4. Click the **Continue** button.

The installation continues with the confirmation of the Release Notes (cf. [Section 4.3.6, “Confirming the Release Notes”](#)).

4.3.6 Confirming the Release Notes

In the Release Notes you find among other things information about the following topics:

- Build number of the software
 - General hardware requirements
 - The latest upgrade information
 - New-feature descriptions
 - Bug fix descriptions
 - Test scenario descriptions
 - Compatibility list
1. Up comes a dialog that represents the `ReleaseNotes.rtf` file, which is found in the `XpressionsInstall` directory of the setup medium.
 2. Please read the Release Notes. Via the **Open in external viewer** button you can open the corresponding file in the application that is registered in the operating system for the file type *RTF*.
 3. Select the **I have read the Release Notes** checkbox. This activates the **Next** button.

If you do not select the check box, the **Next** button stays inactive and you cannot continue the installation.

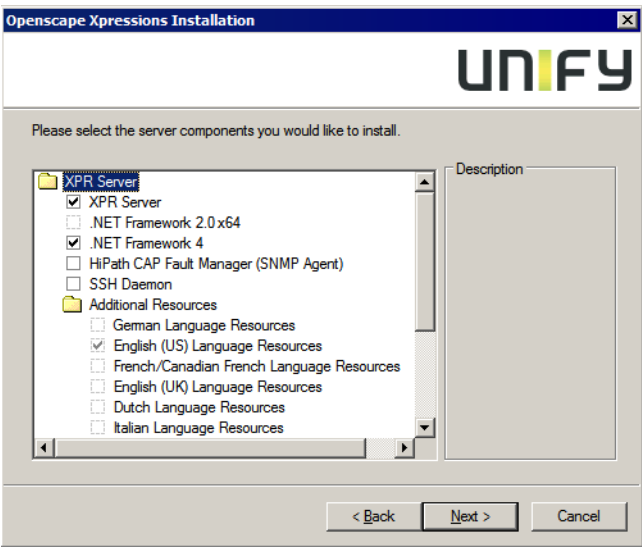
4. After you have read the Release Notes, click on **Next**.

The installation continues with the selection of the system components (cf. [Section 4.3.7, “Selecting System Components”](#)).

4.3.7 Selecting System Components

In this step you select the components of the XPR system to be installed. These include the actual XPR server software as well as additional resources, such as language packets and administrative components.

1. Up comes this dialog:



Language packets that you have already selected in [Section 4.3.5, “Selecting the Server Languages and the Default Language”](#) are indicated in this dialog. The checkbox that you have activated for the default language there is displayed here in gray and cannot be deselected.

2. Select the components to be installed.

In the following table you find descriptions of the components:

Server Component	Description
XPR server	If you select this option, the Wrapper starts the XPR server installation (cf. Section 4.5.1, “Selecting Features”).
.NET Framework 2.0x64	This option installs the .NET Framework 2.0x64. Note: This option is only active if no .NET Framework 4 is available for selection.
.NET Framework 4	This option installs the .NET Framework 4. Note: If you wish to install the web conference server on Windows Server 2008 at a later date, .NET Framework must be activated and installed.

Table 5 Server Components

Server Component	Description
HiPath CAP Fault Manager (SNMP Agent)	Installs the HiPath CAP Fault Management, which evaluates error messages and error logs of the XPR system. The SNMP service of the operating system must be installed for this purpose. You find information on the SNMP service in the Windows Server 2008 documentation. See Section 4.5.16.2, "Installing the HiPath CAP Fault Management" , on page 154.
SSH Daemon	Service that lets the service personnel of the Unify GmbH & Co. KG securely access this system for remote maintenance. Note: SSH Daemon is not installed if the Smart Services Delivery Platform (SSDP) is set up.
Additional resources	Here you may select additional language packets for the web interface and/or the telephone user interface of the voice mail system.
Communications	Starts the setup of the Communications client, which can be used as administrative client of the XPR server (not for the U.S.).
Exchange 2003 Administration (MMC Snap-In)	Installs the expansion (Snap-In) of the Microsoft Management Console (MMC), which is displayed for the administration of the XPR-specific user data and the connector in the Active Directory. The snap-in is only used in connection with setting up an Exchange 2003 gateway and can be used on any computer that hosts the Exchange System Manager. We do not recommend the installation of the SnapIn in combination with Outlook and the Outlook extensions on the Exchange server. The Exchange 2003 MMC Snap-in displays the XPR-specific administration dialogs for users (under Active Directory Users and Computers) and the connector (in the Exchange System Manager).

Table 5 Server Components

3. Click on **Next**.

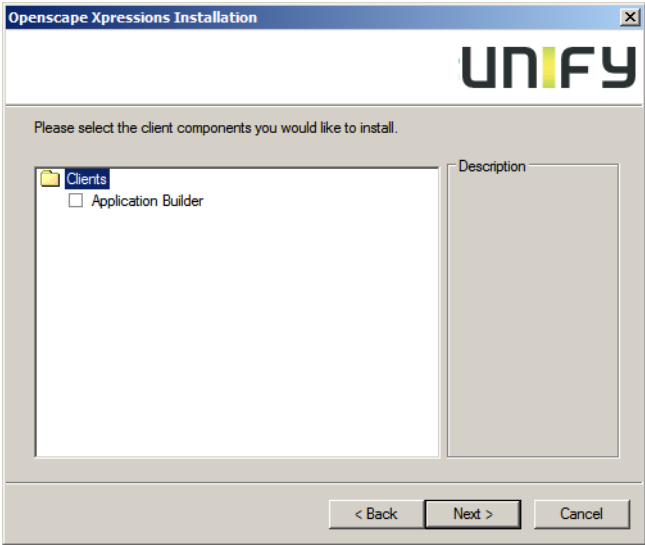
The installation continues with the selection of the client applications (cf. [Section 4.3.8, "Selecting Client Components"](#)).

4.3.8 Selecting Client Components

The client components include the Application Builder. In this dialog you may select the client applications that are to be installed on your computer after the XPR server setup.

Which components are offered here depends on the purchased licenses.

1. Up comes this dialog:



2. Select the desired client components via the corresponding checkbox.

Please heed the following table with short component descriptions:

Client Component	Description
Application Builder	The <i>Application Builder</i> is an administrative application enabling the creation of voice menu applications that can be played to a caller. The voice menu applications that have been created may be used as Automated Attendant and IVR solutions.

Table 6 Client Components

3. Click on **Next**.

The installation continues with the selection of external software (cf. [Section 4.3.9, “Selecting External Software”, on page 83](#)).

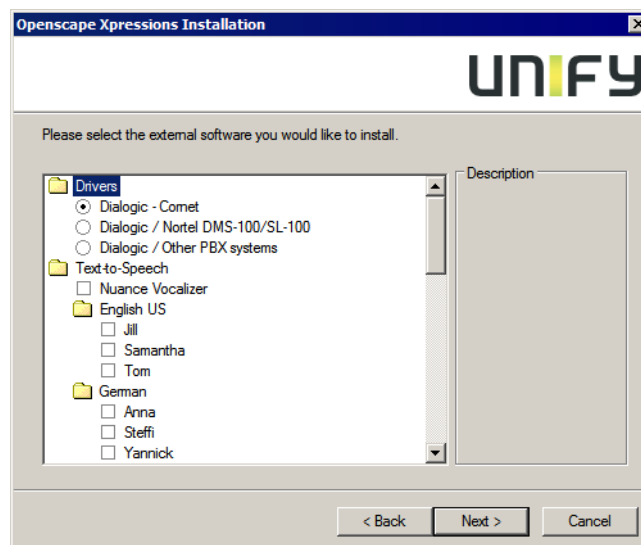
4.3.9 Selecting External Software

As external software the driver for communication hardware (ISDN card) by Dialogic/Eicon as well as text-to-speech software (Nuance Vocalizer for Networks 5) is available.

The software selected here is installed on the computer before the XPR server setup.

NOTE: The Dialogic/Eicon drivers must be set up manually and **before** the XPR server installation (cf. [Section 5.1, “Installation and Configuration of the Sangoma Diva\(R\) ISDN Boards”](#), on page 177).

1. Up comes this dialog:



2. Use the check boxes to select the external software that you want to install.

XPR System Installation

Performing the Initial Installation

3. In the **Drivers** section select the PBX that the XPR server is to connect to.
The following PBX systems are available:

Communication system	ISDN board	Prot./IP	Driver software
OpenScape Voice - SIP	—	IP	internal SIP stack of the IP APL
HiPath 3000 - CorNet IP	—	CorNet-IP	H.323 stack of the IP APL
HiPath 4000 - CorNet IP	—	CorNet-IP	H.323 stack of the IP APL
Hicom 300 US	Dialogic/ Eicon	CorNet-T	Dialogic DIVA driver and configuration software as of version 8.0.
Hicom 300 (outside of the USA)	Dialogic/ Eicon	CorNet-N	Dialogic DIVA driver and configuration software as of version 7.x.
HiPath 3000 - Eicon	Dialogic/ Eicon	CorNet-N	Dialogic DIVA driver and configuration software from version 7.x as well as TAPI Service Provider.
HiPath DX	Dialogic/ Eicon		Dialogic DIVA server
HiPath 4000 - Eicon	Dialogic/ Eicon	CorNet-N(Q)	Dialogic DIVA driver and configuration software as of version 7.x.

Table 7 Matrix Communication System - Drivers

Depending on your selection, options will already be selected in future dialogs.

4. In the **Other PBX systems (DSS-1, QSIG, VMle)** section select a communication system if the table in step 3 does not list your communication system.
5. In the **Text-to-Speech** section select whether the text-to-speech software *Nuance Vocalizer for Networks 5* shall be installed.

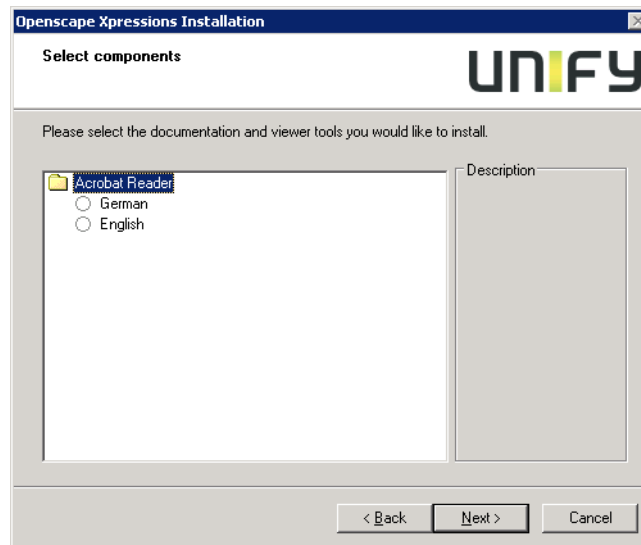
NOTE: The installation requires a corresponding text-to-speech license for the XPR server as well as a Nuance Vocalizer for Networks 5 license. Please also note [Section 4.1.1, “Text-to-Speech Engine Nuance Vocalizer for Networks 5”](#), on page 50 for operating *Nuance Vocalizer for Networks 5*.

6. If you have selected *Nuance Vocalizer for Networks 5* in the **Text-to-Speech** section, select in the language sections the names of the TTS voices to be installed.
7. Click on **Next** to confirm your selection.

The installation continues with the Adobe Reader setup (cf. [Section 4.3.10](#), “Installing the Adobe Reader”).

4.3.10 Installing the Adobe Reader

1. Up comes this dialog:



2. Select here the respective language version for the viewer (Adobe Reader).
3. Then click **Install**.

At this point the Wrapper has all information required for starting the installation of the selected components.

If you have an Automatic Speech Recognition (ASR) license, the dialog features the **Next** button instead of **Install**. Click it to continue the installation with the determination of the installation type for ASR (cf. [Section 4.3.11](#), “Installation Type for Automatic Speech Recognition”, on page 85).

If you do not have an ASR license, the setup continues with the XPR server installation and the service configuration (cf. [Section 4.5](#), “Installing the XPR Server and Configuring the Services”, on page 90).

4.3.11 Installation Type for Automatic Speech Recognition

NOTE: This installation step is only displayed when you have an ASR license.

The ASR server can be installed with the XPR server on one common computer or on two individual computers.

Common computer

This increases the load on this computer since two servers must be operated at the same time. If, however, the hardware is sufficiently dimensioned, this solution may lead to a speed advantage, since the communication between both servers can be handled within the system and not via network.

Individual computer

Here, ASR is implemented with the installation wizard as ASR server, and the XPR server as ASR client. This distributes the load among two computers, but the speed of the communication between ASR server and XPR server depends on the LAN connection performance.

The following options are available:

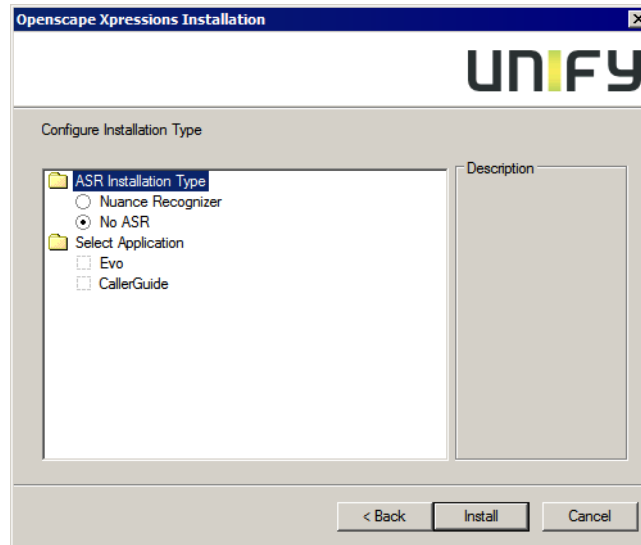
ASR installation type	
• ASR Client	Installs the ASR client for operation with an already installed ASR server. An ASR client can be installed on the same computer on which the XPR server is already installed.
• No ASR	Does not install any ASR components. Select this option after you have already installed the ASR components correctly and only additional XPR applications need to be installed.

Table 8 ASR Installation Types

Applications	
• EVO	Installs the <i>EVO</i> protocol.
• CallerGuide	Installs the <i>CallerGuide</i> protocol.

Table 9 ASR Applications

1. Up comes this dialog:



2. For installation, select the ASR setup type **Nuance Recognizer** or **no ASR**.
3. Select the ASR applications to be installed.
4. Click the **Install** button.

The installation of the selected components starts.

Depending on whether you have selected the **Dialogic hardware driver** (cf. [Section 4.3.9, “Selecting External Software”, on page 83](#)), this component will be installed first:

- cf. [Section 4.3.12, “Installing the Dialogic/Eicon Drivers for Communication Hardware”, on page 87](#) for the installation of the Dialogic/Eicon hardware driver

If you have not selected a Dialogic/Eicon hardware driver, the setup continues with the XPR server components installation and the services configuration (cf. [Section 4.5, “Installing the XPR Server and Configuring the Services”, on page 90](#)).

4.3.12 Installing the Dialogic/Eicon Drivers for Communication Hardware

If you have selected the Dialogic/Eicon hardware driver in [Section 4.3.9, “Selecting External Software”, on page 83](#), the installation of this component starts now.

NOTE: A manual, retrospective setup of the drivers is required.

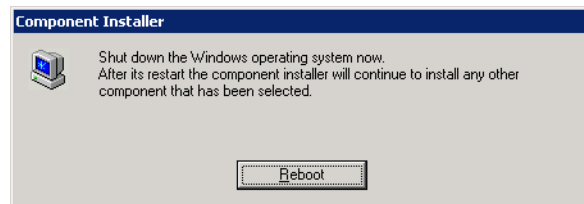
XPR System Installation

Performing the Initial Installation

Please read [Chapter 5, “Installing and Configuring the Driver Software”](#) about the installation and configuration of the Dialogic/Eicon hardware driver for communication hardware. After the driver installation, continue with [Section 4.4, “Installation of the Microsoft .NET Framework”](#), on page 89.

IMPORTANT: Do not reboot after the installation! Your answer to the corresponding dialog is: **No, I will restart my computer later.**

Do not reboot until the component setup program asks you to do so via the following dialog:

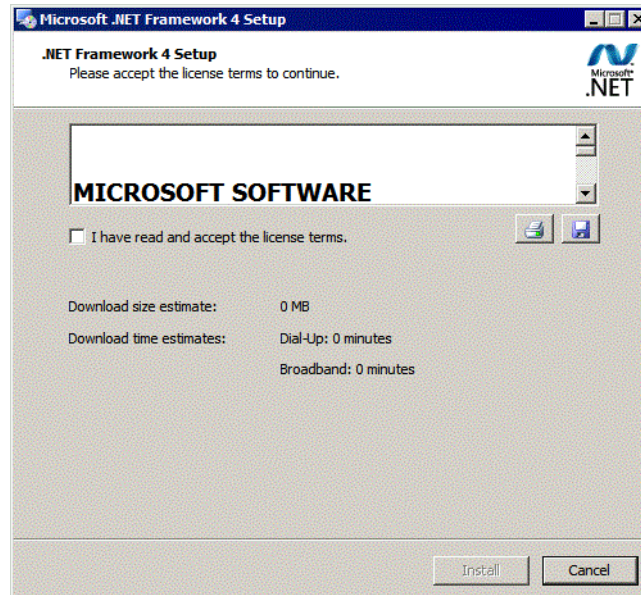


If you have not selected a driver, please continue with [Section 4.4, “Installation of the Microsoft .NET Framework”](#).

4.4 Installation of the Microsoft .NET Framework

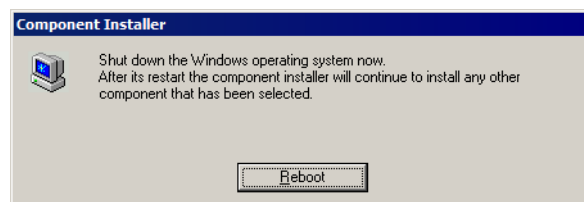
NOTE: Depending on the selected components, the installation of Microsoft .NET Framework may move within the setup procedure.

1. The setup wizard for the Microsoft .NET Framework 4 starts. The enduser license contract is displayed.



Activate the **I accept the terms of the License Agreement** checkbox and click on the **Install** button.

The system must be rebooted after the .NET Framework installation.



2. Click on the **Reboot** button.

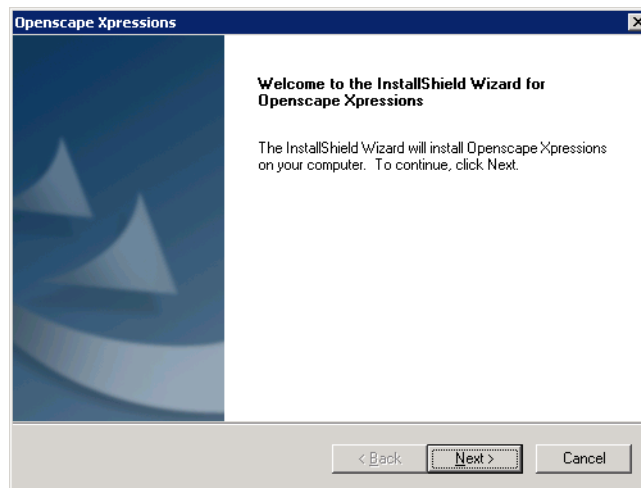
The system is rebooted. The setup process continues automatically.

4.5 Installing the XPR Server and Configuring the Services

After you have selected the desired components for installation in [Section 4.3, “Performing the Initial Installation”](#), on page 69, the corresponding services and software packets will now be installed.

NOTE: Via the **Cancel** button you may end the installation in all dialogs prematurely.

1. Up comes this dialog:



2. Click on **Next**.

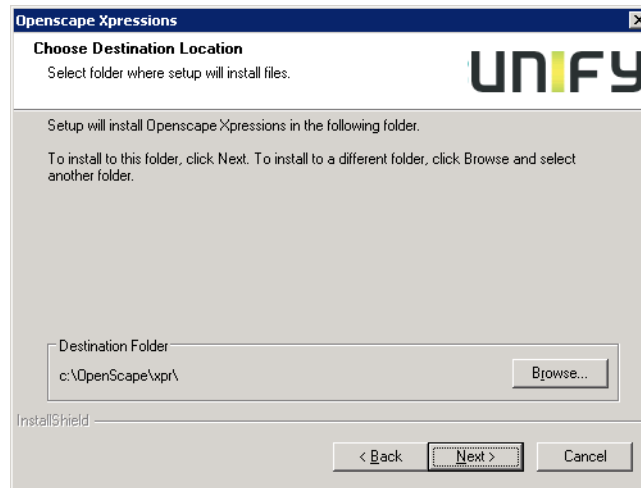
Up comes this dialog:



The **End User License Agreement (EULA)** is displayed. Choose the **I accept the terms of the license agreement** option. If needed, print the EULA to be able to read it properly.

3. Click on **Next**.

Up comes this dialog:



4. Check whether the defaulted target folder is on the largest available partition. In this case you can copy the value defaulted in the dialog.

If the defaulted target path is not on the largest available partition, find a folder on the largest available partition via the **Browse...** button.

IMPORTANT: Be sure that the partition on which the XPR server software is installed has a minimum size of 10GB. The target path must not contain any blanks (e. g. c:\OpenScape Xpressions\xpr!).

5. Then click on **Next**.

The installation continues with the selection of the features that are to be installed (cf. [Section 4.5.1, “Selecting Features”, on page 91](#)).

4.5.1 Selecting Features

Based on the entered license keys and the hard and software installed in your computer, the setup wizard determines which components and services can be displayed and selected for installation in this dialog.

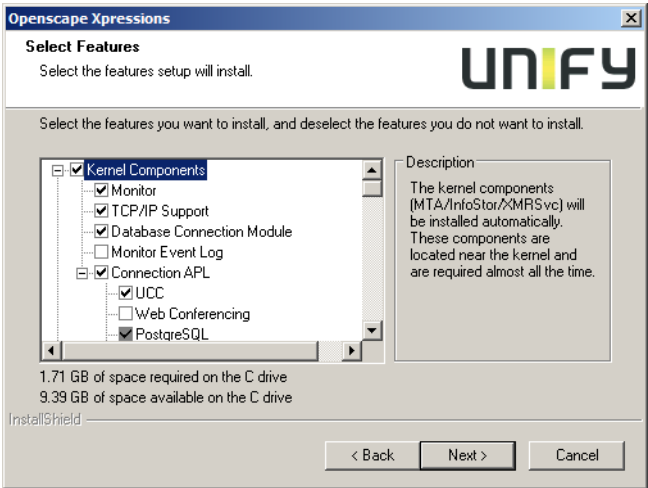
For example, if no ISDN card and no associated driver were available, the corresponding *ISDN Hardware* option, which assumes the existence of such hard and software, would not be automatically selected.

A component is also not displayed if an invalid license has been entered.

The XPR system components are thematically grouped. A group can be opened via the plus sign to display the components contained therein, and also be closed via the minus sign. Components indicated with a tick will be installed.

A component is selected with a mouse click on the box that precedes the entry. A mouse click on an already selected component cancels the selection, and consequently, this component will not be installed.

1. Up comes this dialog:



2. Select the components to be installed. The component selection is divided into the following groups.

In the following table you find information about all server components and services.

Kernel components group	
Monitor	The XPR monitor serves to supervise the status and performance of the single XPR server components, and to display possible malfunctions. Furthermore, the single components are configured via the XPR monitor. The XPR monitor should always be installed. You can start the installed XPR monitor also later from a different Windows computer connected in the network. The corresponding installation directory is provided as “MRS Mon” sharing on the server computer for this purpose.
TCP/IP Support	The installation of this network protocol is the basic requirement for the connection of the XPR clients with the server computer.
Database Connection Module (DB APL)	The database connection module 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 corresponding data sources. ADO is used for this purpose, which can also use already configured ODBC drivers for data source queries.
Monitor event log	This software component is installed without any further interaction with the user. The application is entered in the list of APLs to be automatically started by the server.

Table 10 Feature List

Notification Module (NOT APL)	The Notification module is used for sending server-generated notifications about newly arrived messages (e-mail, fax or voicemail) to devices. Notification can be via MWI, SMS or a voice mail system call (User Outcall).
Connection APL	APL to enable an RPC communication via the XMLRPC protocol between the XPR and Java programs • UCC This option installs the Media Server required for voice conferencing. The voice conference service is also a requirement for scheduling web conferences. • Web conference server This option installs the web conference server. • PostgreSQL This option installs the PostgreSQL database server. • OpenScape Web Client This option installs the OpenScape Web Client. Attention: The OpenScape Web Client must not be installed if the XPR is or is to be integrated in a ComAssistant. Attention: If the web conference server is to be installed on a computer in a demilitarized zone (DMZ), the Web Conference Server option must not be selected here. The options UCC and PostgreSQL however must then be selected. To install the web conference server please follow the instructions given in Section 4.5.22, "Voice Conferences with SIP", on page 165.
Services group	
Web server	• Web Assistant Using the Web server module you can install the web-based Web Assistant application, which enables users to access their mailbox via Web browser. Furthermore, the Web Assistant offers comprehensive configuration options for the components of the XPR system. • IppAssistant Xpressions client IP-Phone assistant for telephone OpenStage 60 or 80. Please refer to Section A.5, "Installation and Configuration of the IppAssistant", on page 222. • System Info SNMP Agent Installs the OpenScape Xpressions System Info SNMP Agent. This agent provides various system information via the SNMP protocol. Such information can thus be displayed in the CMP. Requirement is an installed Windows SNMP service. More details are provided in the manual <i>Server Administration</i> in section <i>SNMP Agents</i>.

Table 10

Feature List

XPR System Installation

Installing the XPR Server and Configuring the Services

Internet E-mail Server (SMTP APL)	Besides the SMTP (Simple Mail Transfer Protocol) service the SMTP APL provides further services for sending and receiving e-mails via the Internet. The SMTP APL supports the protocols SMTP, POP3, IMAP4 and VPIM (to network voice mail servers). The SMTP APL requires a TCP/IP network protocol and a connection to the Internet on the computer. Furthermore, the Windows proprietary SMTP server must be uninstalled before the installation of the XPR system (see Section 2.1.3, "Checking Windows 64-bit Server Settings", on page 29).
Fax Server (ISDN APL)	Fax-on-Demand This option allows you to install a fax-on-demand server module. This module can be added as protocol within a Telematic APL. Subsequently, corresponding fax polling documents can be deposited.
Voicemail server	A voicemail server is an IVR application, which is integrated in a Telematic APL as protocol. The following voice mail servers can be directly installed via the setup program: Note: PhoneMail, VMS and ERGO must not be installed parallel in the languages D, US and UK. • Unified Messaging Voicemail (ERGO) ERGO is the most modern type of a voicemail server and particularly used for True Unified Messaging (cf. <i>ERGO Voicemail System</i> manual). • PhoneMail telephone user interface PhoneMail as a telephone user interface is based on the PhoneMail originally developed on its own hardware in the US (cf. the <i>OpenScape Xpressions PhoneMail</i> manual). • VMS VMS as a telephone user interface has been developed from the hardware based Hicom 300 version (cf. <i>OpenScape Xpressions VMS Voicemail System</i> manual). • Voicemail (AMIS) AMIS is an analog protocol for exchanging voicemails between voicemail servers. • Conversion of text to speech Provides transcriptions of voice recordings via "voicemail to text". The transcribed text is sent along with the voicemail.
Pager	Supports sending notifications to a pager.
Voice guide	Installs the VOGUE script that enables the automatic realization of a telephone exchange (Automated Attendant) as well as the generation of IVR applications, which allow controlling user functions by voice or dial tones (DTMF).
Web Service Provider	SOAP web service provider (XML APL)
Single Number	The Single Number feature can be used to reach the fax, voice and telephone numbers of a user via one single number.

Table 10

Feature List

Short Message Service	Installs the SMS Connector that enables sending and receiving SMS messages.
Telematic hardware group (This selection is only displayed if the corresponding drivers have been installed.)	
ISDN Hardware (ISDN APL)	The installed Dialogic/Eicon ISDN boards are addressed by the ISDN hardware. Digital FaxG4 as well as analog FaxG3 is possible. A fax polling server can also be installed. Further options are voice mail server and XPR server/server interconnection via ISDN. • Fax G3 Post Dial The FaxG3PD script enables sending fax documents to addresses with automated attendant solutions, even if extension information (direct inward dialing) is not available at the receiving station. Be sure to execute the steps described in Section 4.5.19, "Checking Fax G3 Post-Dialing", on page 159 after the XPR setup.
IP telephony (IP APL)	Voice-over-IP connection. Here, IVR applications can be linked with extension numbers, which are then addressed via Voice-over-IP. An IP APL can be operated in parallel to an ISDN APL on one computer. One IP APL cannot support two protocols of the infrastructure layer (e. g. H.323, CorNet-IP or SIP) in parallel. But the following scenarios are possible, for example, provided the protocols mentioned are supported by the connected PBX: • Parallel operation of Voice via H.323 and T.38 Fax via H.323 • Parallel operation of Voice via SIP and T.38 Fax via SIP You find details on this in the <i>OpenScope Xpressions Server Administration</i> manual.
IP-/PBX integration group	
CTI Computer Telephony Integration	CTI APL Connection for CTI client applications to divers PBXs (see hardware compatibility list). This normally implies that the CTI link of the PBX is released and the corresponding CTI driver, probably to be obtained from the PBX manufacturer, have been installed beforehand.
Alcatel 4400 ABCA Protocol	ABC APL This APL enables Message Waiting Indication (MWI) at an Alcatel 4400 PBX via the ABC-A protocol of Alcatel.
CSTA protocol	This option installs the CSTA protocol interface.
Messaging and directory integration group	
LDAP Directory Synchronization	The LDAP directory synchronization must be installed for using the Active Directory Service in connection with the Microsoft Exchange 2003 Connector respectively Microsoft Exchange 2007 Connector.
MS Exchange 2003 Connector	This component represents the gateway to Microsoft Exchange 2003.

Table 10

Feature List

XPR System Installation

Installing the XPR Server and Configuring the Services

MS Exchange TUM Connector (ExUm APL)	Additional connector that allows True Unified Messaging with a Microsoft Exchange 2003 or 2007 connection.
Lotus Notes Gateway (LnAPL)	These files contain the actual gateway to IBM/Lotus Notes. This gateway requires an installed IBM/Lotus Notes client of version 6 or later on the XPR server. Attention: Before you install the Lotus Notes gateway, execute procedures described in the installation and administration manual <i>OpenScape Xpressions IBM Notes Gateway</i>.
Lotus Notes True Unified Messaging Gateway (LnUmAPL)	Additional connector that allows True Unified Messaging with a IBM/Lotus Notes connection.
MS Exchange Foreign Connector	This component represents the gateway to Microsoft Exchange 2010.
HiPath User Administration & Fault Management group	
User administration with HPM-UM	This component implements the user administration with the HiPath User Management With the help of the HiPath User Management System (HPM-UM) user data can be administered and stored independent of their data format.
Presence support group	
Presence APL	The presence feature informs you about the system, telephone and work state of selected users and you can let other users know your work state. The Presence APL is also required for the web conference server and instant messaging with optiClient 130.
CRM/ERP Integration group	
SAPconnect (Unified Messaging)	This component installs the Unified Messaging gateway to SAP R/3 via the SAPconnect interface.
SAPphone (CTI)	SAPphone is an interface under SAP RR/3 that provides the SAP users with CTI functions. The XPR SAPphone component serves as SAPphone server as well as SAPphone client. It converts function calls of the SAP system into XPR transactions for a CTI provider, e.g. the CTI APL.
SapConnect: routing	This component installs the SAPBR APL enabling the SAP Business Routing.
Add-Ons/Tools group	
File Interface (FI APL)	General file interface for creating gateways to other systems. Application cases are e.g. the pure fax gateway via SAPcomm to SAP R/3, the gateways to Novell Groupwise or HP Open Mail and the connection to HP Digital Sender.
Print Module (Print APL)	If you want to be able to specify an existing network printer as the output device for automatic copies of incoming and outgoing fax messages, you must select these files for the installation; the Print APL also allows you to print e-mails or fax messages from the telephone user interface.

Table 10

Feature List

V.24 Support (V.24 APL)	These files are required if you want to operate protocols via analog modems. A possible application would be e.g. the activation of telephone LEDs to indicate new messages with several older PBXs.
Utilities	Some help programs that are installed in the directory <XPR Install>\SDKTools.
"Lear" Testing Module	Lear is a module to automatically transmit messages and transactions for testing purposes.
Reporting Module (Report APL)	Drawing up statistics or reports using predefined standard forms. The Reporting Module provides the display of statistical data of all XPR modules. For further information on the configuration of the reporting module please refer to the <i>System Architecture</i> manual. Attention! Using the CodeBase database is exclusively supported for upgrades. In case of new installations, please use an SQL database (cf. Section A.2, "Using the Report APL with SQL Databases", on page 207).

Table 10

Feature List

XPR System Installation

Installing the XPR Server and Configuring the Services

Scheduler for Report Module (Report Schedule APL)	The scheduler for the report module creates and sends statistical reports in different formats. This module assumes an installed report module and either an installed Crystal Reports XI Developer Edition or BIRT (Business Intelligence and Reporting Tool). The BIRT runtime component is on the installation medium and installed in the <XPR_installationpath>/ReportEngine directory during the ReportScheduleApl setup. BIRT requires the Sun-Java runtime environment version 6 or higher. BIRT does not work with an older version or with a JVM of another producer. The JRE must be installed on the same computer as the ReportSchedule APL. The JVM is neither shipped nor set up with the XPR. You can download it from http://java.sun.com free of charge. Use a 32-bit JVM on a 64-bit operating system. If a 64-bit JVM has already been installed, it need not be uninstalled. BIRT requires the installed Microsoft SQL Server 2005 JDBC driver. This driver is neither shipped nor set up with the XPR. You can download it from http://msdn2.microsoft.com/en-us/data/aa937724.aspx free of charge. Extract the sqljdbc.jar file from the downloaded file and copy it to the <xpr_setuppath>/ReportEngine/plugins/ org.eclipse.birt.report.data.oda.jdbc_2.2.0.v20070615/ drivers directory. Layout files of Crystal Report (RPT files) and BIRT (RPTDESIGN files) are not compatible. BIRT provides the export formats PDF and HTML. We recommend PDF exports. For the time being, BIRT reports are available in English only. To modify BIRT layout files you need to download the BIRT report designer component from www.eclipse.org/birt free of charge, considering the matching eclipse components and versions, and install it in the <XPR_setuppath>/ReportEngine. • Crystal Reports Runtime <i>The Crystal Report Runtime is required for the Report Schedule APL and set up during the Report Schedule APL installation.</i> <i>The Crystal Report Runtime requires the Microsoft .Net Framework.</i> IMPORTANT: Crystal Report Viewer 2008 The Crystal Report Viewer is no longer part of the OpenScope Xpressions scope of delivery. If you wish to view the reports of the RepScheduleApl, you need to download the Crystal Report Viewer 2008 from the internet.
Print Output Management (LPR APL)	Print Output Management . 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.
SSDP Service Plug-in	The SSDP Service Plug-in stores all relevant information in a central location and provides it to the user as set of information. Note: If you do not install the SSDP Service Plug-in, then the SSH Daemon must be set up.

Table 10

Feature List

License Info SNMP Agent	Installs the OpenScope Xpressions License Info SNMP Agent. This agent provides the licenses used in the scope of the Software Subscription Licensing Model in the CMP. The license information is reported to the CMP by SNMP. This enables the service to retrieve the corresponding information in the CMP. Requirement is an installed Windows SNMP service. More details are provided in the manual <i>Server Administration</i> in section <i>SNMP Agents</i> .
Clients & components group When you select a client application, its installation files are copied to the XPR server and made available in the network with a share. Thus, the client application can be installed on a client computer via the network. Furthermore, this function is needed for the Smart Client Update.	
Communications setup (Admin/User Application)	Communications is an XPR client with a graphical user interface; it enables the operation and administration of all functions available with XPR.
Application Builder setup	The <i>Application Builder</i> is an administrative application enabling the creation of voice menu applications that can be played to a caller. The voice menu applications that have been created may be used as Automated Attendant and IVR solutions.
Lotus Notes Conference Plugin Setup	See <i>Client Installations</i> , <i>IBM Notes Extensions</i> or <i>Microsoft Outlook Extensions</i> manual.
Lotus Notes Fax Printer Driver Setup	See <i>Client Installations</i> , <i>IBM Notes Extensions</i> or <i>Microsoft Outlook Extensions</i> manual.
Local Forms Setup	See <i>Client Installations</i> , <i>IBM Notes Extensions</i> or <i>Microsoft Outlook Extensions</i> manual.
Lotus Notes ActiveX Components Setup	See <i>Client Installations</i> , <i>IBM Notes Extensions</i> or <i>Microsoft Outlook Extensions</i> manual.
Outlook Conference Plugin Setup	See <i>Client Installations</i> , <i>IBM Notes Extensions</i> or <i>Microsoft Outlook Extensions</i> manual.
Server Based Forms Client Components Setup	See <i>Client Installations</i> , <i>IBM Notes Extensions</i> or <i>Microsoft Outlook Extensions</i> manual.
Server Forms Setup	See <i>Client Installations</i> , <i>IBM Notes Extensions</i> or <i>Microsoft Outlook Extensions</i> manual.
MAPI Fax Printer Drivers Setup	See the <i>Client Installations</i> , <i>MAPI Fax Printer Driver</i> manual.

Table 10 Feature List

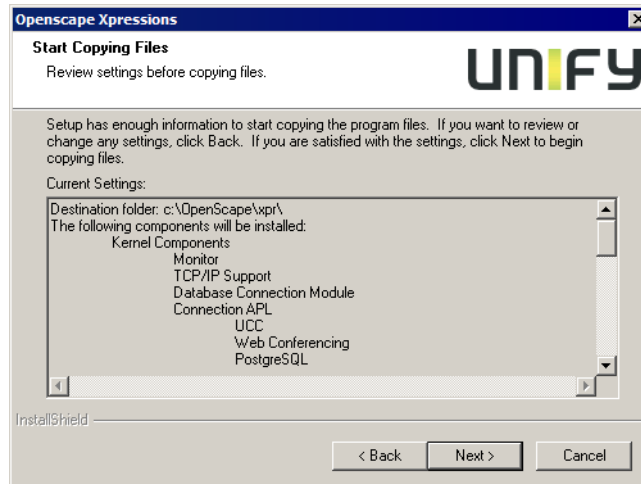
3. Then click on **Next**.

The setup continues with the selection of the directories for the **Database** and the **Document folder** (cf. [Section 4.5.2, "Summary of the Specifications and Settings"](#), on page 100).

4.5.2 Summary of the Specifications and Settings

In this dialog you can check the specifications and settings you have made in the previous dialogs.

1. Up comes this dialog:

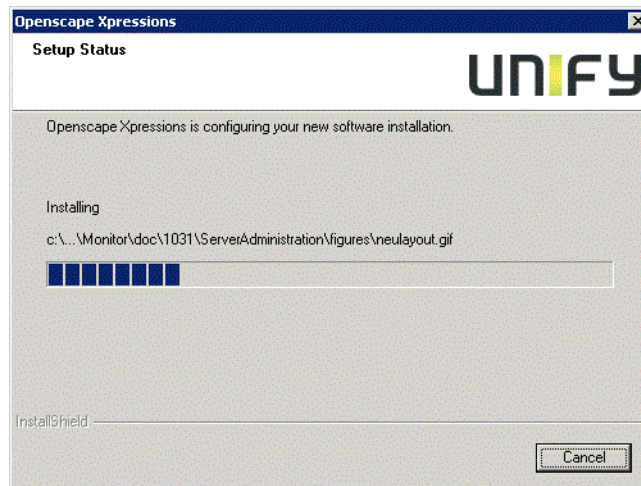


2. Check all settings and specifications for correctness.

With a click on **< Back** you can return to already edited dialogs for correcting faulty settings or specifications.

3. Click on **Next** when all specifications and settings are correct.

Setup starts and the required files are copied. The installation status is displayed in the following dialog:



The setup continues with the XPR server component configuration and services (cf. [Section 4.5.3, "Selecting the Folder for the Database and the Document Folder"](#), on page 101).

4.5.3 Selecting the Folder for the Database and the Document Folder

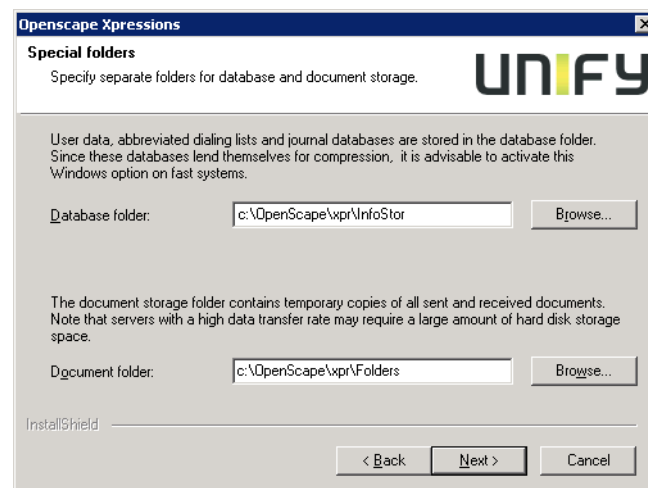
In this dialog you specify the folder for the database and the document folder. For both folders, defaults are suggested.

The **Database folder** must be located on the largest harddisk partition with the fastest random access. This folder contains the database with user data, speed dialing and distribution lists.

The **Document folder** should be located on the largest harddisk partition with the fastest linear access. All in and outbound documents are stored in the document folder. After a configurable period or when specific circumstances occur, the documents are automatically deleted.

NOTE: The size of the required harddisk memory depends on the number of in and outbound documents and on the period until documents are automatically deleted. Check in regular intervals, especially during the startup phase, whether harddisk memory is sufficiently available. If not, expand it.

1. Up comes this dialog:



2. In the **Database folder** field specify the database folder or accept the default. Via the **Browse...** button you can find a folder in the file system and select it.
3. In the **Document folder** field specify the document folder or accept the default. Via the **Browse...** button you can find a folder in the file system and select it.
4. Click on **Next**.

4.5.4 Assigning Service Accounts

The XPR components are started as services.

1. The user account under which these services are started is assigned in step 2.

IMPORTANT: In certain situations, for example if the XPR is to be connected to a Microsoft Exchange server, this account must be a domain account and belong to the same domain in which the XPR server is installed.

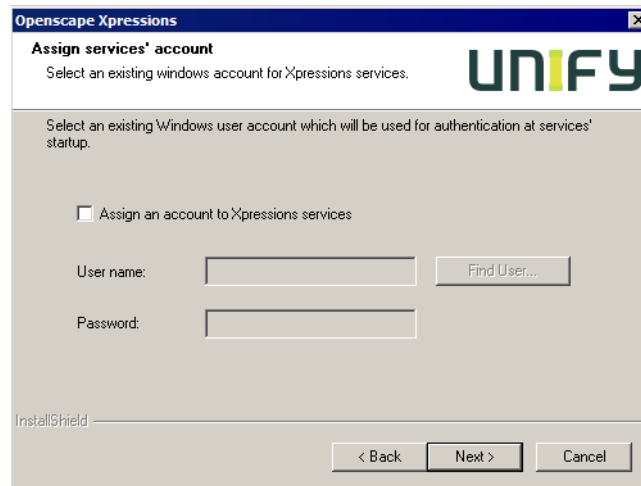
You need to check whether the user account you wish to deploy has administrator privileges on the local computer. If you deploy a local user account, execute the following substeps. Proceed analog if you use a domain account.

- a) Open **Start > Control Panel > Administrative Tools > Computer Management**.
- b) Open **Computer Management (Local) > System Tools > Local Users and Groups > Users**.
- c) Doubleclick the user that you want to use.
- d) Click on the **Member Of** tab.

The **Member of** area must list a group that has administrator privileges.

During the installation the automatic attempt is made to assign the **Logon as a service** privilege to this user account and to configure all XPR services in a way that they log on with this user account.

2. Specify in the **User** field the user account under which these services are to be started.



NOTE: The **Smart Backup & Restore** feature assumes the user assigned to the MTA service also being the installing one.

3. Specify this account's password in the **Password** field.
4. Click on **Next**.

The installation continues with the selection of the default speech-encoding (cf. [Section 4.5.5, "Selecting the Default Speech-Encoding", on page 103](#)).

4.5.5 Selecting the Default Speech-Encoding

In this step you set the coding used in your country for voice files. The following codings are available:

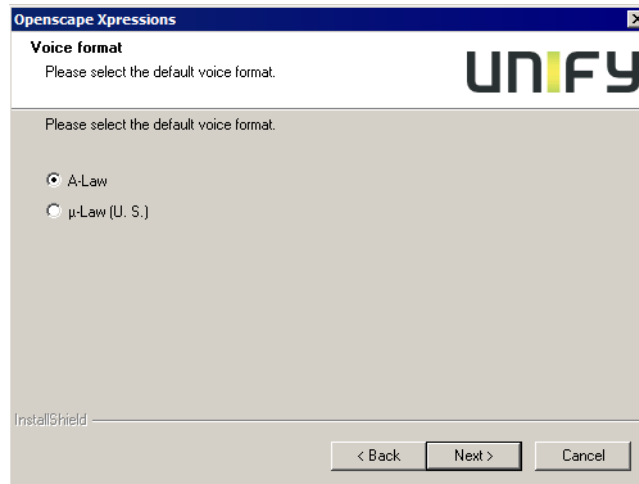
Coding	Description
A-Law	Mainly used in Europe.
μ -Law	Mainly used in Canada, Hong Kong, Japan, Mexico, Taiwan, and the USA.

Table 11 *Default Speech-Encodings*

XPR System Installation

Installing the XPR Server and Configuring the Services

1. Up comes this dialog:



2. Select the default voice format.

Please note that the registry key `VoiceRecFormat` of type `REG_DWORD` specifies the codec used by the IP APL for recordings. The following values are possible:

- 0x02000000 (33554432): A-Law, sample rate 8 kHz, mono
- 0x10000000 (268435456): μ -Law, sample rate 8 kHz, mono
- 0xffffffff (4294967295): PCM (normal WAV), sample rate 8kHz, mono

The last value is the default value.

If you want to change the relevant default behavior, you need to manually create this key in the registry first.

For further information about this key please refer to the *OpenScape Xpressions Server Administration* manual.

3. Then click on **Next**.

The installation continues with the selection of the program folder (cf. [Section 4.5.3, “Selecting the Folder for the Database and the Document Folder”](#), on page 101).

4.5.6 Configuring the User Authentication

OpenScape Xpressions offers two authentication methods for users to log on to the system:

Login via the Windows user account

This is the standard method. If this method is applied, the user's Windows account is used for authentication against the XPR server. All password-specific functions in the XPR server are deactivated. After you have selected this option, the next installation step is to choose the Windows accounts to serve as XPR administrator or XPR postmaster (cf. [Section 4.5.6.1, “Login via the Windows User Account”, on page 106](#)).

IMPORTANT: Login via the XPR account cannot be changed retrospectively.

Login via XPR account (user name + password (PIN))

With this authentication method, user accounts for the XPR administrator and the XPR postmaster are created in the XPR database. It is still possible though to activate the authentication via the Windows user account for some users in hindsight. In the next installation step you need to specify a name and password for the administrator and the postmaster of the XPR server each (cf. [Section 4.5.6.2, “Login via XPR Account”, on page 107](#)).

1. Up comes this dialog:



2. Select one option and click on **Next**.

You continue the installation depending on your selection. Therefore please refer to [Section 4.5.6.1, “Login via the Windows User Account”](#) or [Section 4.5.6.2, “Login via XPR Account”](#).

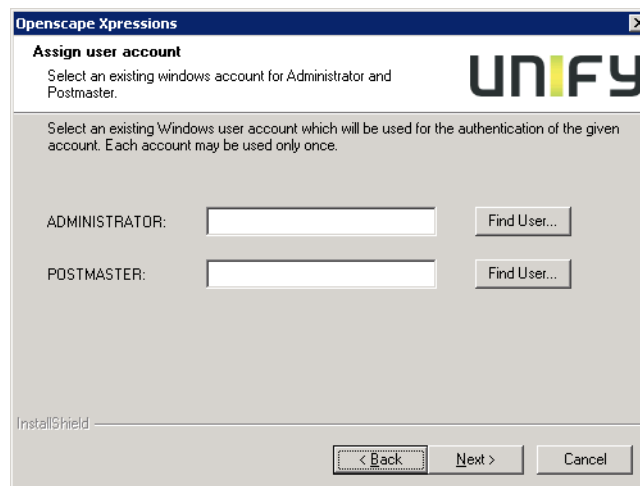
4.5.6.1 Login via the Windows User Account

If you have opted for this authentication method, you need to choose a Windows user who is to have administrative privileges for the XPR server, and another user to appoint XPR postmaster.

IMPORTANT: The user accounts for administration and routing (see [Section 4.5.6.2, “Setting up the Postmaster User Account”, on page 107](#)) are not only stored in the database, but also saved encrypted in the Windows registry database. If the database completely fails (e.g. because of a harddisk crash), the information stored in the registry is used to recover such user accounts

Related password alterations are NOT maintained in the Windows registry database. The recovery after a complete failure always requires the password entered here.

1. Up comes this dialog:



2. Click on the **Find User** button next to the **Administrator** field and select a Windows user in the dialog then open.
3. Click on the **Find User** button next to the **Postmaster** field and select a Windows user in the dialog then open.
4. Then click on **Next**.

In the next step you need to specify a password for the administrator account on the XPR server (cf. step 1 in [Section 4.5.6.2, “Setting up the User Account for the XPR Administrator”, on page 107](#)), which different XPR tools still require.

4.5.6.2 Login via XPR Account

If you have selected this authentication method, you need to specify names and passwords for the administrator and postmaster of the XPR server.

Both XPR users are defined in the XPR database and authenticate themselves in future via XPR mechanisms. You can switch to Windows authentication at a later date. Please read the corresponding chapter in the *OpenScape Xpressions Web Assistant* manual on this.

Setting up the User Account for the XPR Administrator

The user account for the administrator is used for the configuration and later administration of the system. We recommend to keep the suggested user name.

1. Up comes this dialog:

2. In the **Password** field enter the password for the administrator account. Choose as complex a password as possible to avoid misuse of this account.
3. Reenter the selected password in the **Confirm password** field to make sure that access will not be denied on grounds of a typing error.
4. Click on **Next**.

The dialog to set up the postmaster user account opens (cf. the following section).

Setting up the Postmaster User Account

The postmaster contains all incoming documents that cannot be delivered because, for example, the address is incorrect. You can define so-called alarm rules that automatically send a copy of unread documents to the postmaster after expiration of a specific period (cf. section "Message Transfer Agent" (MTA) of the *OpenScape Xpressions Server Administration* manual.

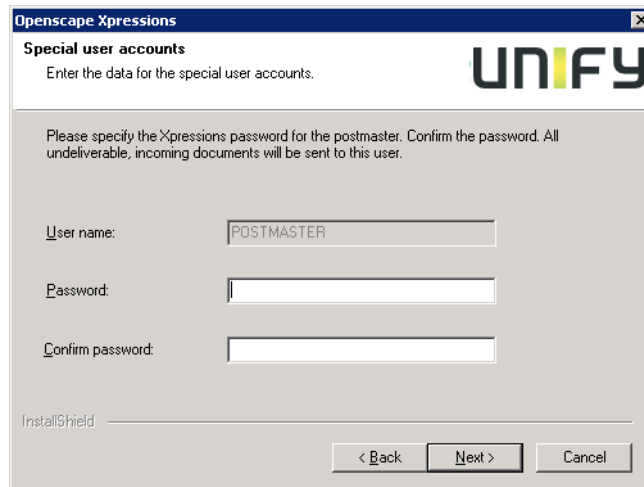
XPR System Installation

Installing the XPR Server and Configuring the Services

Via the user administration the postmaster must later be assigned a phone number (*Voice* field) so that users can divert to the postmaster from the telephone user interface (ERGO, PhoneMail or VMS).

You cannot modify the account name.

1. Up comes this dialog:



2. In the **Password** field enter the password for the postmaster account. Choose as complex a password as possible to avoid misuse of this account.
3. Reenter the selected password in the **Confirm password** field to make sure that access will not be denied on grounds of a typing error.
4. Click on **Next**.

The setup continues with the XPR server component configuration and services (cf. [Section 4.5.7, “Configuring the XPR Server Components and Services”, on page 108](#)).

4.5.7 Configuring the XPR Server Components and Services

Some server components require an initial configuration during the installation, so that the XPR system can be started for the first time at all. As soon as the setup program starts with the installation of one of these components, you are prompted by dialogs to enter necessary configuration parameters for the respective server component.

The following table shows the server components that require an initial configuration:

Component	See description in
Configuring regional Connection Settings	Section 4.5.7.1, "Configuring regional Connection Settings", on page 109
Additional IP Addresses for the Web Conference Server	Section 4.5.7.2, "Additional IP Addresses for the Web Conference Server", on page 113
Connection APL	Section 4.5.7.3, "Connection APL", on page 114
Setup Wizard for the SMTP APL	Section 4.5.7.5, "Setup Wizard for the SMTP APL", on page 121
Installing and Configuring the CTI APL	Section 4.5.7.6, "Installing and Configuring the CTI APL", on page 124
Installing the Exchange 2003 Gateway	Section 4.5.7.8, "Installing the Exchange 2003 Gateway", on page 125
Installing the Lotus Notes Gateway	Section 4.5.7.10, "Installing the Lotus Notes Gateway", on page 126
Installing the SAP R3 Components	Section 4.5.7.11, "Installing the SAP R3 Components", on page 126
Installing and Configuring the V.24 APL	Section 4.5.7.12, "Installing and Configuring the V.24 APL", on page 126

NOTE: Server components not configured during the installation (e.g. IP APL, ISDN APL, MTA), must be configured after the installation via the XPR monitor. You find detailed information about the configuration of single components in the *OpenScape Xpressions Server Administration* manual.

Between the server components that must be configured, components may be installed that do not require a configuration, so that you see the **Setup Status** dialog before configuration dialogs are displayed again.

The order in which the following sections appear corresponds to the sequence in which you are prompted to configure the above server components.

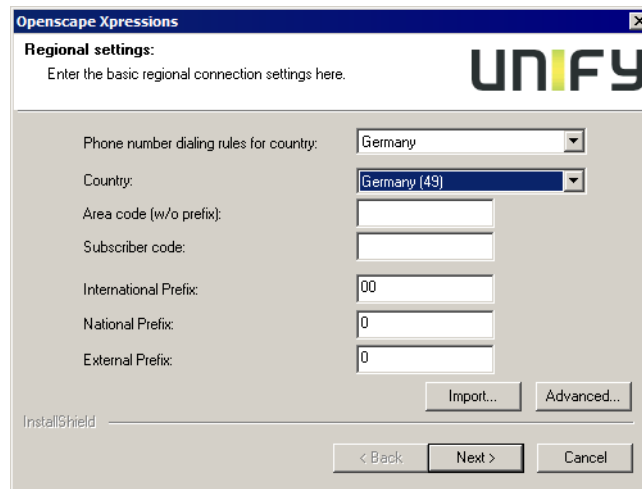
4.5.7.1 Configuring regional Connection Settings

The regional connection settings are used by the Telematic APLs or the CTI connection, but you can also configure them individually for each connection there.

XPR System Installation

Installing the XPR Server and Configuring the Services

1. The configuration of the regional connection settings starts with the following dialog:



2. In the **Phone number dialing rules for country** field select the country in which the system is located.

Some of the other fields will then automatically be filled in with the corresponding default settings for the selected country.

NOTE: If the list does not contain the desired country, select a country that corresponds to the desired connection settings, or use the General option. When you select the **General** option, you need to fill in all fields of this dialog.

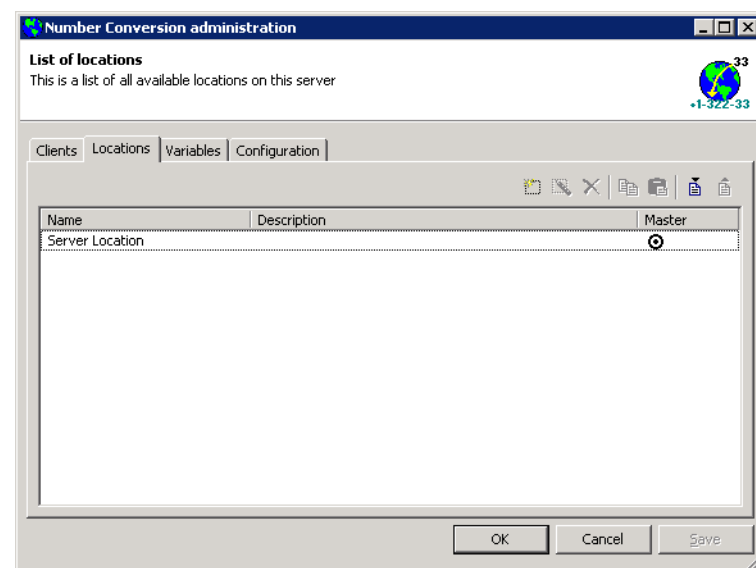
3. Check whether the fields that were automatically filled in feature the correct connection settings. If they do not, modify the entries according to your requirements. Heed the following table:

Field/Button	Description
Country	Select your country from this list to define the international country code.
Area code (without prefix)	Enter here the area code without prefix. In Germany this is thus the area code without the leading 0, in the US the area code without the leading 1. Example: 2404 from +49-2404-901-195
Subscriber code	Enter here the subscriber code of a phone number. Example: 901 from +49-2404-901-195 In US this is called <i>Office Code</i> .
International prefix	Specify here the international prefix. In the US this is 011, in Germany 00.
National prefix	Enter here the prefix that is part of your area code. In Germany this is the leading zero of the area code, in the US this is the 1.
External prefix	Enter here the external prefix.

Table 12 Fields and Buttons in the **Regional settings** Dialog

4. In the **Area code (w/o prefix)** field enter the area code of the system location **without** prefix.
5. Specify the **Subscriber code** of the XPR server in the corresponding field. In the US this is the *Office Code*.
6. Click the **Advanced...** button.

The **Number Conversion administration** dialog opens with a list of all locations:



XPR System Installation

Installing the XPR Server and Configuring the Services

7. Open the **Locations** tab.
8. Doubleclick the location entry that you want to edit.

The **Location editor** opens:

The screenshot shows a Windows-style dialog box titled "Server Location - Location" with a subtitle "Location editor". Below the subtitle is a text box with the message "This is the configuration for one location". The dialog is divided into several sections:

- Description:** A single-line text input field.
- Location codes:** A table with two columns: "Code" and "Type". It contains four entries: 49 (CountryCode (Country code)), 2404 (AreaCode (Area code)), 901 (SubscriberCode (Office code)), and 84 (TrunkCode (Trunk code)).
- Location prefixes:** A table with two columns: "Prefix" and "Type". It contains three entries: 00 (InternationalPrefix (International ...)), 0 (NationalPrefix (National prefix)), and 0 (ExternalPrefix (External prefix)).
- Variables:** A table with two columns: "Name" and "Value". It contains one entry: MaxExtensionLength with a value of 6.

At the bottom right of the dialog are "OK" and "Cancel" buttons.

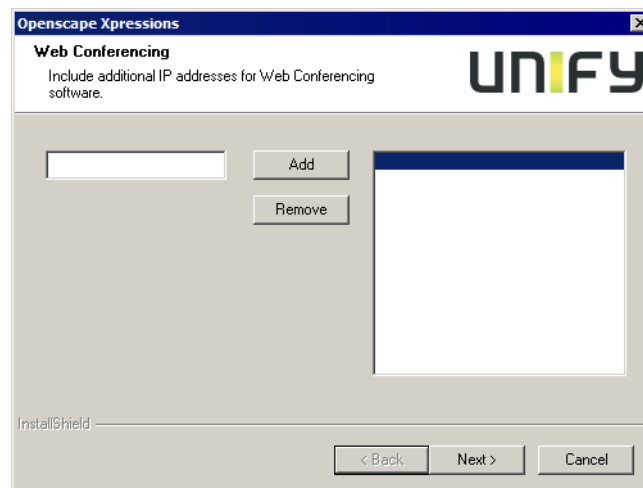
9. Check and configure the correct range codes for the locations. If several subscriber codes are to be used, the **SubscriberCode** entry must be deleted. Use **RangeCode** instead to subsequently specify the subscriber codes with the corresponding DID-ranges. How to specify a RangeCode:
 - a) Click in the **Location Codes** field with the right mousebutton and select the **Add** entry in the context menu. Then select the **RangeCode** entry.
 - b) A dialog opens for you to enter the data to the new RangeCode. Enter the corresponding values.
 - c) Click the **OK** button to save the RangeCode settings.
10. In the **Location editor** click the **OK** button.

You are taken back to the **Number Conversion administration** dialog.
11. Perform step 9 and 10 for all available locations.
12. Click on **OK** to save the changed location.

You are taken back to the **Regional Settings** dialog.
13. In the **Regional Settings** dialog click on **Next**.

4.5.7.2 Additional IP Addresses for the Web Conference Server

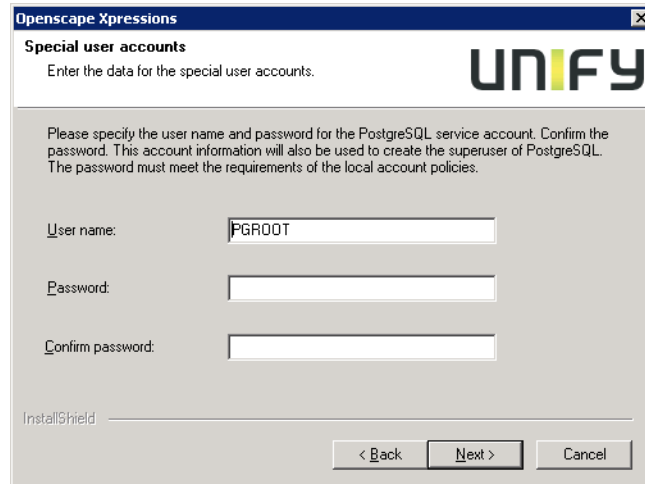
Web conferences use HTTPS as transport protocol for external subscribers. For performance reasons several HTTPS connections are established. Between the external subscribers and the web conference server service you usually do not only find firewalls but also HTTPS proxy servers. Some HTTPS proxy servers only allow a very limited number of connections, for example two, between two IP addresses. To evade such restrictions, the computer on which the web conference server service operates should at least be assigned one additional IP address. These IP addresses should be entered in the following dialog so that the web conference server service can inform the connected clients about the target IP addresses these clients are to use.



1. Enter an additional IP address for the web conference server in the field on the left-hand side and click on **Add**.
2. Repeat this for each further IP address.
3. Click on **Next** when all additional IP addresses are entered.

4.5.7.3 Connection APL

The following dialog requires entering a password for a user account of the PostgreSQL database in which general conference data are stored.



1. In the **Password** field enter the password for the user account. Choose as complex a password as possible to avoid misuse of this account. It must comprise at least eight characters and contain at least one special character or one digit.

IMPORTANT: If you use a password that is not sufficiently complex, you can neither modify this password at a later date nor access the PostgreSQL database.

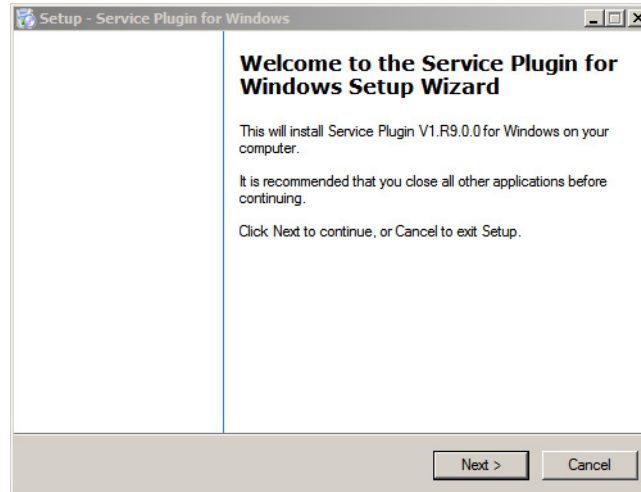
IMPORTANT: Certain upgrades require a fresh XPR installation. If the setup you perform is a fresh installation within the scope of an upgrade, be sure to enter the password you already used for setting up the old XPR in the **Password** field.

2. Reenter the selected password in the **Confirm password** field to make sure that access will not be denied on grounds of a typing error.
3. Click on **Next**.

IMPORTANT: After a server reboot the privilege **Log on as service** may be overridden in the local account **PGROOT**. In this case, assign the privilege **Log on as a service** under `Local Security Policy>Local Policies>User Rights Assignment`.

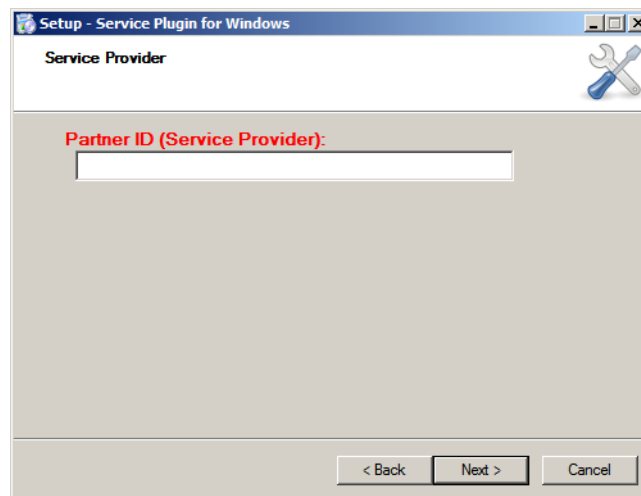
4.5.7.4 Installing the Smart Services Delivery Platform (SSDP)

1. Open the `XpressionsInstall\AddOn\Misc\SSDP` directory on the setup medium. Click with the right mouse button on the application **ssdp** and execute the application as administrator.
2. The setup wizard of the **Service Plugin for Windows** starts.



Click on **Next**.

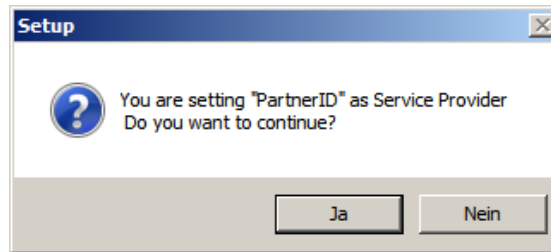
3. Enter your **Partner ID** and click on **Next**. If you are a Unify GmbH & Co. KG customer, your partner ID is **SEN**. Your service provider will give you a partner ID otherwise.



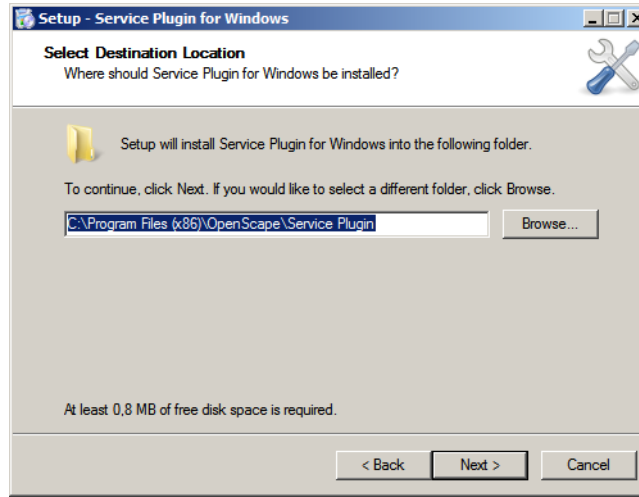
You will now be prompted to confirm your entry.

XPR System Installation

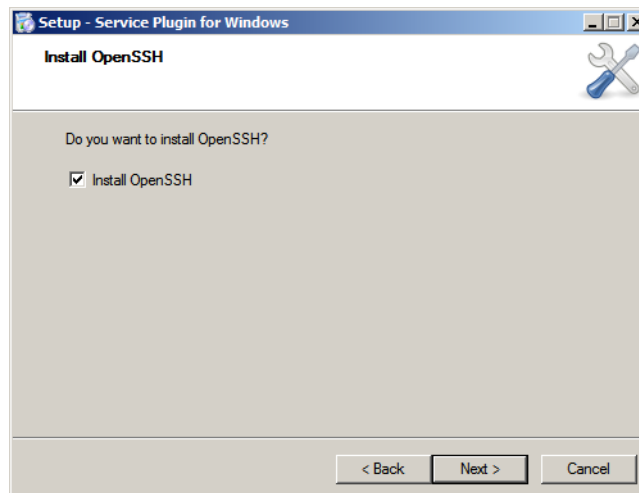
Installing the XPR Server and Configuring the Services



Confirm your input with **Yes**. The next installation dialog opens.

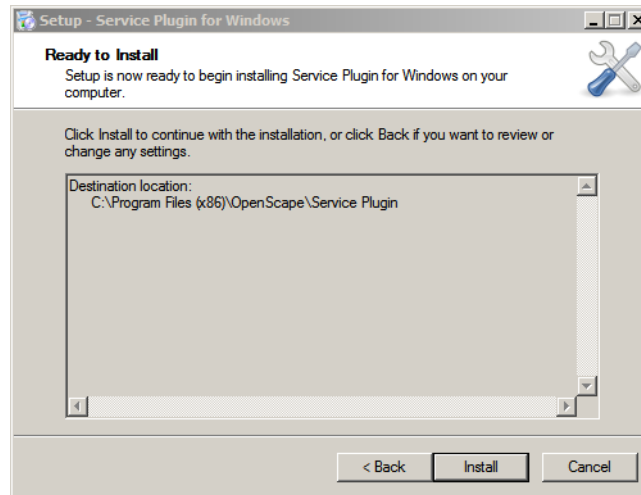


4. Click on the **Browse...** button if you wish to change the setup directory. The continue with **Next**.



In this dialog you are asked if you wish to install the SSH-Daemon.

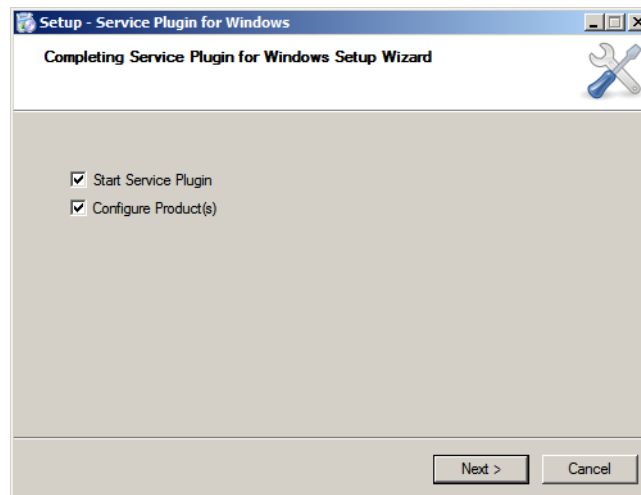
5. Click on **Next**.



This dialog provides an overview of the selected components and settings.

6. Click on **Install**.

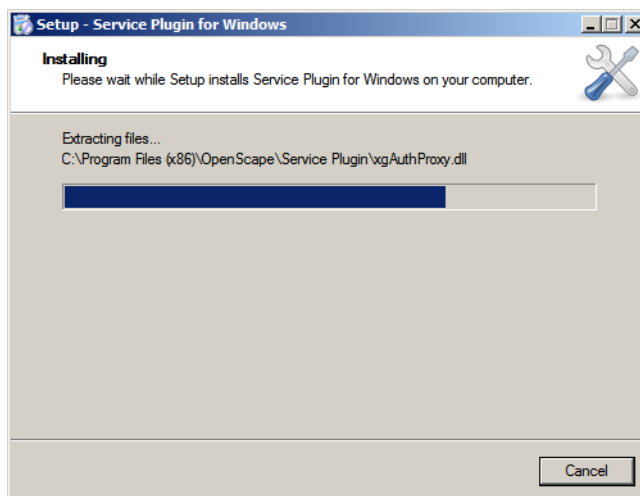
In this dialog you can decide whether to start the Service Plugin and to configure the product. We recommend to copy the default.



7. Click on **Next**.

XPR System Installation

Installing the XPR Server and Configuring the Services



The installation progress is displayed and the setup wizard of **Copssh** starts.

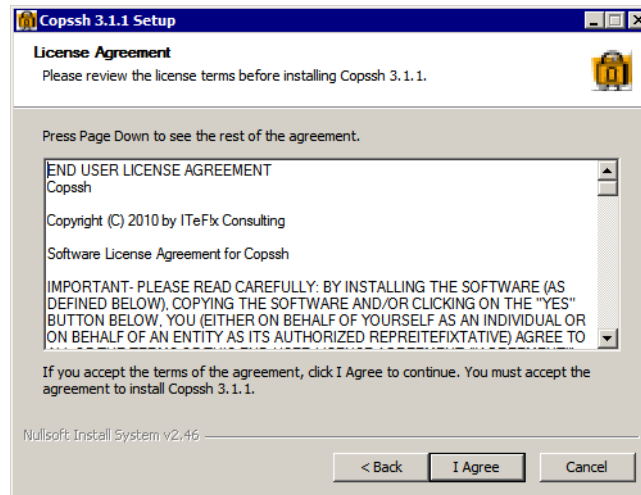
NOTE: If **Copssh** has not been installed yet, the **Copssh** setup starts automatically.



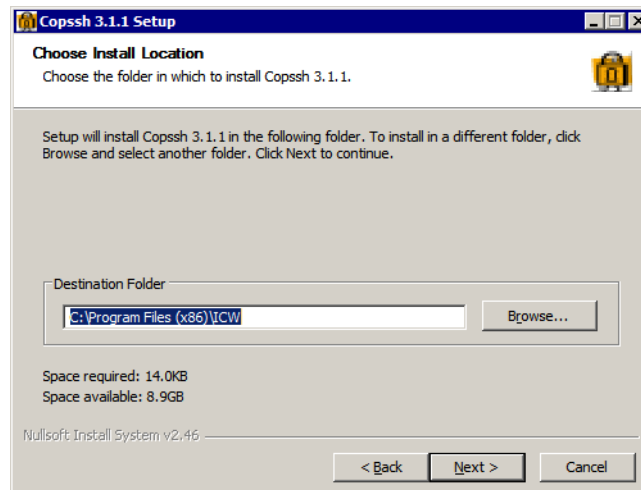
8. Click on **Next**.

XPR System Installation

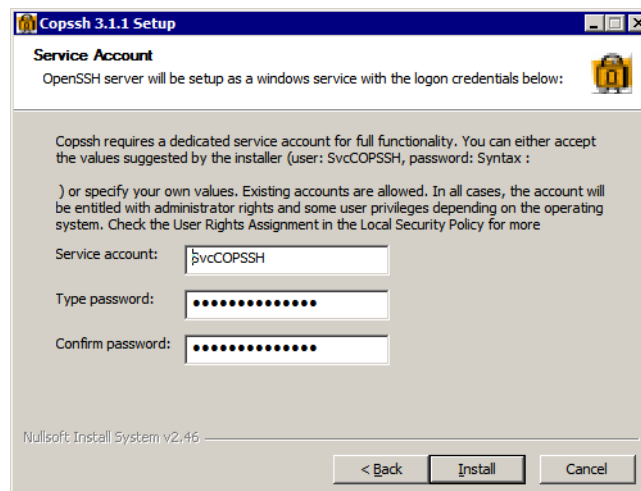
Installing the XPR Server and Configuring the Services



9. Click on **I agree**.



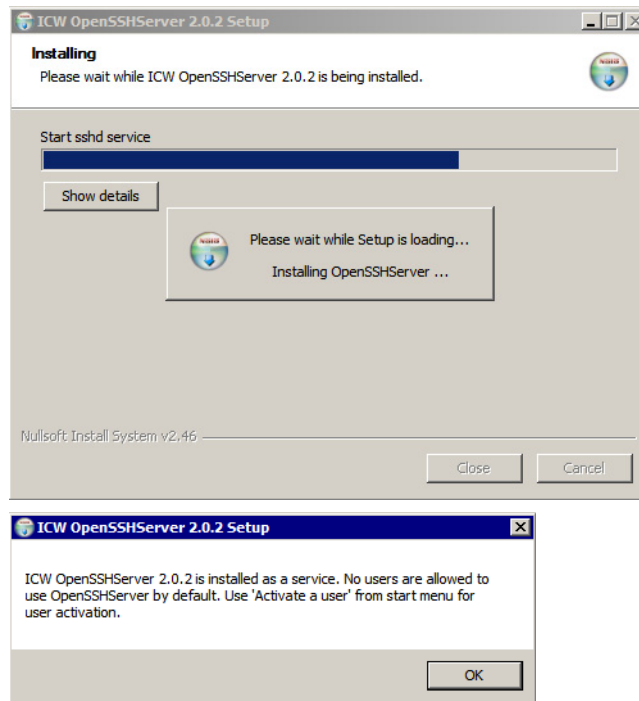
10. Accept the defaulted target path for the installation or click the **Browse...** button to specify another installation target path. Click on **Next**.



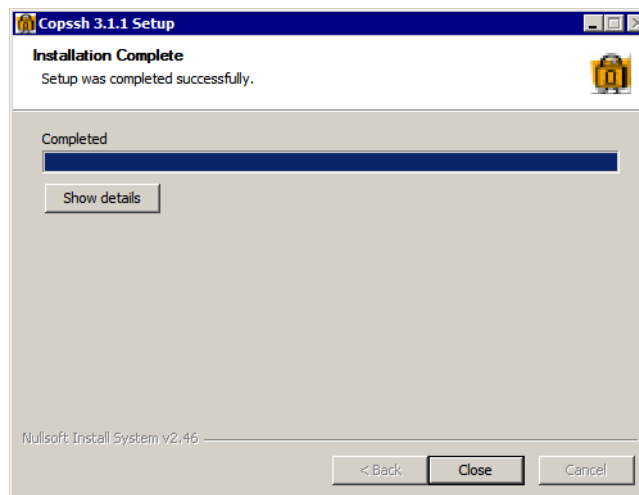
XPR System Installation

Installing the XPR Server and Configuring the Services

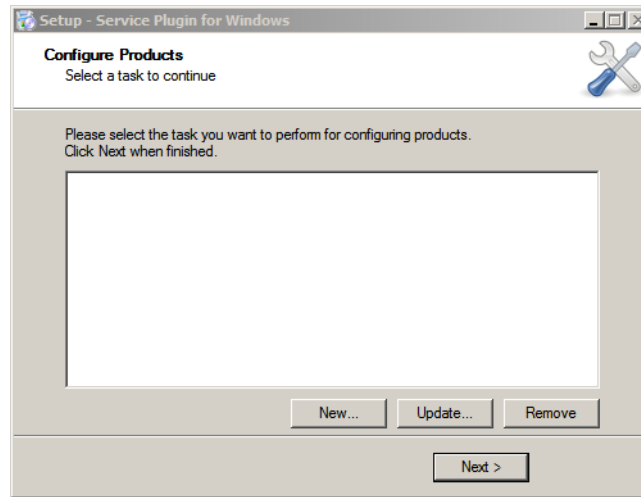
11. You need to create a user account for Copssh for using the full Copssh functionality. You can accept the defaulted data, create a new account or select an existing account. Click on **Install** to start the installation.



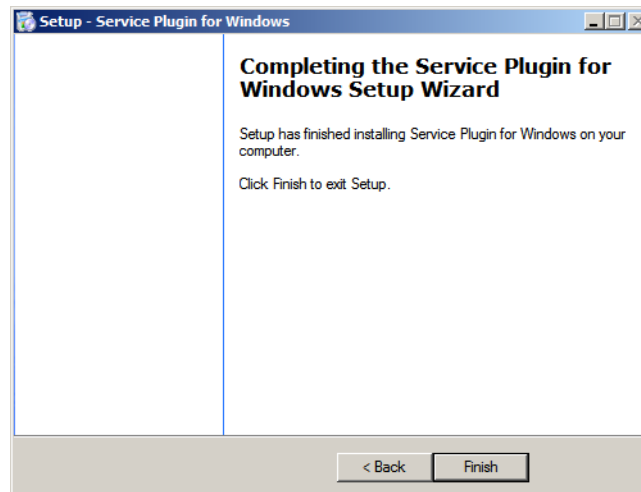
12. Click on **OK**.



13. Click on **Close**. The **Copssh** installation is complete and the setup of Service Plugin for Windows continues.



14. Configure your product and click on **Next**.



15. Click on **Finish** to complete the SSDP plug-in setup.
The SSDP plug-in is installed.

4.5.7.5 Setup Wizard for the SMTP APL

The SMTP APL provides the following services:

- sending and receiving SMTP messages via the Internet
- access for POP3 and IMAP4 clients,

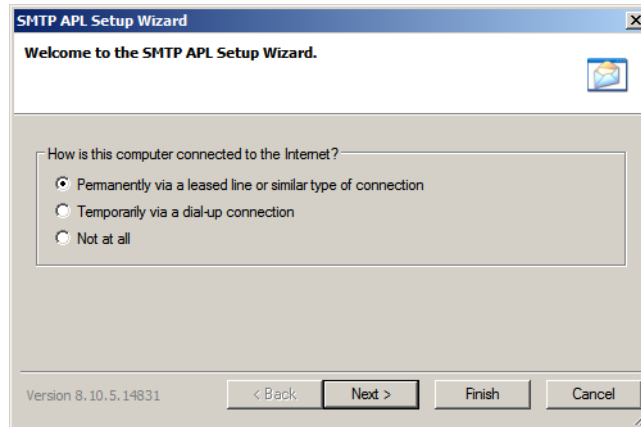
XPR System Installation

Installing the XPR Server and Configuring the Services

- time-dependent import of messages with a POP3 server.

NOTE: So that the SMTP APL can be used, the SMTP service of the operating system must be stopped and deactivated. You find information on this in the documentation of the operating system.

1. The SMTP APL setup starts with the following dialog:



2. Select one of the available options.

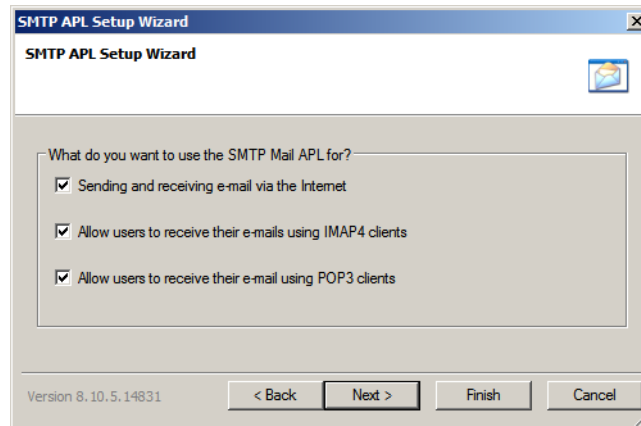
When you select the **Not at all** option, e-mails can only be sent to other XPR server users.

If you select the **Temporarily via a dial-up connection** option, the RAS service of the operating system is used to establish a PPP connection to a provider or to another Windows network.

NOTE: A Dialogic/Eicon card used for connecting the PBX **cannot** be used for the RAS service. This requires another ISDN board.

When using the RAS service, please heed the special security aspects.

3. Then click on **Next**. The dialog for selecting the usage option opens:

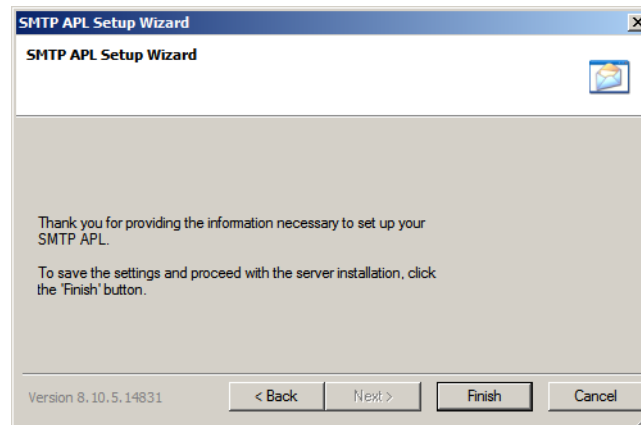


4. Select the options that you require.

The **Sending and receiving of e-mails via the internet** option requires an existing internet connection. If you select this option, it is possible to send and receive Internet mail via any client/gateway connection to the XPR server.

The two other options in this dialog make the use of POP3- or IMAP4 clients available in order to access to the XPR server. This can be done, for example, from any computer with internet connection if there is a steady internet connection, but it can also be done locally within the internal Intranet as a client for the XPR server.

5. Click on **Next**.



6. Click on **Finish**.

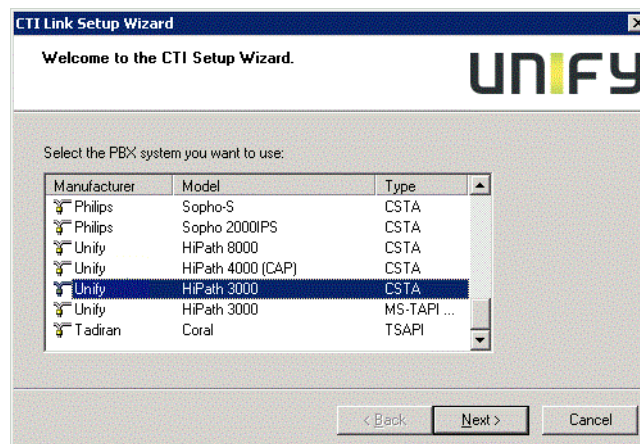
4.5.7.6 Installing and Configuring the CTI APL

The CTI APL provides different features for controlling and monitoring PBX systems and telephones. The most important ones are:

- Control of telephone devices (accept call, show display information etc.)
- Control of telecommunication connections (initiating the connection setup, conferences, “park calls”, “alternate” etc.)
- Monitoring telecommunication connections by setting monitor points within the PBX system
- Usage of all available features by other server components via the dialog/ transactions interface.

You find detailed information about the CTI APL in the *OpenScope Xpressions Server Administration* manual.

1. The CTI APL setup starts with the following dialog:



2. Select the PBX that you want to connect to the XPR server via a CTI link.

Depending on the CTI link set, further settings have later to be performed via the XPR Monitor. This is particularly necessary with connections via CSTA. With the first XPR server start the CTI APL also points to missing parameters in the log.

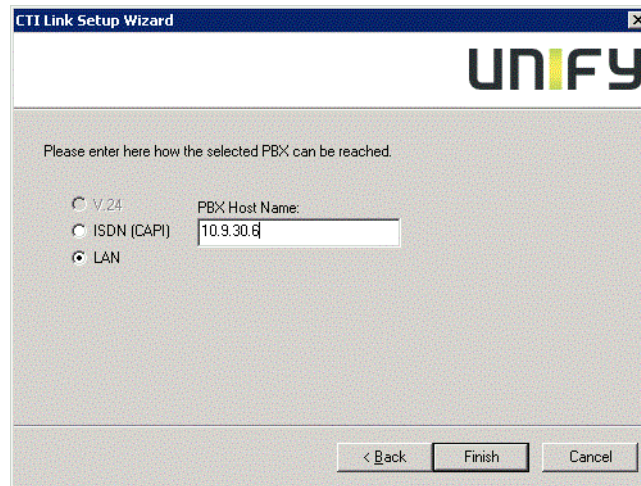
NOTE: If you have only one TAPI Service Provider installed that interacts with the CTI APL, you will not see the selection. The CTI link will be configured automatically. This is the case for the following TAPI drivers:

Hicom 150 of the Unify GmbH & Co. KG
Cisco Call-Manager
Elmeg C88M

Ascom AscoTel
DeTeWe OpenCom
Nortel Meridian

3. Click on **Next**.

Up comes this dialog:



4. Select the connection type.

If you have selected **ISDN (CAPI)** as connection type, you need to enter a phone number in the **Phone number for CTI link** field for the CTI APL to connect to the PBX.

If you have selected **LAN** as connection type, you need to enter the IP address or the network host name of the PBX in the **PBX Host Name** field.

5. Then click on **Finish**.

4.5.7.7 Setup Wizard for the LDAP APL

You find detailed information about the setup and configuration of the LDAP APL in combination with an Exchange connection in the *OpenScape Xpressions Exchange Gateway* manual. In case of usage without Exchange connection please refer to the *OpenScape Xpressions Server Administration* manual.

4.5.7.8 Installing the Exchange 2003 Gateway

You find detailed information about the setup and configuration of the Exchange gateway in the *OpenScape Xpressions Exchange Gateway* manual.

4.5.7.9 Installing the Exchange 2007 Gateway

You find detailed information about the setup and configuration of the Exchange gateway in the *OpenScape Xpressions Exchange Gateway* manual.

4.5.7.10 Installing the Lotus Notes Gateway

You find detailed information about the setup and configuration of the Lotus Notes gateway in the *OpenScape Xpressions IBM Notes Gateway* manual.

4.5.7.11 Installing the SAP R3 Components

You find detailed information about the setup and configuration of the SAP R3 gateway (SAPPhone APL and SAPR3 APL) in the *OpenScape Xpressions SAP Gateway* manual.

4.5.7.12 Installing and Configuring the V.24 APL

Via the V.24 APL, XPR servers may be connected by Remote System Link (SML transport). Furthermore, the V.24 APL enables sending and receiving of Fax G3 documents via Class 2 fax modems, and polling of documents from a fax-on-demand server.

NOTE: A list of all tested modems can be found in the Release Notes and the Hardware Compatibility List.

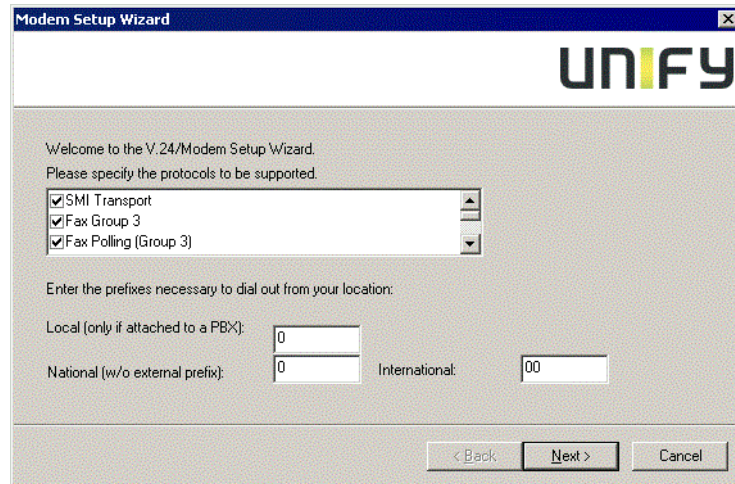
NOTE: Remote System Link is not compatible with [Crypt_Sec], it is designed to only work with [KRYPT].

Since documents are polled via a number to be dialed, a maximum of one file can be set as polling document per modem. A convenient fax-on-demand server, where the documents are assigned to single extensions, requires ISDN usage.

Another protocol, the Message Waiting Indication for new messages, is available via the SMDI protocol and for the following PBX systems:

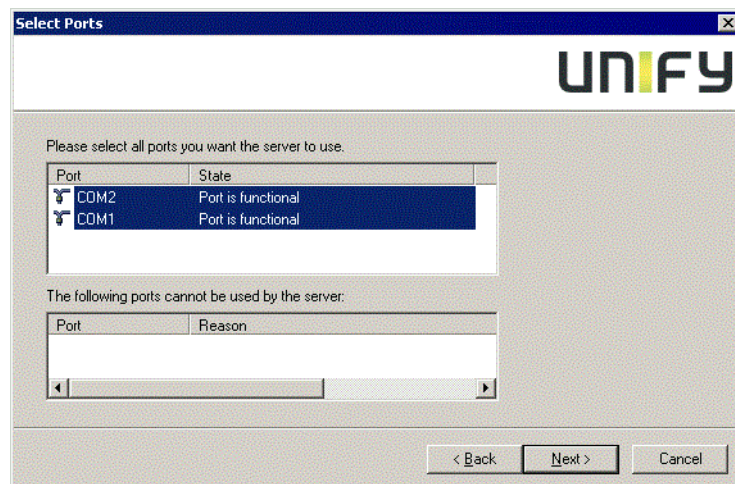
- Hicom of the Unify GmbH & Co. KG
- Ericsson MD 110
- DeTeWe OpenCom 1000

1. The V.24 APL setup starts with the following dialog:



2. In the list select the protocols to be supported.
3. In the **Local (only if attached to a PBX)** field enter the external prefix. The field is already allocated with a basic setting.
4. In the **National (w/o external prefix)** and **International** fields enter the national or international prefix. The field is already allocated with a basic setting.
5. Click on **Next**.

Up comes this dialog:



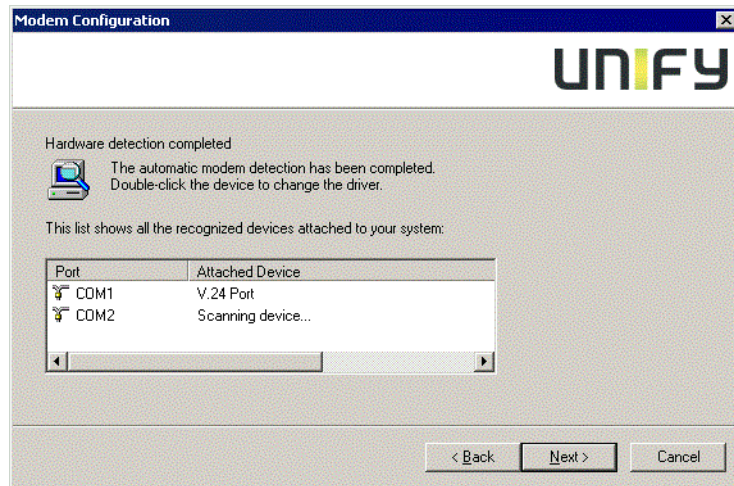
6. Select the serial ports to which you have connected a modem, or that you use for a fixed connection between two computers. You can only use the ports COM1 to COM9.
7. Click on **Next**.

XPR System Installation

Installing the XPR Server and Configuring the Services

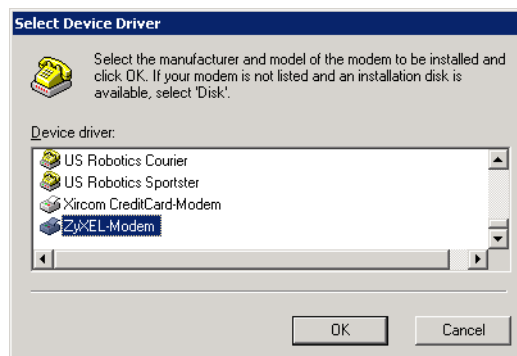
The setup program checks whether modems are connected to the serial ports you have specified and tries to determine their make. If the modem make cannot be identified, the system attempts to determine the capabilities of the modem as regards transmitting, receiving, and polling fax documents. A standard modem script that corresponds to such capabilities will then be installed.

The result is displayed in the following dialog:



8. Doubleclick the port that you want to assign a modem in the list.

Up comes this dialog:



9. Select the installed modem in the list.
10. Click on **OK**.

The selected modem is entered in the **Modem Configuration** dialog.

11. In the **Modem Configuration** dialog select the modem that you want to configure and click on **Next**.

Up comes this dialog:

Device Configuration

UNIFY

Modem on port: COM1

Type: ZyXEL-Modem

Baud rate: 38400

Line name: ZyXEL-Modem COM1

☒ Use touch-tone dialing (DTMF)

Phone Number

+ 49 - 2404 - 1234 - 130

< Back Next > Cancel

NOTE: Deactivate the **Use touch-tone dialing (DTMF)** option only if the modem is operated at a switching center addressed by pulse dialing (loop interruption).

12. If necessary, change the entries. In most cases the entered values are correct though.
13. Click on **Next**.

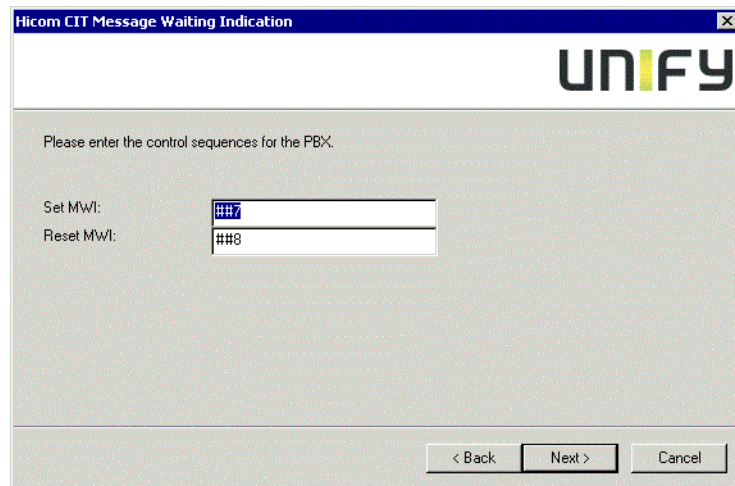
The protocols that you have selected in step 2 on page 127 will now be configured in succession.

XPR System Installation

Installing the XPR Server and Configuring the Services

Hicom CIT Message Waiting Indication

The sequences entered here are transmitted to a Hicom PBX via a modem.



Hicom CIT Message Waiting Indication

UNIFY

Please enter the control sequences for the PBX.

Set MWI: ##7

Reset MWI: ##8

< Back Next > Cancel

1. In the **Set MWI** field enter the sequence for activating the mailbox LED.
2. In the **Reset MWI** field enter the sequence for deactivating the mailbox LED.
3. Click the **Continue** button.

Fax Settings

The screenshot shows the 'Fax Settings' window with the following fields:

- User-defined settings:**
 - Default fax originator ID: +49 2404 1234 130
 - Default fax headline: (empty)
- System-wide settings:**
 - Continuation message for interrupted faxes: Continuation of an interrupted message
 - Default fax recipient: POSTMASTER

Navigation buttons at the bottom: < Back, Next >, Cancel.

1. In the **User-defined settings** section enter the **Default fax originator ID** and the **Default fax headline**, which are both issued in the sent fax, for the FaxG3 protocol.
2. In the **Continuation message for interrupted faxes** field of the **System-wide settings** section enter a text that is added to a fax if the fax message output is continued from the point where it was stopped by an interrupted transmission.
3. In the **Default fax recipient** field specify the name of the user who is to receive all incoming faxes.
4. Click the **Continue** button.

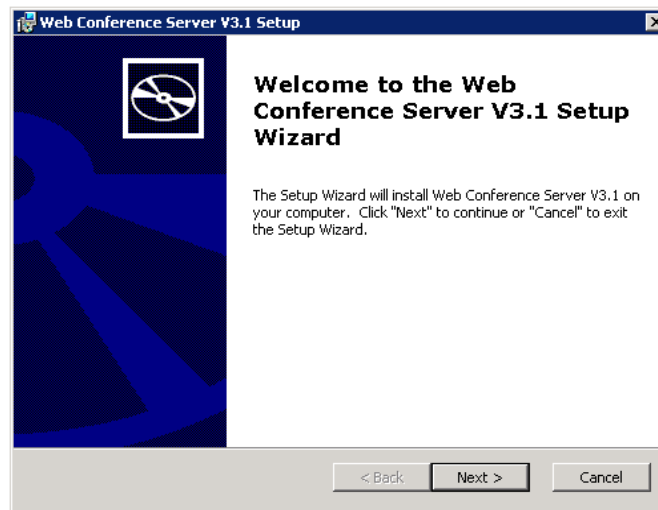
NOTE: This entry is required since analog modem technology prohibits direct inward dialing/routing to individual users.

4.5.8 Installing and Configuring the Web Conference Server

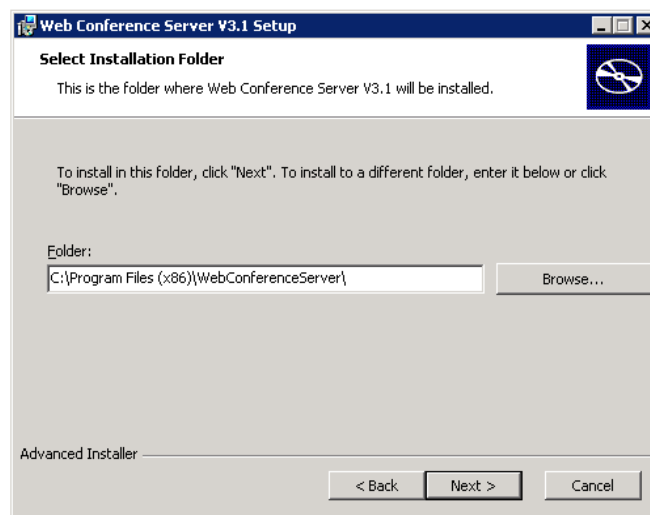
4.5.8.1 Installing the Web Conference Server

1. Start the file

XpressionsInstall\AddOn\AppSharing\setup.exe
on the installation medium.

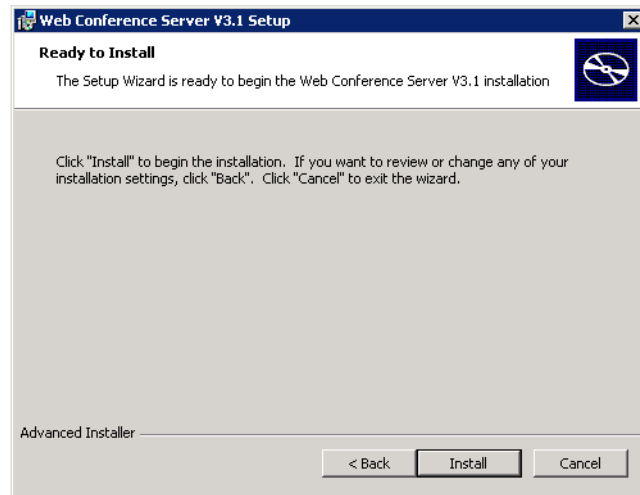


2. Click on **Next**.
3. Select the installation folder.

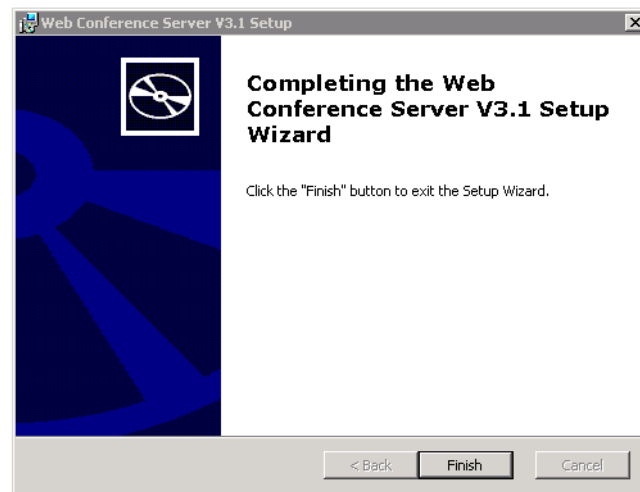


4. Click on **Next**.

5. Click on **Install** to start the Web Conference Server installation.



6. Click on **Finish**.



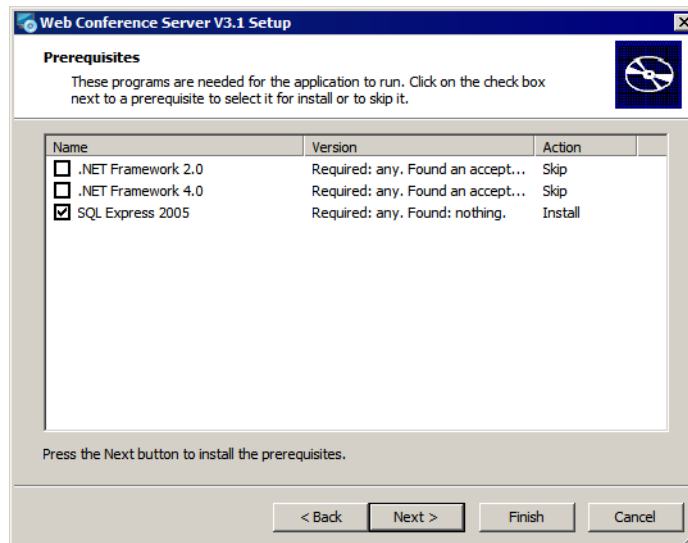
7. The following dialog displays in case some of the prerequisites needed to run this program are missing.

XPR System Installation

Installing the XPR Server and Configuring the Services



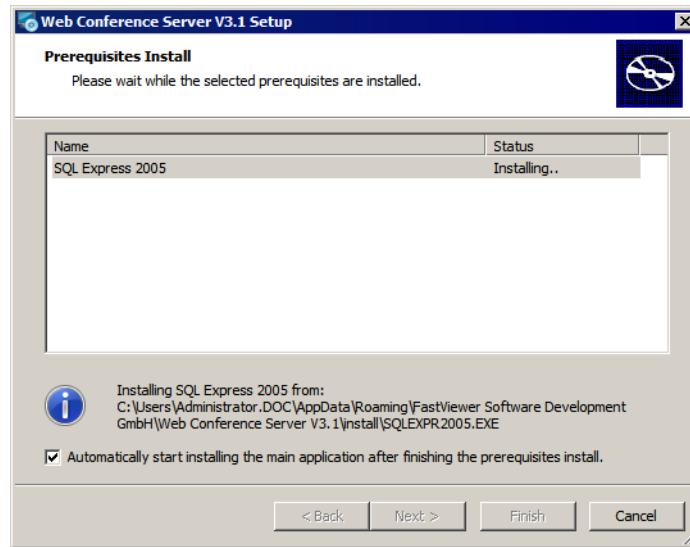
8. Click on **Next**.



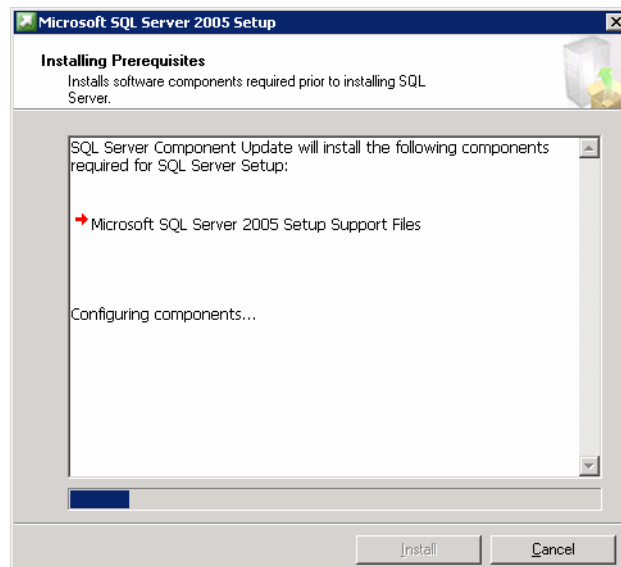
IMPORTANT: If you install the web conference server on Windows Server 2008, you need to download Microsoft SQL Server 2005 Express SP2 from Microsoft and manually install it. During the installation you need to deactivate the **Hide extended configuration options** check box and enter FASTVIEWER instead of SQLEXPRESS as entity name at a later date.

9. Click on **Finish**.

The following dialogs show the installation of the Microsoft SQL Server 2005 Express.



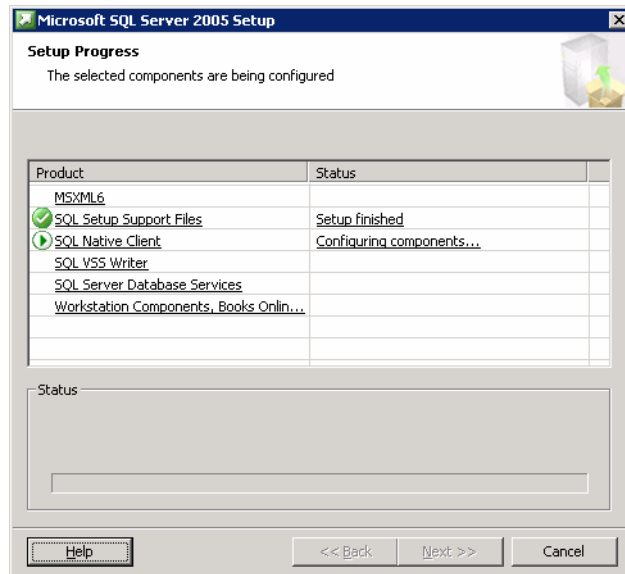
The Microsoft SQL Server 2005 Express setup is performed automatically. You need not click any button.



The following dialog displays the components to be installed for the Microsoft SQL Server 2005 Express.

XPR System Installation

Installing the XPR Server and Configuring the Services



10. The installation process continues.

4.5.8.2 Configuring the Web Conference Server

NOTE: The web conference server cannot be configured until the XPR server setup is complete.

1. Open the `settings.ini` file in the setup folder of the web conference server in an editor. This is the path
`C:\Program Files(x86)\WebConferenceServer` by default.

2. Look for the following line:

```
ExternalAddress=Change2YourServer
```

3. Replace value `Change2YourServer` with the external, fully qualified domain name (FQDN) of the web conference server computer.

NOTE: The external FQDN is the full outward name of the web conference server computer. The internal FQDN is the full name of this computer seen from the internal company network. If only a single FQDN is available, use it.

4. Look for the following line:

```
ClientURLBase=http://Change2YourServer/client/  
fastclient_i_%1.exe
```

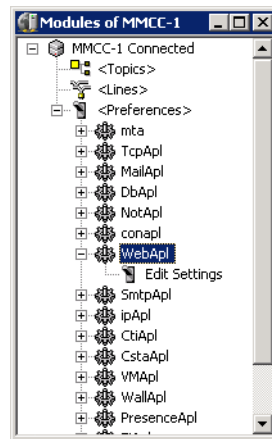
Replace value `Change2YourServer` with the external, fully qualified domain name (FQDN) of the web conference server computer.

5. Save the modifications.

Assigning a permanent IP

The system must have two IP addresses. One of them is used by the web conference server and the other one by the WebAPL. A permanent IP must be assigned to the web conference server for this purpose.

6. Open the **XPR monitor** under **Start >Programs> Xpressions>**.
7. Select in the dialog **Modules of> Preferences> WebApl**.



8. Doubleclick **Edit Settings**.

The **Web APL Configurations** dialog opens. The **HTTP** tab indicates the Web Apl IP address used.

9. Open the **command prompt** and enter the `ipconfig` command.

IMPORTANT: Enter this command exactly as described. Heed upper and lower case, inverted commas and blanks.

The available IP addresses are listed. Note down the IP address not used by the WebAPL, since it is assigned to the web conference server.

10. Enter the command `cd "\\programm files"` in the command prompt.
11. Enter the command `cd WebConferenceServer` in the command prompt.

IMPORTANT: If you use the `httpcfg` tool, **do not** assign port information to the IP address.

You can query the already present settings with the `httpcfg query iplisten` command. If the configuration has more than one port entry, the web conference server starts imperfectly.

XPR System Installation

Installing the XPR Server and Configuring the Services

12. Enter the command `httpcfg set iplisten -i <IP for the web conference server>` in the command prompt.
13. Enter the command `httpcfg set iplisten -i 127.0.0.1` in the command prompt.

Reboot the web conference server

14. Select **Start> Administrative Tools> Services**.
15. Open the context menu of the **Web Conference Server** and select **Stop**.
16. Switch to the command prompt and enter the `net stop http` command.
17. Enter the command `net start http`.
18. Enter the command `net start httpfilter`.
19. Switch to the **Services**.
20. Open the context menu of the **Web Conference Server** and select **Start**.

The configuration is complete. The Web Conference Client can be downloaded. You find detailed information under [Section 4.5.22, "Voice Conferences with SIP"](#).

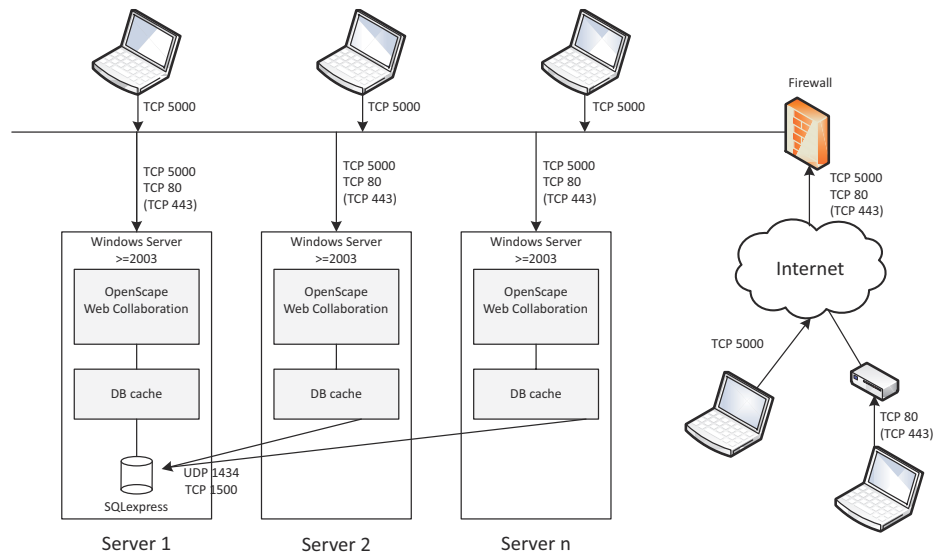
4.5.8.3 Configuring several Web Conference Servers

Connecting several web conference servers optimizes load balancing, thus increasing the performance of the single conferences.

The following figure shows the structure with several web conference servers:

XPR System Installation

Installing the XPR Server and Configuring the Services



NOTE: The web conference server cannot be configured until the XPR server setup is complete.

Configuring the web conference server

1. Configure the web conference servers in advance as described in [Section 4.5.8.2, "Configuring the Web Conference Server"](#).

Configuring the TCP/IP protocol

2. Open the **Protocols for FASTVIEWER** entry under **SQL Server 2005 Network Configuration**.
3. Doubleclick the **TCP/IP** entry to open it.
4. Set value **Activated** to **Yes** on the **Protocol** tab.
5. Check under **Control Panel/Administrative Tools/Services** whether the **SQL Server Browser** service has been started.

Configuring Settings.ini

6. Open the `settings.ini` file in the setup folder of the web conference server in an editor. This is the path
`C:\Program Files(x86)\WebConferenceServer` by default.

XPR System Installation

Installing the XPR Server and Configuring the Services

7. Adjust the following values:

NOTE: The values must be adjusted on every server in the system!

NOTE: Only internal **or** external FQDNs may be used! The external FQDN is the full outward name of the web conference server computer. The internal FQDN is the full name of this computer seen from the internal company network.

- **Server1:**

```
SQLConnectionString="Data
Source=(local)\fastviewer;Initial
Catalog=fastviewer;Persist Security Info=True;User
ID=sa;Password=<<ZLY5VPd8byicus01ottxqQ==>>"1
SessionIDStart=10001
SessionIDEnd=50000
ServerName=<specify ServerName>
```

- **Server2:**

```
SQLConnectionString="Data
Source=IhrFastViewerServer\fastviewer;Initial
Catalog=fastviewer;Persist Security Info=True;User
ID=sa;Password=<<ZLY5VPd8byicus01ottxqQ==>>"2
SessionIDStart=50001
SessionIDEnd=99999
ServerName=<specify ServerName>
```

8. Reboot the tunnel server from every configured server.

9. Check the function of all servers by entering `http://localhost/` in the browser of each server.

NOTE: If the servers that access the SQL database of the first server do not start, they are not connected to the database.

The configuration is complete. The Web Conference Client can be downloaded. You find detailed information under [Section 4.5.22, "Voice Conferences with SIP"](#).

-
1. The previous lines result in the **settings.ini** to one line. The line breaks in the **settings.ini** must be removed.
 2. The previous lines result in the **settings.ini** to one line. The line breaks in the **settings.ini** must be removed.

4.5.9 Installing and Configuring Voice Conferences

4.5.9.1 Installing Voice Conferences

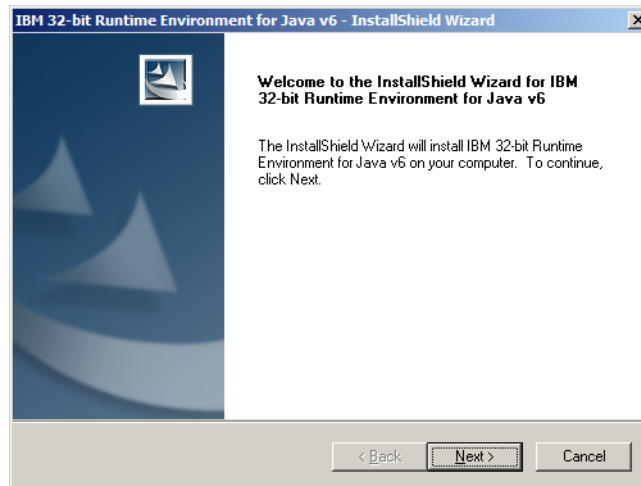
Installing voice conferences requires the **UCC** component to be active in the setup dialog in [Section 4.5.1, “Selecting Features”](#) .

4.5.9.2 Configuring Voice Conferences

You find detailed information about configuring voice conferences in the *XPR Server Administration* manual, sections *Media Server* and *Voice Conferences*.

4.5.10 Installing the Java Runtime Environment

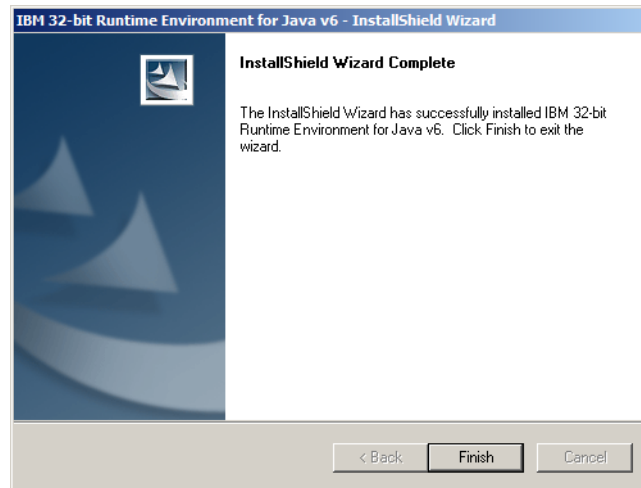
Various components, e. g. the Report Schedule APL, conferences and the Application Builder require at least one Java runtime environment.



NOTE: The Java Runtime Environment installation package can be found in the setup media under **XpressionsInstall> Prerequisites>Frame-works>java**.

If the Java Runtime Environment is already installed, upgrade it to the version distributed with the setup media.

1. The installation of the Java runtime environment starts. Click on **Next**.
2. Confirm the license agreement with **Yes**.
3. Use the defaulted target path or specify another one using the **Browse** button. Click the **Continue** button.
4. You see the installation settings. If you wish to change your settings, click on **Back**. If you wish the perform the installation under these settings, click on **Next**.
5. You see the installation progress.
6. IBM selects the Microsoft Internet Explorer as default browser for you. If you do not want this, remove the tick from the check box. Then click on **Next**.



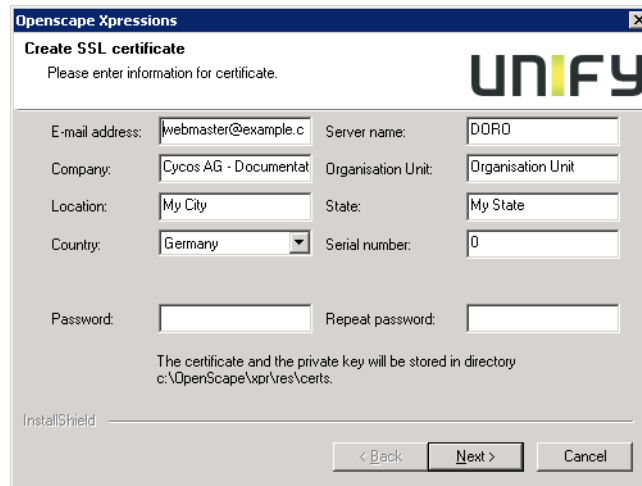
7. The Java runtime environment installation is thus complete. Click on **Finish**.

4.5.11 Creating the SSL Certificate

NOTE: If you want to use an individual certificate, please definitely make sure that the resulting files are coded with the Base64 method. All certificates coded in a different way lead to an error message in the XPR monitor and are not accepted.

The certificate created here enables the use of the HTTPS protocol with SSL encryption for the Web Assistant. The entire communication between client and server is encrypted.

1. The creation of the SSL certificate starts with the following dialog:



2. In the dialog's fields make the specifications that are to become elements of the certificate.

IMPORTANT: The content of the **Server name** field is important for the certificate. Enter here the name of the computer that is specified as URL in an Internet browser to access the XPR server via the WebAssistant. This is typically the computer name of the XPR server. If an alias URL is configured in the proxy server for this computer, this alias name must be entered in the **Server name** field.

3. In the **Password** field enter a sufficiently complex password.
4. Repeat the password in the **Repeat password:** field.
5. Then click on **Next**.
6. Creating the SSL certificate for stunnel starts with the following dialog: You find further information about stunnel in [Section 4.5.11.1, "Configuring stunnel", on page 145](#)

Openscape Xpressions

Create SSL certificate
Please enter information for certificate.

UNIFY

E-mail address: webmaster@example.c Server name: DORO

Company: Cycos AG - Documentat Organisation Unit: Organisation Unit

Location: My City State: My State

Country: Germany Serial number: 0

The certificate and the private key will be stored in directory
c:\OpenScape\xpr\bin\stunnel.

InstallShield

< Back Next > Cancel

7. In the dialog's fields make the specifications that are to become elements of the certificate.

IMPORTANT: The content of the **Server name** field is important for the certificate. Enter here the name of the computer that is specified as URL in an Internet browser to access the XPR server via the WebAssistant. This is typically the computer name of the XPR server. If an alias URL is configured in the proxy server for this computer, this alias name must be entered in the **Server name** field.

8. Then click on **Next**.

4.5.11.1 Configuring stunnel

Stunnel is a service for encrypting TCP connections by using SSL. Stunnel encrypts protocols such as POP, IMAP, LDAP independently with the help of SSL, thus creating a secure connection.

Immediately after the SSL certificate has been created for stunnel, stunnel is active as service. Setup stores all required files in the
<XPR_Installationpath>\bin\stunnel\ directory.

If you wish to use stunnel with other connections, execute the following steps:

1. On the XPR server you find the `stunnel.conf` file under
<XPR_Installationpath>\bin\stunnel\. Open the file for editing.
The following example shows how to add a new connection with port 80 for receiving and a port 8080 for creating the connection.

```
cert = cert.pem  
key  = privkey.pem  
socket = 1:TCP_NODELAY=1
```

XPR System Installation

Installing the XPR Server and Configuring the Services

```
socket = r:TCP_NODELAY=1
session = 60
options = NO_SSLv2
options = NO_SSLv3
options = NO_TLSv1
options = NO_TLSv1.1
[crypto]
accept = 8945
connect = 10.9.30.49:8944
[newconnection]
accept = 80
connect = 10.9.30.50:8080
```

Save the file. The new settings become active after a reboot of the stunnel service. The name **newconnection** is freely selectable.

2. The following is required for creating an encryption on the client computer with the help of stunnel: Copy the stunnel.exe and stunnel.conf files from the XPR server into any directory. You need to modify the stunnel.conf file as follows:

client = yes

```
socket = l:TCP_NODELAY=1
socket = r:TCP_NODELAY=1
session = 60
options = NO_SSLv2
options = NO_SSLv3
options = NO_TLSv1
options = NO_TLSv1.1
[remote]
accept = 8946
connect = <IP address of the remote server>:8944
The name remote is freely selectable.
```

The stunnel configuration setup is thus complete.

4.5.12 Installing the Copssh

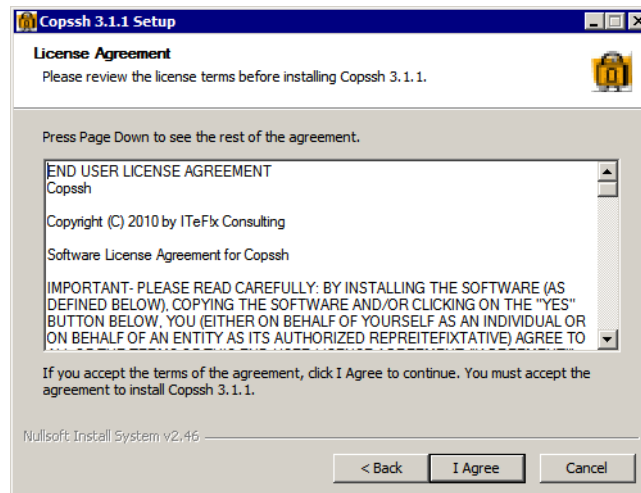
The Copssh setup starts automatically if you have performed the following:

- Activated the **SSH Daemon** check box when selecting the server components
- Activated the **Install WIBU-KEY software.** check box during the Dialogic setup
- Activated the **SSDP Service Plugin** check box when selecting the feature components

The Copssh setup starts with the following dialog:



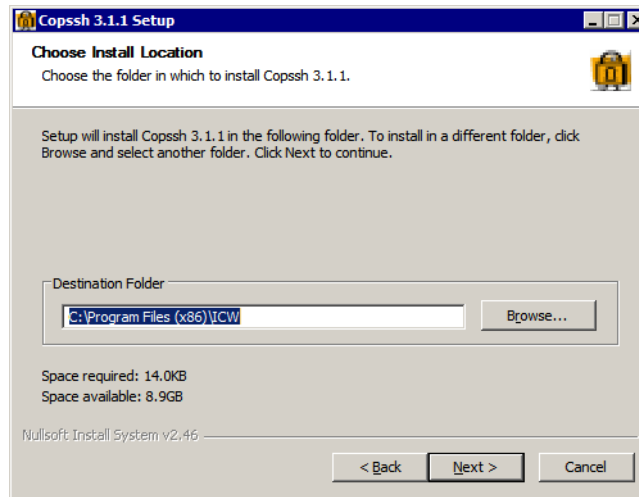
1. Click on **Next**.



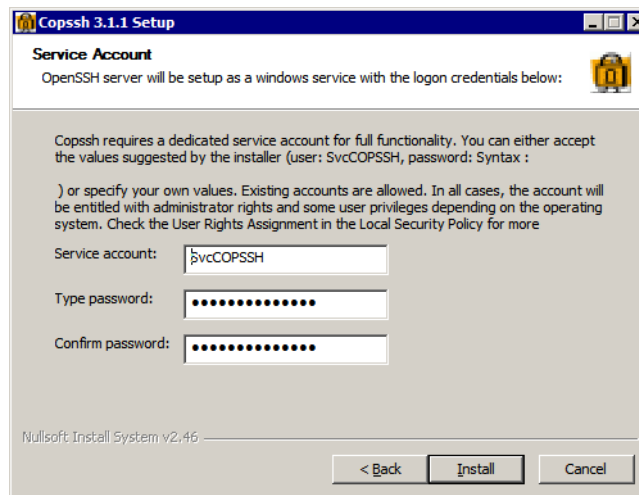
2. Click on **I agree**.

XPR System Installation

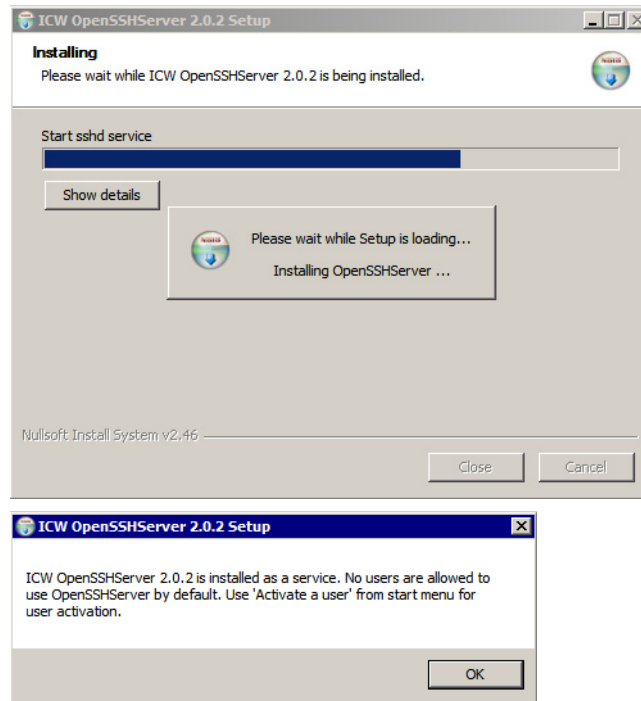
Installing the XPR Server and Configuring the Services



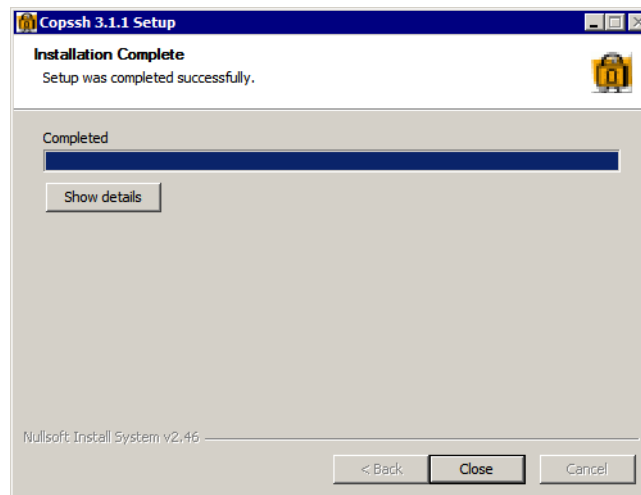
3. Accept the defaulted target path for the installation or click the **Browse** button to specify another installation target path. Click on **Next**.



4. You need to create a user account for Copssh for using the full Copssh functionality. You can accept the defaulted data, create a new account or select an existing account. Click on **Install** to start the installation.



5. Click on **OK**.



6. Click on **Close**.

The server software installation is thus complete. The component installer continues with the client application setup.

If you have not selected any client applications for installation, the completion of the component installer is displayed (cf. [Section 4.5.17, "Completing the Component Installer", on page 157](#)).

4.5.13 Installing the Language Packets

The setup files of the language packets for German, British English and American English are found in the `Languages` directory. You find all languages on the installation medium. You find a list of all available languages in [Section 4.3.5, “Selecting the Server Languages and the Default Language”, on page 77](#).

A language packet comprises a large number of files, so that its installation will take some time. The scope of a language packet includes, for example, all TUI voice prompts as well as the Web Assistant interface.

4.5.13.1 Installing Language Packets belatedly

To install further language packets at a later date, start the installation from the installation medium (`setup.exe` file in the root directory), and select the new language in the corresponding dialog (cf. [Section 4.3.5, “Selecting the Server Languages and the Default Language”, on page 77](#)). Then continue with the setup.

NOTE: To install another language packet you need another language license.

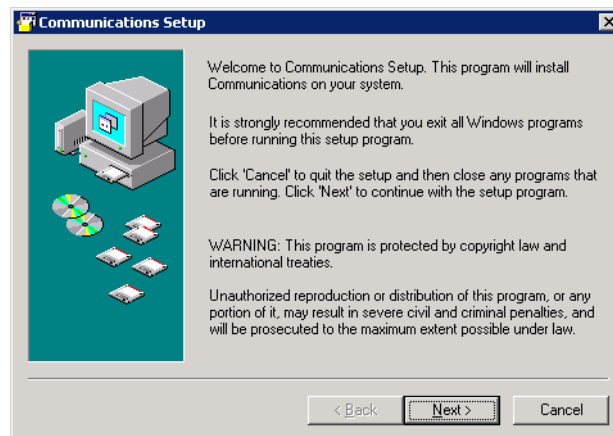
The setup programs of the language packets check whether licenses for the language-dependent components (Web Assistant and TUI) are available. If such licenses are found and you have selected these components during the XPR server installation, the language support for such products is installed fully automatically.

4.5.14 Installing Client Applications

After the XPR server software installation, the setup programs of the administrative client applications that have been selected in [Section 4.3.8, “Selecting Client Components”](#), on page 81 are invoked.

NOTE: The setup programs of the client applications all follow the same pattern. We describe the process based on the *Communications* client application.

1. After the setup program start, the following dialog opens:



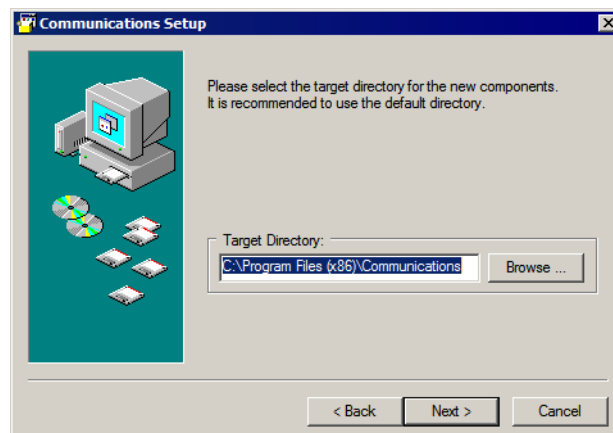
2. Click on **Next**.

Up comes this dialog:

The End User License is displayed. Activate the checkbox.

3. Click on **Next**.

Up comes this dialog:



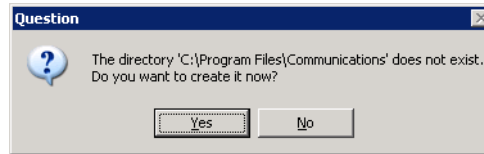
4. This dialog displays the target directory of the installation. We recommend to copy the default.

XPR System Installation

Installing the XPR Server and Configuring the Services

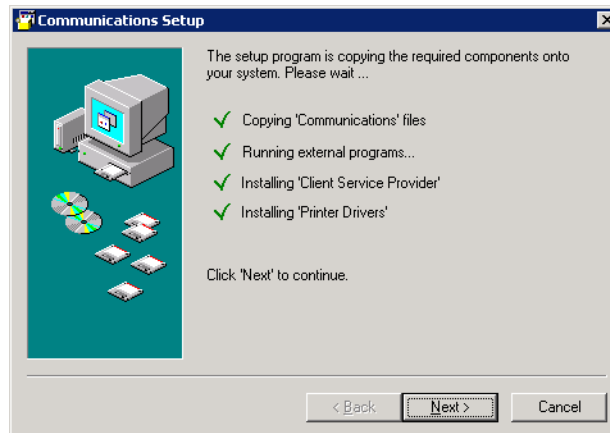
5. Click the **Continue** button.

Up comes this dialog:



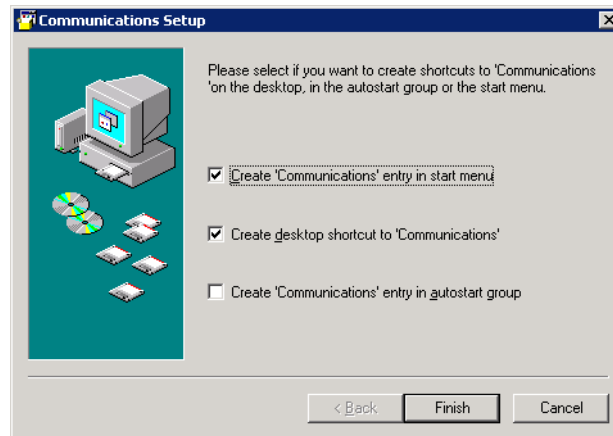
6. Click the **Yes** button to define the installation directory.
7. The installation is being performed. The installation progress is indicated as follows:
 - You can recognize an action just carried out by the pointed bracket preceding the corresponding text, which is set off in bold.
 - A successfully accomplished installation step is indicated with a green tick.
 - If an installation step goes wrong, the corresponding entry is preceded with a red cross. In this case please check the installation preconditions and restart the setup program.

As soon as all installation steps are complete, the following dialog opens:



8. Click on **Next**.

Up comes this dialog:

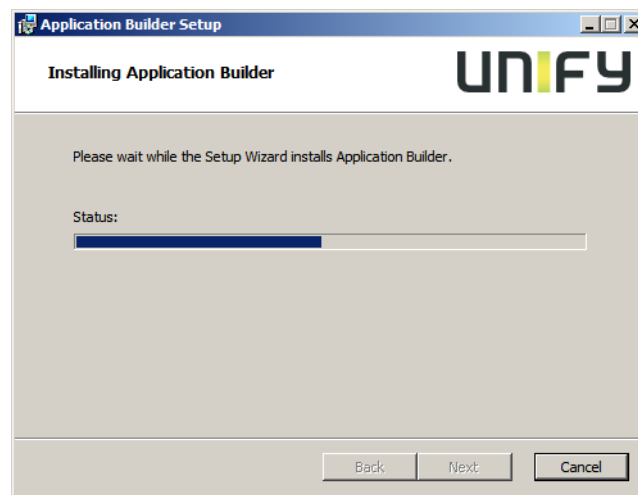


9. Specify whether and where shortcuts to the client application should be defined. Any combination goes. Then click on the **Finish** button.

The installation of a client application is thus complete.

4.5.15 Installing the Application Builder

The Application Builder setup starts and proceeds fully automatically. You need not click any button.



4.5.16 Installing the Add-On Components

Any add-on component that was selected during the choice of system components (see [Section 4.3.10, “Installing the Adobe Reader”](#)) should be installed at this point.

4.5.16.1 Adobe Reader

The Adobe Reader 9 is set up fully automatically.

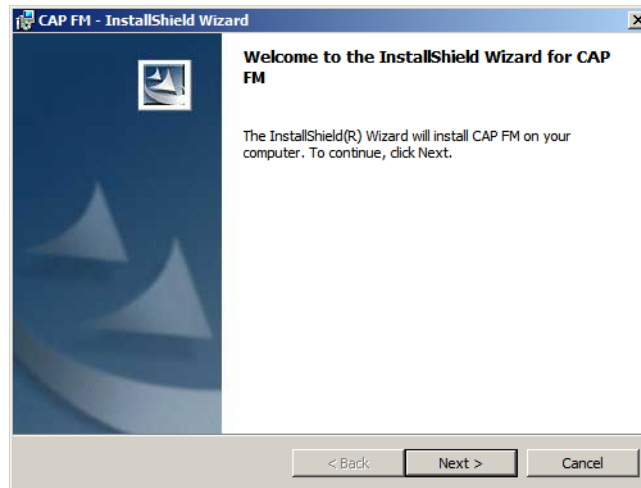
4.5.16.2 Installing the HiPath CAP Fault Management

The HiPath CAP Fault Manager is an SNMP browser that displays error messages and statuses of the installed XPR software components. Using the HiPath CAP Fault Manager requires an SNMP service installed in the operating system.

IMPORTANT:

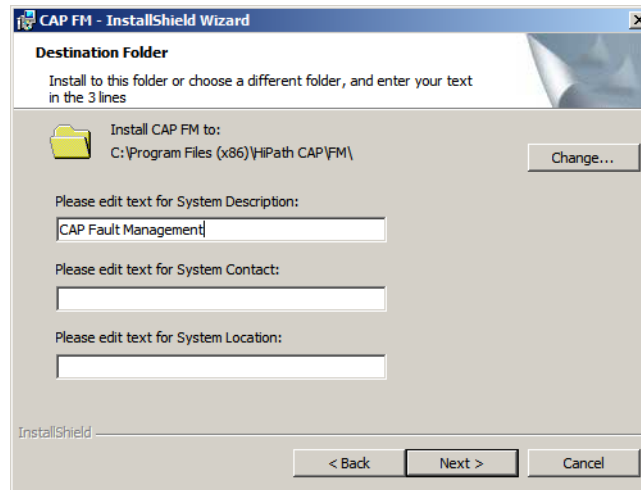
The HiPath CAP Fault Manager cannot be installed via a remote desktop connection.

1. Up comes this dialog:



2. Click on **Next**.

Up comes this dialog:



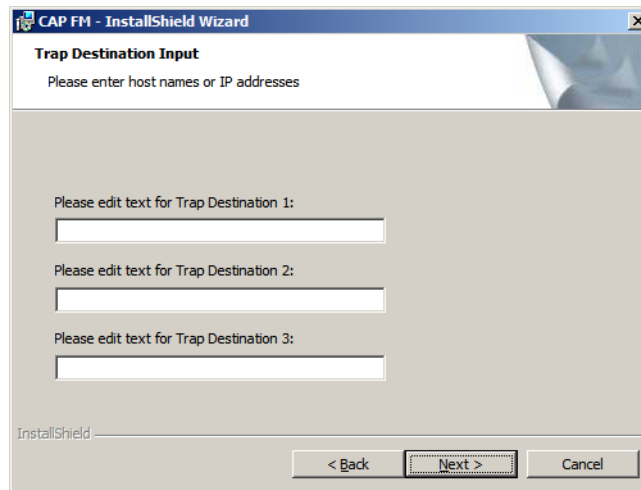
XPR System Installation

Installing the XPR Server and Configuring the Services

3. Click on **Next**.

If you wish to use another installation path, click the **Change...** button and specify a different installation path before you click on **Next**.

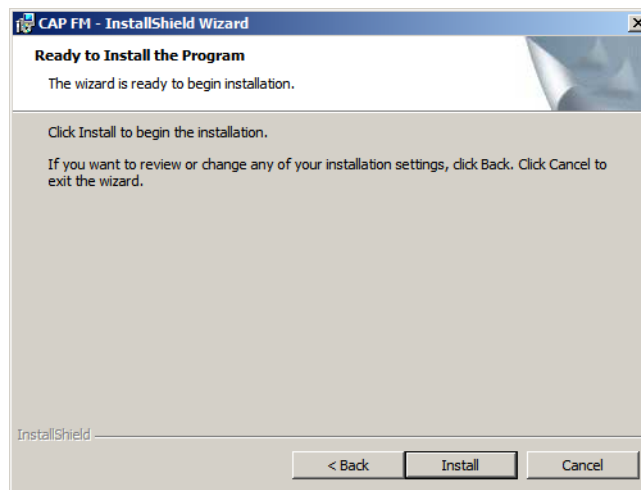
Up comes this dialog:



The dialog box is titled "CAP FM - InstallShield Wizard" and has a subtitle "Trap Destination Input". It contains the instruction "Please enter host names or IP addresses". Below this, there are three text input fields, each preceded by the label "Please edit text for Trap Destination 1:", "Please edit text for Trap Destination 2:", and "Please edit text for Trap Destination 3:" respectively. At the bottom, there are three buttons: "< Back", "Next >", and "Cancel". The "Next >" button is highlighted with a dashed border.

4. Click on **Next**. If you know trap destinations, specify them optionally.

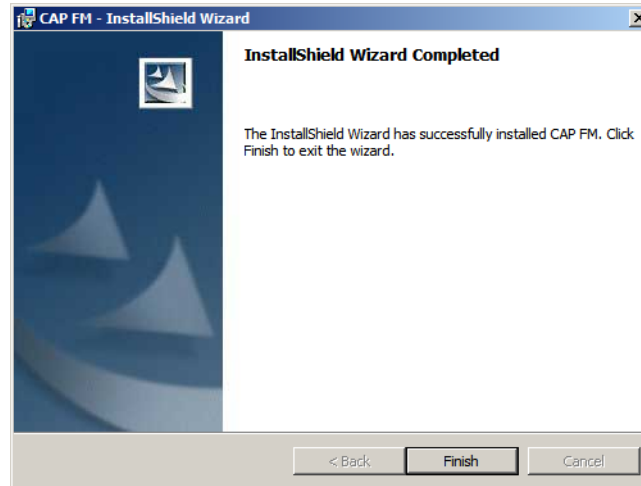
Up comes this dialog:



The dialog box is titled "CAP FM - InstallShield Wizard" and has a subtitle "Ready to Install the Program". It contains the text "The wizard is ready to begin installation." and "Click Install to begin the installation." Below this, it says "If you want to review or change any of your installation settings, click Back. Click Cancel to exit the wizard." At the bottom, there are three buttons: "< Back", "Install", and "Cancel". The "Install" button is highlighted with a dashed border.

5. Click on **Install**. If you want to check the settings made so far, click the **Back** button to open the previous dialogs.

Up comes this dialog:

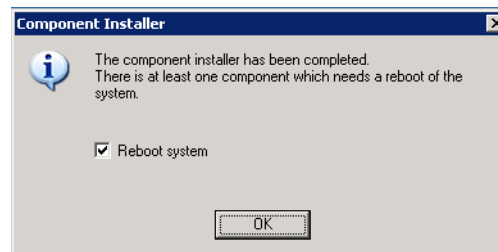


6. Click on **Finish**.

The installation of the HiPath CAP Fault Manager is complete.

4.5.17 Completing the Component Installer

A successful completion of the Component Installer is displayed in the following dialog.



Click on **OK**.

4.5.18 Checking Policies and Services

During the installation the automatic attempt was made to assign the user account under which the XPR services operate (see step 1 on page 102) the **Logon as a service** privilege, and to configure all XPR services in a way that they log on with this user account. Execute the following steps to check this and correct it if required.

XPR System Installation

Installing the XPR Server and Configuring the Services

Security policy

1. Open **Start > Control Panel > Administrative Tools > Local Security Policy**.

If you deploy a domain user account, proceed analog.

2. Open **Security Settings > Local Policies > User Rights Assignment**.
3. Rightclick the **Logon as a service** entry and select the **Properties** option.
4. Check whether this security setting is assigned to the user deployed by the XPR services or to a group this user belongs to. If this is not the case, correct it.
5. If you have made modifications, they must be activated by the following substeps:
 - a) Open a Windows command prompt.
 - b) Execute the `gpupdate /force` command.

NOTE: Executing this command may take some time, especially if many users are registered in the XPR.

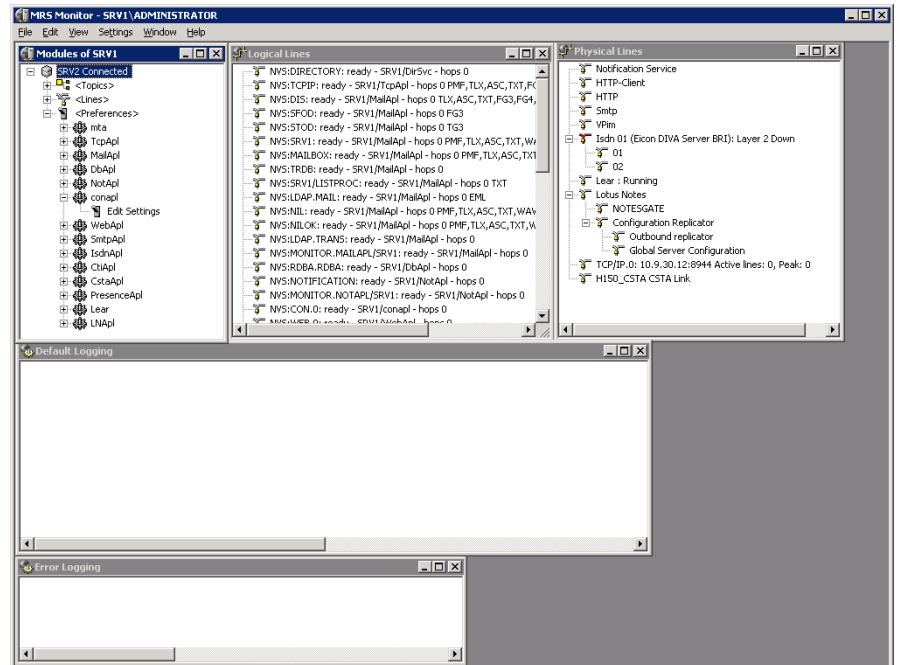
Services

6. Open **Start > Control Panel > Administrative Tools > Services**.
7. Rightclick an XPR service.
8. Select the **Properties...** option.
9. Click on the **Log On** tab.
10. Verify that the **This account** radio button is active and the user account selected in step [2 on page 102](#) has been entered.
11. Execute steps [7](#) to [10](#) for all XPR services.

4.5.19 Checking Fax G3 Post-Dialing

If you have the **Fax G3 Post Dial** option activated in [Table 10 on page 92](#) in [Section 4.5.1, “Selecting Features”, on page 91](#) in the **Telematic hardware** group, you need to check whether the following configuration steps have been executed when you configure the corresponding telematics APL (see administrator documentation *OpenScope Xpressions Server Administration*):

1. Open **Start > All Programs > XPR > Monitor - System Logging**.

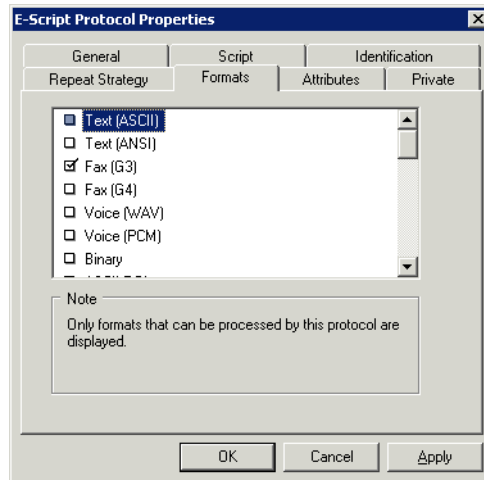


2. Doubleclick **ISDNApi** in the **Modules of <XPR server name>** window.
3. Doubleclick **Advanced Settings**.

XPR System Installation

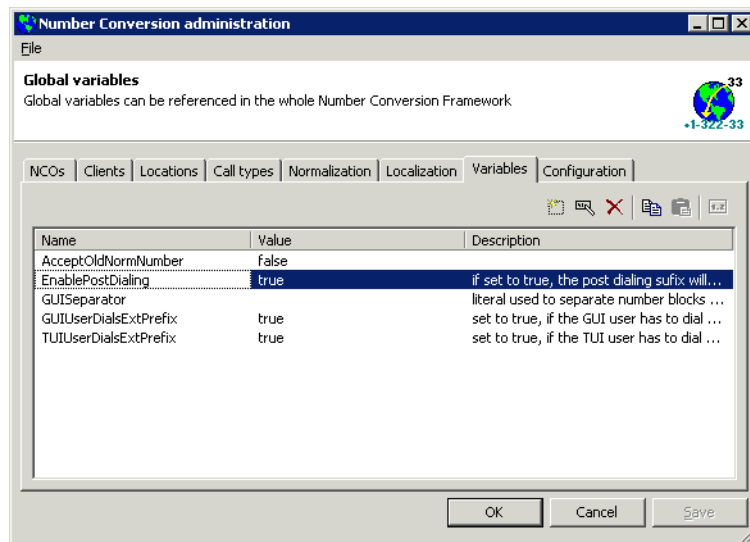
Installing the XPR Server and Configuring the Services

4. Doubleclick the entry of the Fax G3 protocol on the **Protocols** tab.



5. Verify that only the **Fax (G3)** checkbox is active and all other entries are inactive.
6. Click on **OK**.
7. Click on the **Devices** tab.
8. Click on the **NCO administration**  icon and then on the **Variables** tab.

As alternative, you can also click on the **OK** button, start the `<XPR_Install>/bin/NumberConversionAdmin.exe` file and click on the **Variables** tab. The analog dialog opens then with additional tabs.



9. Verify that the variable **EnablePostdialing** has value **true**.
10. Click on **OK**.
11. Click on **OK**.

4.5.20

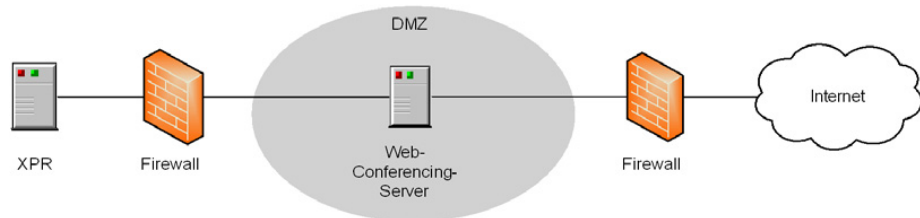
4.5.21 Installing the Web Conference Server in a DMZ

NOTE: If the web conference server is not to be installed in a DMZ but on the same computer as the XPR server, you need to activate the **Web Conference Server** checkbox in [Section 4.5.1, “Selecting Features”, on page 91](#) under the **Connection APL** item.

A demilitarized zone (DMZ) describes a computer network with controlled access options to the servers contained therein. The systems set up in the DMZ are shielded by one or several firewalls against other networks (e. g. internet, LAN). This separation allows access to publicly available services (Bastion Hosts with e. g. e-mail, WWW or similar) and protects the internal network (LAN) from unauthorized access at the same time.

IMPORTANT: You must not install a web conference server on Window XP or Windows 7.

The following figure shows a web conference server in a DMZ.



To install a web conference server in a DMZ you require the following:

- The XPR V7 installation medium
- A license file that contains a MAC ID of the license server and is bound to the web conference computer. This file contains only the licenses for the features WEBCONFROOM, WEBCONFPARTICIPANT and WEBCONFSERVER.
- Processor and RAM
 - Up to 20 parallel sessions: 2 GHz and 1 MB
 - In case of 20 - 100 parallel sessions: Xeon with 2,5 GHz and 2 GB
- We recommend free memory of 50 GB for file transmissions during sessions. The hard disk size is not critical because, with the exception of writing log files, no considerable data amount is written on the hard disk.
- Network board with 1 Gbit/s

- The IIS (Internet Information Server) or another web server may only be installed if it is configured not to use the default ports 80 and 443 but the ports 8080 and 8443, for example.
- Bandwidth to the internet
 - In each session, 15 kbit/s must be made available per simultaneously connected master and per simultaneously connected client. If 10 parallel sessions take place, i. e. there are 10 masters and 10 clients, a bandwidth of 300 kbit/s is required.
 - When using top video quality, the necessary transmission rate is five times higher.
- Port 80 (TCP; HTTP) and port 443 (TCP; HTTP) must be accessible. Using port 5000 (TCP) is optional. When using HTTPS, a certificate must be present for each server. Using HTTPS increases the necessary bandwidth via proxy server.
- Every server requires an IP address. IP V6 is not supported yet.
- Virtualization
 - Virtualization using
 - VMware ESX V4.0 and V4.1,
 - VMware ESXi V4.0, V4.1, V5.0, V5.1 and V5.5is supported. VMware ESXi is also called VMware vSphere Hypervisor.
 - A dedicated, real CPU of the host must be assigned to the virtual XPR computer.

NOTE: Please refer to the *OpenScape Xpressions Release Notice, Service Documentation*, to see which VMware versions have been released for using XPR in a virtual environment.

- If the web conference server is to be installed on a computer in a DMZ, the following applies for the Connection APL components (see [Section 4.5.1, “Selecting Features”, on page 91](#)):
 - UCC **must** be installed on the XPR computer in the intranet.
 - PostgreSQL **must** be installed on the XPR computer in the Intranet.
 - Web Conference Server **must not** be installed on the XPR computer in the Intranet.
 - OpenScape Web Client may be installed on the XPR computer in the

XPR System Installation

Installing the XPR Server and Configuring the Services

intranet.

NOTE: Except for step [13 on page 169](#) all of the following steps in this chapter are to be performed on the web conference computer in the DMZ.

4.5.22 Voice Conferences with SIP

If you use SIP (port 5060) in the IP APL and voice conferences with SIP, configure two IP addresses. See the section “SIP Configuration” in the administrator documentation *OpenScape Xpressions Server Administration* for details.

4.6 Modifying, repairing or removing the XPR Installation

To maintain an existing XPR system, the XPR system setup program provides further modes. To modify or repair an installation you need the installation sources from the installation medium.

Modify

An existing installation is supplemented by further components or features. This requires a valid license for the new component or feature.

Repair

In this mode an existing system is repaired. For this purpose the running XPR server must be stopped. During a repair, all components and features that are already installed are reinstalled. When you repair the XPR system, you cannot change the scope of installation. Use the **Modify** mode for this.

Remove

In this mode the entire XPR system is uninstalled. To uninstall single components, use the Modify mode.

IMPORTANT: If you want to **modify** or **repair** the installation, you need to stop the XPR server, which is then not available. Perform such maintenance work only when no users are logged in at the system.

4.6.1 Running Xpressions Setup with OpenSSL files on Hotfix folder

Some Xpressions services, in order to run, require you to have updated OpenSSL files. When running Xpressions Setup those OpenSSL files are replaced with old versions making some services not able to run again or some features not able to be installed.

In order to prevent such problems, when running the Xpressions setup, the OpenSSL files must be copied to the Xpressions setup **HOTFIX** folder. Those files are now available on the latest OpenSSL hotfix. The OpenSSL hotfix contains a folder named **Files** and its content must be copied to the HOTFIX folder on the Xpressions setup installation path.

XPR System Installation

Modifying, repairing or removing the XPR Installation

4.6.1.1 Installing the SNMP feature

If you select the **SNMP for license and SystemVersionInfo** feature when running the Xpressions setup with the OpenSSL file on the **HOTFIX** folder, you may be prompted with a message informing you that the files are in use when the setup tries to install the feature.

That is because the MS Windows **SNMP Service** is running. You will need to manually stop this service and click 'try again' in order to make the setup continue.

The SNMP service will be running after the setup finishes

4.6.2 Stopping and starting the XPR Server

If you need to install single components belatedly or repair a troublesome installation, you may have to manually stop the XPR server.

Proceed as follows:

1. Open the menu **Start > Programs > Xpressions** and click on the **Stop Server** entry.

The XPR server is stopped. Depending on the number of active components this may take some time. You can watch the stopping process in the XPR monitor.

As soon as you have completed all administrative jobs, or the new components are installed, you may reboot the XPR server.

2. To start the XPR server, open the menu **Start > Programs > Xpressions** and click on the **Start Server** entry.

The XPR server is rebooted. Depending on the number of installed components this may take some time. You can follow the server start in the XPR monitor.

Please keep an eye on the newly installed components, which possibly issue error messages.

4.6.3 Modifying an existing Installation

You need to modify an existing installation when, for example, an additional component has been purchased, or this component is to be installed.

IMPORTANT: If you change an existing installation, the entire XPR server will be shut down and the installed features will not be available during the modification. This was different in previous versions.

Therefore only modify an existing installation if the XPR server can be smoothly stopped.

If you want to uninstall a feature, thus a specific OpenScape Xpressions server functionality, it is sufficient to remove the corresponding checkmark in the **Select Components** (cf. [Section 4.5.1, "Selecting Features", on page 91](#)) dialog. The setup program of the *OpenScape Xpressions Server* component then modifies the available features on the basis of the selection in this dialog.

How to modify an existing installation:

XPR System Installation

Modifying, repairing or removing the XPR Installation

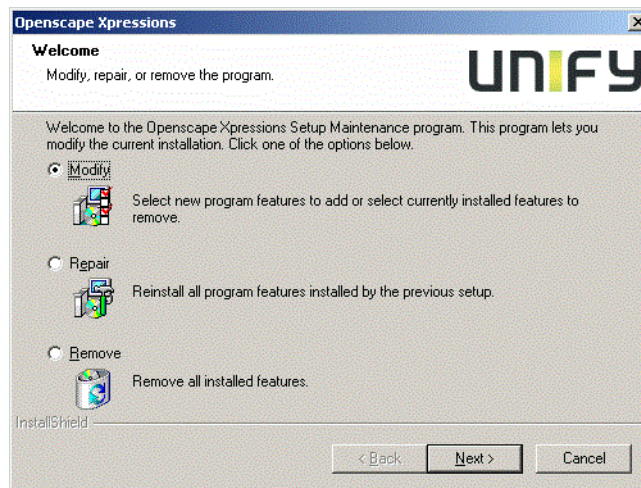
1. Connect the installation medium to the server computer.
2. The welcome screen is displayed. The Wrapper starts and displays in succession the dialogs that you can also see during an initial installation (cf. [Section 4.3.5, “Selecting the Server Languages and the Default Language”, on page 77](#)).

Each of these dialogs displays the default settings. The Wrapper does not have an update logic, in other words, it does not know which components have already been installed. The *Server Setup* component and the language packets are always selected in the corresponding dialog though.

Select in the corresponding dialogs the components to be reinstalled. Components that you additionally select will be additionally installed.

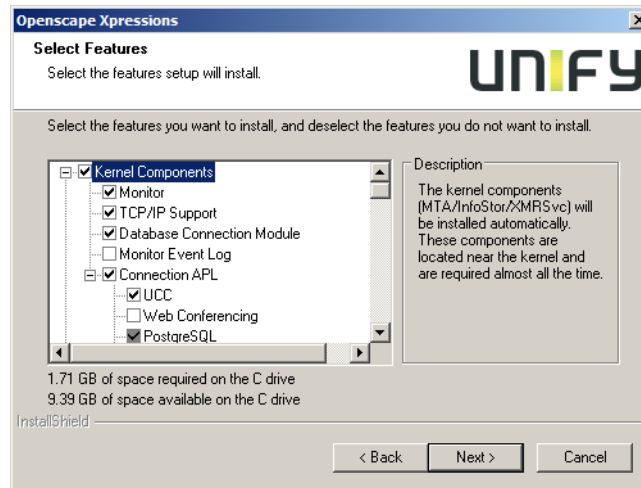
NOTE: Since modifying an available setup usually means that merely a OpenScape Xpressions server feature is to be added or removed, we suggest you do not select any other component except the OpenScape Xpressions server for installation and perform the required modifications in the **Select Components** dialog. This will significantly shorten the modification process.

As soon as all Wrapper dialogs have been edited, the Wrapper starts the XPR server setup program. Since an XPR server is already installed, the setup program selects in the following dialog the **Modify** option:



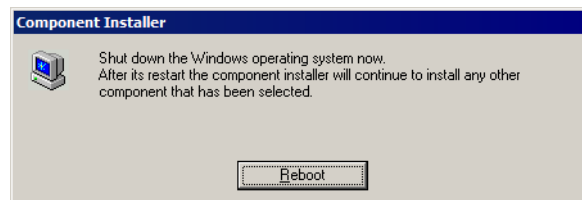
3. Make sure that the **Modify** option is selected. Click the **Continue** button.

Up comes this dialog:



4. Select the components that you want to add to the installation or cancel the selection of the components that you want to uninstall. For further information and descriptions about the XPR features please refer to [Section 4.5.1, “Selecting Features”, on page 91](#). Click the **Continue** button.
5. The setup program executes the necessary operations.
6. Subsequently, further components may be installed (e.g. language packets). These installations are performed fully automatically, as all required specifications are already available.

Up comes this dialog:



7. If you want to start the XPR server, select the **Start** OpenScape Xpressions option and click on **OK**.

If you do not want to start the XPR server, make sure that the option is deselected and click on **OK**.

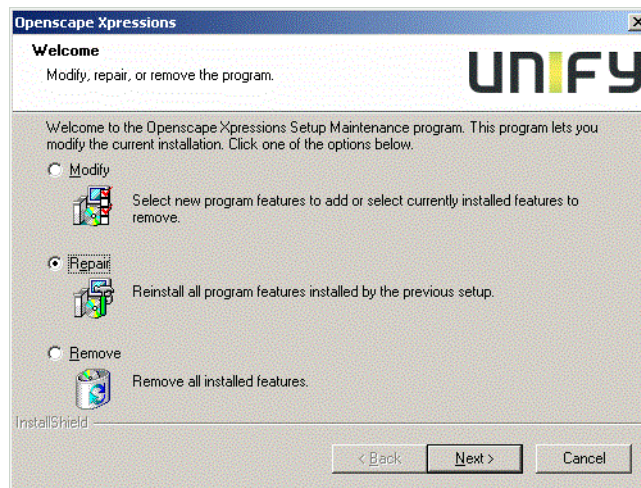
4.6.4 Repairing an Installation

With the **Repair** function you can repeat the last completed installation. It is not possible to add new program components or to remove any of them.

A new installation will **not** override the configuration of single components. The configuration of the XPR system is after the repair the same as before. Special configuration settings that you have performed for the components are kept.

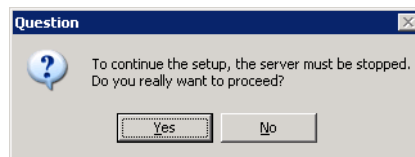
Proceed as follows:

1. Connect the installation medium to the computer on which the XPR server. Confirm the dialogs with **Next** until the following dialog opens:



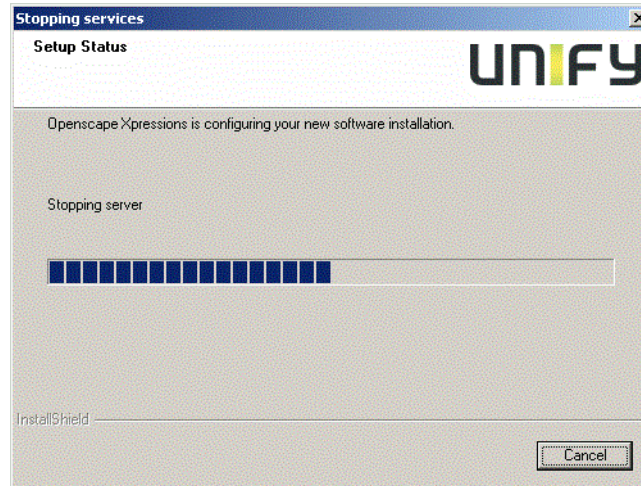
2. Enable the **Repair** option and confirm with **Next**.

Up comes this dialog:

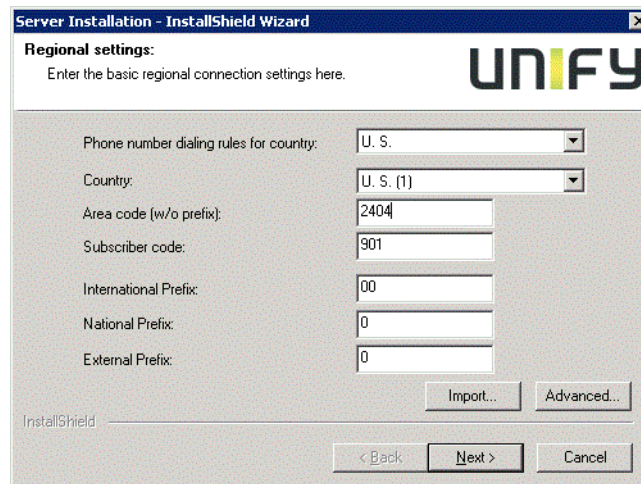


3. So that the components can be repaired, the XPR server must be stopped. Click on the **Yes** button to automatically stop the XPR server.

Up comes this dialog:



After the server stop the following dialog opens:



XPR System Installation

Modifying, repairing or removing the XPR Installation

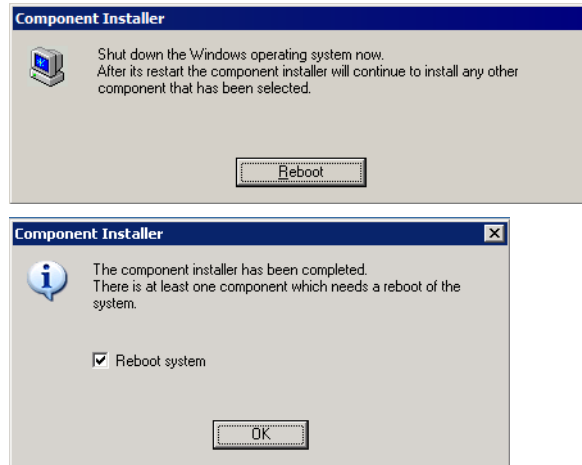
4. If required, correct the settings in this dialog and then click on **Next**.

All components already installed are reinstalled.

5. The setup programs of the other system components (e.g. the installed language packets, Communications, Application Builder) will then be executed, so that possible errors in these installations can be repaired.

Repairing is complete as soon as these setup programs terminate.

Depending on the modifications one of the following dialogs is displayed.



Click on **OK**.

4.6.5 Removing the XPR System completely

You can use the **Remove** function to uninstall the entire XPR server installation and the components (e.g. language packets) on your computer. Client applications will not be removed. If required, this can be done individually via the software management of the operating system.

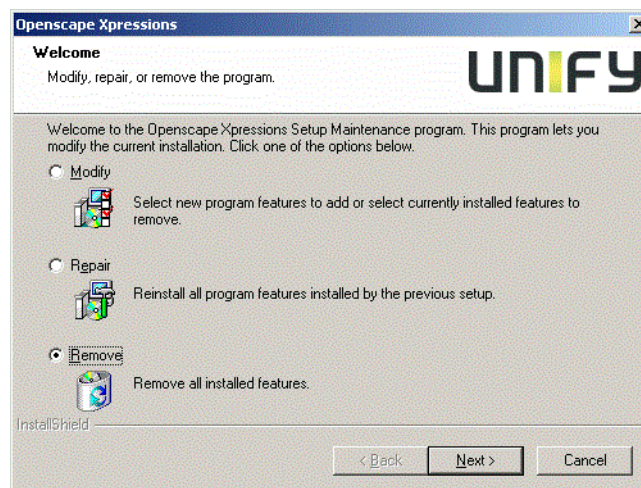
NOTE: You can also remove the XPR system via the software management of the operating system. In doing so, you must explicitly uninstall the language packets then as well.

How to remove the XPR system:

1. Connect the installation medium to the server computer.
2. The welcome screen is displayed. The Wrapper starts and displays in succession the dialogs that you can also see during an initial installation (cf. [Section 4.3.5, "Selecting the Server Languages and the Default Language", on page 77](#)).

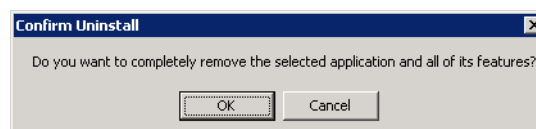
Click on **Next** in each dialog.

As soon as all Wrapper dialogs have been edited, the Wrapper starts the XPR server setup program. Since an XPR server is already installed, the following dialog is displayed:



3. Select the **Remove** option. Click the **Continue** button.

Up comes this dialog:



XPR System Installation

Modifying, repairing or removing the XPR Installation

4. Click the **OK** button to confirm the uninstallation. The **Cancel** button cancels the action without removing any components.

The files and registry entries associated with the XPR system are deleted. Depending on the installation scope, this may take a while.

5. Subsequently, the available language packets are uninstalled.
6. Restart the computer.

5 Installing and Configuring the Driver Software

During an initial XPR system installation you can have the necessary ISDN hardware driver automatically installed (cf. [Section 4.3.9, "Selecting External Software", on page 83](#)). The hardware driver installation is then started by the Wrapper. After the installation, the configuration interface to the installed driver opens automatically, so that you can make the required settings.

For more information about the driver installation, please also refer to the documentation of the ISDN card manufacturer.

5.1 Installation and Configuration of the Sangoma Diva(R) ISDN Boards

IMPORTANT: At times, Dialogic uses different version numbers for the same board. For example, the hardware description features a specific version number for a board, but in the Sangoma Diva(R) Configuration Manager you find another version number for the same board. The version numbers used for Sangoma Diva(R) ISDN boards in this XPR V7 guide are always the version numbers specified in the Sangoma Diva(R) Configuration Manager!

Refer to the *OpenScape Xpressions Release Notice* for a list of the supported Sangoma Diva(R) ISDN boards.

Mixed operation between different BRI or PRI cards as well as mixed operation of BRI and PRI cards on a server computer is not released.

5.1.1 Driver Installation under Windows Server 2008 (R2) / Windows 7 Prof.

NOTE: 64-bit systems require a manual and retrospective setup of the drivers.

The driver installation is the same for all types of supported Sangoma Diva(R) board types.

Dialogic does not offer Eicon ISDN board drivers anymore, "Sangoma Technologies" took over the support. For this reason, we recommend to download the latest Sangoma Diva(R) driver that is only available at Sangoma site:

<https://wiki.sangoma.com/display/DVC/Diva+System+Release+for+Windows>

After downloading the driver, execute the `DivaAll-64bit.exe` file:

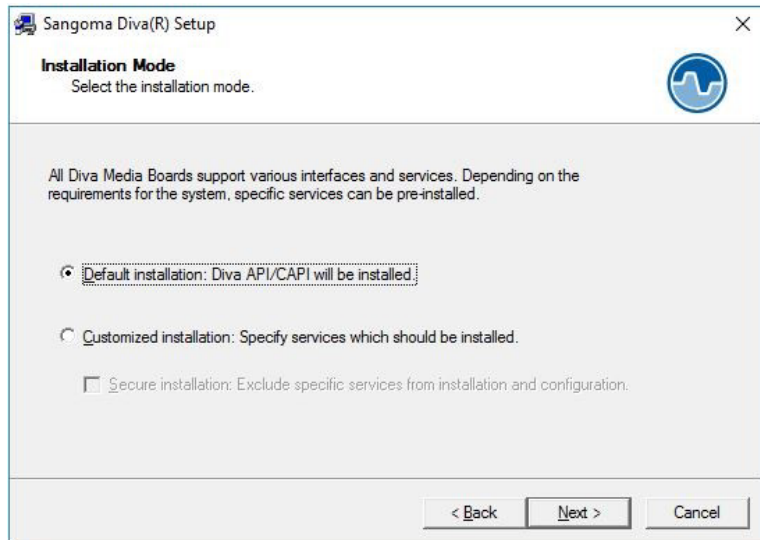
1. The setup program starts with the following welcome dialog.



Installing and Configuring the Driver Software

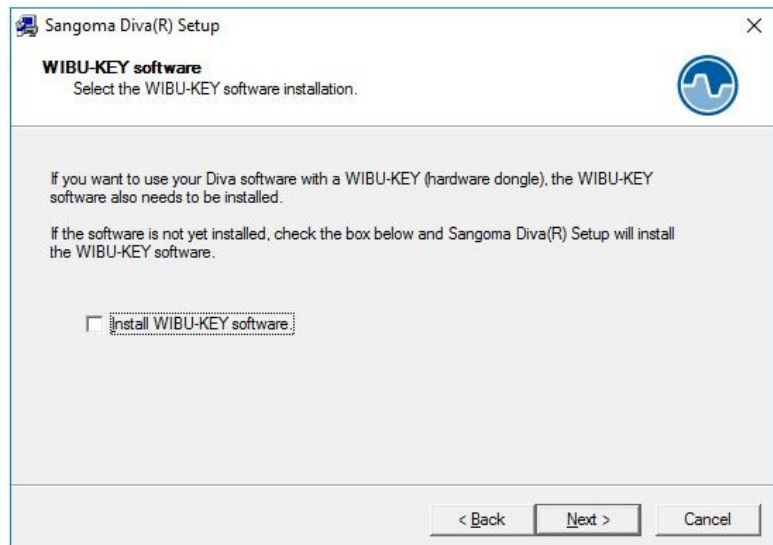
Installation and Configuration of the Sangoma Diva(R) ISDN Boards

2. Click on **Next**. Up comes this dialog:



3. Select the option **Default installation: Diva API / CAPI will be installed**. Then click on **Next**.

Up comes this dialog:

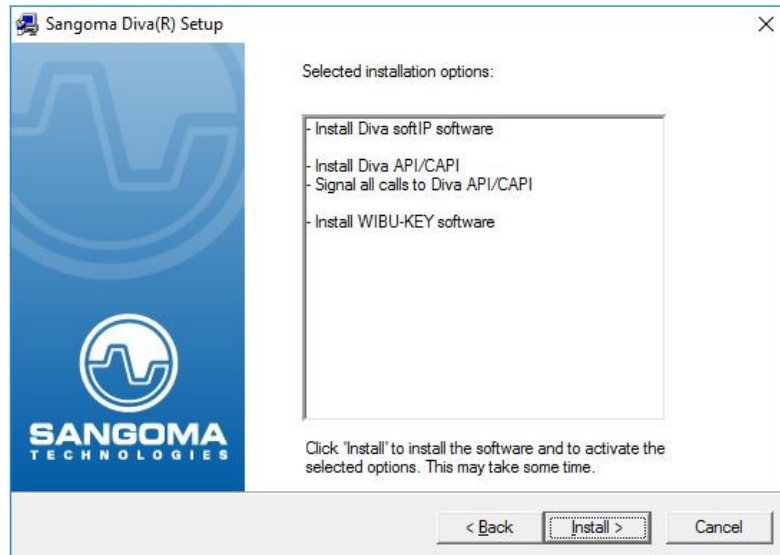


4. If you use WIBU-KEY, select the option **Install WIBU-Key software**. Then click on **Next**.

Up comes this dialog:

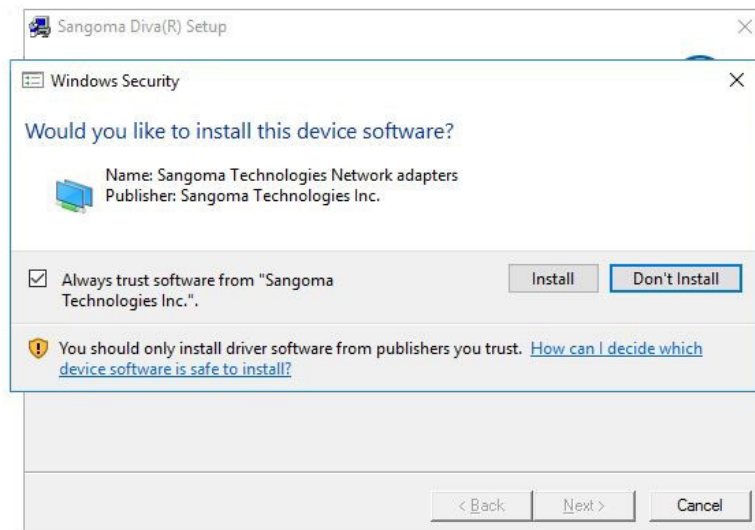
Installing and Configuring the Driver Software

Installation and Configuration of the Sangoma Diva(R) ISDN Boards



5. Check the selected the installation options. Then click on **Next**.

Up comes this dialog:



6. Select **Install** on Windows Security warning message.

Up comes this dialog:

Installing and Configuring the Driver Software

Installation and Configuration of the Sangoma Diva(R) ISDN Boards



7. If the driver installation was started automatically by the Wrapper, it is **essential** that you **deactivate** the **Restart your computer** option here. Finally, click **Finish**.

NOTE: After the driver installation the **eicnet.dll** file must be copied from:

....\XpressionsInstall\Drivers\Dialogic\64bit\Cornet

to:

<drive>\Windows\System32

5.2 Configuration of the Sangoma Diva(R) ISDN Boards

NOTE: The Sangoma Diva(R) ISDN board configuration is performed with the **Sangoma Diva(R) Configuration Manager** program. If you perform the driver installation outside the XPR Component Installer, you need to start the configuration program manually in the Windows start menu.

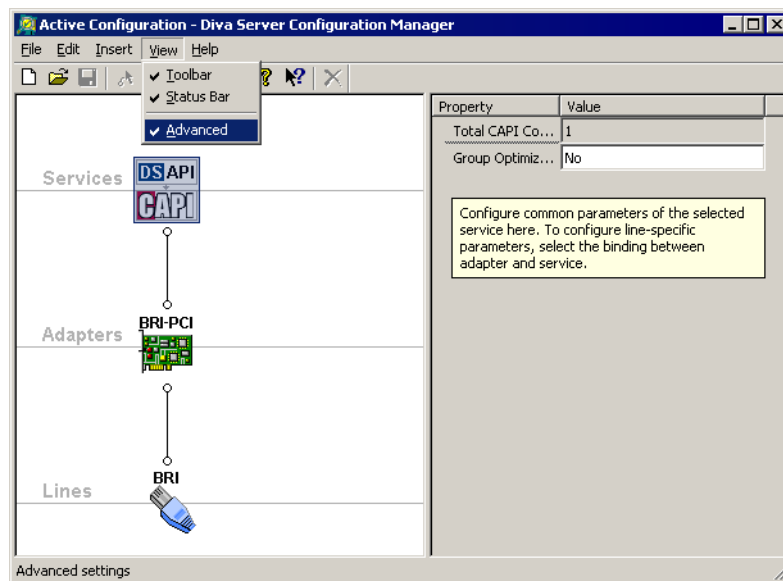
You find detailed information about configuring a Sangoma Diva(R) board in connection with PBXs of the Unify GmbH & Co. KG in [Appendix C](#).

5.2.1 Configuration of the Sangoma Diva(R) Server BRI Board respectively 4BRI Board

The left side of the window shows the connections that can be administered on the right-hand side. These are connections from the PBX (**Lines** level, **BRI** icon) via the Sangoma Diva(R) board (**Adapters** level, **BRI** icon) up to the **Services** level (**CAPI** icon).

NOTE: The Capi driver is now branded with **Sangoma Technologies** by default. A pull-down menu for **Eicon Networks** is available in the configuration.

1. Open the **View** menu and select the **Advanced** option. This option releases extended configuration options for the driver in the Sangoma Diva(R) Configuration Manager.

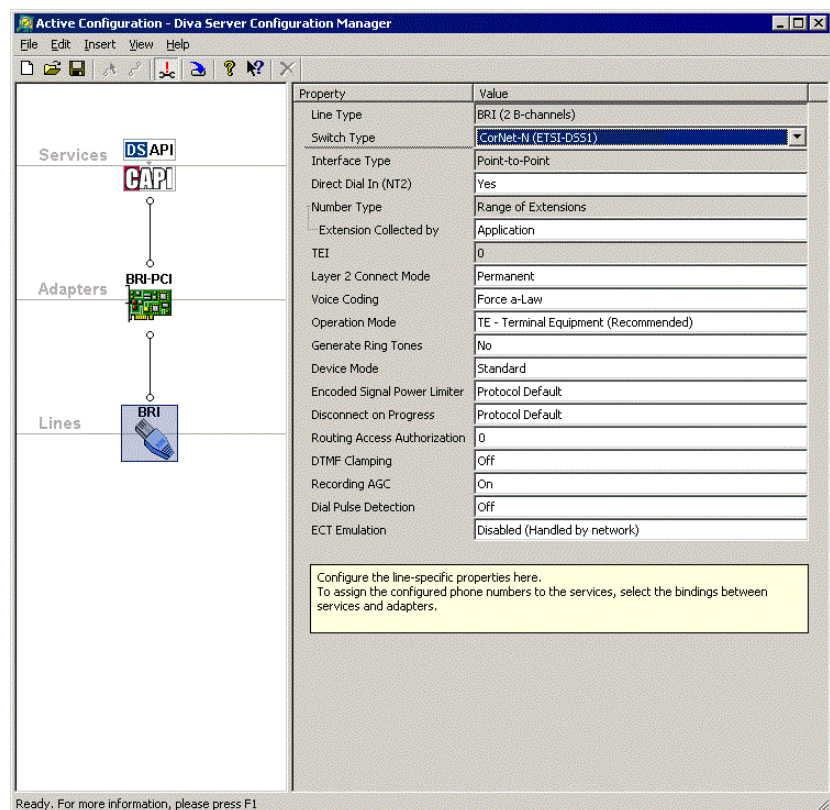


2. On the **Lines** level select the **BRI** icon.

Installing and Configuring the Driver Software

Configuration of the Sangoma Diva(R) ISDN Boards

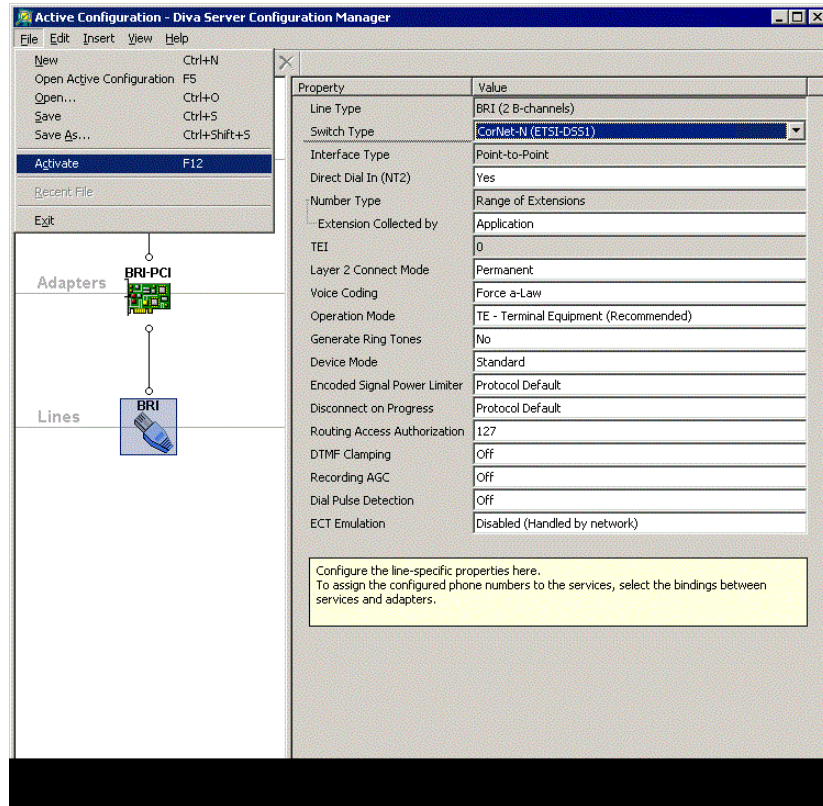
3. Set the following parameters in the right window portion:
 - a) Select one of the following settings in the **Switch Type** field:
 - **CorNet-N** when using a HiPath 3000 PBX
 - **CorNet-NQ** when using a HiPath 4000 PBX
 - **CorNetN E1** when using a Hicom 300/9006 PBX
 - b) In the **Interface Type** field select the **Point-to-Point** setting.
 - c) In the **Direct Dial In** field select the **Yes** setting.
 - d) In the **Number Type** field select the **Range of Extensions** setting.
 - e) In the **Extension Collected by** field select the **Application** setting.
 - f) In the **Layer 2 Connect Mode** field select the **Permanent** setting.
 - g) In the **Voice Coding** field select the **Force a-Law (USA: Force μ -Law)** setting.
 - h) In the **Recording AGC** field select the **On** setting.
 - i) In the **Routing Access Authorization** field select setting **0**.
 - j) Repeat these configuration steps for all further BRI lines, if you use a 4BRI board.



Installing and Configuring the Driver Software

Configuration of the Sangoma Diva(R) ISDN Boards

4. Open the **File** menu and click on the Activate menu option to activate the settings.



5. A message says that the settings have been saved successfully and you are prompted to reboot the computer.

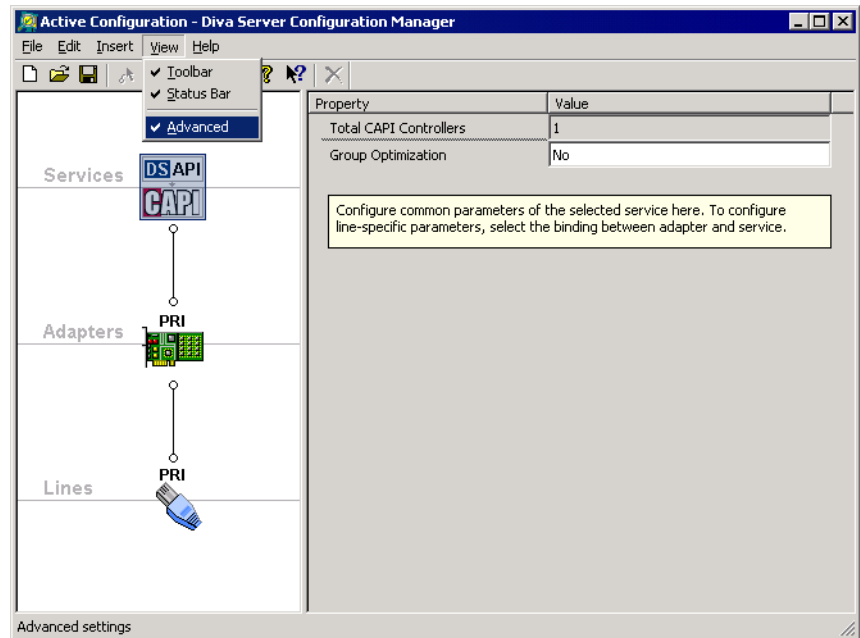
If the driver configuration was set off by the Wrapper, **do not** reboot at this point, but do it after the corresponding prompt by the Wrapper.

6. To resume the installation continue with [Section 4.5, "Installing the XPR Server and Configuring the Services"](#), on page 90.

5.2.2 Configuration of the Sangoma Diva(R) Server PRI Board

The left side of the window shows the connections that can be administered on the right-hand side. These are connections from the PBX (**Lines** level, **PRI** icon) via the Sangoma Diva(R) board (**Adapters** level, **PRI** icon) up to the **Services** level (**CAPI** icon).

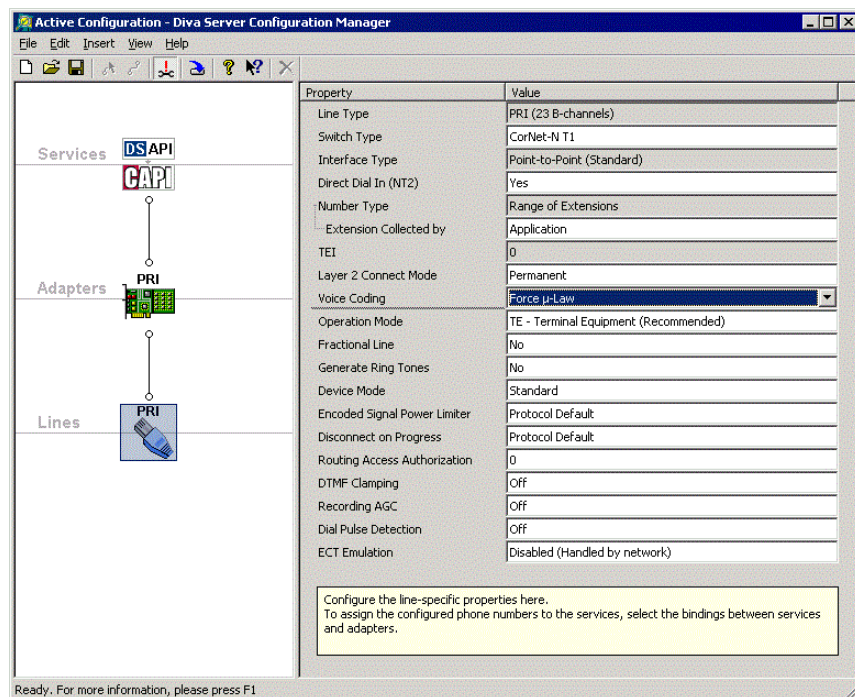
1. Make sure that the **Advanced** option is enabled in the **View** menu.



Installing and Configuring the Driver Software

Configuration of the Sangoma Diva(R) ISDN Boards

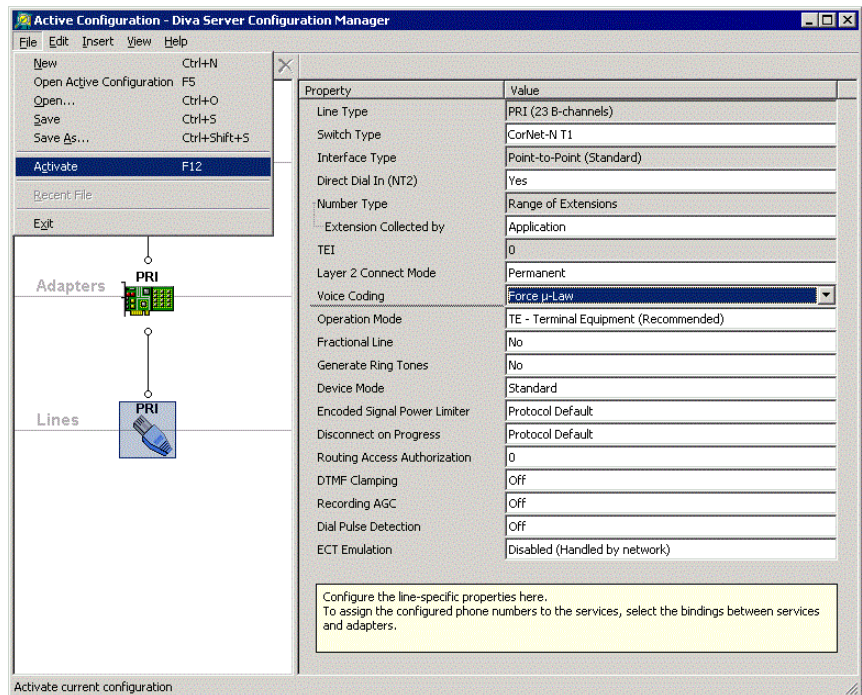
2. Next you need to select the **PRI** icon on the **Lines** level with a mouse click.
Set the following parameters in the right window portion:
 - a) Select one of the following settings in the **Switch Type** field:
 - **CorNet-N** when using a HiPath 3000 PBX
 - **CorNet-NQ** when using a HiPath 4000 PBX
 - **CorNetN E1** when using a Hicom 300/9006 PBX
 - b) In the **Interface Type** field select the **Point-to-Point** setting.
 - c) In the **Number Type** field select the **Range of Extensions** setting.
 - d) In the **Layer 2 Connect Mode** field select the **Permanent** setting.
 - e) In the **Voice Coding** field select the **Force a-Law** (USA: **Force μ -Law**) setting
 - f) In the **Recording AGC** field select the **On** setting.



Installing and Configuring the Driver Software

Configuration of the Sangoma Diva(R) ISDN Boards

3. The current changes must now be saved. In the **File** menu click the **Activate** option.



4. You now receive a message that the update was correctly saved and you are prompted to restart the computer.

If the driver configuration was set off by the Wrapper, **do not** reboot at this point, but do it after the corresponding prompt by the Wrapper.

5. To resume the installation continue with [Section 4.5, "Installing the XPR Server and Configuring the Services"](#), on page 90.

5.2.2.1 Restricting the Number of active Channels

Sangoma Diva(R) Server PRI boards provide a maximum of 30 B-channels and one D-channel. The D-channel is used for e.g. MWI control, the B-channels are used for sending messages. Besides the B- and D-channels there is another one for providing structure information, but this one can be ignored here.

If you do not want to use all channels in a first XPR upgrading phase, the number of active B-channels can be restricted.

NOTE: The configuration described here cannot be performed until the XPR server has been successfully installed.

Proceed as follows:

1. Start the XPR monitor and open the advanced configuration pages of the ISDN APL.
2. Open the **Device** tab.
3. Click the board entry that you want to change with the right mouse button and select the **Edit** menu option.

The dialog that displays the number of B-channels currently used appears.

4. Enter the desired number in the **Number of physical channels** field and click **OK**.
5. Restart the ISDN APL.

After the ISDN APL restart the number of B-channels newly set is used.

5.2.3 Configuration of the Sangoma Diva(R) Server PRI Board V3.0 and higher for Voice Conferences

Dialogic Diva does not support SIP control anymore. Therefore voice conferences are not supported anymore for ISDN PBXs with Sangoma Diva(R) ISDN boards of the hardware version 3.0 or later.

Installing and Configuring the Driver Software

Configuration of the Sangoma Diva(R) ISDN Boards

6 Setting up a Distributed XPR System

6.1 Overview

If the installation of a XPR server is distributed over several computers, this is called distributed XPR system.

In a distributed XPR system we differentiate between the kernel system and the associated satellite systems. The kernel system may be available in the network only once. The main advantage of distributed XPR systems is the scalability of their hardware resources.

In principal, virtually all hardware components and their transport protocols (ISDN, TCP/IP, IP APL, etc.) can be distributed on one or more satellites. Here, though, we consider only two configurations:

- One or several satellites, on which ISDN hardware is installed in each case and the required components are executed on the satellite(s).
- One satellite on which the Web server that provides the Web-based application Web Assistant is executed.

IMPORTANT: Setting up an XPR Connection APL on a satellite has not been released. It can be released project-specifically only if this satellite is connected to an XPR kernel on a Windows cluster (see the setup guide *OpenScape Xpressions Cluster Installation*). No further XPR Connection APL may be installed on any other satellite. If UC components (web conference server etc.) are installed, they may only be set up on the satellite on which the XPR Connection APL is installed also.

IMPORTANT: We do not recommend setting up the Print APL on a satellite system.

If you need a Print APL just the same, install it on the kernel system.

A XPR system with Exchange Connectors on another computer is also a distributed XPR system. The following table contains a list of program components that can be installed on a satellite computer:

Program component	
Web server	• Web Assistant
Fax server	• Fax-on-Demand
Voicemail server	NOTE: PhoneMail, VMS and ERGO must not be installed parallel in the languages D, US and UK. • PhoneMail • VMS • Unified Messaging Voice Mail (ERGO) • Automated Attendant (Vogue) • Speech Enabled Voicemail (EVO)
Hardware	• Dialogic/Eicon ISDN boards
Other components	• LDAP Directory Synchronization • IP telephony • MS Exchange 2003 Connector • MS Exchange True Unified Messaging Gateway

Table 13 Program Components of a Distributed System

IMPORTANT: Both kernel and satellite computers must have the **same** software level. When updating the XPR server, **all** server computers involved must be updated!

The **LAN switch setting** for the connection between the kernel computer and the satellite computer must be **FullDuplex/100 MBit/s** or **1 GBit/s**! Contrary to this minimum transmission rate to be provided by the interface the minimum transmission rate of the end-to-end connection must at least be 1 Mbit/s plus 150 kbit/s per voice channel on the satellite. Furthermore, the latency period in the network between all systems involved must not exceed 5 milliseconds.

Make sure that all language packets are already installed on the kernel computer before they are installed on a satellite computer.

A language packet may only be installed on a satellite if the satellite computer does not have a connection to a kernel computer.

6.1.1 Hardware Requirements

The hardware requirements for the kernel computer are the same as for the satellite computer. You find them in [Section 2.1.2, “Checking the System Requirements for the Server PC”](#), on page 24.

6.2 Firewalls between the Computers 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	Target
netbios-ns	TCP/UDP	137	137
netbios-dgm	TCP/UDP	138	138
netbios-ssn	TCP/UDP	1024-65535	139
Microsoft-SMB	TCP/UDP	1-65535	445
License Server	TCP/UDP	1-65535	61740
License Service	TCP/UDP	1-65535	13010
Con APL	TCP/UDP	1-65535	10000-10006

Table 14 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**.

6.3 Configure User Account

For the operation of a distributed XPR system, a new user account must be configured, which must have the following properties.

- The user account must be a member of the domain the kernel and satellite computer are in.
- The user account must have local administrative rights on the kernel and the satellite computer.
- The user account must have the “Logon as a service” privilege on all satellite computers.

NOTE: This user account must be assigned to all XPR services of the kernel computer and all XPR services of the satellite computer as login account.

If the password is changed, either because it expires automatically or the customer changes the password for this account, it must also be changed in the properties of each single service on the kernel computer and on all satellite computers. **Otherwise the satellite system functionality is no longer warranted!**

Assigning the “Logon as a service” privilege to a user account

Proceed as follows:

1. Open the Windows security settings on the satellite computer via **Start -> Control Panel -> Local Security Policy**.
2. Doubleclick the **Local Policies** entry in the list on the left hand side and then click **User Rights Assignment**. The **Log on as a service Properties** dialog opens. This dialog lists all user accounts that have the “Log on as a service” privilege.
3. Click on **Add User or Group...**
4. Enter the name of the user account and click on **Check Names**. When the account has been found in the domain, its name is represented underscored.
5. Click on **OK**.
6. Click on **OK**.
7. Close the Windows security settings.
8. Perform the steps 1 to 7 on each satellite computer.

6.3.1 Assign User Account

You must perform the following steps on the kernel and satellite computer to assign the created user account to the respective services.

1. Open the Windows service management (for example via **Start > Administrative Tools > Services**)
2. Doubleclick the **XPR Administrator (OpenScape Xpressions)** entry. The properties dialog of this service opens.
3. Open the **Log On** tab and select the **This account** option. Enter the desired account and the associated password in the now active fields. Via **Browse** you can select a login account previously set up.
4. Click on **OK**.
5. Repeat steps 2 and 3 for all XPR services.

IMPORTANT: XPR services that are no kernel services can be executed under the system account. But owing to the security aspects of the corresponding named pipes we expressly recommend not to do so.

6.4 Local Status Dispatcher Server on Satellite Computers

In distributed XPR systems the log communication of the APLs on the satellite computers in direction to the kernel status dispatcher on the kernel computer competes for transfer capacities with the other satellite to kernel communication, for example database traffic, transactions etc. To minimize the log communication and enhance the performance, the `satprep.exe` file installs status dispatcher servers on the satellite computers. They are called local status dispatcher servers in contrast to the kernel status dispatcher server. Per default they are neither configured nor started. They are shown as **XPR Status Dispatcher (xmrsvc)** in the Microsoft services window. When the local status dispatcher servers are started, the APLs on a satellite computer connect to the kernel status dispatcher server and to the local status dispatcher server. A local status dispatcher server can be configured by using the `xmrcfg` tool. The log file of a local status dispatcher server is in the `<XPR_Install>\log` directory on the satellite computer and can be examined by using the LogTool.

To establish the communication between the kernel computer and the local status dispatcher servers on the satellite computers, the `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\PP-COM\MRS\Service\Kernel` key (type `REG_MULTI_SZ`) in the registry of the kernel computer must be extended by an entry for each satellite computer according to the following pattern:

```
xmrsvc,<Name of the satellite computer>
```

Example for two satellite computers:

```
nameloc,sat1
cfgsvc,sat1
xmrsvc,sat1
nameloc,sat2
cfgsvc,sat2
xmrsvc,sat2
```

IMPORTANT: Verify that the commas are not followed by blanks.

IMPORTANT: Verify that the `xmrsvc` entry immediately follows the `cfgsvc` entry of the corresponding satellite computer.

6.5 Installation Routine

The installation or configuration of a distributed XPR system is performed in four steps. These four steps will be explained in detail in the following paragraphs.

First step	Installation of an XPR system on the kernel computer, i. e. at least the XPR Server component with the following kernel services contained therein: • XPR Administrator (mrs) • XPR Configuration Service (cfgsvc) • XPR Information Store (infstor) • XPR Message Router (mta) • XPR Name Locator (nameloc) • XPR Status Dispatcher (xmrsvc) The services named are combined as kernel components in the component selection list.
Second step	• Configuration of a domain-wide user account for the connection with the satellite computer (see Section 6.3, "Configure User Account", on page 194). • Assignment of this user account to all XPR services of the kernel computer (see Section 6.3.1, "Assign User Account", on page 195). XPR services that are no kernel services can be executed under the system account. But owing to the security aspects of the corresponding named pipes we expressly recommend not to do so.
Third step	• Preparation of the satellite computer with the satellite setup program (<code>Satprep.exe</code> on the XPR Installation CD).
Fourth Step	• Satellite computer: Assign the domain-wide user account to All services of the satellite computer (see Section 6.3.1, "Assign User Account", on page 195).
Fifth Step	• Configuration of the satellite computer with hardware driver and server components.

Table 15 *Installation Steps for a Distributed System*

6.6 Installation Checklist

Before you install a distributed XPR system, you should have already performed or familiarized yourself with the steps listed in the following table.

Topic	Description
Windows network and domain	- All computers in a distributed XPR system should reside in a common network segment. The topmost administration layer is a Windows domain. You can use an already existing domain, or one that has been created specifically for this purpose. - The kernel computer and all satellite computers must be integrated in this common domain. It is possible to use computers from several domains as satellites, if a corresponding position of trust has been established between the domains involved. Considering the administration effort in such a scenario, we do not recommend such a configuration.
Satellite computer	When the components are installed and put into operation on the satellite, the XPR server must have been started on the kernel computer.
User account	- A new user login account must be configured for the operation of the distributed XPR system. This is assigned to all services of the kernel and satellite computer as login account, so that these can start the required networked services. - During the installation, administrator privileges are required on the satellite computer and in the domain. The network conditions determine whether an individual user account must be created for the installation and startup procedure as well. We recommend to name the user accounts after their intended use. - The user accounts must be incorporated in the domain user group and on all computers of the distributed XPR system in the local-administrator group.

Table 16 Installation Checklist for a Distributed Installation

Topic	Description
XPR Kernel computer	• Make sure that all language packets are already installed on the kernel computer before you set up a satellite. • We recommend not to install the components on the kernel computer that are intended for installation on a satellite computer. • When you reinstall the kernel system and select the components, deactivate those components to be installed on a satellite. • You find further information about installing program components at a later date in Section 4.6.3, “Modifying an existing Installation”.

Table 16

Installation Checklist for a Distributed Installation

6.7 Installation on the Satellite Computer

You find the components that can be installed on the satellite computer in the table in [Section 6.1, “Overview”, on page 191](#). The installation requirements of a distributed XPR system are listed in the table in [Section 6.6, “Installation Checklist”, on page 198](#).

NOTE: Make sure that the domain-wide user account (see [Section 6.3.1, “Assign User Account”, on page 195](#)) has been assigned to the kernel services on the kernel computer. Additionally, make sure that this user account the right "Logon as a service" on all satellite computers (cf. [Section 6.3, “Configure User Account”](#))

During the installation the setup routine checks the following requirements:

- The specified domain exists.
- The specified user is member of this domain.

If one of these requirements is not met, you receive an error message.

Preparations

How to prepare the installation:

1. Make sure that an already operative kernel system is available and that it is started during the following installation and runs trouble-free. For the installation of this system please refer to [Chapter 4, “XPR System Installation”](#).

Make also sure that all language packets are installed on the kernel computer.

IMPORTANT: If the kernel system is not started during the installation of a satellite, another kernel system will be installed!

IMPORTANT: If the kernel system has been installed on a Windows cluster, execute the instructions given in section “Satellite Environment with clustered Kernel Computer” of the setup guide *OpenScape Xpressions Cluster Installation* to check the following keys in the Windows registry:

```
HKLM\SOFTWARE\Wow6432Node\PP-COM\MRS\Services\Kernel
HKLM\SOFTWARE\Wow6432Node\PP-COM\MRS\Services\Access
Protocol Layers
```

2. Start the `SatPrep.exe` program on the satellite system in the `XpressionsInstall\Satellite` directory on the setup medium.

Up comes this dialog:

The screenshot shows a Windows-style dialog box titled "Satellite System Preparation". It contains two main sections. The first section, "Environment information", includes a text box for "Server:" and a "Destination folder:" text box containing the path "c:\OpenScape\xpr\". To the right of the destination folder is a "Browse..." button. The second section, "Login information", contains three text boxes for "Account", "Password", and "Confirm Password". At the bottom of the dialog is a button labeled "Prepare Satellite System...".

3. Enter the computer name or the IP address of the kernel computer in the **Server:** field.

Setting up a Distributed XPR System

Installation on the Satellite Computer

4. In the **Destination folder:** field specify the directory in which the XPR components are to be installed. Via the **Browse...** button you can find a directory in the file system. We recommend to copy the default.
5. In the **User name:** field enter the user account that you have specified in [Section 6.3, “Configure User Account”, on page 194](#). Use the notation *Domain\user name*.
6. In the **Password:** field enter the password of the user account.
7. Click the **Prepare Satellite System...** button.

The components required on the satellite, such as the Name Locator, will now be installed.
8. Close the dialog via the **Finish** button.
9. If a Connection APL is installed on the satellite computer, the IP address of the satellite computer must be assigned to the entry `Xpressions.remoteIpAddr` in the following file: `<XPR_Install>/xprWebClient/config/common/Xpressions.cfg`
10. Then restart the satellite computer. The satellite preparation is thus complete.

Installation

11. Start the `Setup.exe` file from the `XpressionsInstall` setup directory on the satellite computer for installing the hardware drivers and the XPR server components. The components selected here are copied to the directory that you have specified in [step 4 on page 202](#).

NOTE: Do not start the `XpressionsnInstall\Satellite\satprep.exe` file. This file was already started in [step 2 on page 201](#).

NOTE: You find further information on installing XPR components in [Section 4.5.1, “Selecting Features”](#) and in [Section 4.6, “Modifying, repairing or removing the XPR Installation”](#).

IMPORTANT: After the installation of a Telematic APL, the corresponding service must be manually assigned the user account for satellite operation (cf. [Section 6.3.1, “Assign User Account”, on page 195](#)).

6.7.1 Installation of a Text-to-Speech System on Satellite Nodes

How to install a TTS system:

- Create a domain user with local administrator privileges for the kernel server.
- Log on to the kernel node as this user.
- As this user, install XPR on the kernel node.
- As this user, install TTS.
- Start MTA, NAMELOC etc. under this user account.
- As this user, log on to the satellite node and perform all above preparative steps for the satellite.
- Install XPR on this satellite node.
- As this user, install TTS on this satellite node.

6.7.2 EVO on Satellite Systems

Install an automatically starting batchjob that copies the file TargetNames.grxml from the kernel node to the satellite node.

Example:

```
copy \\<kernel
node>\D$\OpenScape\XPR\res\e\evo\asr\german\TargetNames.grxml
\\<satellite
node>\D$\OpenScape\XPR\res\e\evo\asr\german\TargetNames.grxml
```

In doing so please heed the following:

- Replace <kernel-node> with the name of the kernel node and <satellite-node> with the name of the satellite computer.
- Have this batchjob run under a user account that has access to the corresponding D\$ shares on the system.
- Have the batchjob run once a day as new users receive their entries in this file automatically.

6.8 Checking the XPR System

To check the correct configuration of the distributed XPR system, close and restart the XPR server on the kernel computer. In doing so, ensure that the XPR-specific processes on the satellites are correctly closed down. The display of all APLs on the individual satellites should also be checked.

Setting up a Distributed XPR System

Checking the XPR System

An incomplete or faulty startup is usually caused by an incorrectly entered or incorrectly administered user ID that was assigned to the XPR services.

The availability of the connection between the satellite and the kernel can be automatically checked in an interval. In this context please note the registry keys `NetworkAliveCheck` and `NetworkTryReconnect`. You find a description on this in the corresponding section of the *XPR Server Administration* manual.

A Appendix

A.1 Installation under Windows 7 Professional

NOTE: Follow the instructions given in [Section 2.1.3, “Checking Windows 64-bit Server Settings”](#), on page 29 also for Windows 7 as far as applicable.

The setup process for an XPR server under Windows 7 Professional does not differ from the one under Windows Server 2008 (cf. [Chapter 4, “XPR System Installation”](#)).

An installation under the Windows 7 Professional SP 1 operating system provides the following functionality:

- Up to 8 channels
- Up to 200 users
- SMTP and IMAP4
- Web Assistant (WebApl)
- Support of the ISDN hardware via ISDN APL (CAPI)
- Unified Messaging for Voice, Fax and Mail
- Ergo
- PhoneMail
- VMS
- Connection to Microsoft Exchange

The following XPR features are **not** supported under Windows 7 Professional:

- Satellite systems
- Clusters
- Connection to the groupware systems IBM/Lotus Notes and SAP

A.1.1 Configuring the Windows 7 Firewall

So that the services HTTP, IMAP4, POP3, and SMTP can be used under Windows 7 Professional, the following ports must be opened in the Windows 7 Firewall:

Appendix

Installation under Windows 7 Professional

- 80 (HTTP)
- 110 (POP3)
- 25 (SMTP)
- 143 (IMAP4)

Please read the relevant section of the Windows 7 documentation on this

A.2 Using the Report APL with SQL Databases

IMPORTANT: CodeBase is only supported for upgrades but not for new installations.

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 approaches to the problem described in the following sections should be used according to the current or expected data volume.

A.2.1 Using Microsoft SQL Server 2012 Express

Microsoft SQL Server 2012 Express is a limited version of the Microsoft SQL Server 2012. The Microsoft SQL Server 2012 Express serving reporting purposes is not included in the scope of delivery of OpenScape Xpressions but can be downloaded for free under the following URI:

<https://www.microsoft.com/pt-BR/download/details.aspx?id=29062>

Microsoft SQL Server 2012 Express requires .NET Framework 4 Redistributable. .Net Framework 4 can be provided by the XPR installation (see [Section 4.3.7, “Selecting System Components”, on page 80](#)), or you start the installation manually by executing the dotNetFx40_Full_x86_x64.exe file from the setup medium under Xpressions\Install\Prerequisites\Frameworks\NET\.

The Microsoft SQL Server 2012 Express and the OpenScape Xpressions server can be operated on one computer in parallel.

The default TCP port for the communication between Microsoft SQL Server 2012 Express and the XPR server is 1433.

You need to **Allow remote connections to this server** following the procedure below:

1. Enable remote connections to your SQL Server.
 - a) Open **SQL Server Management Studio**.
 - b) Right-click your server's name and select **Properties**.
 - c) Tick the checkbox **Allow remote connections to this server**.

- d) Click **OK**.

Microsoft SQL Server by default uses TCP 1433 but this can be changed using **SQL Server Enterprise Manager** or the database **Management Studio**.

2. Enable TCP/IP.
 - a) Open **SQL Server Configuration Manager**.
 - b) In **SQL Server Network Configuration** select **Protocols for ...**
 - c) In the right-hand pane, make sure that **TCP/IP** is **Enabled**.
3. Open the 1433 port in your firewall.
 - a) In the **SQL Server Configuration Manager**, right-click TCP/IP and select **Properties**.
 - b) Select the **IP Addresses** tab and make sure the *TCP Port for IP1* is 1433.

When logging on to the Microsoft SQL Server 2012 Express you need to select SQL server authentication.

A.2.1.1 Installation

The Microsoft SQL Server 2012 Express is not installed via the XPR setup. Manual installation is required.

A database and a user must be created that are both to be deployed by the Report APL. Use the Management Studio Express for this purpose.

IMPORTANT: The name of the database must correspond to rules that you find on the page

<http://msdn2.microsoft.com/en-us/library/ms175874.aspx>

under the heading Rules for Regular Identifiers. The name must not contain blanks, for example. A valid name would be ReportAPLDB, but not Report APL-DB or Report APL DB.

NOTE: The Microsoft SQL Server can be operated on one computer in parallel.

IMPORTANT: Microsoft SQL Server 2005 does not recognize the data type *datetime*. For a patch see <http://support.microsoft.com/kb/913089>.

IMPORTANT: Remove after the installation the read and write privileges from the folder C:\Program Files(x86)\Microsoft SQL Server\MSSQL.1\MSSQL\Binn for the **User** group.

A.2.1.2 Configuring the Report APL

NOTE: You find detailed information of the Report APL configuration in chapter *Report APL* in the *OpenScape Xpressions Server Administration* manual.

How to use the database defined in the previous section with the Report APL:

1. Open the OpenScape Xpressions monitor and log in as administrator.
2. Open the Report APL configuration dialog.
3. Open the **Database** tab.
4. Select the **ADO** entry under **Access mode** and click the **Configure...** button.
Another dialog opens.
5. Select the **Microsoft OLE DB Provider for SQL Server** entry on the **Provider** tab and click on **Next**.
The **Connection** tab opens.
6. Enter the following information on the **Connection** tab:
 - a) The name of the server on which the database defined above runs. You can make a selection from the pull-down list.
 - b) User name and password

NOTE: The data specified during the Microsoft SQL Server 2012 Express installation must be entered as user name and password.

- c) The database to be used by the Report APL
7. 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 notice dialog and the Report APL configuration is thus complete.

If the test fails, check the Report APL configuration.

A.2.2 Using a Microsoft SQL Server

If the data amount exceeds 1GB, 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. Possible scenarios are:

- OpenScape Xpressions server and Microsoft SQL server parallel on one computer
- OpenScape Xpressions server and Microsoft SQL server on an individual computer each

In both cases the customer needs to provide the required licenses (among others Microsoft SQL Server and if necessary Windows Server) as well as the required hardware. If both servers are operated parallel on one computer, this computer's hardware is to be measured accordingly.

You can manage very large data amounts with a Microsoft SQL server. Besides the actual SQL server the package includes a number of management and analysis tools.

You can obtain details about setting up a Microsoft SQL server from the corresponding product documentation or from the product homepage under <http://www.microsoft.com/sql/>. Details for connecting the Report APL to the Microsoft SQL server are coordinated in the project scope.

IMPORTANT: Microsoft SQL Server 2005 does not recognize the data type *datetime*. For a patch see <http://support.microsoft.com/kb/913089>.

IMPORTANT: Remove after the installation the read and write privileges from the folder C:\Program Files(x86)\Microsoft SQL Server\MSSQL.1\MSSQL\Binn for the **User** group.

A.2.3 Microsoft SQL Server Memory Restriction

It is highly recommended to set a 'Maximum server memory' because by default, SQL Server can change its memory requirements dynamically based on available system resources.

To prevent Microsoft SQL Server from consuming too much memory, you can use the following formula to determine the recommended maximum server memory:

- Reserve 4GB from the first 16GB of RAM and then 1GB from each additional 8GB of RAM for the operating system and other applications.
- Configure the remaining memory as the maximum server memory allocated for the Microsoft SQL Server buffer pool.

To set the maximum server memory for SQL Server:

1. Open the **SQL Server Management Studio**
2. Enter the **SQL Server properties - Memory**
3. Set the **Maximum server memory (in MB)**.

More information is detailed at:

<https://docs.microsoft.com/en-us/sql/database-engine/configure-windows/server-memory-server-configuration-options>

A.2.4 Switching from CodeBase to Microsoft SQL Server Express or Microsoft SQL Server

When switching from CodeBase to Microsoft SQL Server Express or Microsoft SQL Server, available data can only be copied by installing the `st*.log` files. Prerequisite is the use of a suitable backup concept and that `st*.log` files are available.

To perform a **Backup/Restore** of the databases, please read the *Backup/Restore* section in chapter *Report APL* of the *OpenScape Xpressions Server Administration* manual.

IMPORTANT: When changing from CodeBase to Microsoft SQL Server Express or Microsoft SQL Server, available customer-specific reports cannot be used any further. Default reports are available in revised version. Customer-specific reports must either be created by the customer or with the support of the Professional Service Organization.

A.3 XPR in a virtual Environment

NOTE: Refer to the *OpenScape Xpressions Release Notice, Service Documentation*, for information about the following items:

- Supported Virtual Machine versions
 - Supported Virtual Machine features
 - Restrictions
 - Minimum virtual hard disk size
 - Minimum virtual RAM size
 - Minimum number of virtual CPUs
 - Hard disk throughput
 - Network bandwidth
-

When operating an XPR server in a virtual environment, please note the following:

- The host system has to meet the total of the system requirements that result from the system requirements of all the virtual systems and the system requirements of the host system itself. This applies in particular for RAM and hard disk capacity. Besides the system requirements of the host system and the software installed on it, the system requirements of the operating systems of all the projected virtual machines and the system requirements of the software installed in the virtual machines have to be taken into consideration.
- When using the load and dimensioning tool you need to set that the values shall be calculated for a virtual environment.
- A host system not properly dimensioned results in a reduced performance of the XPR server and of all operated virtual machines. This is particularly true when load-intensive applications are operated or high loads are generated by a large number of accesses. When operating a TUI, greetings may be played with delay or distorted, for example.
- Please also note, that the host system represents a so-called *Single Point of Failure*. That means, as soon as a hardware failure occurs in the host system, the virtual machines may not be operable any longer. Therefore, it is not possible to implement a highly available solution with a single host system.
- The number of possible guest operating systems in which an XPR server may be installed and operated depends to a great extent on the performance of the host system. Please note that the real load generated in real operation is hard to estimate in advance and depends on many factors. Therefore, we recommend copious load tests before a host system starts real operation.

The following configuration parameters apply:

Property		Minimum hardware	Number of XPR users					
			300	1000	3000	5000	10000	15000 ¹
Server		XPR (Messaging Only System)						
	Scenario	Single-node scenario					Kernel-satellite scenario	
	Number of kernel computers	1						
	Number of satellite computers (minimum)	0					2	3
Configuration parameters of the virtual computer								
	Guest operating system	Windows						
	Version	Microsoft Windows Server 2016 (64 bit) Microsoft Windows Server 2012 (64-bit), Microsoft Windows Server 2008 R2 (64-bit) Microsoft Windows Server 2019 (64-bit) Microsoft Windows Server 2022 (64-bit) Microsoft Windows Server 2025 (64 bit)						
	Type of disk provisioning ²	Thin Provision Eager Zeroed or Thick Provision Lazy Zeroed						
	Hard disk mode ³	Any, Independent persistent recommended						
	Number of network boards ⁴	1	1	1	1	1	Kernel: 1, per satellite: 1	Kernel: 1, per satellite: 1
	Support of VMXNET3 network boards ⁵	Yes						
	MAC address ⁶	Automatic						
	CPU shares ⁷	High						
	CPU reservation in MHz (minimum)	1000	1000	2000	2000	3000	Kernel: 3000, per satellite: 2500	Kernel: 3000, per satellite: 3000
	CPU limit ⁸ in MHz (minimum)	1000	1000	2000	2000	3000	Kernel: 3000, per satellite: 2500	Kernel: 3000, per satellite: 3000
	Memory shares ⁷	High						
	Memory reservation in GB (minimum)	2	2	2	2	3	Kernel: 3, per satellite: 2	Kernel: 4, per satellite: 2
	Memory limit ⁸ in GB (minimum)	2	2	2	2	3	Kernel: 3, per satellite: 2	Kernel: 4, per satellite: 2
Further parameters.								

Table 17 Virtual Machine configuration parameters

Appendix
XPR in a virtual Environment

Property	Minimum hardware	Number of XPR users					
		300	1000	3000	5000	10000	15000 ¹
Real-time application	Yes						
IOPS ⁹	Unavailable						

Table 17 *Virtual Machine configuration parameters*

- 1 XPR on Virtual Machine is supported only for up to 10000 users.
- 2 Possible values: **Thin Provision**
- 3 Possible values: **Independent persistent**, **Independent nonpersistent** or **snapshot**
- 4 Parameter **How many NICs do you want to connect?**
- 5 Parameter **Adapter**
- 6 Possible values: **Automatic** or **Manual**
- 7 Possible values: **High** or **Normal**
- 8 Possible values: Numerical value or **Unlimited**
- 9 Input output operations per second (Storage I/O). See the Virtualization solution Resource Management Guide for details.

A.3.1 Distributing CPU Cores in the virtual Host System

To configure load balancing in a virtual system you need to assign a CPU to the virtual computers. Please be sure to assign an individual CPU to systems with heavy load.

IMPORTANT: No CPU core must be permanently assigned to a virtual computer during the migration (e.g. VMware vMotion). If you use permanently assigned CPU cores, cancel this assignment before the migration and reassign the cores after the migration. You can do this while the virtual computer operates.

NOTE: The XPR server contains two CPU cores in a virtual system that are not used by any other computer.

A.3.1.1 Example of an XPR System in a virtual Environment using VMware

- Host system: virtual server with 4 CPUs
- XPR system: XPR server, two servers with front-end services
- Virtual environment: VMware vSphere Client 5

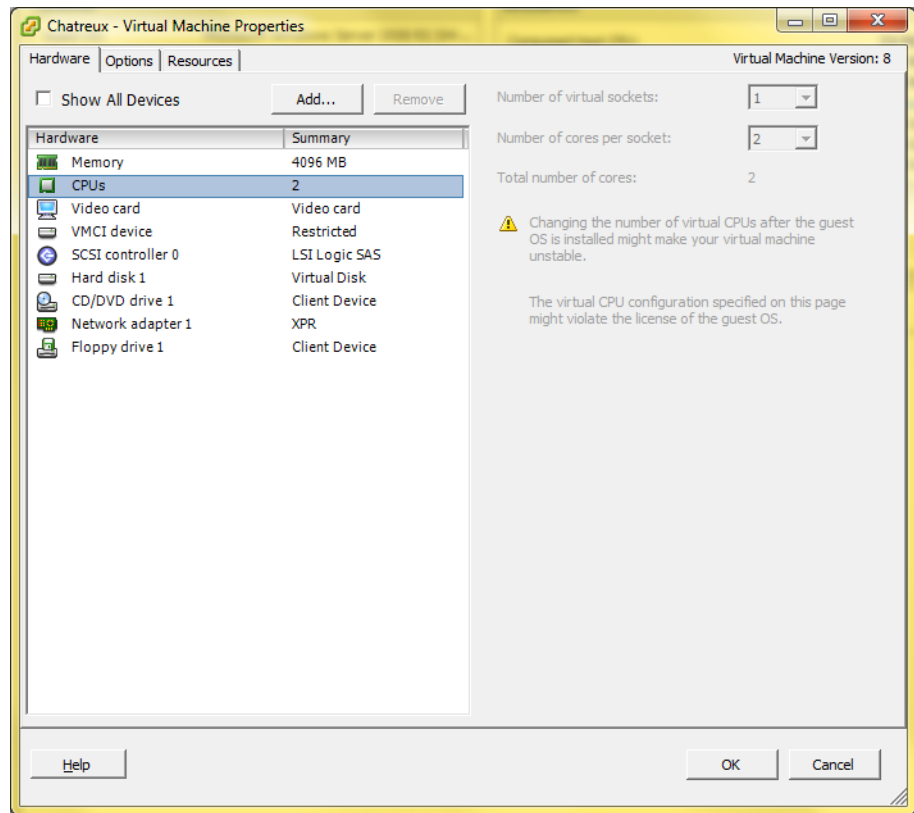
Configuring the XPR server

1. Open the vSphere client of your virtual host system.
2. In the navigation tree of the virtual computers, click with the right mouse button on the XPR server and select **Edit Settings...** in the context menu. The dialog **<computer name> - Virtual Machine Properties** opens.
3. Click with the left mousebutton on **CPUs**. The display to the right of **Total number of cores:** shows how many CPU cores are assigned to your virtual computer. Multiplying the values to the right of **Number of virtual sockets:** and **Number of cores per sockets:** result in the values to the right of **Total number of cores:**.
Select from the combo box to the right of **Number of virtual sockets:** value 1 and to the right of **Number of cores per sockets:** value 2.

NOTE: You can configure the number of CPUs of a virtual computer only if the virtual computer is disabled.

Appendix

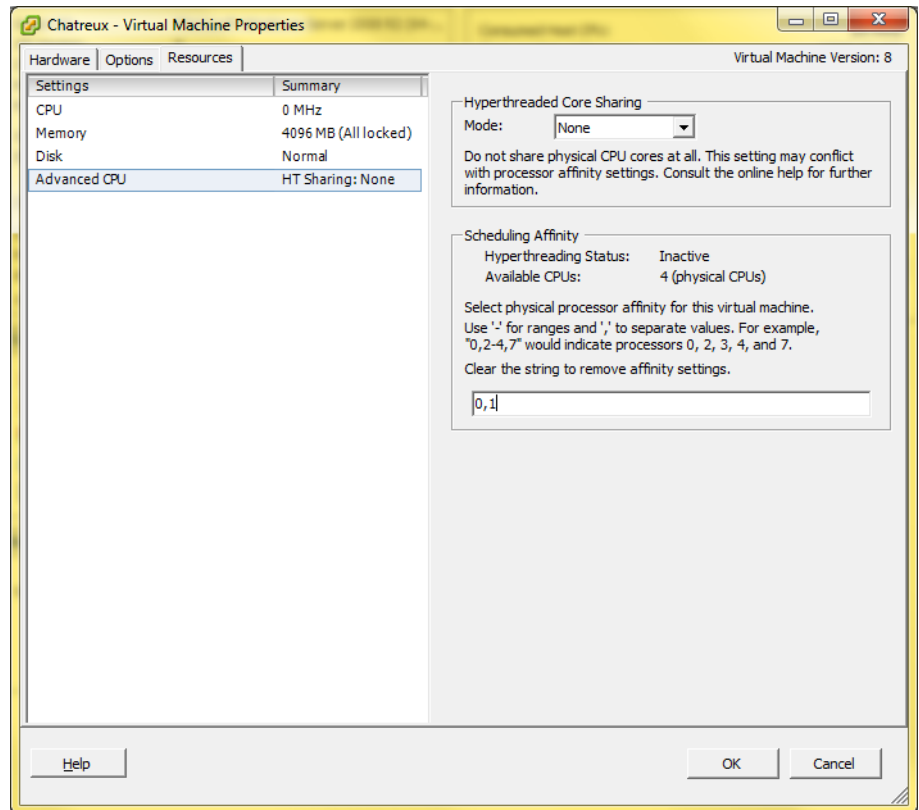
XPR in a virtual Environment



You have now assigned two CPUs to your virtual XPR server.

4. Click on the **Resources** tab and subsequently on **Advanced CPU**.
5. In the **Hyperthreaded Core Sharing** group you need to set the mode to the right of **Mode:** to **None**.
6. In the **Scheduling Affinity** group you need to enter the numbers of the CPUs to be used by the virtual XPR server in the lower editing field. Enter **0, 1** in there.

7. Click on **OK** to apply the settings.



Your virtual XPR server has two CPUs now and uses cores 0 and 1 of the host system.

Configuring the first front-end computer

1. Open the vSphere client of your virtual host system.
2. In the navigation tree of the virtual computers, click with the right mouse button on the first virtual front-end computer and select **Edit Settings...** in the context menu. The dialog **<computer name> - Virtual Machine Properties** opens.
3. Click with the left mousebutton on **CPUs**. The display to the right of **Total number of cores:** shows how many CPU cores are assigned to your virtual computer. Multiplying the values to the right of **Number of virtual sockets:** and **Number of cores per sockets:** result in the values to the right of **Total number of cores:**.
Select from the combo box to the right of **Number of virtual sockets:** value 1 and to the right of **Number of cores per sockets:** value 1.

NOTE: You can configure the number of CPUs of a virtual computer only if the virtual computer is disabled.

You have now assigned one CPU to your first virtual front-end computer.

4. Click on the **Resources** tab and subsequently on **Advanced CPU**.
5. In the **Hyperthreaded Core Sharing** group you need to set the mode to the right of **Mode:** to **None**.
6. In the **Scheduling Affinity** group you need to enter the numbers of the CPUs to be used by the virtual XPR server in the lower editing field. Enter **2** in there.
7. Click on **OK** to apply the settings.

Your first virtual front-end computer has one CPU now and uses core 2 of the host system.

Configuring the second front-end computer

1. Open the vSphere client of your virtual host system.
2. In the navigation tree of the virtual computers, click with the right mouse button on the second virtual front-end computer and select **Edit Settings...** in the context menu. The dialog **<computer name> - Virtual Machine Properties** opens.
3. Click with the left mousebutton on **CPUs**. The display to the right of **Total number of cores:** shows how many CPU cores are assigned to your virtual computer. Multiplying the values to the right of **Number of virtual sockets:** and **Number of cores per sockets:** result in the values to the right of **Total number of cores:**.
Select from the combo box to the right of **Number of virtual sockets:** value 1 and to the right of **Number of cores per sockets:** value 1.

NOTE: You can configure the number of CPUs of a virtual computer only if the virtual computer is disabled.

You have now assigned one CPU to your second virtual front-end computer.

4. Click on the **Resources** tab and subsequently on **Advanced CPU**.
5. In the **Hyperthreaded Core Sharing** group you need to set the mode to the right of **Mode:** to **None**.
6. In the **Scheduling Affinity** group you need to enter the numbers of the CPUs to be used by the virtual XPR server in the lower editing field. Enter **2, 3** in there.
7. Click on **OK** to apply the settings.

Your second virtual front-end computer has one CPU now and uses core 2 or 3 of the host system.

A.4 MAPI Fax Printer Driver

This section was shifted to the *OpenScape Xpressions Client Installations* manual.

A.5 Installation and Configuration of the IppAssistant

A.5.1 Features

The IppAssistant is a webscript for the Web APL written in E. This webscript does not create any HTML-formatted files that can be read by any browser but XML files that can be interpreted for OpenStage telephones by the XML application module. It enables the user to log on, to retrieve text and voice messages, to send short messages (SMS) if this is supported by the server, and to record a today greeting and names.

The IppAssistant does not enable recording names or greetings in a simplified way.

A.5.2 Requirements

The following requirements must be complied with:

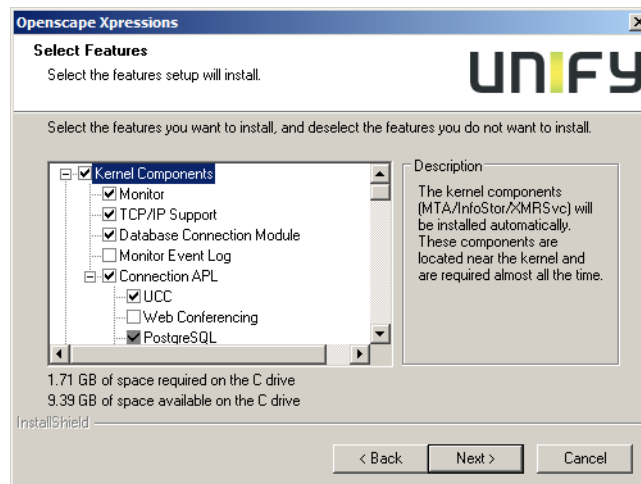
- You can use only OpenStage phones that support the XML applications, i. e. only OpenStage 60 and OpenStage 80. The firmware of the OpenStage phones must be V1R4.x or later.
- The administration password for the OpenStage telephones must be known so that XPR applications can be installed.
- An XPR server must have been connected to the PBX.
- On the PBX an extension must be available for calling the XPR server (see [step 5 on page 225](#)).
- Between the OpenStage telephones and the XPR server at least the following ports must have been released:
 - The TCP port of the Web APL on the XPR server. This is port 80 by default.
 - Port 8085, which is permanently set on the telephone side.

IMPORTANT: No NAT must exist between the OpenStage telephones and the XPR server, since this would prevent voicemail playback.

- The installation and configuration requires the database password. This is **NOT** the password of the administrator account.

A.5.3 Overview

The IppAssistant is installed on the XPR server by activating the check box of the IppAssistant option in step 2 on page 92.



After the IppAssistant installation the following steps are required:

- On the XPR server: Check as to whether the IppAssistant script was correctly configured in the Web APL. Please refer to [Section A.5.4, “Configuring the IppAssistant Script”](#), on page 224.
- On the client (OpenStage telephone): Installation and configuration of the IppAssistant client. Please refer to the *OpenStage Xpressions IppAssistant* user guide on this.
- On the XPR server: Configuration of an extension for the PLAYWAVE script. Please refer to [Section A.5.5, “Configuring an Extension for PlayWave”](#), on page 225.
- On the XPR server: Entering the extensions of the telephones with IppAssistant in the XPR database. Please refer to [Section A.5.6, “Manual Entries in the XPR Database”](#), on page 226.

A.5.4 Configuring the IppAssistant Script

How to configure the IppAssistant script:

1. Start the XPR monitor and open the Web APL configuration dialog.
2. Open the **CGI** tab.
3. Check whether the **CGI Protocols** section displays the *IppAssistant* entry in the **Name** and **Script** column.

If the script has already been entered, the IppAssistant script configuration is complete and you can close the Web APL configuration dialog again.

If the script is not displayed you need to add it manually. Proceed as follows:

- a) Open the Web APL configuration dialog and in there the **CGI** tab.
- b) Click the **Add...** button.
- c) Select the **Enable Protocol** option.
- d) Specify a name in the **Name** field. This name will later be displayed on the **CGI** tab in the **Name** column.
- e) In the **Script** pull-down menu select the **IppAssistant.vo** entry.
- f) Click on **OK**.
- g) Close the Web APL configuration dialog via the **OK** button.

A.5.5 Configuring an Extension for PlayWave

NOTE: The *PlayWave* protocol extension must also be correctly configured in the PBX.

How to configure an extension for the *PlayWave* protocol:

1. Open the IP APL configuration dialog and in there the **Protocols** tab.
2. Make sure that the *PlayWave* protocol has already been installed.
If the *PlayWave* protocol is not installed yet, proceed as follows:
 - a) Click in the tab with the right mousebutton and select the **Add** option.
 - b) In the **Available protocols** list look for the **PlayWave Script** entry and click on **OK**.
3. Open the **Extensions** tab.
4. Click in the tab with the right mousebutton and select the **Add** option in the context menu.
5. Enter the desired extension for the PLAYWAVE script in the **Start** field.
Repeat the entry in the **End** field.
6. In the **Bindings** section select the **PlayWave Script (PLAYWAVE)** entry from the pull-down menu and click on **OK**.
7. Click on **OK**.

A.5.6 Manual Entries in the XPR Database

NOTE: This configuration step requires an OpenStage 60 or OpenStage 80 telephone on which the IppAssistant has already been installed.

The IppAssistant needs to know the *PlayWave* protocol extension for working correctly.

1. Open the XPR monitor and log in as user with administrator privileges.
2. Open a new log window and configure it in a way that it logs the entire logging depth of the *PlayWave* protocol. Proceed as follows:
 - a) Open the menu option **View > Logging Monitor**.
 - b) Open the properties dialog of the new logging monitor via the menu option **View > Properties**
 - c) In the **Monitored Modules** section select from the **Module:** pull-down menu the telematics APL used and from the **Topic:** pull-down menu the **PlayWave** entry.
 - d) Select all check boxes in the **Monitored Data** section. Afterwards, click on **OK**.
3. Check whether the PlayWave script has been configured correctly by dialing the number of the PlayWave protocol from the OpenStage 60 or OpenStage 80 telephone on which the IppAssistant is installed.

NOTE: The logging monitor does not only issue an error message but also the number from which the call was made. Example:

```
PlayWave::OnIncoming() ANI <+492404123999> is calling...
```

Note down the number from the logging monitor as you will need it later on.

4. Enter the number that you have dialed on the OpenStage telephone for the PlayWave protocol in the `PLAYWAVE_ACCESS` database field. Proceed as follows:
 - a) Start the `DBTool.exe` program from the following folder:


```
<XPR setup directory>/SDKTools
```
 - b) Look for a data record with the key name `PLAYWAVE_ACCESS`, for example:

```
SERVERNAME/$SYSTEM  IPPASSISTANT  SETTINGS
PLAYWAVE_ACCESS    <NumberToDial>
```

- c) Enter the number that you have noted down in the **Key** field next to the key name `PLAYWAVE_ACCESS`. Doubleclick the field for this purpose.
 - d) Enter the database password and then specify the number in the field.
 - e) Click on the **Save changes** icon in the DBTool toolbar.
5. Restart the Web APL.

A.5.7 Determining the Normalization Prefix

The step described here cannot be automated since the current software standard of the OpenStage 60 or OpenStage 80 telephones does not allow installed applications to read out the correctly normalized extension of the OpenStage telephone. A correctly normalized extension is, among other things, used to make sure that the voice mails of two simultaneously accessing users are not confused.

As soon as a user logs on with the IppAssistant for the first time, the OpenStage telephone extension is stored in the XPR database in the key `IPP_PHONE#`. Owing to the OpenStage telephone software the format of this number does not correspond to the expected normalized format, though.

In this step the prefix must be determined that the IppAssistant adds to the OpenStage telephone number to turn it into a correctly normalized phone number. Example:

Supposed, an IppAssistant user has the extension 999. The limited OpenStage telephone software may deliver different versions upon retrieval of this number. Examples would be 999 or 492404123999. Both versions deviate from the expected format +492404123999. In case of 999 the prefix searched for would be +4902404123, in case of 492404123999 merely the plus sign.

To come to the correctly normalized extension of the telephone, a call must be made with the OpenStage telephone to the PlayWave protocol. Since PlayWave does not support any incoming calls, the XPR monitor displays an error message that also contains the normalized number of the OpenStage telephone.

This number must now be compared with the number already entered in the database. The prefix searched for comprises the missing characters and digits.

Proceed as follows:

1. If no user has been created for the IppAssistant yet, define one using the Web Assistant. Please read the corresponding section in the *OpenScape Xpressions Web Assistant* manual on this.
2. Verify that the logging monitor you have created in [Section A.5.5](#), “Configuring an Extension for PlayWave”, on page 225 is still active.

NOTE: If you have noted down the number in step 3 in [Section A.5.6](#), “Manual Entries in the XPR Database”, on page 226 you can skip the next step, since the OpenStage telephone number is already stored in the database. In this case continue with step 4 on page 228.

3. Log on to the IppAssistant with the corresponding user account.
As soon as you log on, the phone number configured in the OpenStage telephone is stored in the database. This phone number may not be correctly normalized, so that manual adjustments in the database may be required.
4. Start the `DBTool.exe` program from the following folder:
`<XPR setup directory>/SDKTools`
5. Log on as administrator.
6. Look for the `IPP_PHONE#` entry of the user account with which you are logged in at the IppAssistant.
7. Check how the number of the IppAssistant telephone was entered and note down the resulting prefix. Examples:

Expected number	Number in <code>IPP_PHONE#</code>	Required prefix in <code>NORM_PREF</code>
+492404123999	999	+492404123
+492404123999	492404123999	+

Table 18 Prefix examples

8. Look for the `NORM_PREF` field in the XPR database.
9. Enter the found prefix in the `NORM_PREF` field.
10. Save your modifications in the database.

B Notes for Installing the Operating System

B.1 General Considerations

B.1.1 Preliminary Remark

Because the service documentation does not include an installation manual for Windows, this manual comes with an approved installation version for the service engineer. This version can be reverted to if no preconfigured PC is used, or if a preconfigured PC requires a complete reinstallation.

As is generally the case with PC software, there is a number of different possible approaches which all produce the same result. We recommend that you do not deviate from the procedure proposed here unless you have good reason, as doing so may make troubleshooting more difficult.

After the following settings, which are independent from the operating system, you find instructions for the installation and activation of Windows 2000 Professional for client computers (see [Section B.2, “Installing Windows 7 Server Professional”, on page 230](#)) and Windows Server 2008 R2 (see [Section B.3, “Installing Windows Server 2008 R2”, on page 233](#)).

B.1.2 BIOS Settings

The BIOS settings apply for the server models 1 and 2. If other PCs are used, the installing person is responsible for finding suitable BIOS settings.

- When you start the computer, push the **F2** or **Delete** key to enter the BIOS setup.
- The customer decides whether or not a security setup password is required. The system password should not be set, as this would prevent the computer from rebooting independently in the event of a crash.
- When you start the computer, push the **F2** or **Delete** key. Neither a security setup password nor a system password is set.
- Deactivate the APM (Advanced Power Management) function in the BIOS.
- Save the modifications (Save Changes & Exit).

B.1.3 Preparing the Hardware

B.1.3.1 Modem and SMS Transmitter

- If you use a modem, connect it to the COM1 interface.
- If an SMS send station is required, connect it to the COM2 interface.
- If two SMS send stations are used, implement a suitable interface expansion card and connect the second send station to COM3.

B.1.3.2 Establishing the LAN Connection

For the LAN connection the network cable must be plugged in into the LAN card of the XPR server computer. Many network cards display network activity via LEDs next to the slot. Please read the network card documentation on this topic.

B.2 Installing Windows 7 Server Professional

B.2.1 Starting the Installation

The computer can be booted from the Windows 7 Professional installation medium to install Windows 7 Professional.

- Welcome > Enter key
- Licensing > F8 key
- Press the E key to create a new partition, size: 2024 MB
- Number of partitions: at least two
- Start installation on C: with the Enter key
- Select NTFS as the file system

The necessary files are now copied to the hard disk and the computer reboots.

B.2.2 Basics

Perform the following settings in the further Windows 7 Professional setup:

Regional Settings

Table 19 Basic Settings for Windows Server 7

Regional Settings	Country-specific
Keyboard layout	Country-specific
User Information	
Name	Customer-specific
Organization	Customer-specific
Computer name and administrator password	
Computer name	Customer-specific
Administrator password	Customer-specific
Confirm Password	Customer-specific
Date and Time Settings	
Date & Time	
Time Zone	Select local time zone
Automatically adjust clock for daylight saving changes	Activate
Network Settings	
Select custom settings	
Select and configure Internet protocol (TCP/IP) properties	Customer-specific
Computer Name	
The name of the computer on which the XPR is installed must not exceed 15 characters.	
Workgroup or Domain	
The computer can be integrated into an existing domain immediately or at a later date. Integrating the computer in a work group environment is not permitted.	
Network logon wizard	
Select Users must enter a name and password for this computer.	

Table 19

Basic Settings for Windows Server 7

B.2.3 Advanced Settings

Graphics settings

- **Start > Control Panel > Display > Change display settings > Advanced settings > Adapter > List All Modes...**

Customize resolution, frequency and color depth for the monitor used. You find the ideal values in the monitor documentation.

Create a D partition

Drive D must be formatted with NTFS if this has not already been done during installation of the operating system.

- **Start > Control Panel > Administrative Tools > Computer Management > Disk Management**

Change the drive letter of the DVD drive to E:

- Create a partition in the unassigned area of the hard disk making the following settings:
 - Primary partition, maximum size, drive letter D:
 - File system: NTFS, Allocation unit size: standard, use QuickFormatting

Optimize resource and memory management

- **Start > Control Panel > System > Advanced system settings > Advanced tab > Performance > Settings...**

Visual Effects tab:

Select the **Adjust for best performance** option

Advanced tab:

In the **Processor scheduling** section select the **Background services** option

In the Virtual memory section click on the **Change** button, then switch to drive C: and set the initial and maximum size of the paging file to the same value. In doing so, use at least the size of the RAM available in the computer.

Setting the Startup Options

- **Start > Control Panel > System > Advanced > section Startup and Recovery > Settings**
 - Disable the **Time to display list of operating systems** option
 - Disable the **Time to display recovery options when needed** option
 - Activate the **Write an event to the system log** option
 - Disable the **Send an administrative alert** option
 - Activate the **Automatically restart** option

- In the **Write debugging information** section select **(None)** from the drop-down menu

B.3 Installing Windows Server 2008 R2

B.3.1 Starting the Installation

To install Windows Server 2008 R2, the computer must be booted by the Windows Server 2008 setup DVD.

- Welcome > Enter key
- Licensing > F8 key
- Press the E key to create a new partition, size: 2024 MB
- Start installation on C: with the Enter key
- Select NTFS as the file system

The necessary files are now copied to the hard disk and the computer reboots.

B.3.2 Basics

Perform the following settings in the further Windows Server 2008 R2 setup:

Regional Settings	
Regional Settings	Country-specific
Keyboard layout	Country-specific
User Information	
Name	Customer-specific
Organization	Customer-specific
Computer name and administrator password	
Computer name	Customer-specific
Administrator password	Customer-specific
Confirm Password	Customer-specific
Windows 2008 components	
Copy default settings, except IIS (Internet Information Service). This service must be deselected , as OpenScape Xpressions installs its own Web server.	
Date and Time Settings	
Date & Time	
Time Zone	Select local time zone
Automatically adjust clock for daylight saving changes	Activate
Network Settings	
Select custom settings	
Select and configure Internet protocol (TCP/IP) properties	Customer-specific
Computer Name	
The name of the computer on which the XPR is installed must not exceed 15 characters.	
Workgroup or Domain	
The computer can be incorporated immediately in an existing domain; this procedure can also be performed at a later time. Integrating the computer in a work group environment is not permitted.	
Network logon wizard	
Select Users must enter a name and password for this computer.	

Table 20

Basic settings for Windows Server 2008

B.3.3 Advanced Settings

Graphics settings

- **Start > Settings > Control Panel > Display > Settings > Advanced > Adapter > List All Modes...**

Customize resolution, frequency and color depth for the monitor used

Create a D partition

Format drive D: with the NTFS file system, if this has not been done during the operating system setup yet.

- **Start > Settings > Control Panel > Administrative Tools > Computer Management > Disk Management**

Change the drive letter of the installation medium to E:

- Create a partition in the unassigned area of the hard disk making the following settings:
 - Primary Partition, Maximum Size, drive letter D:
 - File system: NTFS, Allocation unit size: standard, use QuickFormatting

Setting the Startup Options

- **Start > Settings > Control Panel > System > Advanced > Startup and Recovery**
 - Deselect "Time to display list of operating systems"
 - Deselect "Send an administrative alert"
 - Select "Automatically restart"
 - "Write debugging information to:" none

Optimize resource and memory management

- **Start > Settings > Control Panel > Network Connections > LAN > Properties > File and Printer Sharing for Microsoft Networks > Properties**

Select "Balance"

- **Start > Settings > Control Panel > System > Advanced > Performance Options > Advanced**

Optimize system performance for: background services

- **Start > Settings > Control Panel > System > Advanced > Performance Options > Advanced > Virtual Memory > Modify...**

Set the **Initial Size** and **Maximum Size** of the paging file to double the value of the physical memory available

B.3.4 Optional Components

Please note the instructions by the relevant manufacturers for the installation of optional components and for components that are not supported by Windows 2008 Server by default.

B.4 Installing Windows 2012/2016/2019/2022/2025 Server

B.4.1 Starting the Installation

To install Windows 2012/2016/2019/2022/2025 Server, the computer must be booted by the Windows 2012/2016/2019/2022 setup DVD.

- Select your language and other preferences
 - the Language to Install
 - the Time and Currency format
 - Keyboard input method
- Click on **Next**
- Click on **Install Now**
- Enter the product key
- Click on **Next**
- Select the operating system you want to install
- Click on **Next**
- Read/Accept the license terms
- Select the option **Custom: Install Windows only (advanced)**
- Select the partition where you want to install Windows
- Click on **Next**
- The necessary files are copied to the hard disk and the computer reboots
- Set the Administrator user password
- Click on **Finish**

B.4.2 Basics

Perform the following settings after Windows 2012/2016/2019/2022/2025 Server setup:

Computer name and administrator password	
Computer name. The name of the computer on which the XPR is installed must not exceed 15 characters.	Customer-specific
Administrator password	Customer-specific
Windows 2012/2016/2019/2022/2025 Features	
Select Failover Clustering in case you will use the OpenScape Server in High Availability.	
Windows 2012/2016/2019/2022/2025 Roles	
IIS (Internet Information Service) service must be deselected, as OpenScape Xpressions installs its own Web server.	
Date and Time Settings	
Date & Time	
Time Zone	Select local time zone
Automatically adjust clock for daylight saving changes	Activate
Network Settings	
Configure Internet protocol (TCP/IP) properties	Customer-specific
Workgroup or Domain	
The computer can be incorporated in an existing domain. Integrating the computer in a work group environment is not permitted.	

Tabelle 21 Basic settings for Windows Server 2012/2016/2019/2022/2025

B.4.3 Advanced Settings

Graphics settings

- **Start > Control Panel > Appearance > Display...**

Customize resolution, frequency and color depth for the monitor used

Create a D partition

Format drive D: with the NTFS file system, if this has not been done during the operating system setup yet.

- **Start > Settings > Control Panel > Administrative Tools > Computer Management > Disk Management**

Change the drive letter of the installation medium to E:

- Create a partition in the unassigned area of the hard disk making the following settings:
 - Primary Partition, Maximum Size, drive letter D:
 - File system: NTFS, Allocation unit size: standard, use QuickFormatting

Setting the Startup Options

- **Start > Control Panel > System and Security > System > Advanced System Settings > Advanced > Startup and Recovery > Settings**
 - Deselect "Time to display list of operating systems"
 - Select "Automatically restart"
 - "Write debugging information to:" none

Optimize resource and memory management

- **Start > Settings > Control Panel > Network Connections > LAN > Properties > File and Printer Sharing for Microsoft Networks > Properties**

Select "Balance"
- **Start > Control Panel > System and Security > System > Advanced System Settings > Advanced > Performance > Settings > Advanced**

Adjust for best performance of: Background services
- **Start > Control Panel > System and Security > System > Advanced System Settings > Advanced > Performance > Settings > Advanced > Virtual Memory > Change...**

Deselect "Automatically manage paging file size for all drives"

Select "Custom Size"

Set the **Initial Size** and **Maximum Size** of the paging file to double the value of the physical memory available

B.4.4 Optional Components

Please note the instructions by the relevant manufacturers for the installation of optional components and for components that are not supported by Windows 2012/2016/ 2019/2022/2025 Server by default.

C Configuring OpenScape Xpressions as Voice-only System

C.1 Preface

C.1.1 About this Chapter

This chapter addresses service personnel. It describes how to initially install a voice-only OpenScape Xpressions V7.

C.1.2 Previous Knowledge

We assume that the service technician has the following previous knowledge:

- Basic knowledge of the Windows Server 2008 operating system
- Successful participation in OpenScape Xpressions V7 introductory courses

C.2 Installation Fundamentals

C.2.1 Hardware and Software - Minimum Requirements

For the minimum hardware and software requirements please refer to [Section 2.1.2, "Checking the System Requirements for the Server PC"](#), on page 24.

C.2.2 XPR V7 Line Boards

The following line boards by **Eicon** are supported:

- DIVA Server BRI-2M PCI
- DIVA Server 4BRI-8M PCI
- DIVA Server PRI-30M PCI
- DIVA Server PRI-8M PCI

You find detailed information by the manufacturer about the corresponding products on the following web pages:

Dialogic DIVA Server BRI-2M PCI and 4BRI-8M PCI

<http://www.eicon.com/worldwide/products/MediaGateways/sm-business.htm>

Dialogic DIVA Server PRI-30M PCI

http://www.eicon.com/worldwide/products/MediaGateways/m-l_business.htm

C.2.3 Types of Integration/Protocols Supported

- S₀ BRI (CorNet-NQ, CorNet-N, CorNet-T)
- T1 PRI (CorNet-NQ, CorNet-N, QSIG)

C.3 PBX Systems Supported

Please see the *Release Notice* for the supported PBX. To correctly configure the PBX, please refer to the corresponding PBX installation manual.

C.3.1 Connection Matrix for PBX Systems

Interface	PBX	Line Card	PBX Card	Protocol	Max. no. of boards per server	Max. no of channels per session
BRI Connectivity						
S ₀ /BRI	HiPath 4000	Dialogic DIVA BRI	STMD2	CorNet-NQ	5	10
S ₀ /BRI	HiPath 4000	Dialogic DIVA 4BRI	STMD2	CorNet-NQ	5	40
S ₀ /BRI	HiPath 33xx/35xx	Dialogic DIVA BRI	STLS4	CorNet-N	5	10
S ₀ /BRI	HiPath 37xx/ Hicom 150	Dialogic DIVA 4BRI	STMD8	CorNet-N	5	40
S ₀ /BRI	Hicom 300H	Dialogic DIVA 4BRI	SLMS	CorNet-T	5	40
PRI connection (Europe)						
S _{2M} /PRI	HiPath 4000	Dialogic DIVA PRI	DIUN2	CorNet-NQ	2	60
S _{2M} /PRI	HiPath 35xx	Dialogic DIVA PRI	TS2	CorNet-N	1	30
S _{2M} /PRI	HiPath 37xx/ Hicom 150	Dialogic DIVA PRI	TMS2M	CorNet-N	2	60
PRI connection (USA)						
T1/PRI	HiPath 4000	Dialogic DIVA PRI	TMDN H	CorNet-NQ	2	46
T1/PRI	HiPath 35xx	Dialogic DIVA PRI	TST1	CorNet-N	1	23
T1/PRI	HiPath 37xx/ Hicom 150	Dialogic DIVA PRI	TMST1	CorNet-N	2	46
T1/PRI	Nortel Meridian	Dialogic DIVA PRI		QSIG	3	68

Table 22 Connection Matrix for PBX Systems

C.3.2 Installation Overview

Here is an overview of the installation steps:

- Perform checklist
- Install Xpressions
 - License
 - Drivers
 - Xpressions software
 - Settings
 - APLs
 - Xpressions components
- Test system and troubleshooting
 - Create two test users
 - Test system
 - Troubleshooting hints

C.3.3 Performing the Checklist

1. Obtain numbering plan for use during configuration.
2. You obtain the license key (a file with an **.xml** extension) according to the instructions in [Chapter 3, “Generating Licenses”](#). Download the key to some media and bring to customer site.
3. Obtain access numbers:
 - callback _____
 - direct _____
 - forward _____
 - transfer _____
 - others _____
4. Obtain XPR server name _____.
5. Which options has the customer ordered (i.e. Automated Attendant, Report Module, etc.)
 _____ for
 use in the Install the XPR Components section ([Section C.4.7, “Install the Xpressions Components”, on page 259](#), [Section C.5.7, “Install the Xpressions Components”, on page 294](#) or [Section C.6.7, “Install the Xpressions Components”, on page 328](#)).
6. Set up a server requirements statement.
7. Determine which PBX system, PBX system cards and line cards are being used (cf. table in [Section C.3.1, “Connection Matrix for PBX Systems”, on page 241](#))
 - Verify that the PBX system and PBX system cards are correct, installed and configured properly (cf. [Section C.3, “PBX Systems Supported”, on page 240](#))
 - Verify that the line cards have been installed properly in the XPR server
8. Refer to each chapter for additional pre-installation tasks to perform
9. Proceed to the appropriate section:
 - [Section C.4, “BRI/PRI HiPath 4000/CorNet-NQ Installation”](#)
 - [Section C.5, “BRI/PRI/Eicon HiPath 3000/CorNet-N Installation”](#)
 - [Section C.6, “Hicom 300H/CorNet-T Installation”](#)
 - [Section C.7, “PRI/Eicon Nortel Meridian QSIG Installation”](#)

C.4 BRI/PRI HiPath 4000/CorNet-NQ Installation

This section describes the installation of a BRI or PRI interface with Dialogic DIVA Server board(s) using the CorNet-NQ protocol at a HiPath 4000 PBX.

Interface	PBX	Line Card	PBX Card	Protocol	Max. no. of boards per server	Max. no of channels per session
BRI Connectivity						
S ₀ /BRI	HiPath 4000	Dialogic DIVA BRI	STMD2	CorNet-NQ	3	6
S ₀ /BRI	HiPath 4000	Dialogic DIVA 4BRI	STMD2	CorNet-NQ	3	24
PRI Connectivity						
T1/PRI	HiPath 4000	Dialogic DIVA PRI	TMDNH	CorNet-NQ	3	68

C.4.1 Pre-installation Checklist

1. Perform the checklist as specified in [Section C.3.3, “Performing the Checklist”](#), on page 243 and have info ready.
2. Except for steps 8 and 9 on page 257, the installation of BRI and PRI cards is identical:
 - a) **BRI**: Perform step 8, then continue with step 10
 - b) **PRI**: Perform step 9, then continue with step 10

C.4.2 Activate the License

Read [Chapter 3, “Generating Licenses”](#) about licensing. Then make sure that

- a CLM and a CLA is available in the network
- you have the required license as XML file (cf. [Section 3.1, “Licensing Routine”](#), on page 38 and [Section 3.5, “Generating a License Key”](#), on page 41).

After you have obtained the license as XML file, import it into the CLM and transfer the license to the CLA that OpenScape Xpressions is to connect. Please refer to [Section 3.7, “Activating Licenses in the CLA”](#), on page 44.

If you need to obtain the license via the CLA, please read section 5 in the CLM online help. To open the help, click on the **Help** button in the CLM interface.

After successfully activating the license continue with [Section C.4.5, “Install the OpenScape Xpressions Software”](#), on page 250.

C.4.3 Install the License Service

1. Connect the XPR installation medium to the computer.
2. The license service installation starts. In the next dialogs click on **Next** until the following dialog opens:

Xpressions License Service

HiPath License Manager

UNIFY

Please enter the connection data for the HiPath License Management.

IP address:

Port:

Time-out:

Connection attempts:

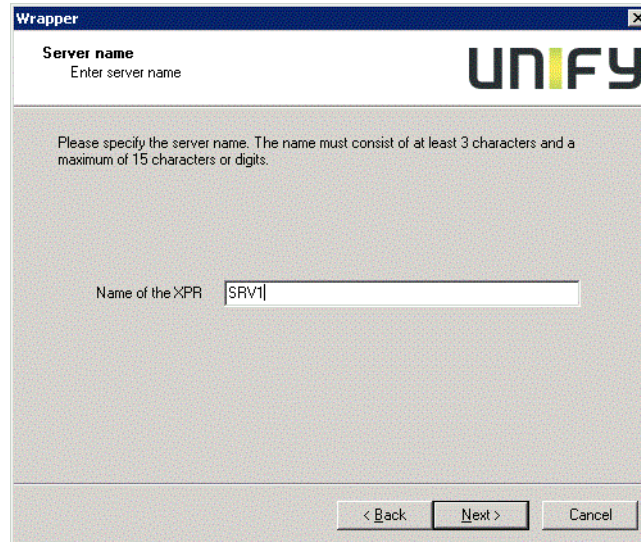
InstallShield

< Back Next > Cancel

3. In this dialog enter the IP address of the computer on which the CLA runs. Then click on **Next**.
4. In the following dialog click **Install**.
5. In the following dialog click **Finish**. The license service installation is thus complete.

C.4.4 Server Name, Languages and Release Notes

1. After the license service installation, the following dialog opens:

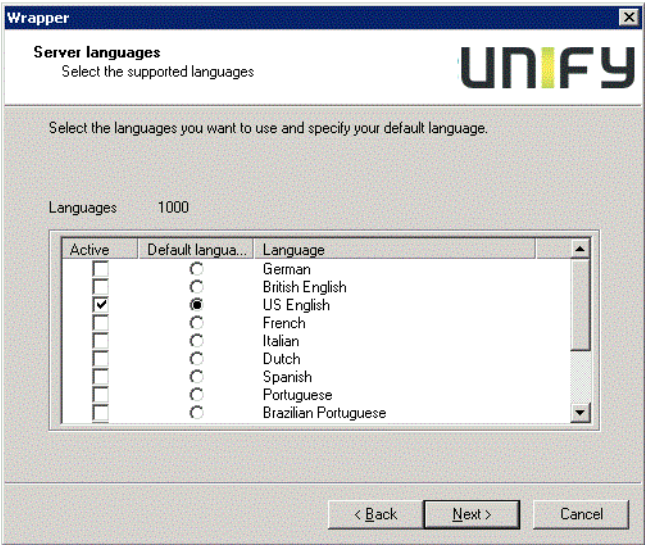


The screenshot shows a Windows-style dialog box titled "Wrapper". It has a "Server name" section with the instruction "Enter server name" and the UNIFY logo. Below this, a text box contains "SRV1". A message states: "Please specify the server name. The name must consist of at least 3 characters and a maximum of 15 characters or digits." At the bottom, there are three buttons: "< Back", "Next >", and "Cancel".

2. Enter the server name and then click on **Next**. When you select the server name, heed the following points:
 - the name you enter here **cannot be modified any more**
 - the name must not contain blanks, special characters such as ;, !, %, &, ... , or German umlauts (ä, ö, ü).
 - you must not use names of logical XPR lines. For example: *PhoneMail*, *VMS*, *COM*, *CON*, *FAXG3*, *FAXG4*, *MWI*, *FOD*, *PlayWave* and *SMTP* will not be accepted.
 - If you want to connect the XPR server to another XPR server via a Remote System Link, the server name selected here must not exceed a length of 11 characters.

NOTE: Remote System Link is not compatible with [Crypt_Sec], it is designed to only work with [KRYPT].

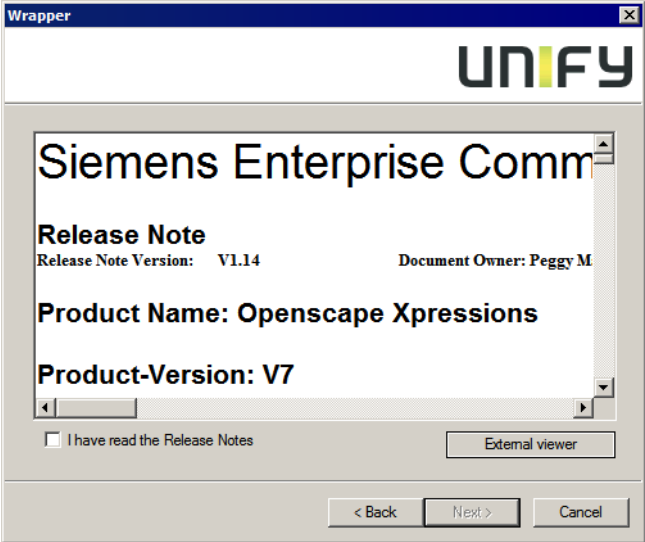
Up comes this dialog:



- In the **Active** column select the languages to be installed. Only select as many languages as licenses are available.

NOTE: You need to select at least one language in order to continue the installation.

- In the **Default language** column select the language that the XPR server is to use as default. You can specify only one language as default language.
- Click the **Continue** button. Up comes this dialog:



This dialog represents the `ReleaseNotes.rtf` file, which is found in the `XpressionsInstall` directory of the setup medium.

6. Please read the Release Notes. Via the **Open in external viewer** button you can open the corresponding file in the application that is registered in the operating system for the file type *RTF*.

7. Select the **I have read the Release Notes** check box. This activates the **Next** button.

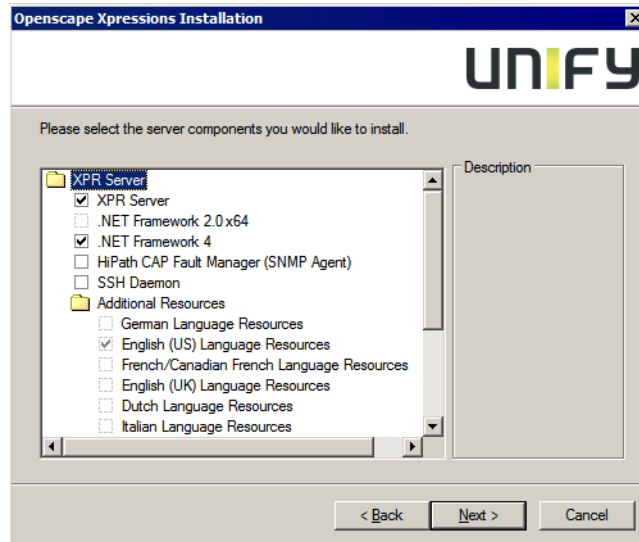
If you do not select the check box, the **Next** button stays inactive and you cannot continue the installation.

8. After you have read the Release Notes, click on **Next**.

The dialog for selecting the server components opens. Please continue reading in [Section C.4.5, “Install the OpenScape Xpressions Software”](#), on [page 250](#).

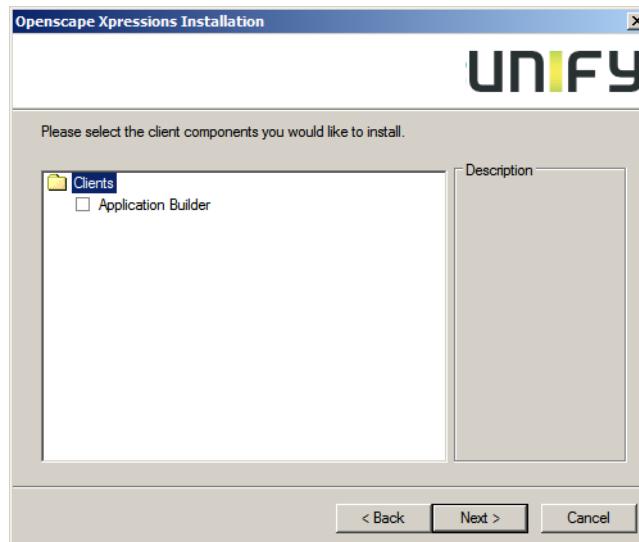
C.4.5 Install the OpenScape Xpressions Software

Up comes this dialog:

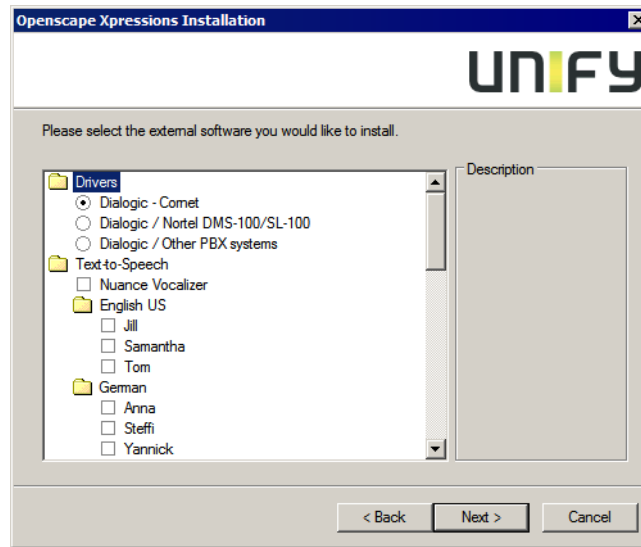


1. Select the **XPR server**. Then click **Next**.

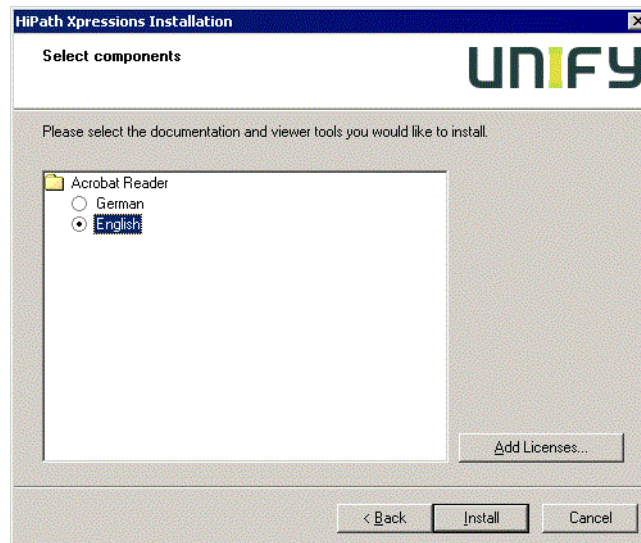
Up comes this dialog:



2. Click on **Next**. Up comes this dialog:



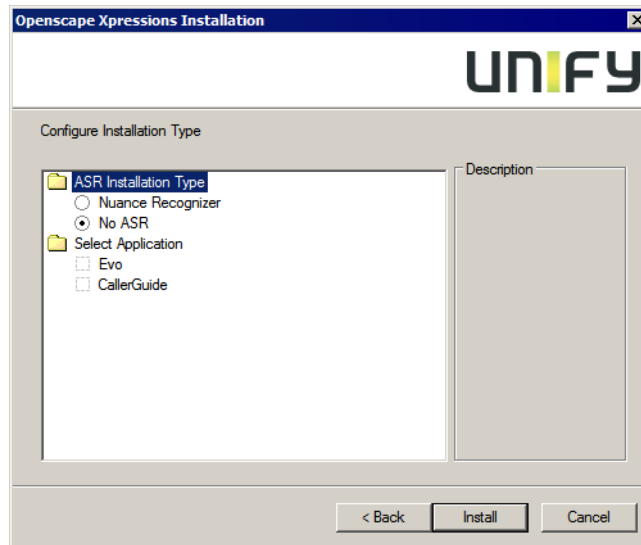
3. Select **Dialogic - Eicon**. Then click **Next**. Up comes this dialog:



4. If you want to install the Acrobat Reader, select a language and click on **Install**. Otherwise click only on **Install** without making a selection.

If the customer has purchased an ASR license, the **Next** button appears instead of **Install**. When you click on **Next**, the following dialog opens:

Configuring OpenScape Xpressions as Voice-only System
BRI/PRI HiPath 4000/CorNet-NQ Installation



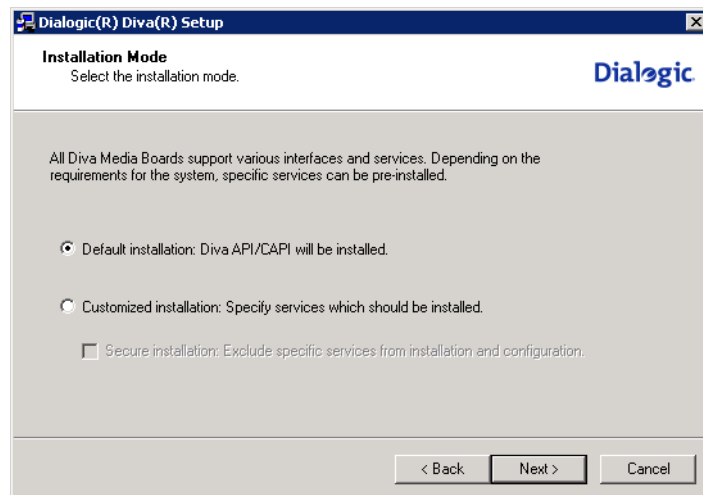
Select the ASR setup type and ASR applications. For further information please refer to [Section 4.3.11, “Installation Type for Automatic Speech Recognition”](#), on page 85. Then click **Install**.

C.4.6 Install the Dialogic DIVA Driver

1. The setup program starts with the following welcome dialog.

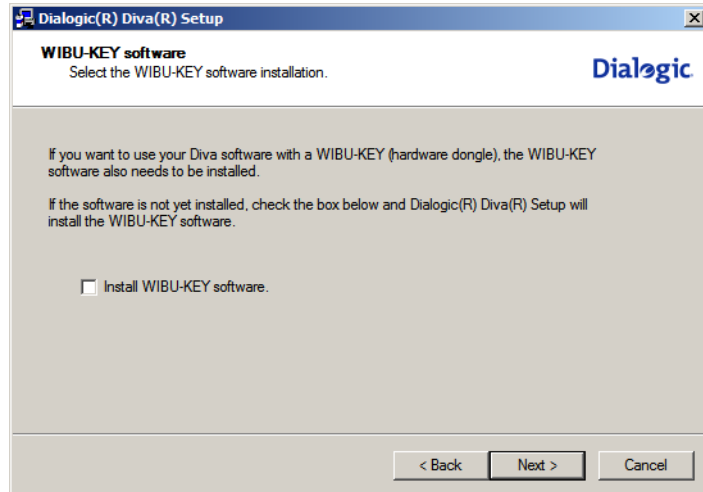


2. Click on **Next**. Up comes this dialog:



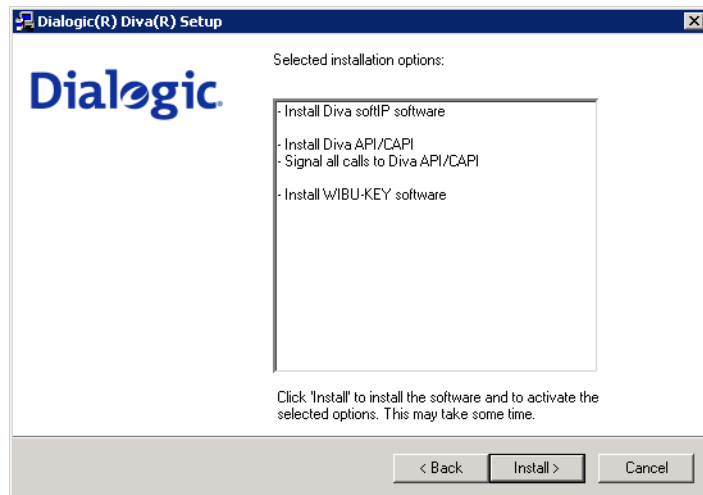
3. Select the option **Default installation: Diva API / CAPI will be installed.** Then click on **Next**.

Up comes this dialog:



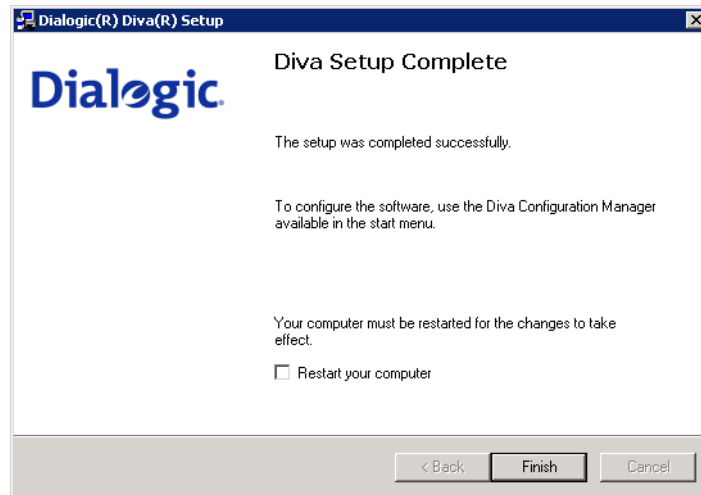
4. If you use WIBU-KEY, select the option **Install WIBU-Key software.** Then click on **Next**.

Up comes this dialog:



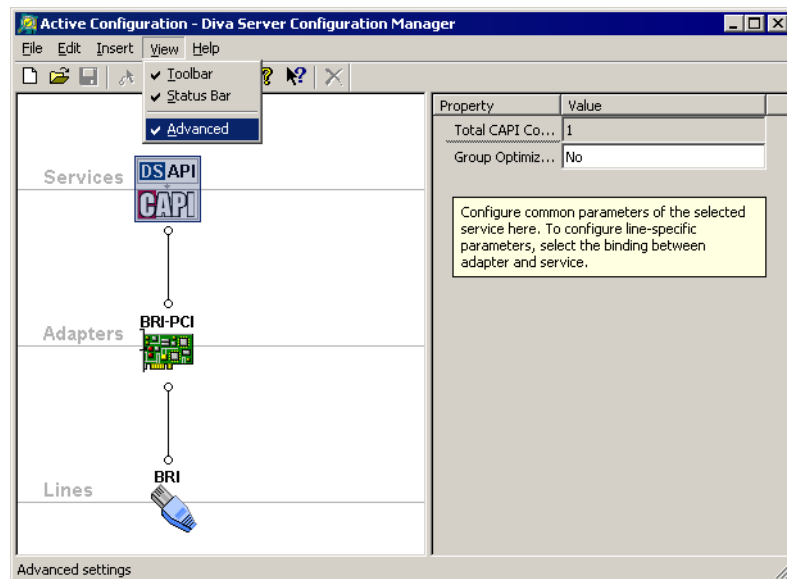
5. Check the selected the installation options. Then click on **Next**.

Up comes this dialog:



6. Deselect the **Restart your computer** option. Finally, click **Finish**.

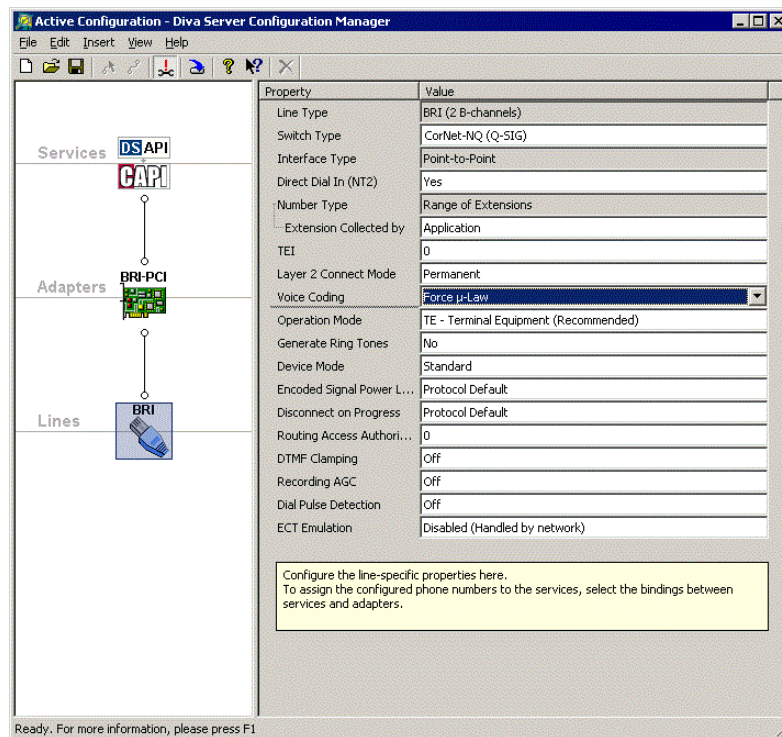
The Eicon driver configuration program starts and the following dialog opens:



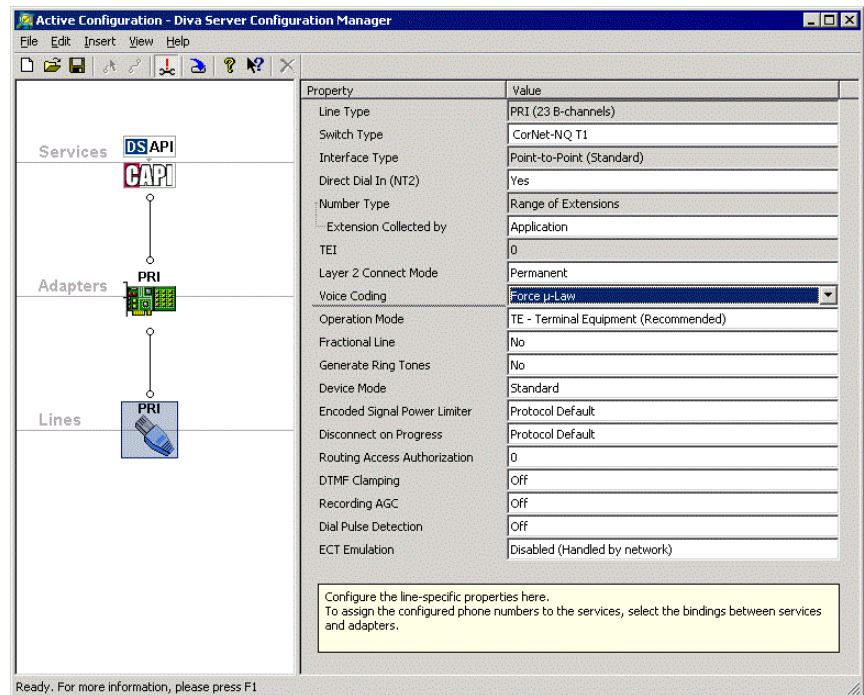
Configuring OpenScope Xpressions as Voice-only System

BRI/PRI HiPath 4000/CorNet-NQ Installation

7. Open the **View** menu option and select the **Advanced** option.
8. **For a BRI interface** select a BRI icon and make the following settings in the fields of the dialog's right hand portion:
 - a) Click on the **Switch Type** field and select **CorNet-NQ (Q-SIG)**.
 - b) Click on the **Interface Type** field and select **Point-to-Point**.
 - c) Click on the **Direct Dial In** field and select **Yes**
 - d) Click on the **Number Type** field and select **Range of Extensions**.
 - e) Click on the **Extension Collected by** field and select **Application**.
 - f) Click on the **Layer 2 Connect Mode** field and select **Permanent**.
 - g) Click on the **Voice Coding** field and select **Force a-Law** (USA: μ -Law).
 - h) Repeat the steps **a** to **g** for each available BRI line.
 - i) Continue with step **10** on [page 258](#).

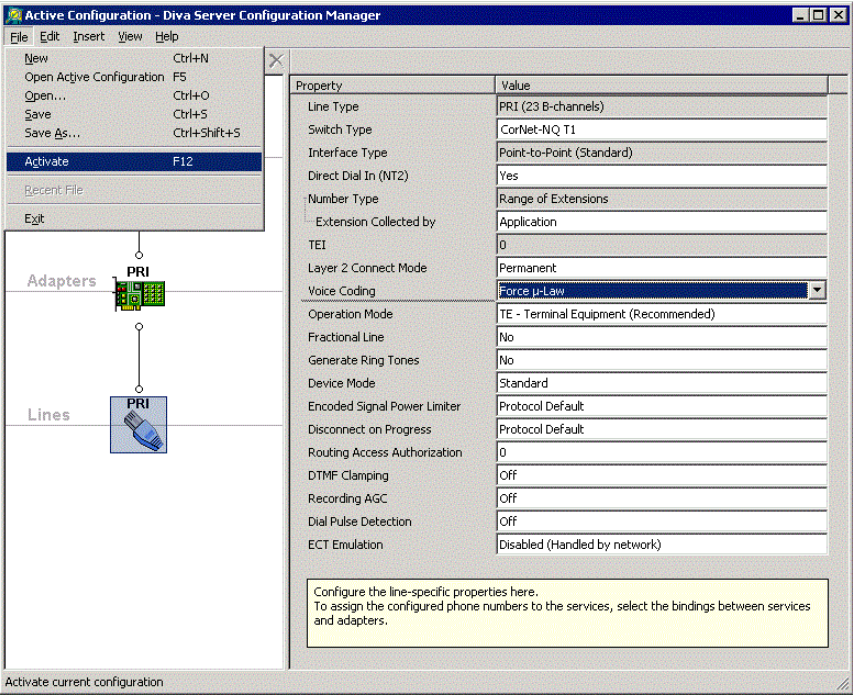


9. **For a PRI interface** select a PRI icon and make the following settings in the fields of the dialog's right hand portion:
 - a) Click on the **Switch Type** field and select **CorNet-NQ T1 (Q-SIG)**.
 - b) Click on the **Interface Type** field and select **Point-to-Point**.
 - c) Click on the **Direct Dial In** field and select **Yes**
 - d) Click on the **Number Type** field and select **Range of Extensions**.
 - e) Click on the **Extension Collected by** field and select **Application**.
 - f) Click on the **Layer 2 Connect Mode** field and select **Permanent**.
 - g) Click on the **Voice Coding** field and select **Force a-Law (USA: μ -Law)**.
 - h) continue to [10 on page 258](#).

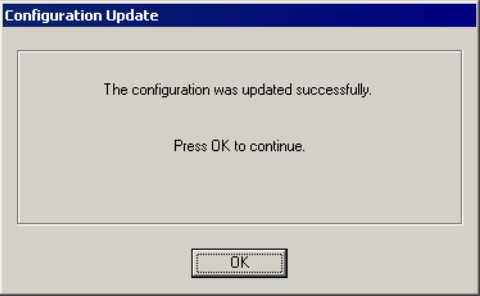


Configuring OpenScope Xpressions as Voice-only System
BRI/PRI HiPath 4000/CorNet-NQ Installation

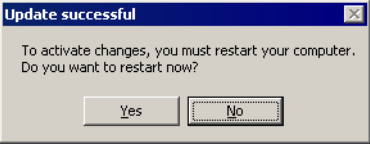
10. Open the **File** menu option and select the **Activate** option. This update may take several minutes.



11. After you settings have been successfully copied, the following dialog opens:

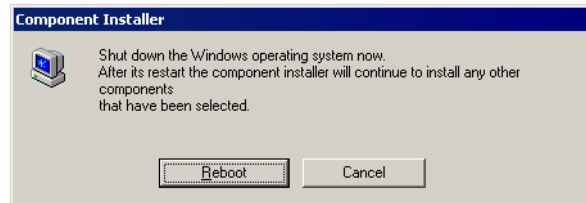


12. Click **OK**. Up comes this dialog:



13. Click on **No**. **DO NOT REBOOT**.

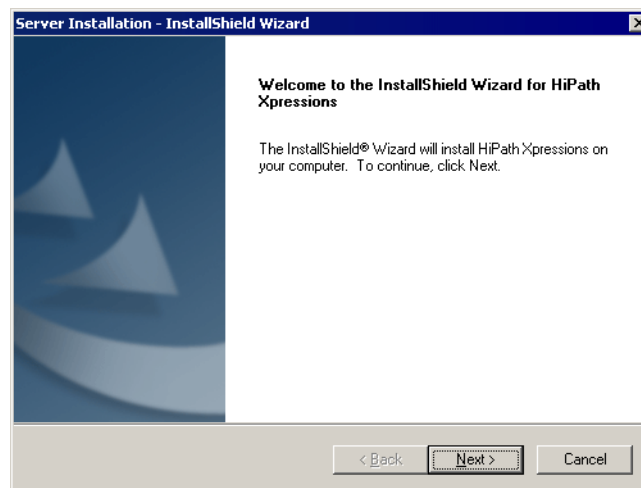
14. Close the **Active Configuration** window. Up comes this dialog:



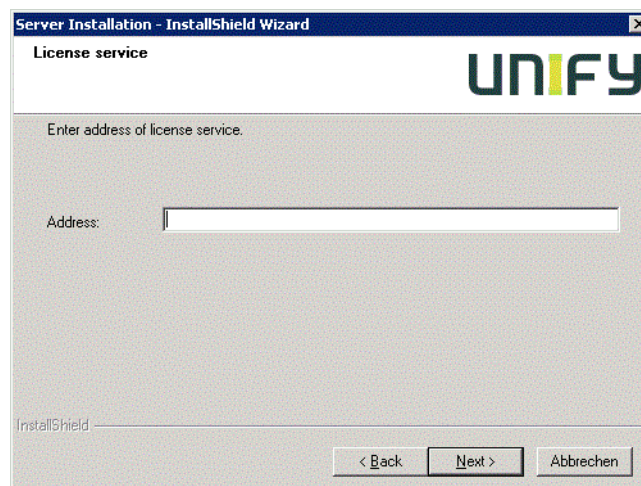
15. Now click **Reboot** to restart the system.

C.4.7 Install the Xpressions Components

1. After rebooting, log on to the server computer with an administrator account. The setup is continued and the following dialog opens:



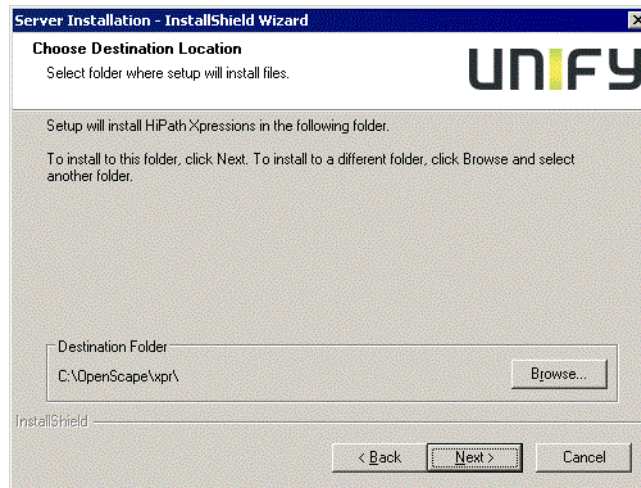
2. Click on **Next**. Up comes this dialog:



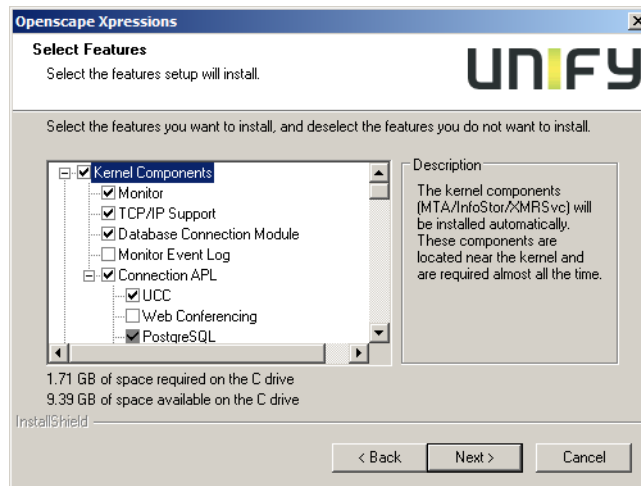
3. Enter the IP address of the computer on which the CLA runs. Then click on **Next**. Up comes this dialog:

Configuring OpenScape Xpressions as Voice-only System

BRI/PRI HiPath 4000/CorNet-NQ Installation

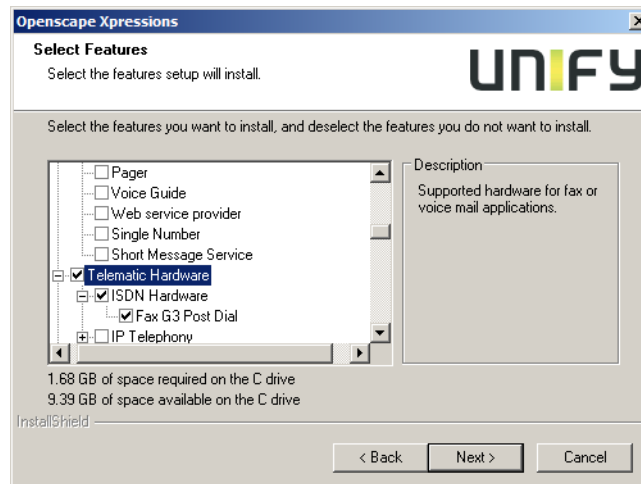
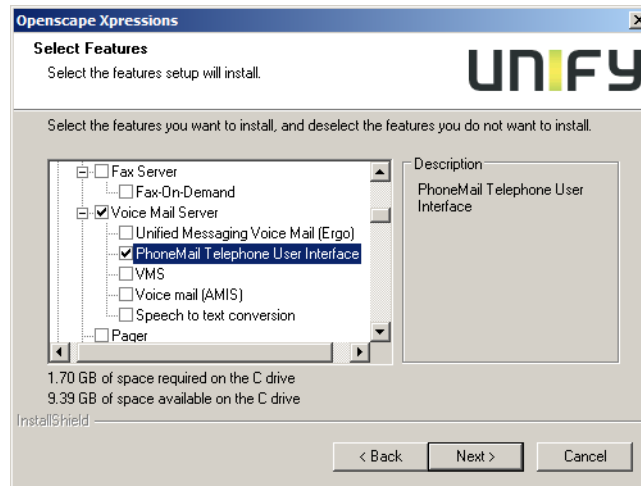
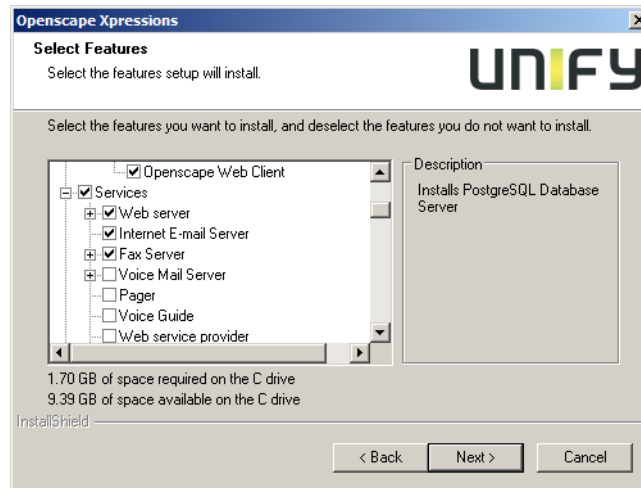


4. Check whether the defaulted setup target folder is on the largest available partition. If this is the case, click on **Next**. Otherwise use the **Browse...** button to select another target folder situated on the largest available partition. Check the customer's order (see [5 on page 243](#)) and select the components associated to the ordered options in this dialog (cf. the selected entries in following figures).



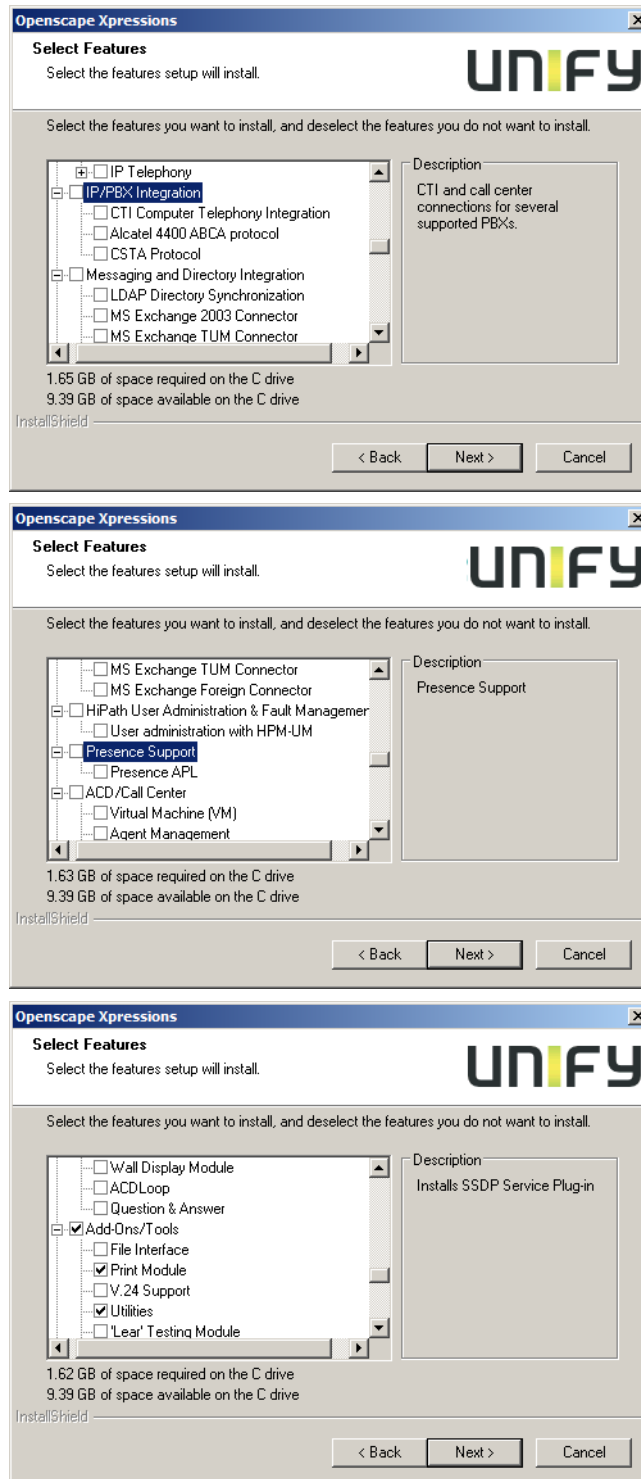
Configuring OpenScope Xpressions as Voice-only System

BRI/PRI HiPath 4000/CorNet-NQ Installation



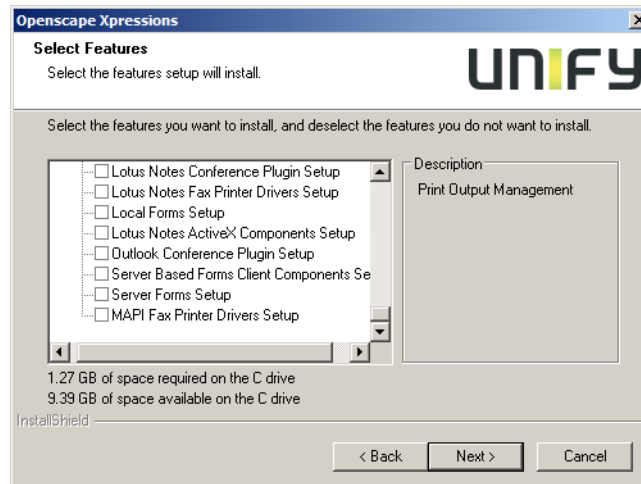
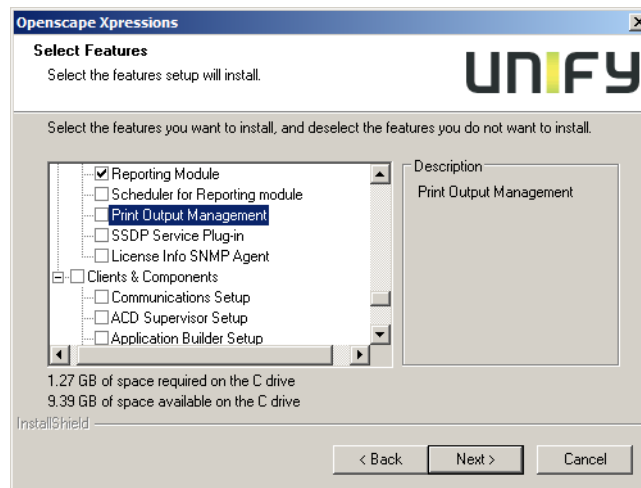
Configuring OpenScope Xpressions as Voice-only System

BRI/PRI HiPath 4000/CorNet-NQ Installation

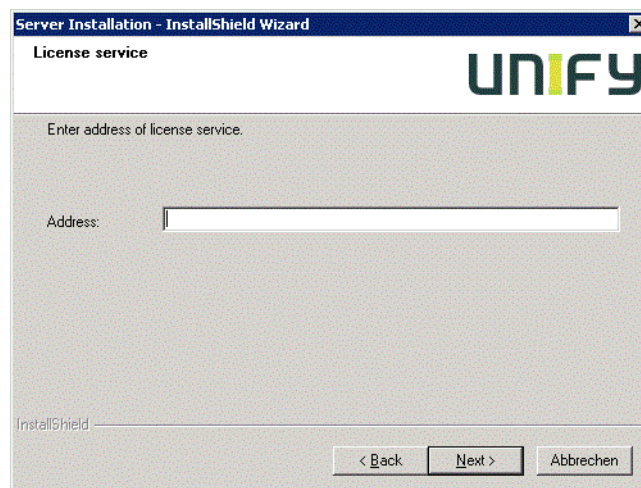


Configuring OpenScape Xpressions as Voice-only System

BRI/PRI HiPath 4000/CorNet-NQ Installation



After selecting all licensed features, click on **Next**. Up comes this dialog:



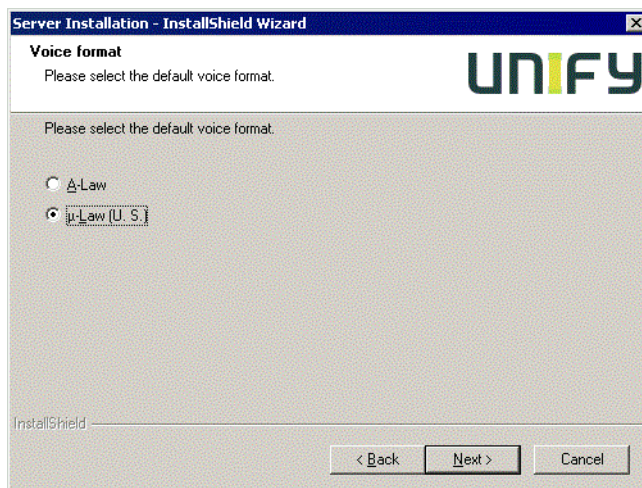
Configuring OpenScape Xpressions as Voice-only System

BRI/PRI HiPath 4000/CorNet-NQ Installation

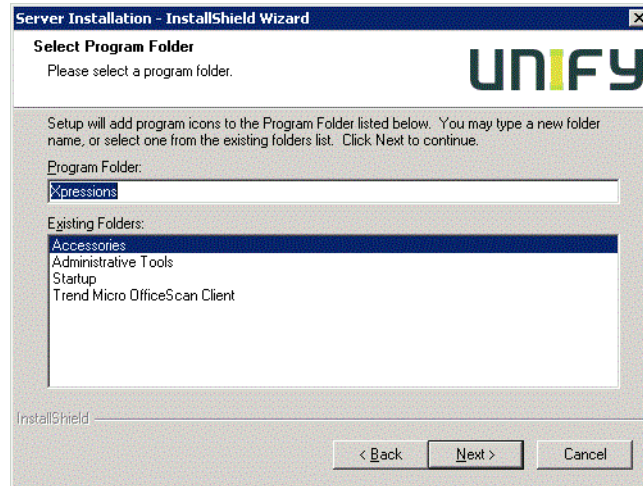
5. Click on **Next**.

NOTE: If desired, you may change the location of one of the folders to another drive. Make sure to use the largest available partition.

Up comes this dialog:



6. Select a default voice format. If you are in the U.S., select **μ-Law**. If you are in another country, select **A-Law**. Then click on **Next**. Up comes this dialog:



7. Click on **Next** to copy the program folder. Up comes this dialog:



8. Select the authentication type:

Login via the Windows User Account

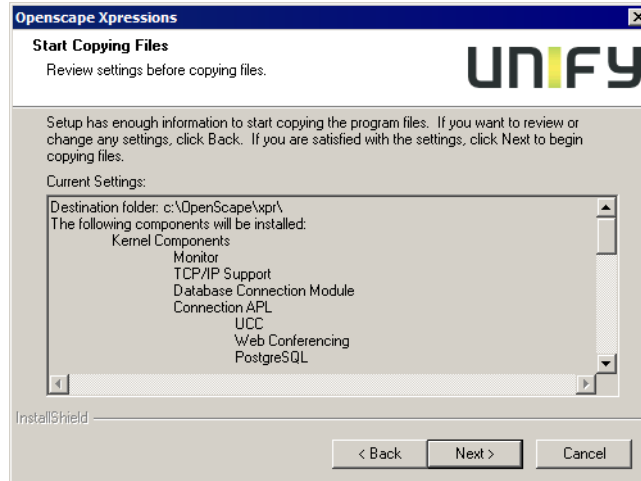
This is the standard method. If this method is applied, the user's Windows account is used for authentication against the XPR server. All password-specific functions in the XPR server are deactivated. After you have selected this option, the next installation step is to choose the Windows accounts to serve as XPR administrator or XPR postmaster (cf. [Section 4.5.6.1, "Login via the Windows User Account", on page 106](#)).

Login via XPR account (user name + password (PIN))

With this authentication method, user accounts for the XPR administrator and the XPR postmaster are created in the XPR database. It is still possible though to activate the authentication via the Windows user account for some

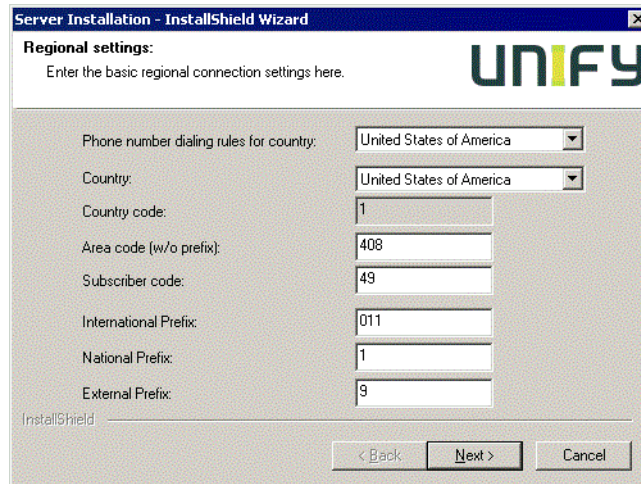
users in hindsight. In the next installation step you need to specify a name and password for the administrator and the postmaster of the XPR server each (cf. [Section 4.5.6.2, “Login via XPR Account”, on page 107](#)).

Then click on **Next**. Up comes this dialog:

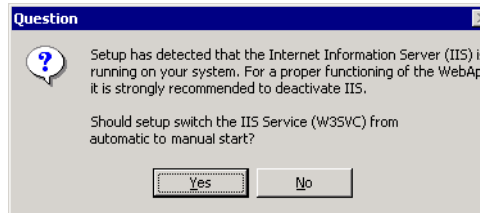


9. Check the listed options and click on **Next**. The copying process begins. A status dialog informs you about the installation progress.

Up comes this dialog:

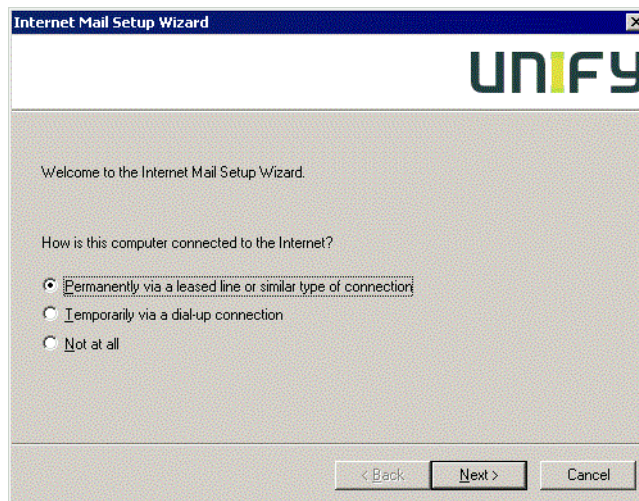


10. In the **Phone number dialing rules for country** field select the country in which the system is to be set up.
11. Enter the area code (without prefix) and the subscriber number. Then click on **Next**.
12. If the Internet E-mail server has been selected as option and the Windows Internet Information Server (IIS) has been installed and activated on the computer, the following dialog appears:

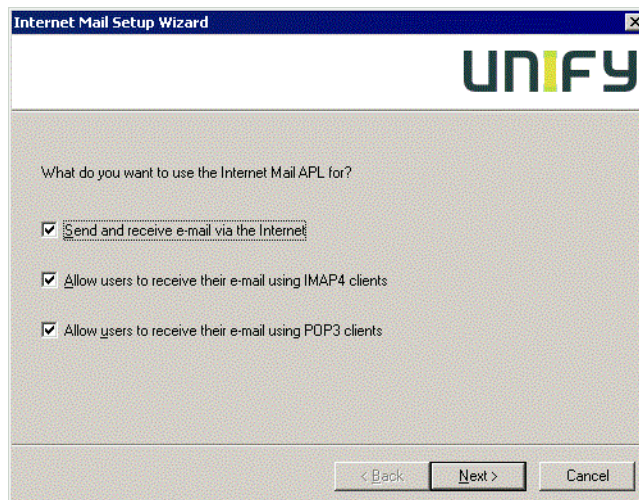


Confirm this dialog with **Yes**.

If the Internet Information Server has not been installed on the computer, the following dialog appears:



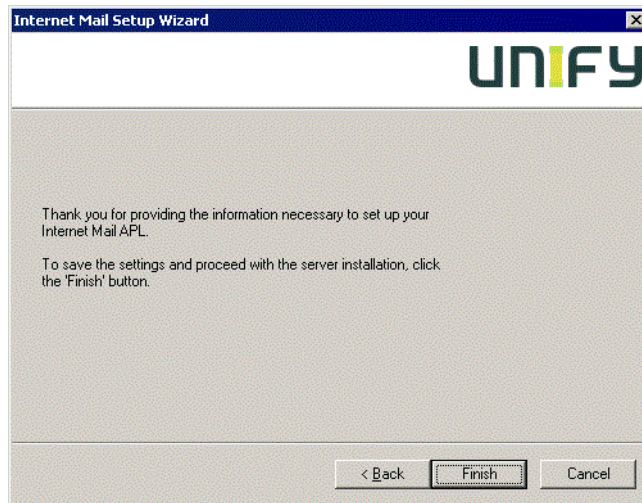
- a) Select the **Permanently via a leased line or similar type of connection** option, then click on **Next**. Up comes this dialog:



- b) Verify that **all options are selected** and click on **Next**. Up comes this dialog:

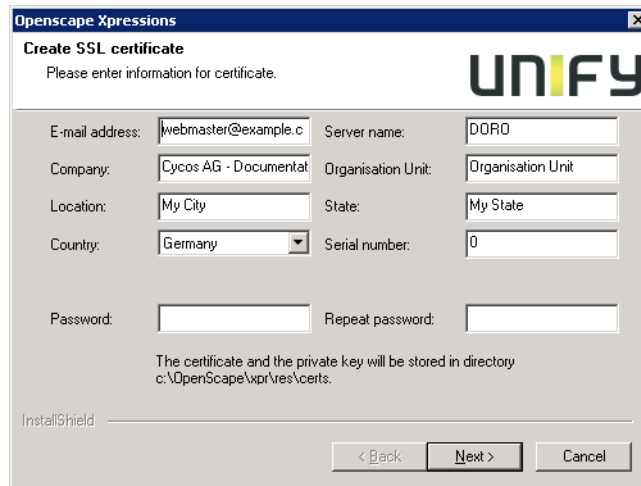
Configuring OpenScape Xpressions as Voice-only System

BRI/PRI HiPath 4000/CorNet-NQ Installation



c) Click **Finish**.

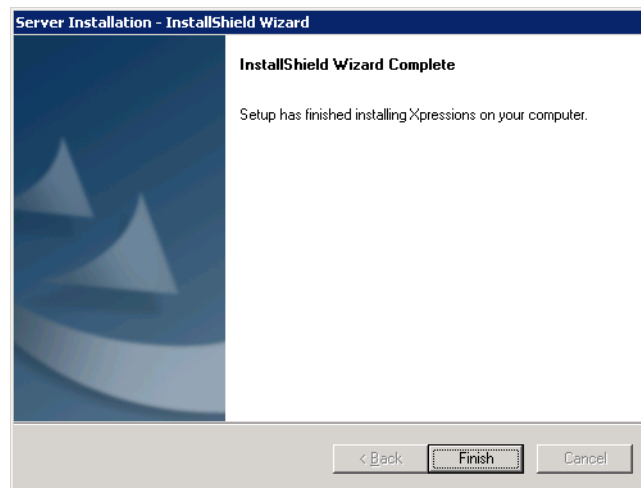
13. The SMTP APL setup is completed. Up comes this dialog:



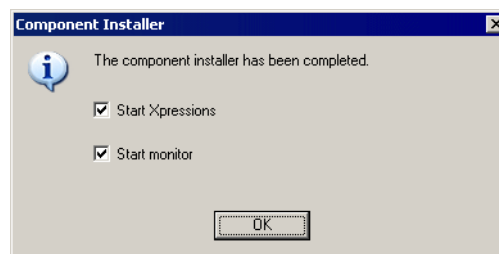
14. In the dialog's fields make the specifications that are to become elements of the certificate. In the **Password** field enter a sufficiently complex password and repeat this specification in the **Repeat password:**. Then click on **Next**.

IMPORTANT: 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.

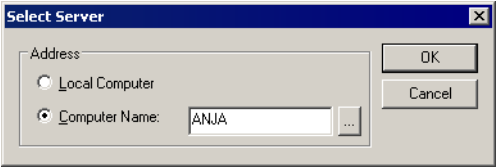
Up comes this dialog:



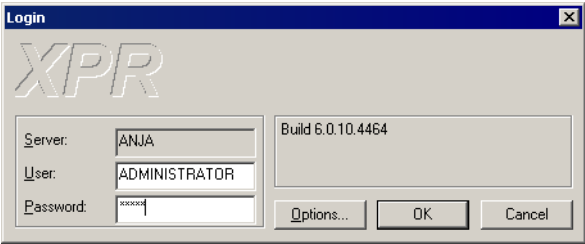
15. Click **Finish**. You may have to click **Finish** several times depending on the selected options. The server setup is thus complete.
16. The selected language packets and other components will now be installed. These installations occur automatically, so that you need not make any entries. As soon as all installations are complete, the following dialog appears:



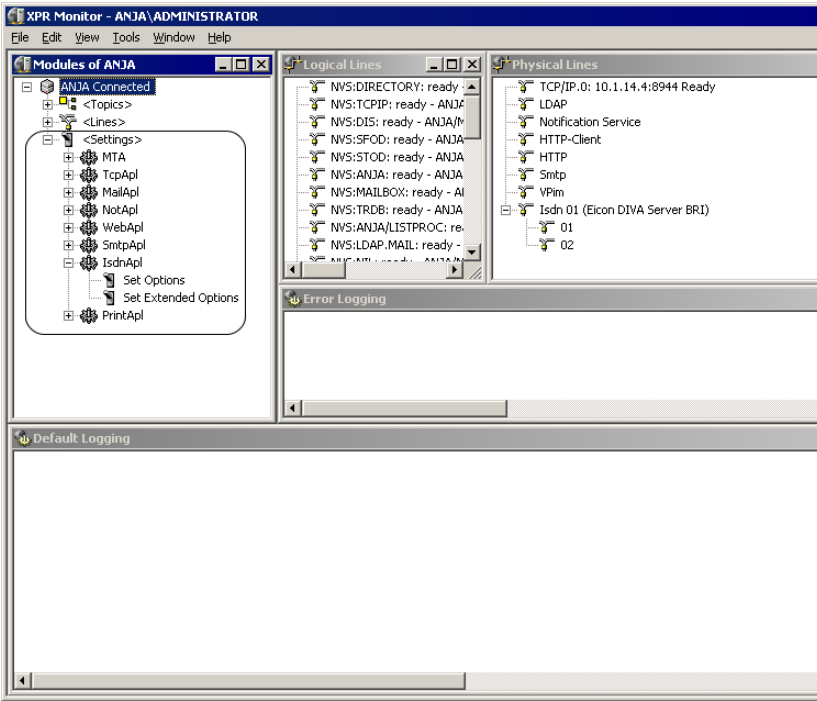
17. Select the options **Start HiPath Xpressions** and **Start monitor** and click on **OK**. Up comes this dialog:



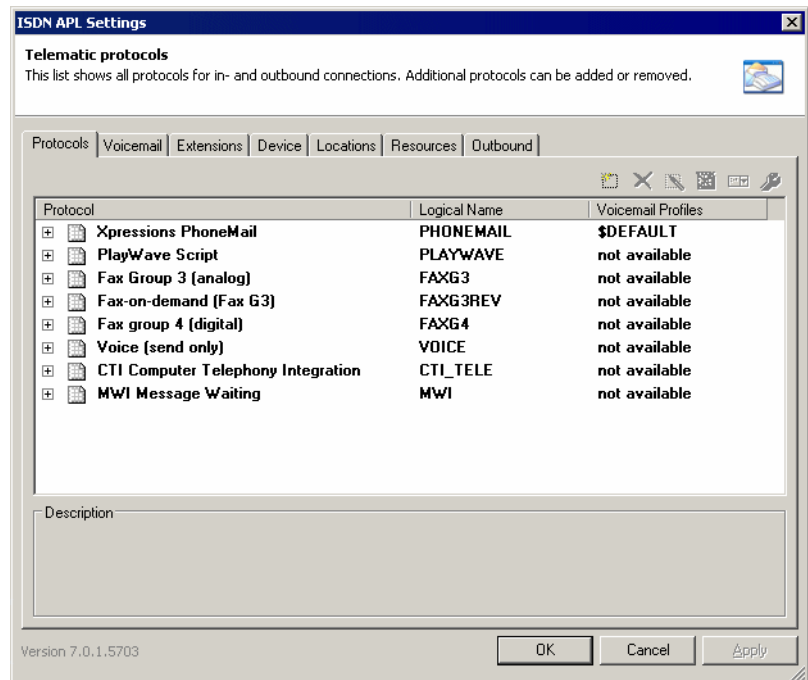
18. Enter or browse the Xpressions server name, then click **OK**. The monitor login dialog opens:



19. Log on to the XPR monitor as **Administrator**, then click on **OK**. The monitor opens:

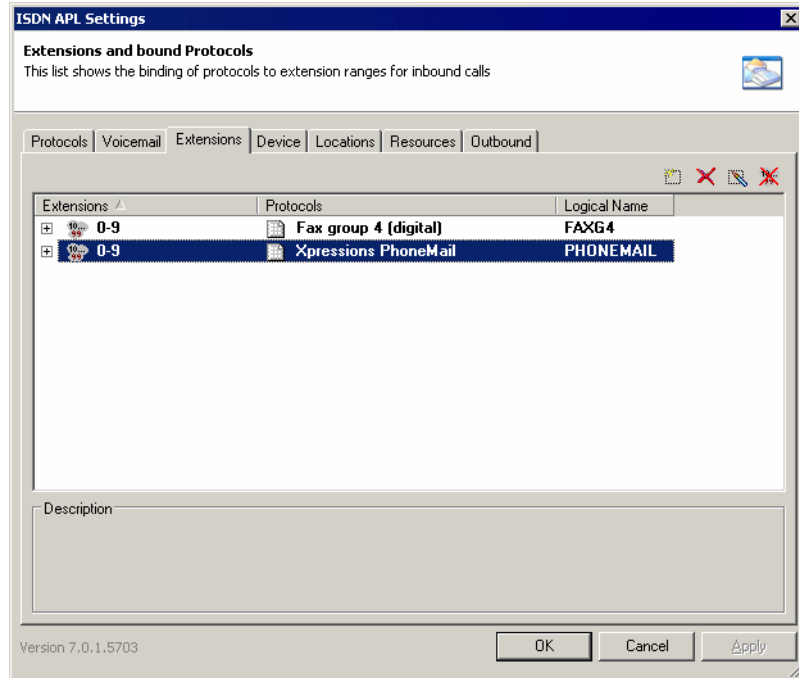


20. In the **Modules of <Xpressions Server>** window under **<Settings>** expand the **IsdnApl** entry and doubleclick **Set Extended Options**. Up comes this dialog:

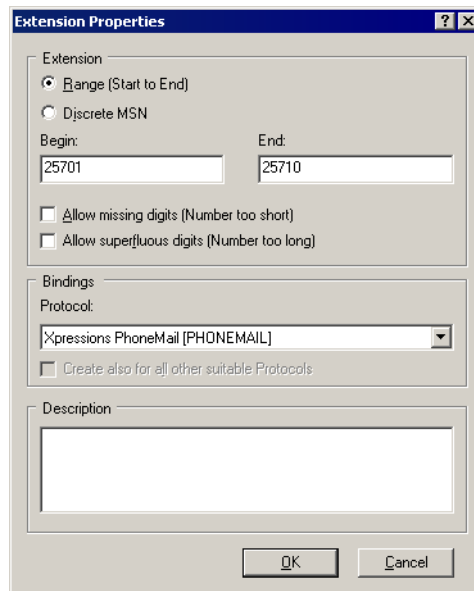


21. Check whether the **Protocols** tab shows all protocols displayed above. Verify that the **CTI_TELE**, **MWI**, **PHONEMAIL**, **PLAYWAVE**, and **VOICE** protocols are displayed at any rate.

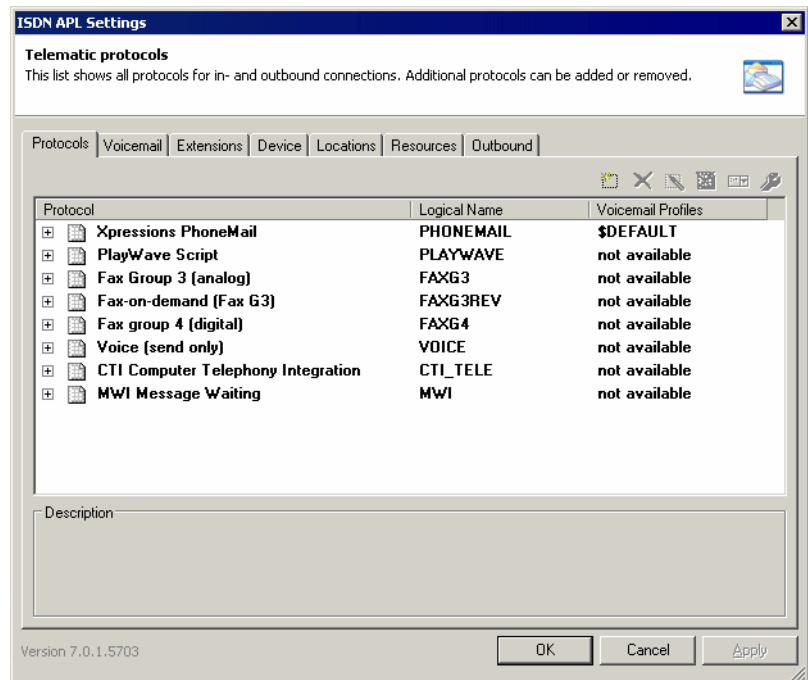
22. Switch to the **Extensions** tab, then double-click **Xpressions PhoneMail**.



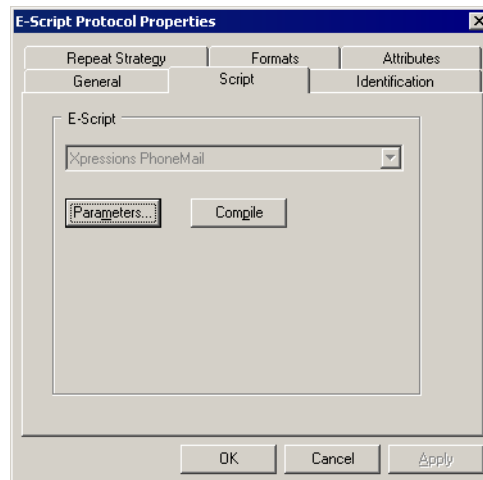
Up comes this dialog:



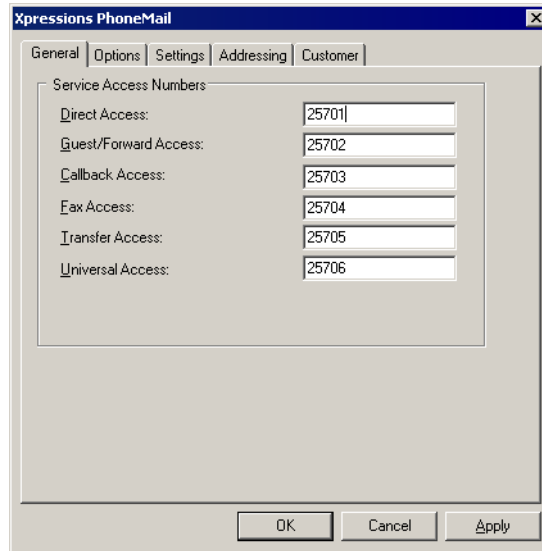
23. In the **Extensions** field enter the first and last digit only for the ACCESS NUMBERS, then click on **OK**. The dialog closes and you return to the following dialog:



24. Open the **Protocols** tab and doubleclick the **Xpressions PhoneMail** entry. Up comes this dialog:



25. Open the **Script** tab and click on the **Parameters** button. Up comes this dialog:

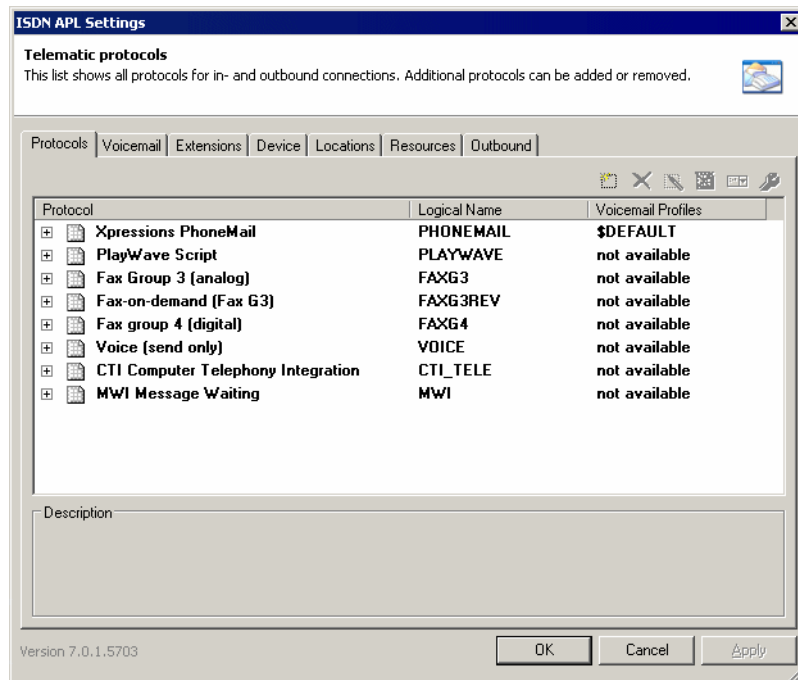


The dialog box is titled "Xpressions PhoneMail" and has tabs for General, Options, Settings, Addressing, and Customer. The "General" tab is selected. Under the "Service Access Numbers" section, there are six input fields with the following labels and values:

Label	Value
Direct Access:	25701
Guest/Forward Access:	25702
Callback Access:	25703
Fax Access:	25704
Transfer Access:	25705
Universal Access:	25706

At the bottom of the dialog are buttons for OK, Cancel, and Apply.

26. Enter the **Service Access Numbers** and click on **OK**.
27. Click on **OK** again to close the **E-Script Protocol Properties** window. You return to the following dialog:

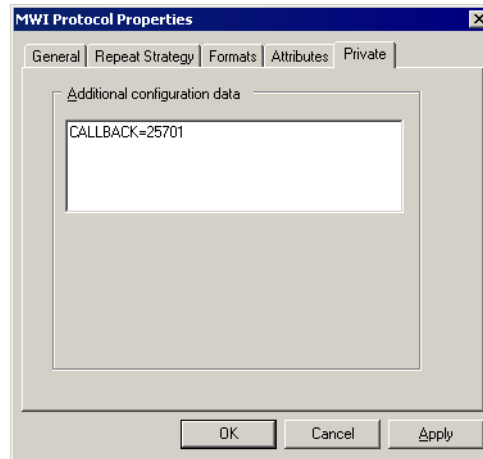


The dialog box is titled "ISDN APL Settings" and has tabs for Protocols, Voicemail, Extensions, Device, Locations, Resources, and Outbound. The "Protocols" tab is selected. Below the tabs, there is a table listing protocols and their configurations.

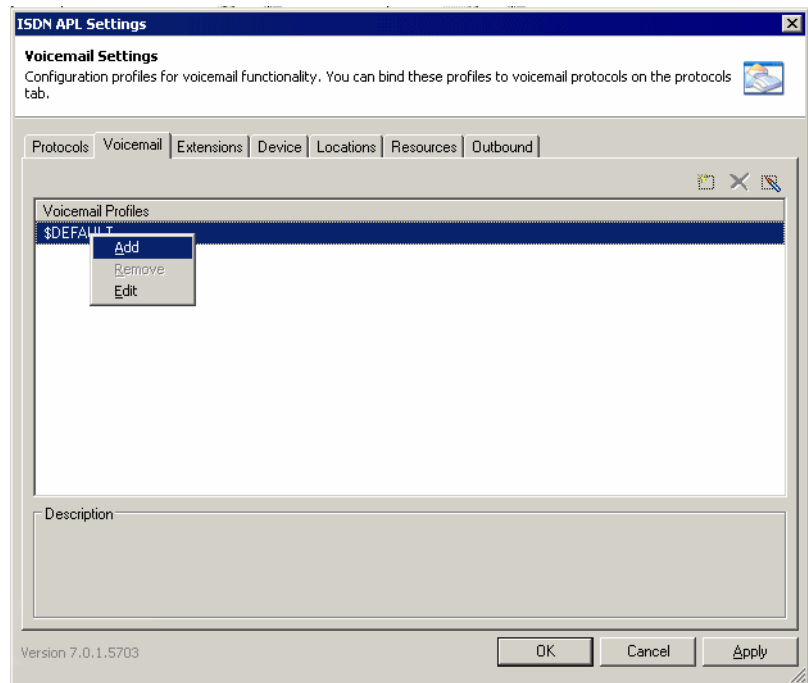
Protocol	Logical Name	Voicemail Profiles
Xpressions PhoneMail	PHONEMAIL	\$DEFAULT
PlayWave Script	PLAYWAVE	not available
Fax Group 3 (analog)	FAXG3	not available
Fax-on-demand (Fax G3)	FAXG3REV	not available
Fax group 4 (digital)	FAXG4	not available
Voice (send only)	VOICE	not available
CTI Computer Telephony Integration	CTI_TELE	not available
MWI Message Waiting	MWI	not available

Below the table is a "Description" field. At the bottom of the dialog are buttons for OK, Cancel, and Apply. The version number "Version 7.0.1.5703" is displayed in the bottom left corner.

28. Open the **Protocols** tab and doubleclick the **MWI** entry. Up comes this dialog:



29. Open the **Private** tab, enter the PBX callback number and click on **OK**. Up comes this dialog:

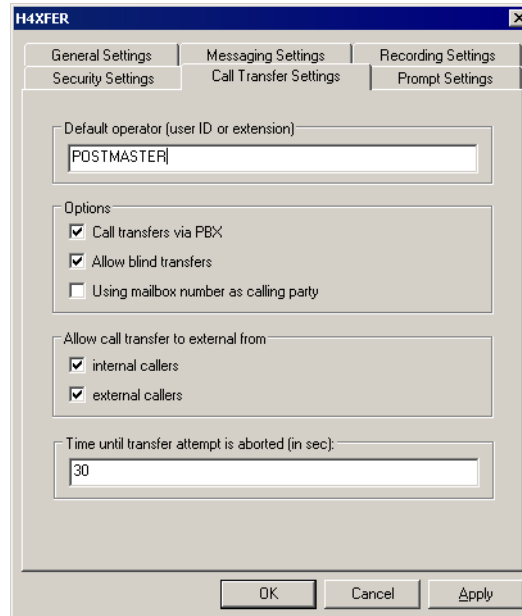


30. Open the **Voicemail** tab, click with the right mousebutton on the **\$DEFAULT** entry and select **Add** in the context menu. Up comes this dialog:

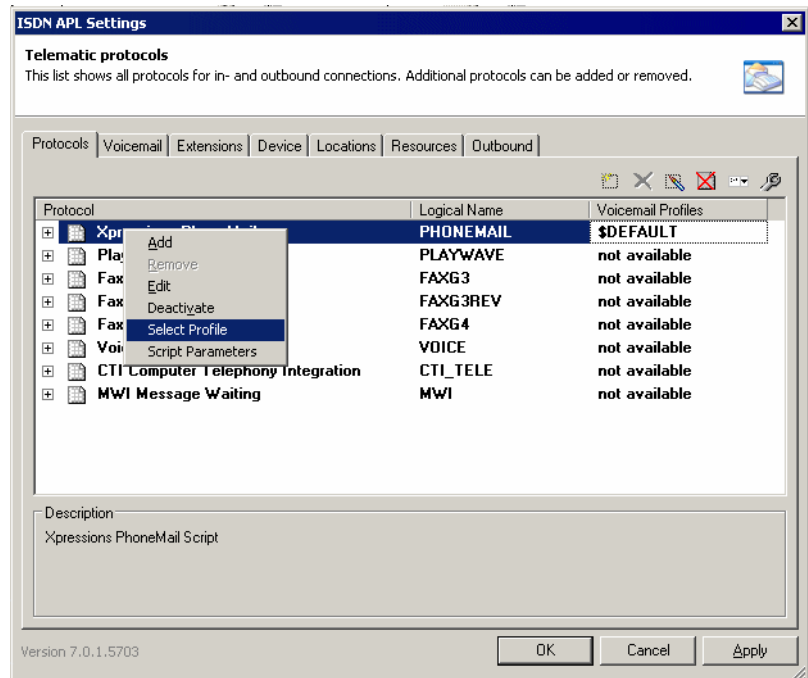
The screenshot shows a Windows-style dialog box titled "H4XFER". It has a tabbed interface with the following tabs: "Security Settings", "Call Transfer Settings", "Prompt Settings", "General Settings", "Messaging Settings", and "Recording Settings". The "General Settings" tab is currently selected. Inside the dialog, there is a "Note" stating: "Note: Some of these parameters are only supported by certain voice mail systems. Please refer to the product documentation for an overview of the relevant parameters." Below the note, there are three main input sections: 1. "Profile name" with a text box containing "H4XFER". 2. "Voicemail data path" with a text box containing "\\ANJA\MrsUserdata\$\vmdata" and a "Browse ..." button to its right. 3. "Alternative warn prompt" with an empty text box. At the bottom of the dialog are three buttons: "OK", "Cancel", and "Apply".

31. Open the **General Settings** tab and enter *H4XFER* in the **Profile name** field.
32. Open the **Call Transfer Settings** tab and,
33. If it does not already exist, enter the user ID or the extension of the **default operator**.
34. Select the **Allow blind transfers** option.

35. Verify that the **internal callers** and **external callers** options in the **Allow call transfer to external from** section are active.



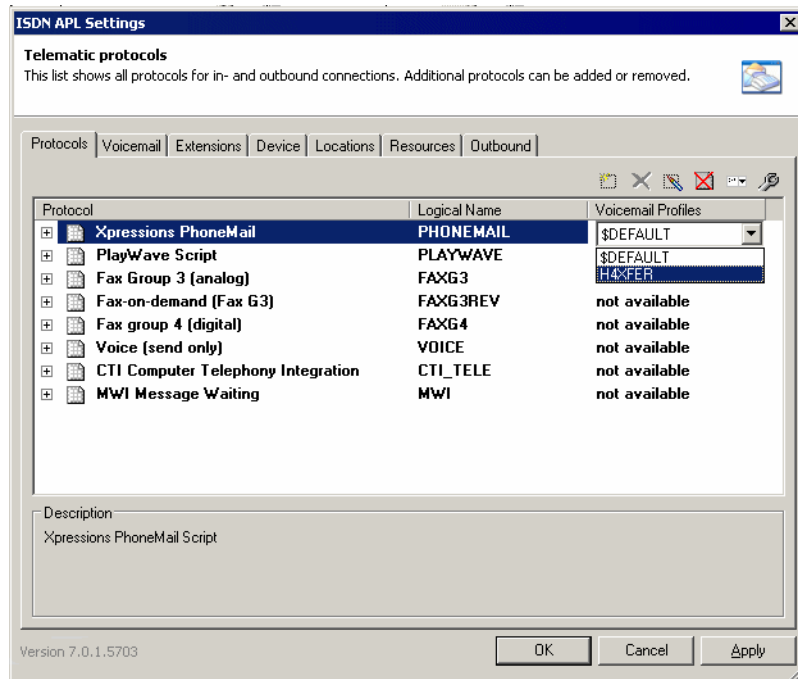
36. Click on **OK** to close the profile configuration. You return to the following dialog:



37. Open the **Protocols** tab, click with the right mousebutton on the **Xpressions PhoneMail** entry and select **Select Profile** in the context menu.

Configuring OpenScope Xpressions as Voice-only System

BRI/PRI HiPath 4000/CorNet-NQ Installation



38. Open the **Voicemail Profiles** pull-down menu and select **H4XFER**.
39. Click on **OK** to close the **ISDN APL Settings** window.
40. Proceed to [Section C.8, "System Test and Troubleshooting"](#).

C.5 BRI/PRI/Eicon HiPath 3000/CorNet-N Installation

This section describes the installation of a BRI or PRI interface using Dialogic DIVA Server board(s) using the CorNet-N protocol at a HiPath 3000 PBX.

Interface	PBX	Line Card	PBX Card	Protocol	Max. Cards per Server	Max. Channels per Session
BRI Connectivity						
S ₀ /BRI	HiPath 33xx/35xx	Dialogic DIVA BRI	STLS4	CorNet-N	3	6
S ₀ /BRI	HiPath 37xx/ Hicom 150	Dialogic DIVA 4BRI	STMD8	CorNet-N	3	24
PRI Connectivity						
T1/PRI	HiPath 35xx	Dialogic DIVA PRI	TST1	CorNet-N	3	68
T1/PRI	HiPath 37xx/ Hicom 150	Dialogic DIVA PRI	TMST1	CorNet-N	3	68

C.5.1 Pre-installation Checklist

NOTE: By the end of the installation you are asked to reset the HiPath 3000 system. Therefore perform the installation outside of business hours.

1. Perform the checklist as specified in [Section C.3.3, “Performing the Checklist”](#), on page 243 and have info ready.
2. The BRI and PRI installation procedures are identical except for steps 8 and 9 on page 292:
 - a) BRI: use step 10 , then continue to step 12;
 - b) PRI: use step 11, then continue to step 12.

C.5.2 Activate the License

Read [Chapter 3, “Generating Licenses”](#) about licensing. Then make sure that

- a CLM and a CLA is available in the network
- you have the required license as XML file (cf. [Section 3.1, “Licensing Routine”](#), on page 38 and [Section 3.5, “Generating a License Key”](#), on page 41).

After you have obtained the license as XML file, import it into the CLM and transfer the license to the CLA that OpenScape Xpressions is to connect. Please refer to [Section 3.7, “Activating Licenses in the CLA”](#), on page 44.

If you need to obtain the license via the CLA, please read section 5 in the CLM online help. To open the help, click on the **Help** button in the CLM interface.

After successfully activating the license continue with [Section C.4.5, “Install the OpenScape Xpressions Software”](#), on page 250.

C.5.3 Install the License Service

1. Connect the XPR installation medium to the computer.
2. The license service installation starts. In the next dialogs click on **Next** until the following dialog opens:

Xpressions License Service

HiPath License Manager

UNIFY

Please enter the connection data for the HiPath License Management.

IP address:

Port:

Time-out:

Connection attempts:

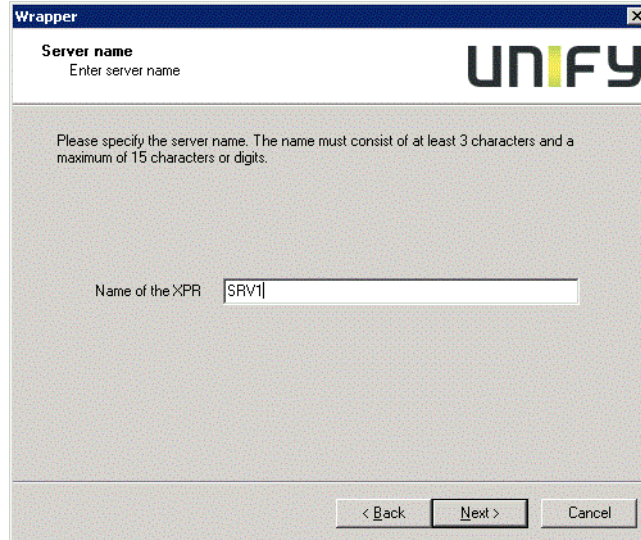
InstallShield

< Back Next > Cancel

3. In this dialog enter the IP address of the computer on which the CLA runs. Then click on **Next**.
4. In the following dialog click **Install**.
5. In the following dialog click **Finish**. The license service installation is thus complete.

C.5.4 Server Name, Languages and Release Notes

1. After the license service installation, the following dialog opens:



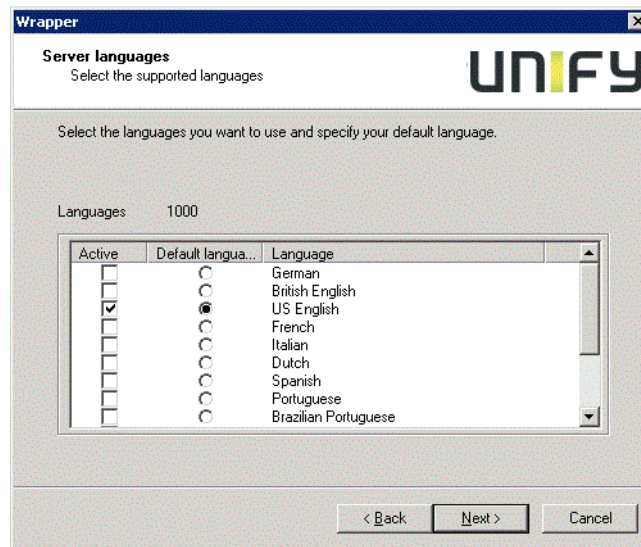
The screenshot shows a Windows-style dialog box titled "Wrapper". It has a "Server name" section with the instruction "Enter server name" and the UNIFY logo. Below this, a text box contains "Name of the XPR" followed by a text input field with "SRV1" entered. A message states: "Please specify the server name. The name must consist of at least 3 characters and a maximum of 15 characters or digits." At the bottom are three buttons: "< Back", "Next >", and "Cancel".

2. Enter the server name and then click on **Next**. When you select the server name, heed the following points:

 - the name you enter here **cannot be modified any more**
 - the name must not contain blanks, special characters such as ;, !, %, &, ... , or German umlauts (ä, ö, ü).
 - you must not use names of logical XPR lines. For example: *PhoneMail*, *VMS*, *COM*, *CON*, *FAXG3*, *FAXG4*, *MWI*, *FOD*, *PlayWave* and *SMTP* will not be accepted.
 - If you want to connect the XPR server to another XPR server via a Remote System Link, the server name selected here must not exceed a length of 11 characters.

NOTE: Remote System Link is not compatible with [Crypt_Sec], it is designed to only work with [KRYPT].

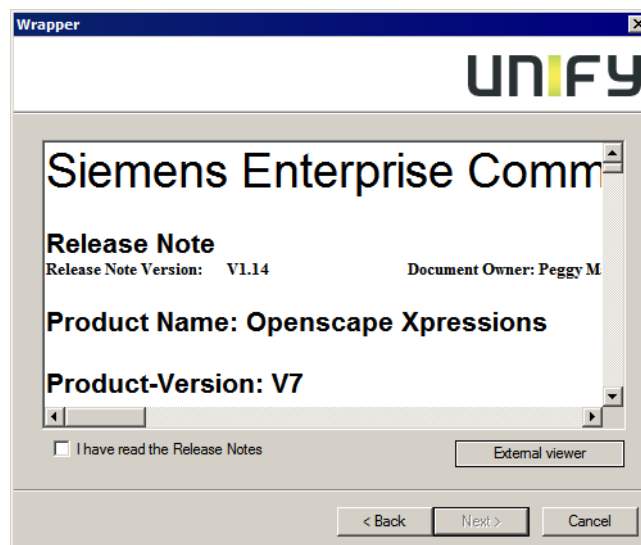
Up comes this dialog:



3. In the **Active** column select the languages to be installed. Only select as many languages as licenses are available.

NOTE: You need to select at least one language in order to continue the installation.

4. In the **Default language** column select the language that the XPR server is to use as default. You can specify only one language as default language.
5. Click the **Continue** button. Up comes this dialog:



This dialog represents the `ReleaseNotes.rtf` file, which is found in the `XpressionsInstall` directory of the setup medium.

Configuring OpenScape Xpressions as Voice-only System

BRI/PRI/Eicon HiPath 3000/CorNet-N Installation

6. Please read the Release Notes. Via the **Open in external viewer** button you can open the corresponding file in the application that is registered in the operating system for the file type *RTF*.

7. Select the **I have read the Release Notes** check box. This activates the **Next** button.

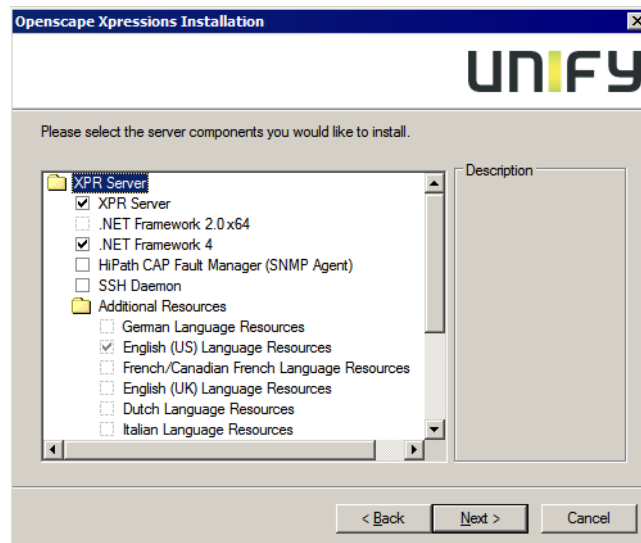
If you do not select the check box, the **Next** button stays inactive and you cannot continue the installation.

8. After you have read the Release Notes, click on **Next**.

The dialog for selecting the server components opens. Please continue reading in [Section C.5.5, "Install the OpenScape Xpressions Software"](#), on [page 285](#).

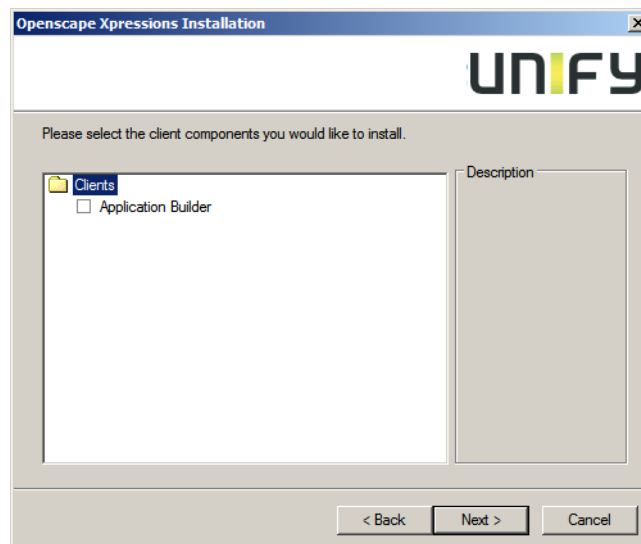
C.5.5 Install the OpenScape Xpressions Software

Up comes this dialog:



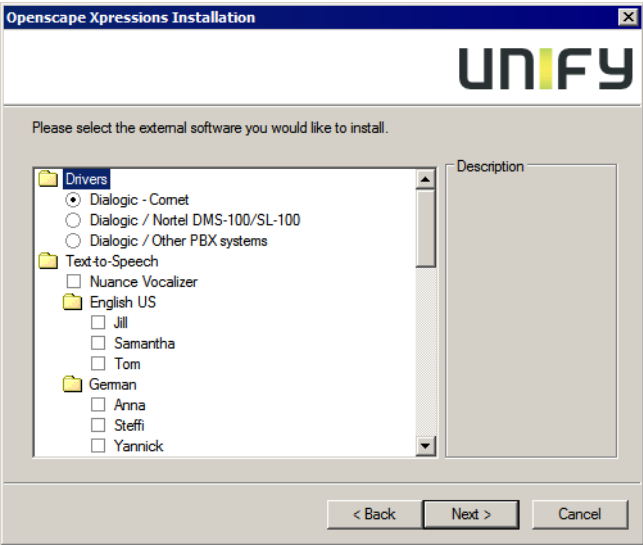
1. Select the **XPR server**. Then click on **Next**.

Up comes this dialog:

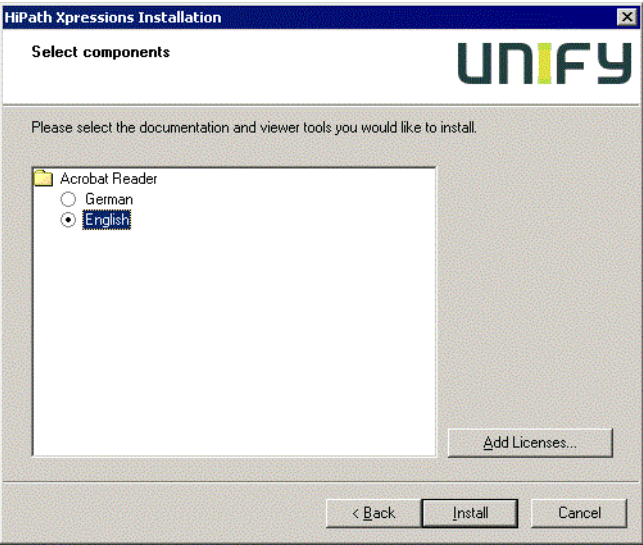


2. Click on **Next**. Up comes this dialog:

Configuring OpenScape Xpressions as Voice-only System
BRI/PRI/Eicon HiPath 3000/CorNet-N Installation

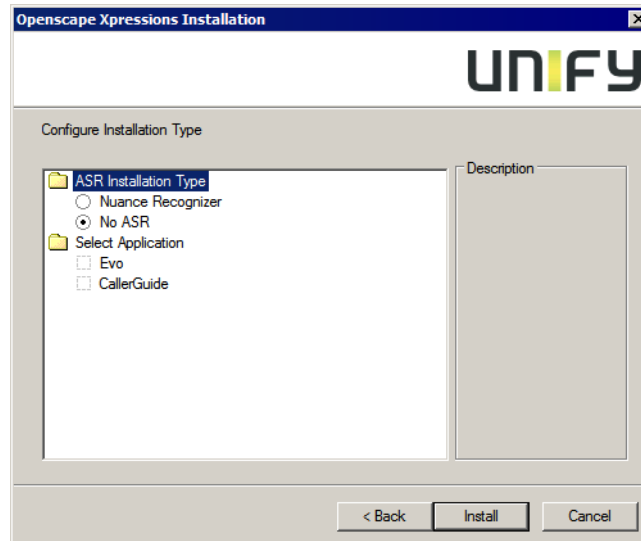


3. Select **Dialogic - Cornet**. Then click on **Next**. Up comes this dialog:



4. If you want to install the Acrobat Reader, select a language and click on **Install**. Otherwise click only on **Install** without making a selection.

If the customer has purchased an ASR license, the **Next** button appears instead of **Install**. When you click on **Next**, the following dialog opens:



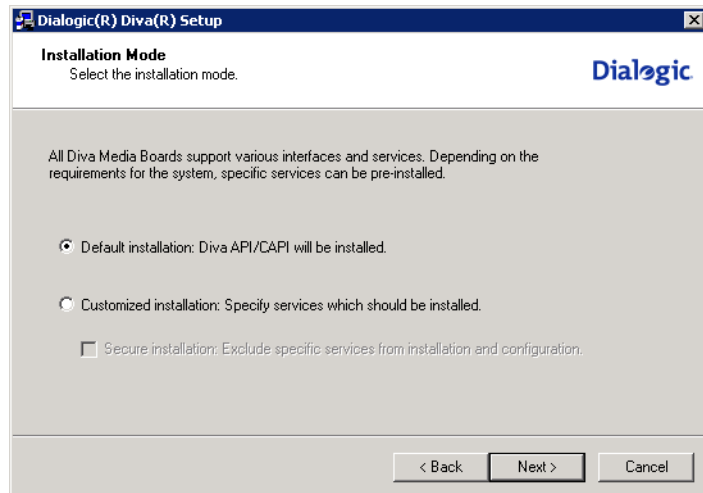
Select the ASR setup type and ASR applications. For further information please refer to [Section 4.3.11, "Installation Type for Automatic Speech Recognition"](#), on page 85. Then click **Install**.

C.5.6 Install the Dialogic DIVA Driver

1. The setup program starts with the following welcome dialog.

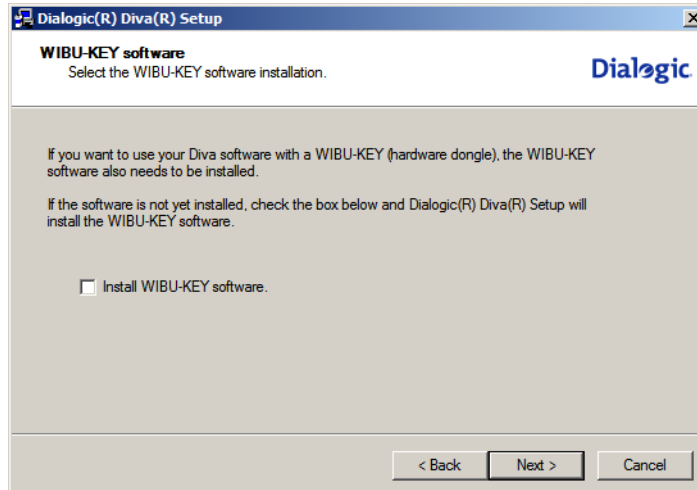


2. Click on **Next**. Up comes this dialog:



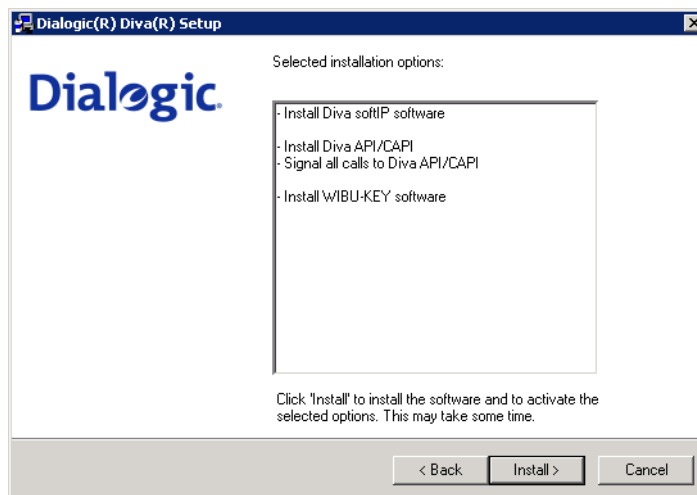
3. Select the option **Default installation: Diva API / CAPI will be installed.** Then click on **Next**.

Up comes this dialog:

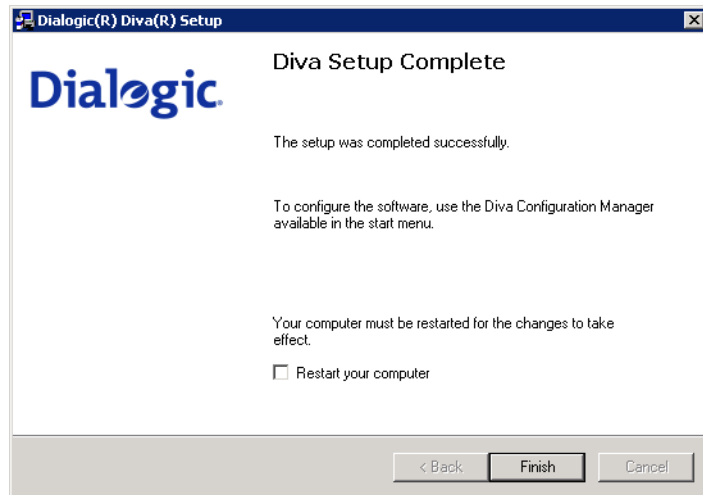


4. If you use WIBU-KEY, select the option **Install WIBU-Key software.** Then click on **Next**.

Up comes this dialog:

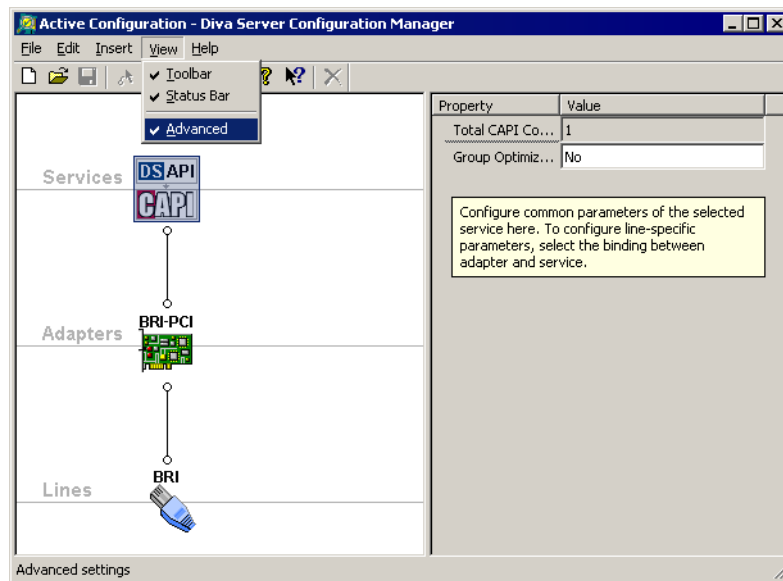


5. Check the selected the installation options. Then click on **Next**.
Up comes this dialog:

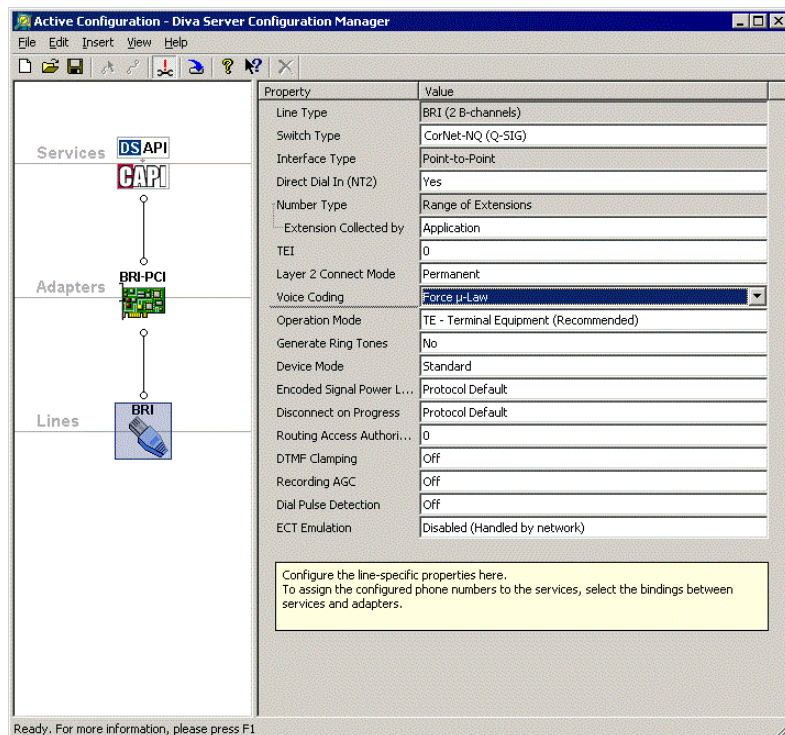


6. Deselect the **Restart your computer** option. Finally, click **Finish**.

The Eicon driver configuration program starts and the following dialog opens:



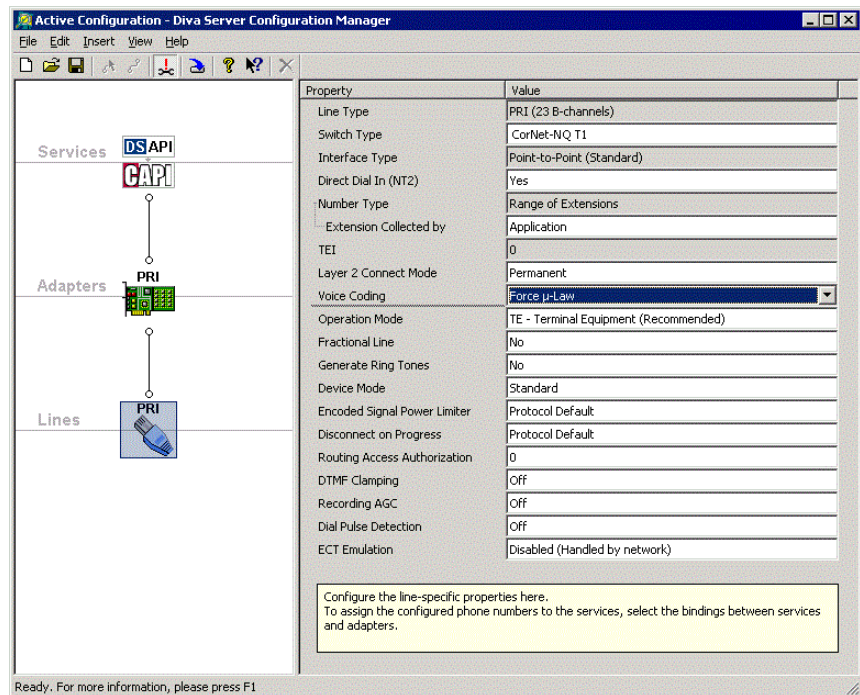
7. Open the **View** menu option and select the **Advanced** option.
8. **For a BRI interface** select a BRI icon and make the following settings in the fields of the dialog's right hand portion:
 - a) Click on the **Switch Type** field and select **CorNet-N (ETSI-DSS1)**.
 - b) Click on the **Interface Type** field and select **Point-to-Point**.
 - c) Click on the **Direct Dial In** field and select **Yes**
 - d) Click on the **Number Type** field and select **Range of Extensions**.
 - e) Click on the **Extension Collected by** field and select **Application**.
 - f) Click on the **Layer 2 Connect Mode** field and select **Permanent**.
 - g) Click on the **Voice Coding** field and select **Force a-Law (USA: μ -Law)**.
 - h) Repeat the steps **a** to **g** for each available BRI line.
 - i) Continue with step **10** on [page 293](#).



Configuring OpenScape Xpressions as Voice-only System

BRI/PRI/Eicon HiPath 3000/CorNet-N Installation

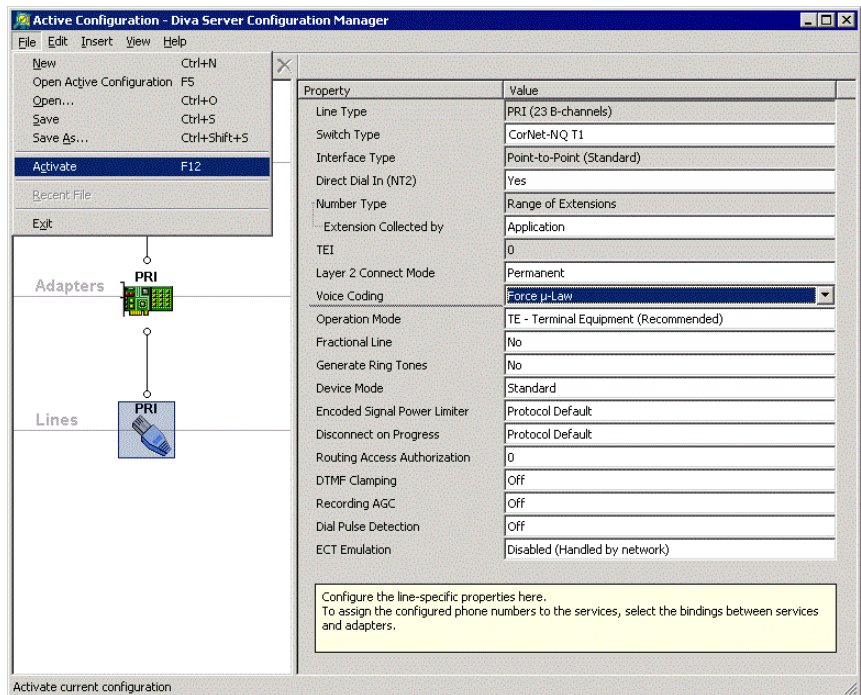
9. **For a PRI interface** select a PRI icon and make the following settings in the fields of the dialog's right hand portion:
 - a) Click on the **Switch Type** field and select **CorNet-N T1**.
 - b) Click on the **Interface Type** field and select **Point-to-Point**.
 - c) Click on the **Direct Dial In** field and select **Yes**
 - d) Click on the **Number Type** field and select **Range of Extensions**.
 - e) Click on the **Extension Collected by** field and select **Application**.
 - f) Click on the **Layer 2 Connect Mode** field and select **Permanent**.
 - g) Click on the **Voice Coding** field and select **Force a-Law** (USA: μ -Law).
 - h) continue to [10 on page 293](#).



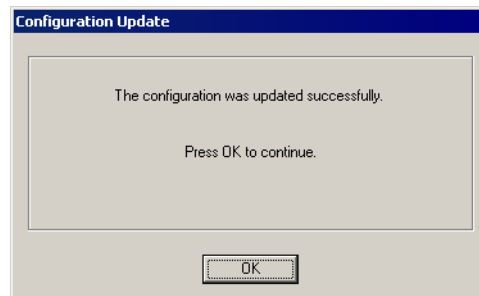
Configuring OpenScape Xpressions as Voice-only System

BRI/PRI/Eicon HiPath 3000/CorNet-N Installation

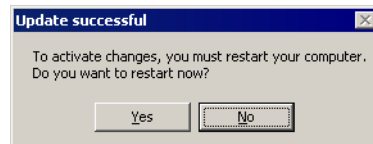
10. Open the **File** menu option and select the **Activate** option. This update may take several minutes.



11. After you settings have been successfully copied, the following dialog opens:

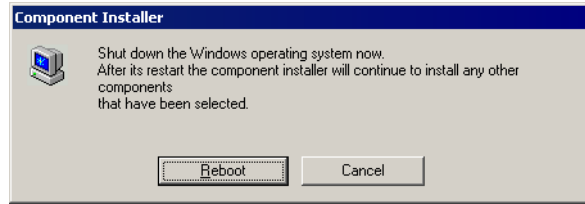


12. Click **OK**. Up comes this dialog:



13. Click on **No**. **DO NOT REBOOT**.

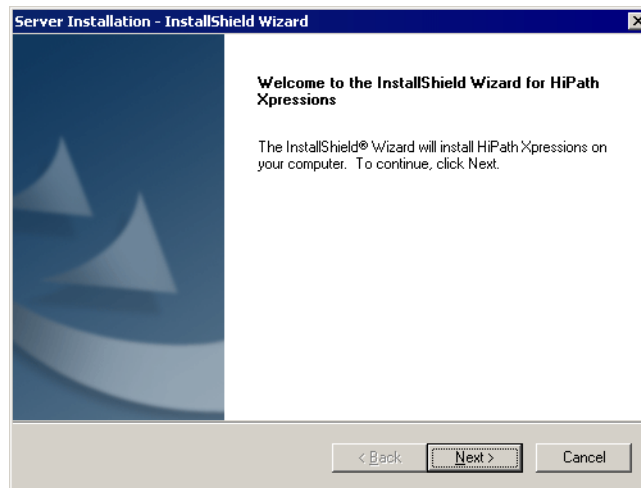
14. Close the **Active Configuration** window. Up comes this dialog:



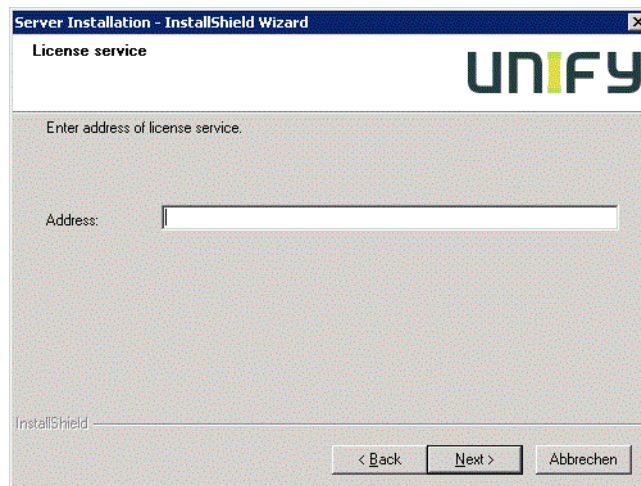
15. Now click **Reboot** to restart the system.

C.5.7 Install the Xpressions Components

1. After rebooting, log on to the server computer with an administrator account. The setup is continued and the following dialog opens:



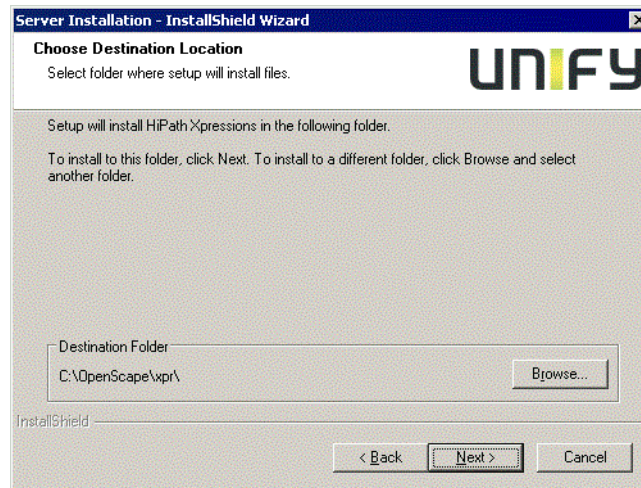
2. Click on **Next**. Up comes this dialog:



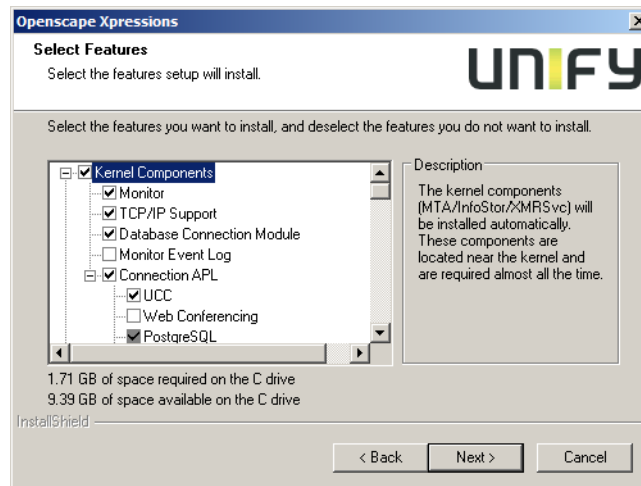
3. Enter the IP address of the computer on which the CLA runs. Then click on **Next**. Up comes this dialog:

Configuring OpenScape Xpressions as Voice-only System

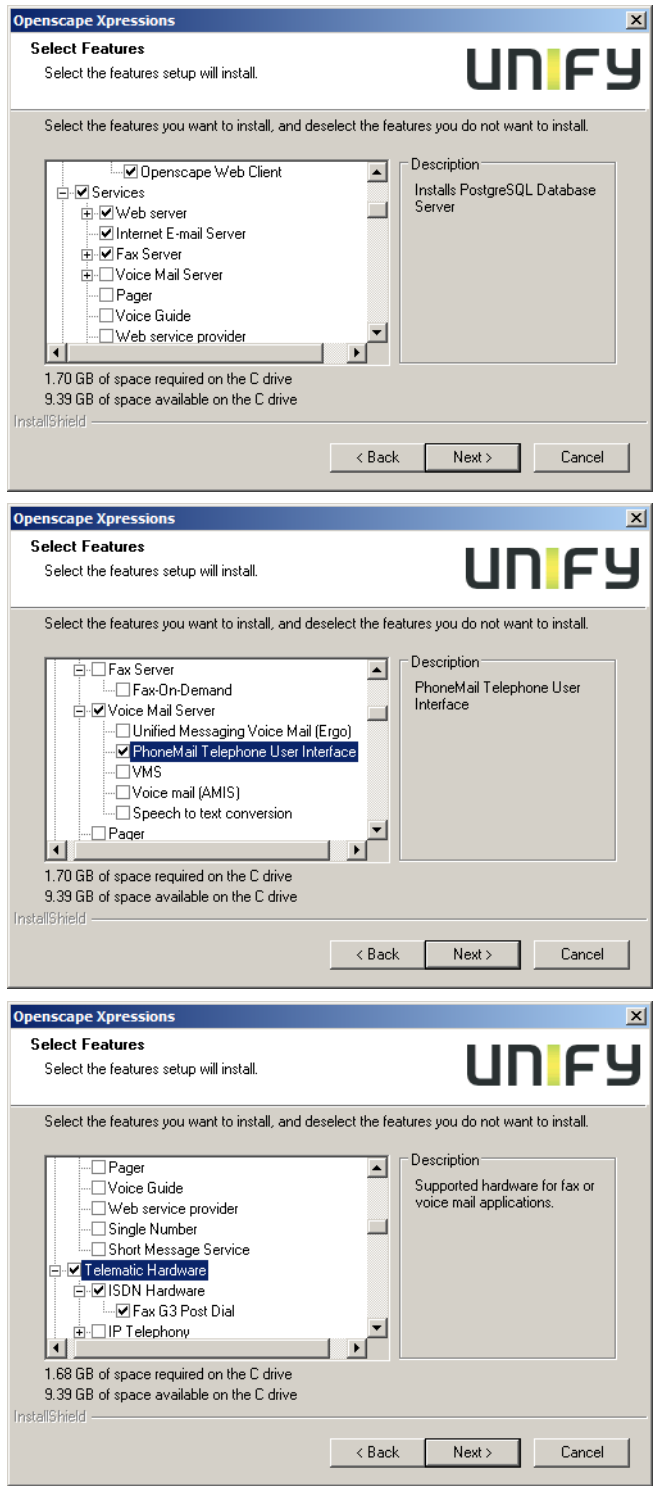
BRI/PRI/Eicon HiPath 3000/CorNet-N Installation



4. Check whether the defaulted setup target folder is on the largest available partition. If this is the case, click on **Next**. Otherwise use the **Browse...** button to select another target folder situated on the largest available partition. Check the customer's order (see [5 on page 243](#)) and select the components associated to the ordered options in this dialog (cf. the selected entries in following figures).

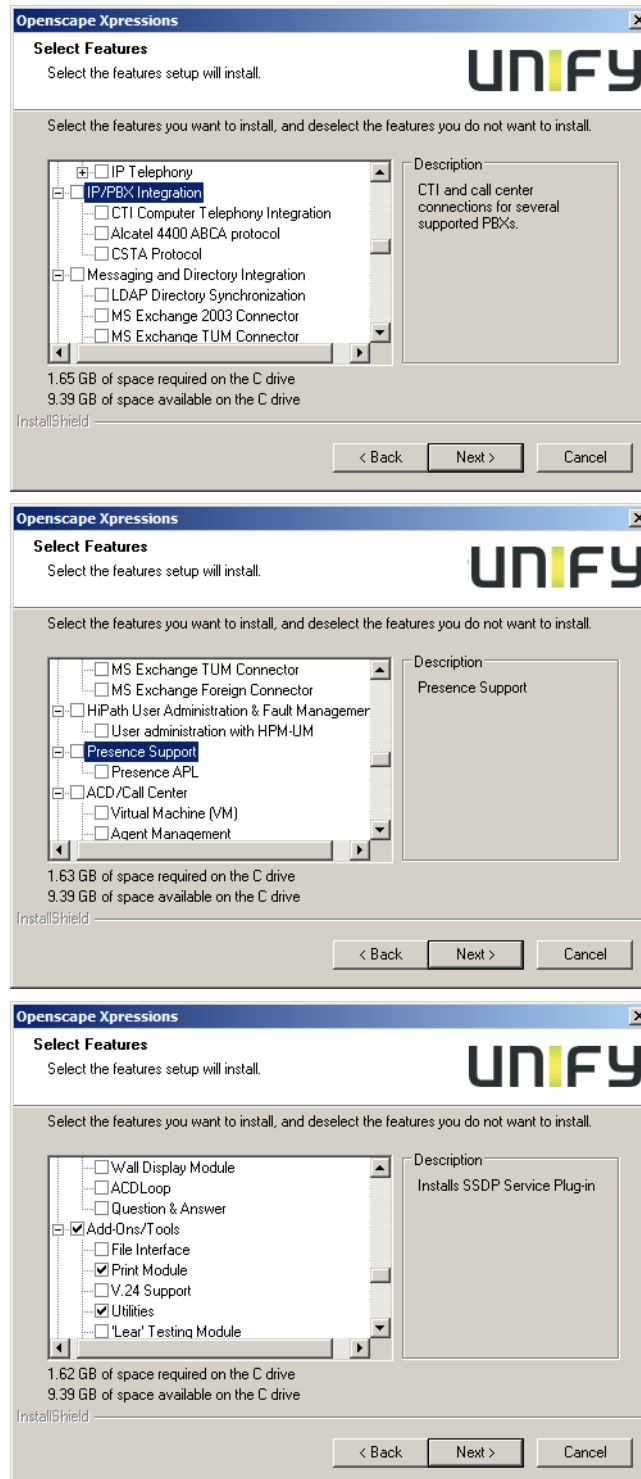


Configuring OpenScope Xpressions as Voice-only System
BRI/PRI/Eicon HiPath 3000/CorNet-N Installation

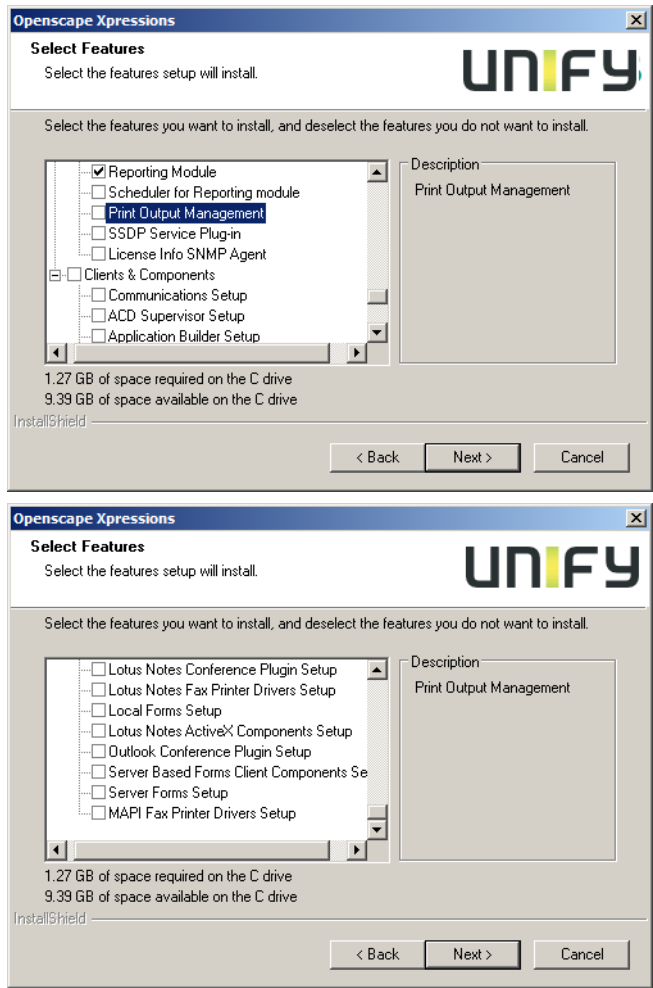


Configuring OpenScope Xpressions as Voice-only System

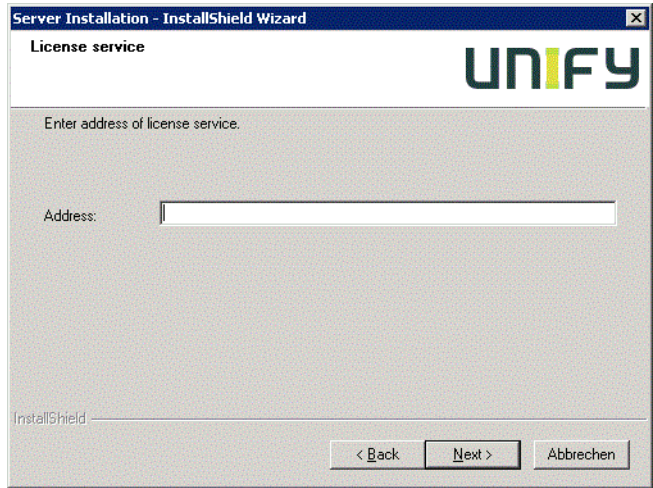
BRI/PRI/Eicon HiPath 3000/CorNet-N Installation



Configuring OpenScape Xpressions as Voice-only System
BRI/PRI/Eicon HiPath 3000/CorNet-N Installation



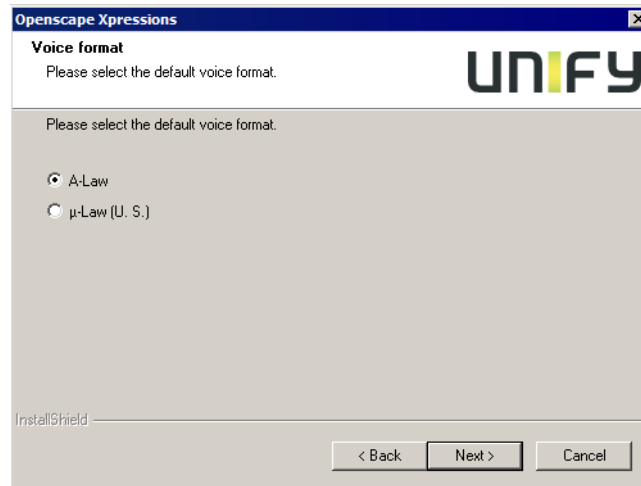
After selecting all licensed features, click on **Next**. Up comes this dialog:



5. Click on **Next**.

NOTE: If desired, you may change the location of one of the folders to another drive. Make sure to use the largest available partition.

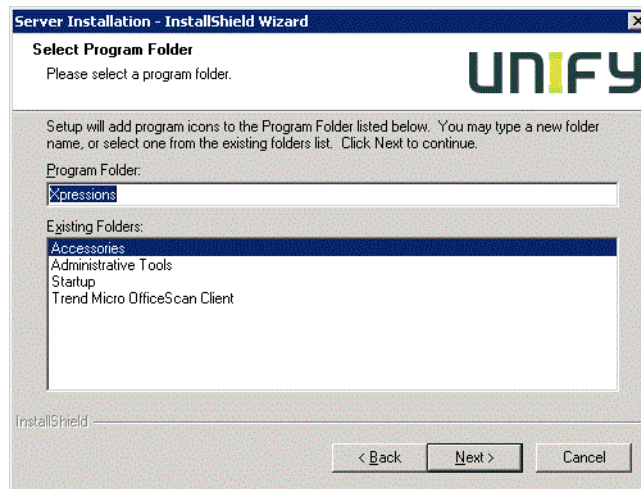
Up comes this dialog:



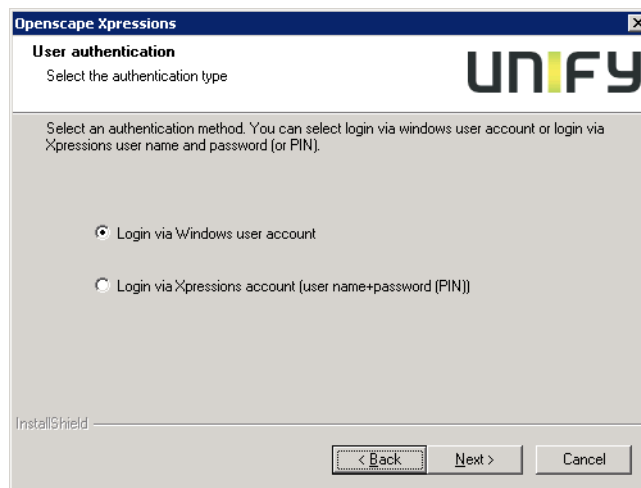
Configuring OpenScope Xpressions as Voice-only System

BRI/PRI/Eicon HiPath 3000/CorNet-N Installation

6. Select a default voice format. If you are in the U.S., select **µ-Law**. If you are in another country, select **A-Law**. Then click on **Next**. Up comes this dialog:



7. Click on **Next** to copy the program folder. Up comes this dialog:



8. Select the authentication type:

Login via the Windows User Account

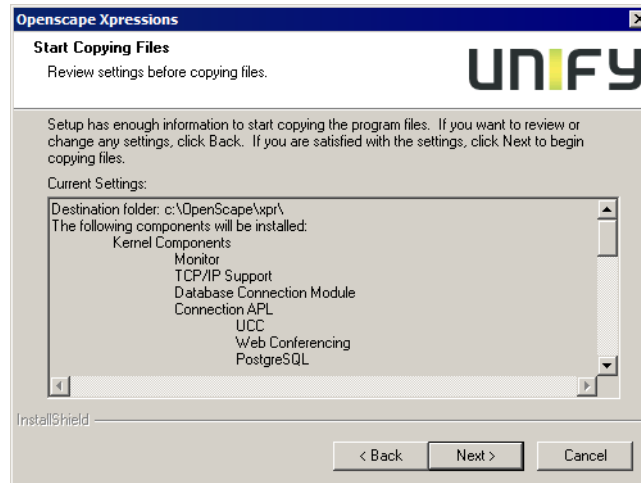
This is the standard method. If this method is applied, the user's Windows account is used for authentication against the XPR server. All password-specific functions in the XPR server are deactivated. After you have selected this option, the next installation step is to choose the Windows accounts to serve as XPR administrator or XPR postmaster (cf. [Section 4.5.6.1, "Login via the Windows User Account"](#), on page 106).

Login via XPR account (user name + password (PIN))

With this authentication method, user accounts for the XPR administrator and the XPR postmaster are created in the XPR database. It is still possible though to activate the authentication via the Windows user account for some

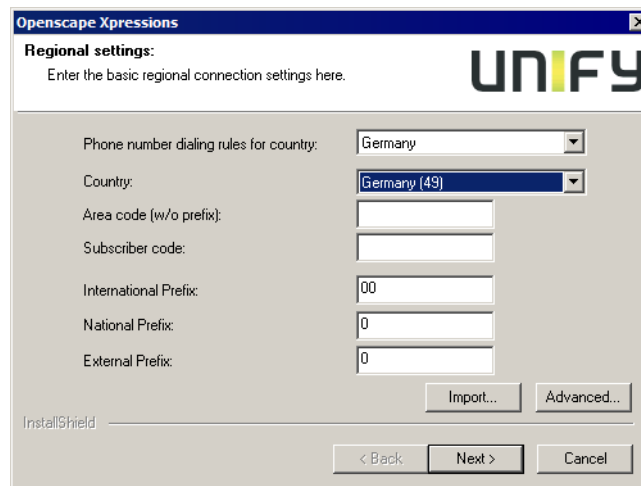
users in hindsight. In the next installation step you need to specify a name and password for the administrator and the postmaster of the XPR server each (cf. [Section 4.5.6.2, “Login via XPR Account”, on page 107](#)).

Then click on **Next**. Up comes this dialog:



9. Check the listed options and click on **Next**. The copying process begins. A status dialog informs you about the installation progress.

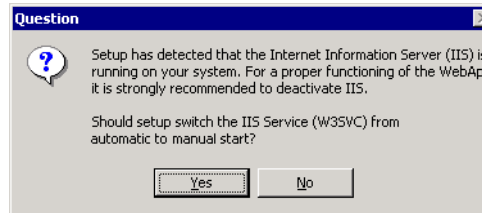
Up comes this dialog:



10. In the **Phone number dialing rules for country** field select the country in which the system is to be set up.
11. Enter the area code (without prefix) and the subscriber number. Then click on **Next**.
12. If the Internet E-mail server has been selected as option and the Windows Internet Information Server (IIS) has been installed and activated on the computer, the following dialog appears:

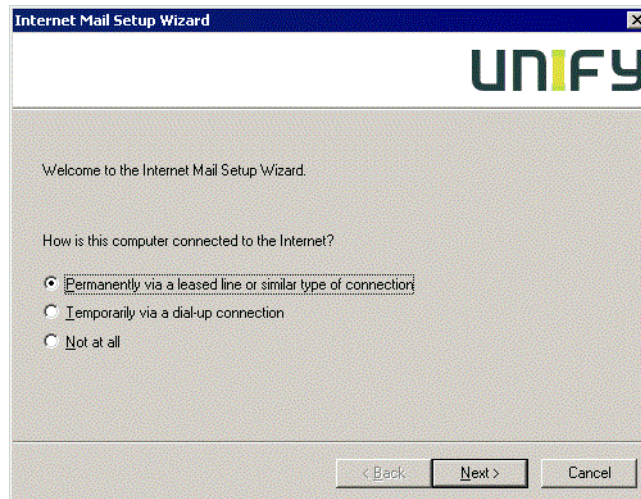
Configuring OpenScape Xpressions as Voice-only System

BRI/PRI/Eicon HiPath 3000/CorNet-N Installation

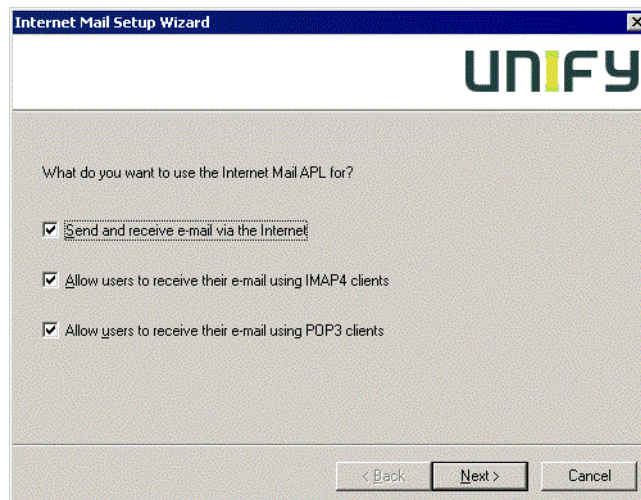


Confirm this dialog with **Yes**.

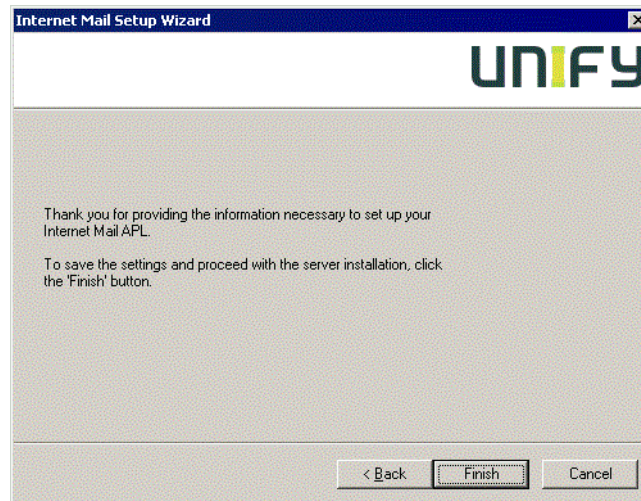
If the Internet Information Server has not been installed on the computer, the following dialog appears:



- a) Select the **Permanently via a leased line or similar type of connection** option, then click on **Next**. Up comes this dialog:

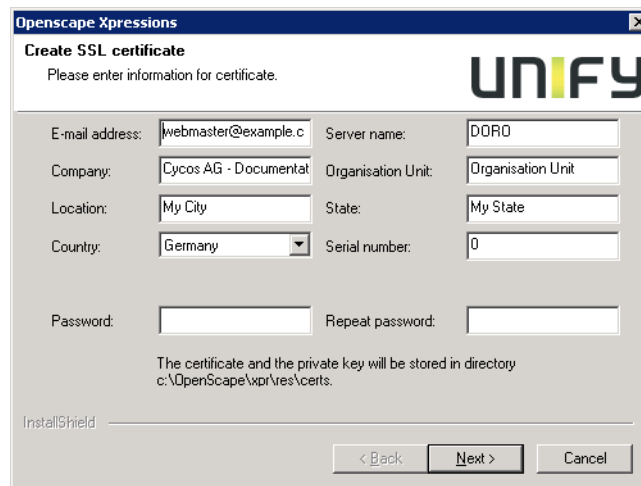


- b) Verify that **all options are selected** and click on **Next**. Up comes this dialog:



c) Click **Finish**. Up comes this dialog:

13. The SMTP APL setup is completed. Up comes this dialog:



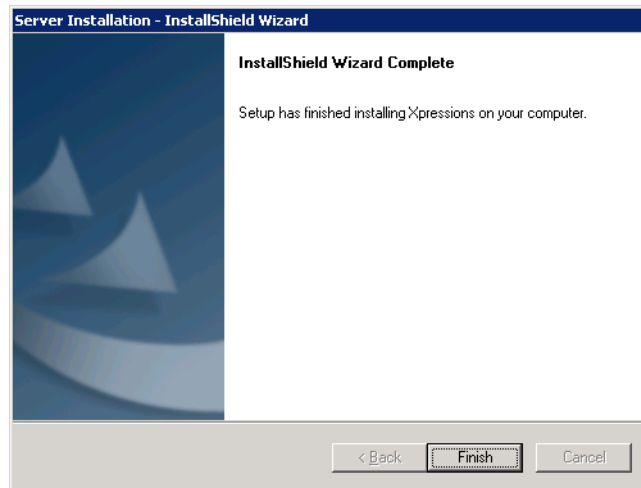
14. In the dialog's fields make the specifications that are to become elements of the certificate. In the **Password** field enter a sufficiently complex password and repeat this specification in the **Repeat password:**. Then click on **Next**.

IMPORTANT: 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.

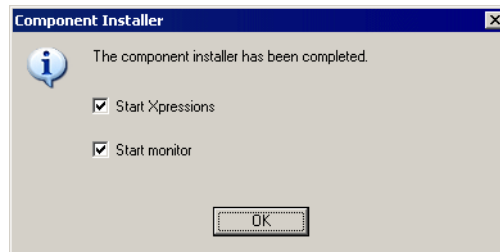
Up comes this dialog:

Configuring OpenScape Xpressions as Voice-only System

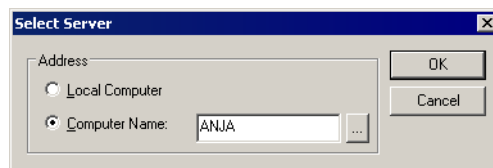
BRI/PRI/Eicon HiPath 3000/CorNet-N Installation



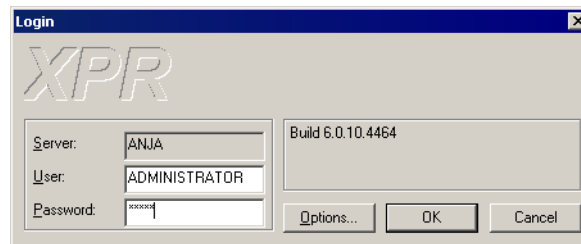
15. Click **Finish**. You may have to click **Finish** several times depending on the selected options. The server setup is thus complete.
16. The selected language packets and other components will now be installed. These installations occur automatically, so that you need not make any entries. As soon as all installations are complete, the following dialog appears:



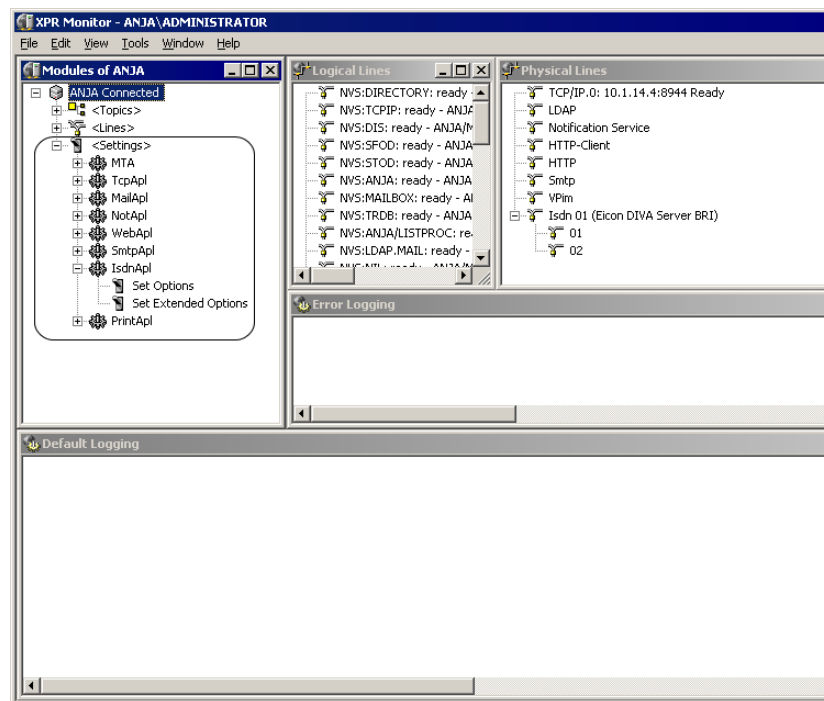
17. Select the options **Start HiPath Xpressions** and **Start monitor** and click on **OK**. Up comes this dialog:



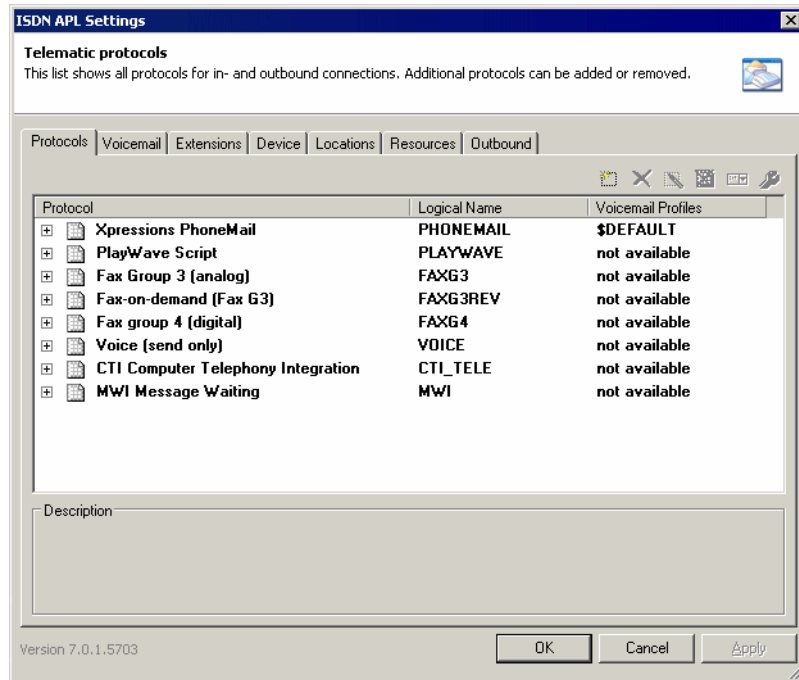
18. Enter or browse the Xpressions server name, then click **OK**. The monitor login dialog opens:



19. Log on to the Xpressions monitor as **Administrator**, then click on **OK**. The monitor opens:

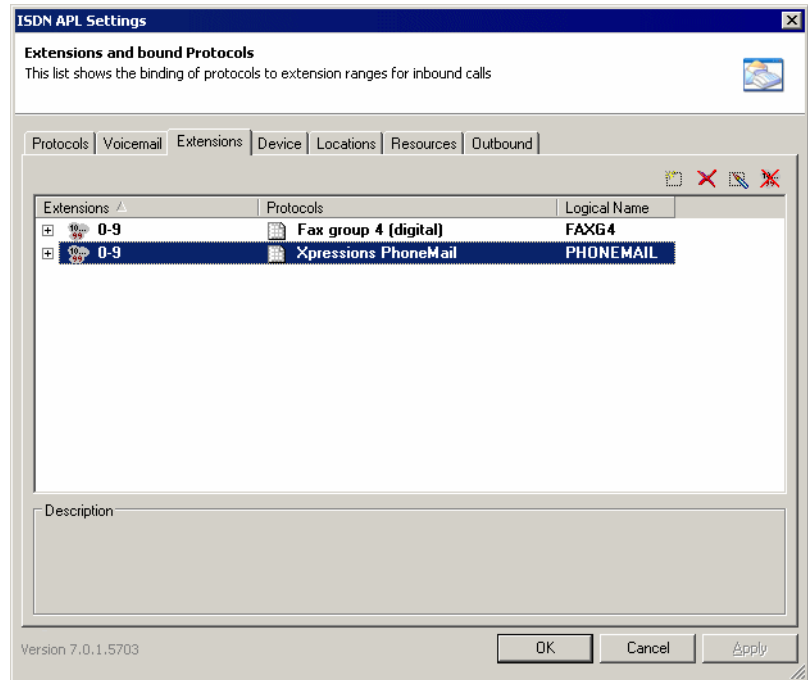


20. In the **Modules of <Xpressions Server>** window under **<Settings>** expand the **IsdnApl** entry and doubleclick **Set Extended Options**. Up comes this dialog:

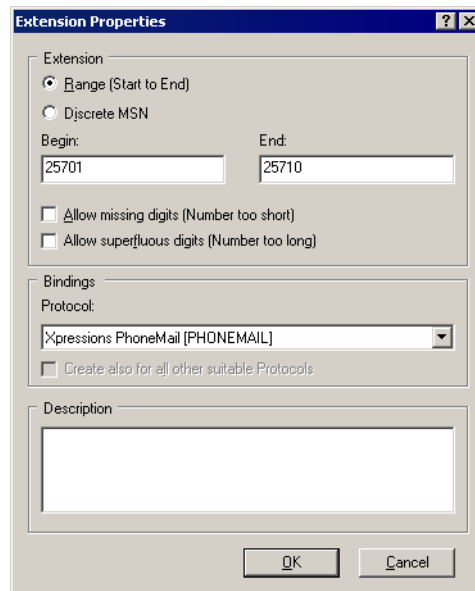


21. Check whether the **Protocols** tab shows all protocols displayed above. Verify that the *CTI_TELE*, *MWI*, *PHONEMAIL*, *PLAYWAVE*, and *VOICE* protocols are displayed at any rate.

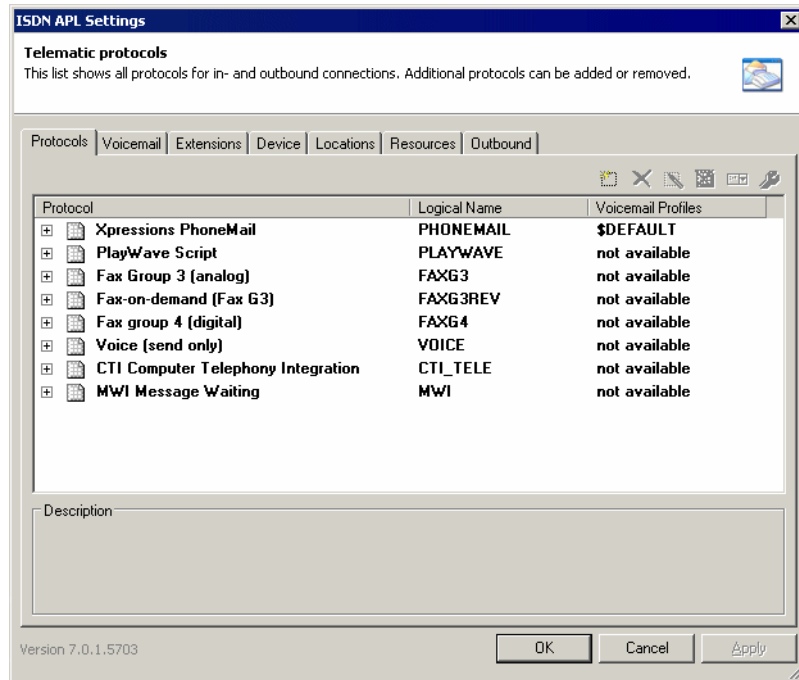
22. Switch to the **Extensions** tab, then double-click **Xpressions PhoneMail**.



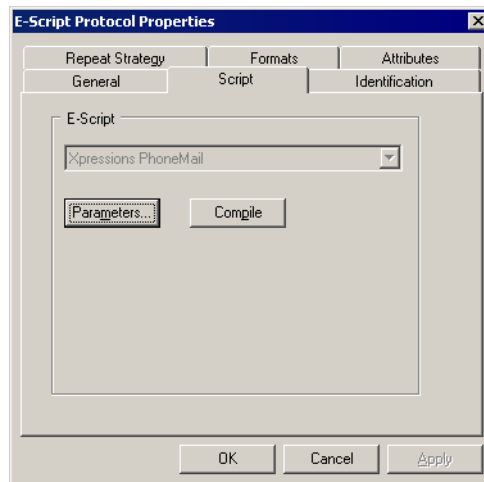
Up comes this dialog:



23. In the **Extensions** field enter the first and last digit only for the ACCESS NUMBERS, then click on **OK**. The dialog closes and you return to the following dialog:



24. Open the **Protocols** tab and doubleclick the **Xpressions PhoneMail** entry. Up comes this dialog:



25. Open the **Script** tab and click on the **Parameters** button. Up comes this dialog:

The dialog box is titled "Xpressions PhoneMail" and has tabs for General, Options, Settings, Addressing, and Customer. The "General" tab is selected. Under the "Service Access Numbers" section, there are six input fields with the following labels and values:

Label	Value
Direct Access:	25701
Guest/Forward Access:	25702
Callback Access:	25703
Fax Access:	25704
Transfer Access:	25705
Universal Access:	25706

At the bottom of the dialog are buttons for OK, Cancel, and Apply.

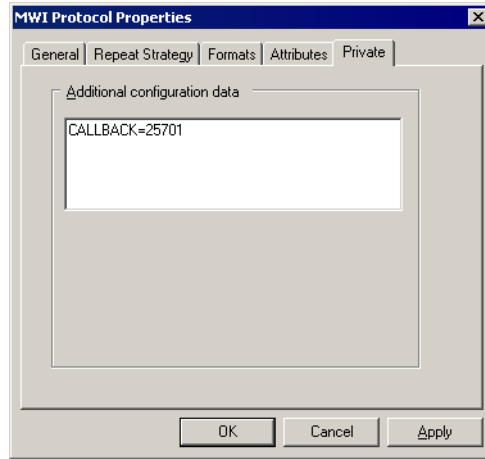
26. Enter the **Service Access Numbers** and click on **OK**.
27. Click on **OK** again to close the **E-Script Protocol Properties** window. You return to the following dialog:

The dialog box is titled "ISDN APL Settings" and has tabs for Protocols, Voicemail, Extensions, Device, Locations, Resources, and Outbound. The "Protocols" tab is selected. It displays a list of telematic protocols with their logical names and voicemail profiles.

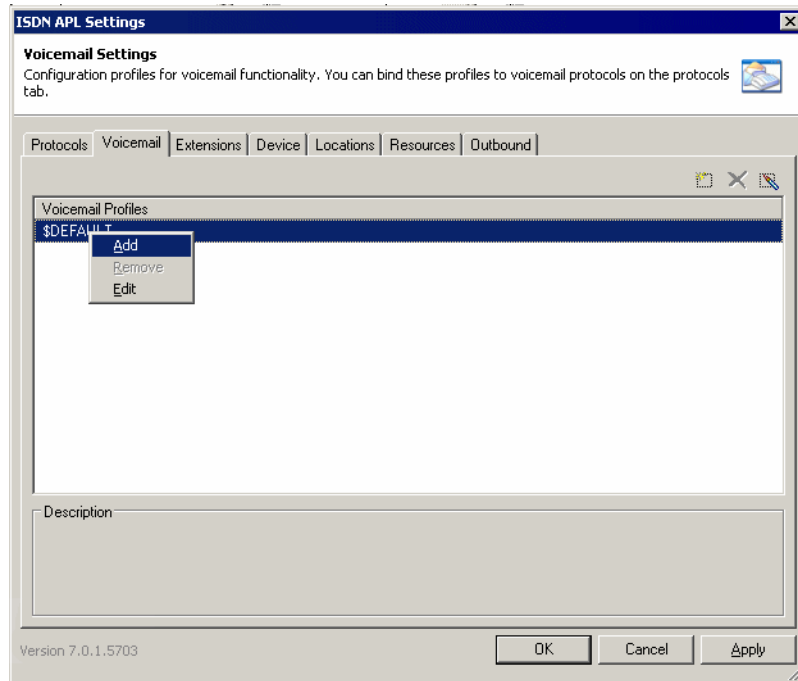
Protocol	Logical Name	Voicemail Profiles
Xpressions PhoneMail	PHONEMAIL	\$DEFAULT
PlayWave Script	PLAYWAVE	not available
Fax Group 3 (analog)	FAXG3	not available
Fax-on-demand (Fax G3)	FAXG3REV	not available
Fax group 4 (digital)	FAXG4	not available
Voice (send only)	VOICE	not available
CTI Computer Telephony Integration	CTI_TELE	not available
MWI Message Waiting	MWI	not available

Below the table is a "Description" field. At the bottom of the dialog are buttons for OK, Cancel, and Apply, and the version number "Version 7.0.1.5703" is displayed.

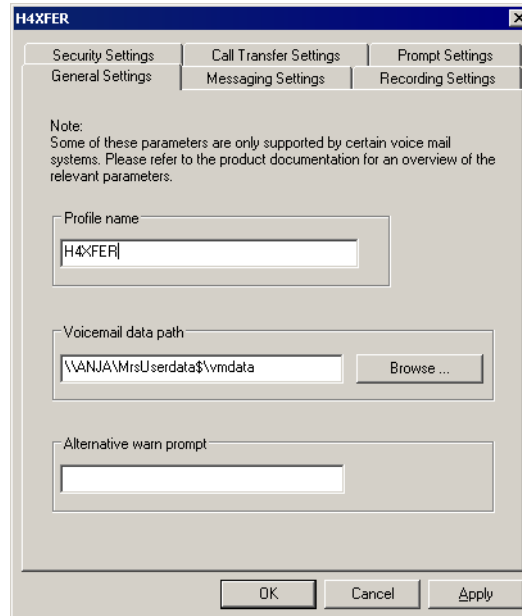
28. Open the **Protocols** tab and doubleclick the **MWI** entry. Up comes this dialog:



29. Open the **Private** tab, enter the PBX callback number and click on **OK**. Up comes this dialog:

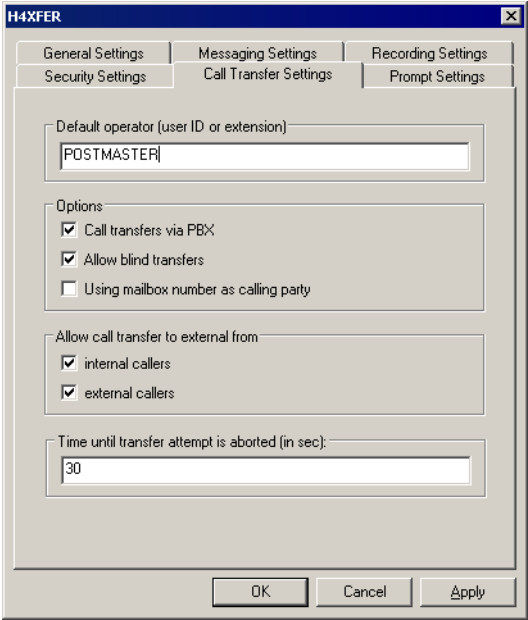


30. Open the **Voicemail** tab, click with the right mousebutton on the **\$DEFAULT** entry and select **Add** in the context menu. Up comes this dialog:

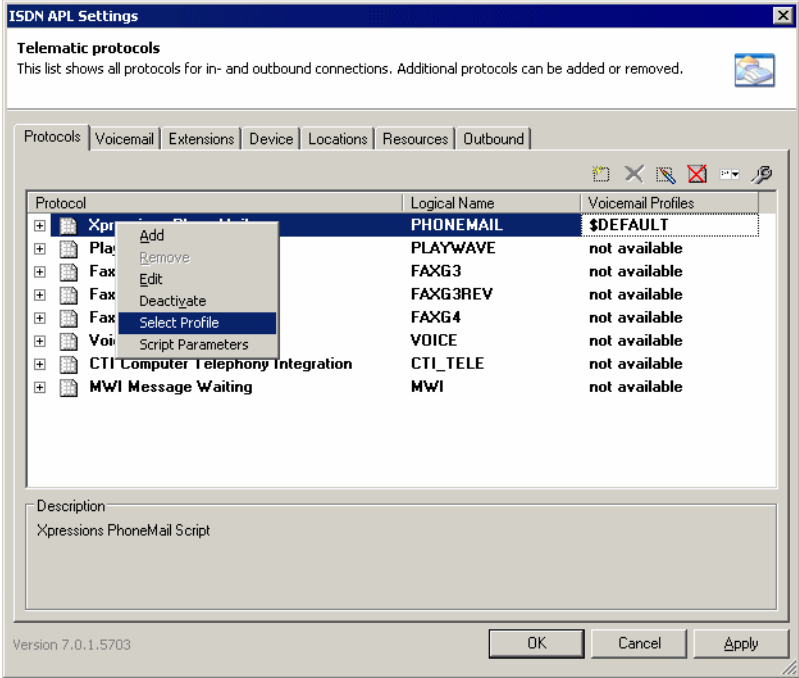


31. Open the **General Settings** tab and enter *H4XFER* in the **Profile name** field.
32. Open the **Call Transfer Settings** tab and,
33. If it does not already exist, enter the user ID or the extension of the **default operator**.

34. Select the **Allow blind transfers** option.
35. Verify that the **internal callers** and **external callers** options in the **Allow call transfer to external from** section are active.



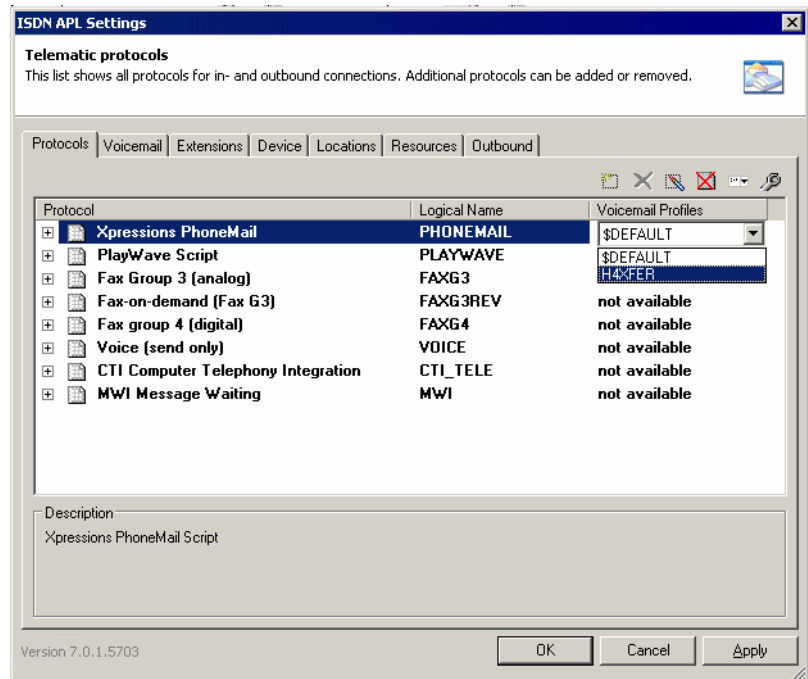
36. Click on **OK** to close the profile configuration. You return to the following dialog:



37. Open the **Protocols** tab, click with the right mousebutton on the **Xpressions PhoneMail** entry and select **Select Profile** in the context menu.

Configuring OpenScape Xpressions as Voice-only System

BRI/PRI/Eicon HiPath 3000/CorNet-N Installation



38. Open the **Voicemail Profiles** pull-down menu and select **H4XFER**.
39. Click on **OK** to close the **ISDN APL Settings** window.
40. Proceed to [Section C.8, "System Test and Troubleshooting"](#).

C.6 Hicom 300H/CorNet-T Installation

This section describes the installation of a BRI interface with Dialogic DIVA server board(s) using the CorNet-T protocol at a Hicom 300H PBX.

Interface	PBX	Line Card/ Resource Card	PBX Card	Protocol	Max. no. of boards per server	Max. no of channels per session
BRI Connectivity						
S ₀ /BRI	Hicom 300H	Dialogic DIVA 4BRI	SLMS	CorNet-T	5	40

IMPORTANT: If more than three Eicon-4BRI boards are used in combination with CorNet-T, **the connection can be bad in case of call forwardings**. As workaround a new key of type REG_MULTI_SZ must be defined under the name Private and set to value TransferViaDeflect=1 for each device (one 4BRI module provides 4 devices) in the registry database under

HKLM\SOFTWARE\PP-COM\MRS\IsdnApl\Devices\XX
(with XX representing the devices).

C.6.1 Pre-installation Checklist

1. Perform the checklist as specified in [Section C.3.3, “Performing the Checklist”](#), on page 243 and have info ready.
2. Make sure to use Eicon drivers starting from version 7.6.3.

C.6.2 Activate the License

Read [Chapter 3, “Generating Licenses”](#) about licensing. Then make sure that

- a CLM and a CLA is available in the network
- you have the required licenses as XML file (cf. [Section 3.1, “Licensing Routine”](#), on page 38 and [Section 3.5, “Generating a License Key”](#), on page 41).

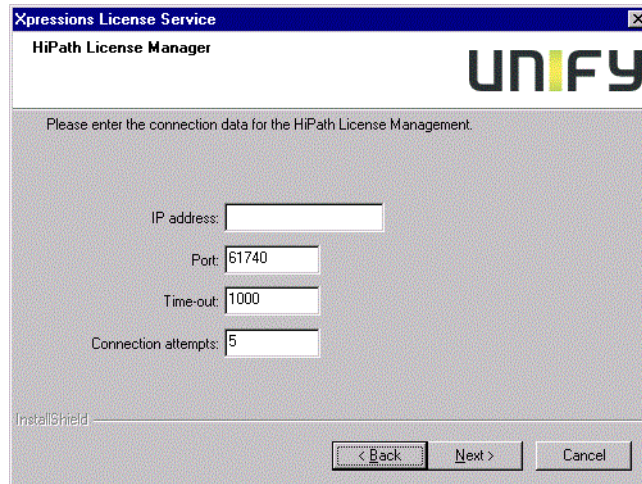
After you have obtained the license as XML file, import it into the CLM and transfer the license to the CLA that OpenScape Xpressions is to connect. Please refer to [Section 3.7, “Activating Licenses in the CLA”](#), on page 44.

If you need to obtain the license via the CLA, please read section 5 in the CLM online help. To open the help, click on the **Help** button in the CLM interface.

After successfully activating the license continue with [Section C.6.5, “Install the OpenScape Xpressions Software”](#), on page 320.

C.6.3 Install the License Service

1. Connect the XPR installation medium to the computer.
2. The license service installation starts. In the next dialogs click on **Next** until the following dialog opens:



3. In this dialog enter the IP address of the computer on which the CLA runs. Then click on **Next**.
4. In the following dialog click **Install**.
5. In the following dialog click **Finish**. The license service installation is thus complete.

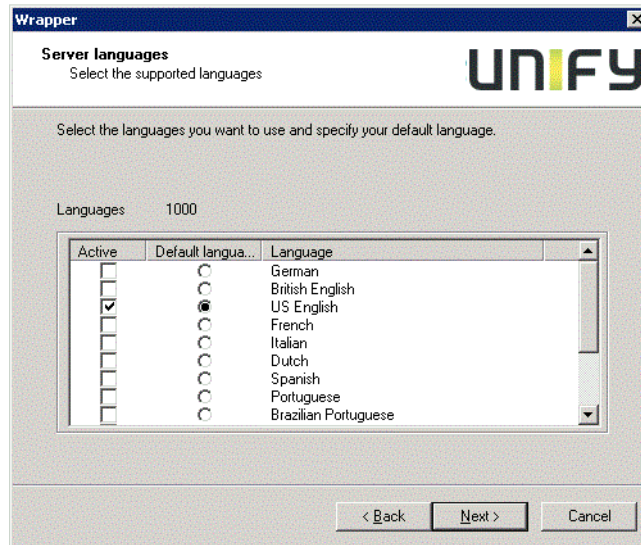
C.6.4 Server Name, Languages and Release Notes

1. After the license service installation, the following dialog opens:

2. Enter the server name and then click on **Next**. When you select the server name, heed the following points:
 - the name you enter here **cannot be modified any more**
 - the name must not contain blanks, special characters such as ;, !, %, &, ... , or German umlauts (ä, ö, ü).
 - you must not use names of logical XPR lines. For example: *PhoneMail*, *VMS*, *COM*, *CON*, *FAXG3*, *FAXG4*, *MWI*, *FOD*, *PlayWave* and *SMTP* will not be accepted.
 - If you want to connect the XPR server to another XPR server via a Remote System Link, the server name selected here must not exceed a length of 11 characters.

NOTE: Remote System Link is not compatible with [Crypt_Sec], it is designed to only work with [KRYPT].

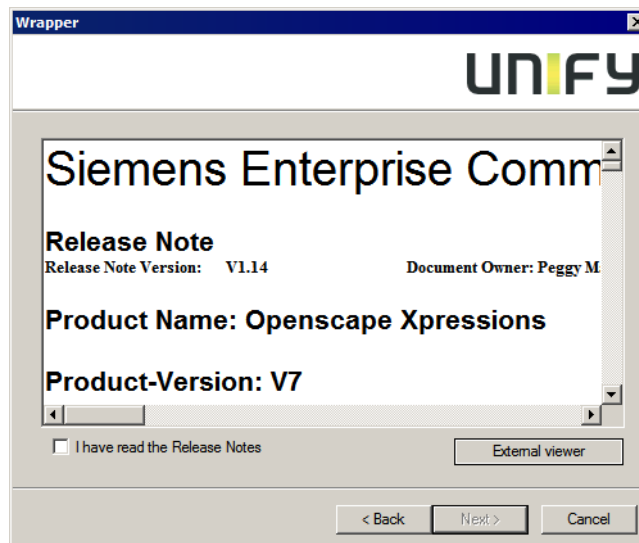
Up comes this dialog:



3. In the **Active** column select the languages to be installed. Only select as many languages as licenses are available.

NOTE: You need to select at least one language, otherwise you cannot continue the installation.

4. In the **Default language** column select the language that the XPR server is to use as default. You can specify only one language as default language.
5. Click the **Continue** button. Up comes this dialog:



This dialog represents the `ReleaseNotes.rtf` file, which is found in the `XpressionsInstall` directory of the setup medium.

6. Please read the Release Notes. Via the **Open in external viewer** button you can open the corresponding file in the application that is registered in the operating system for the file type *RTF*.

7. Select the **I have read the Release Notes** check box. This activates the **Next** button.

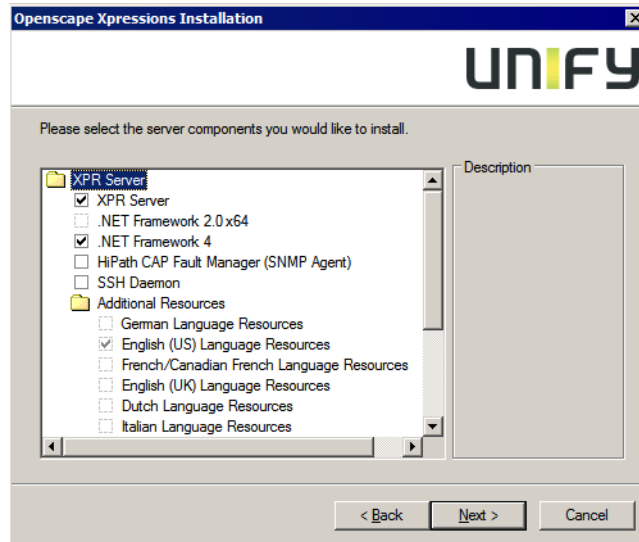
If you do not select the check box, the **Next** button stays inactive and you cannot continue the installation.

8. After you have read the Release Notes, click on **Next**.

The dialog for selecting the server components opens. Please continue reading in [Section C.6.5, “Install the OpenScape Xpressions Software”](#), on [page 320](#).

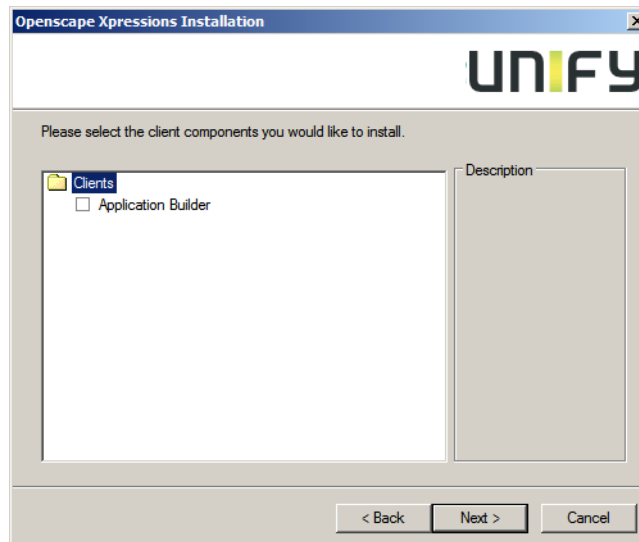
C.6.5 Install the OpenScape Xpressions Software

Up comes this dialog:

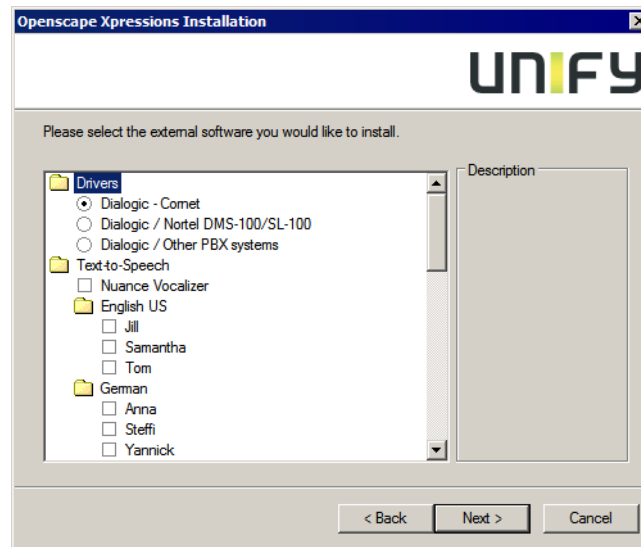


1. Select the **XPR server**. Then click on **Next**.

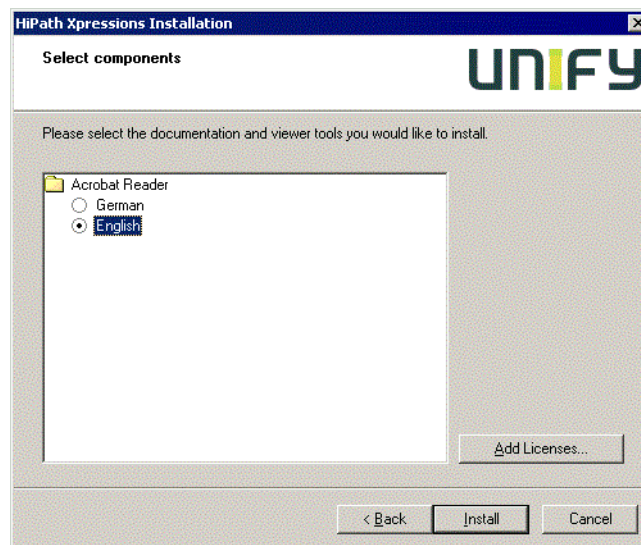
Up comes this dialog:



2. Then click on **Next**. Up comes this dialog:



3. Select **Dialogic - Cornet**. Then click on **Next**. Up comes this dialog:

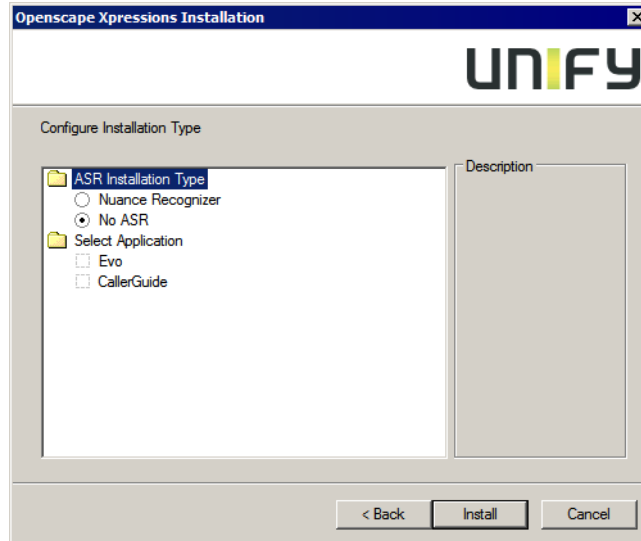


Configuring OpenScape Xpressions as Voice-only System

Hicom 300H/CorNet-T Installation

4. If you want to install the Acrobat Reader, select a language and click on **Install**. Otherwise click only on **Install** without making a selection.

If the customer has purchased an ASR license, the **Next** button appears instead of **Install**. When you click on **Next**, the following dialog opens:



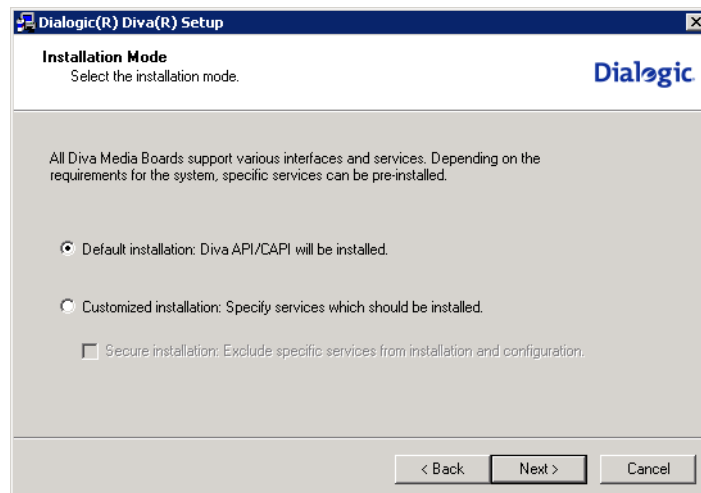
Select the ASR setup type and ASR applications. For further information please refer to [Section 4.3.11, "Installation Type for Automatic Speech Recognition"](#), on page 85. Then click **Install**.

C.6.6 Install the Dialogic DIVA Driver

1. Up comes this dialog:

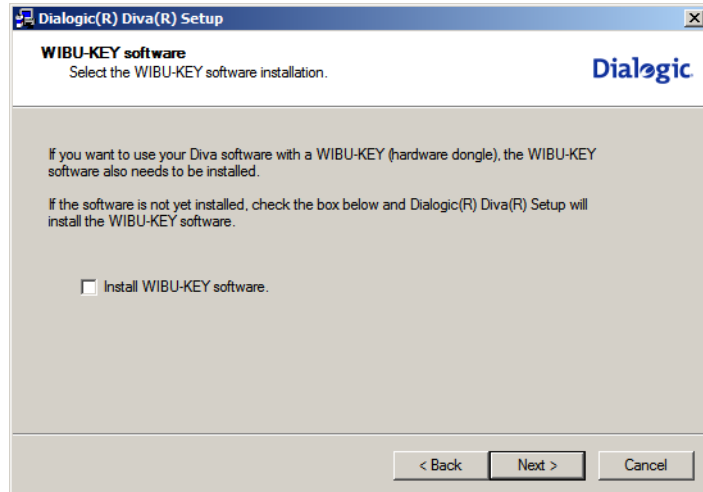


2. Click on **Next**. Up comes this dialog:



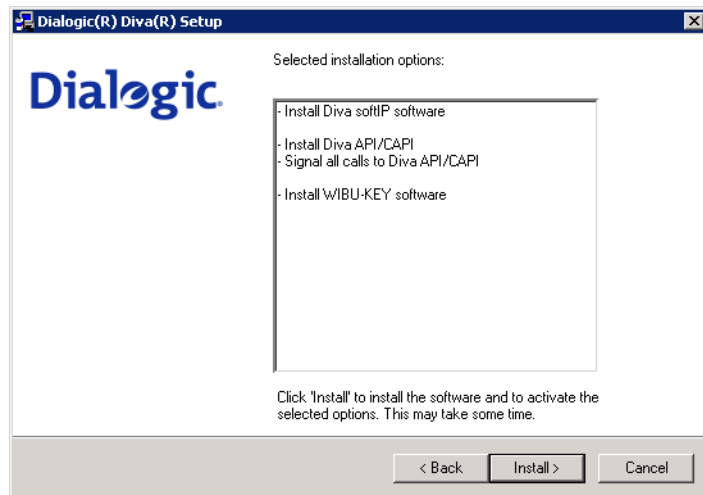
3. Select the option **Default installation: Diva API / CAPI will be installed.** Then click on **Next**.

Up comes this dialog:



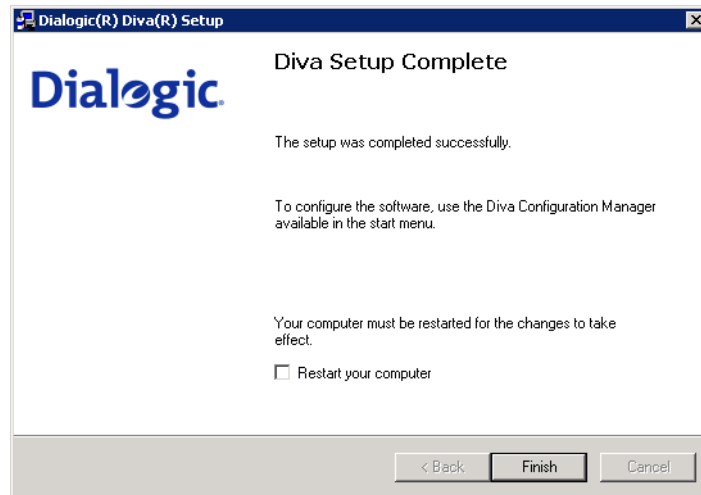
4. If you use WIBU-KEY, select the option **Install WIBU-Key software.** Then click on **Next**.

Up comes this dialog:



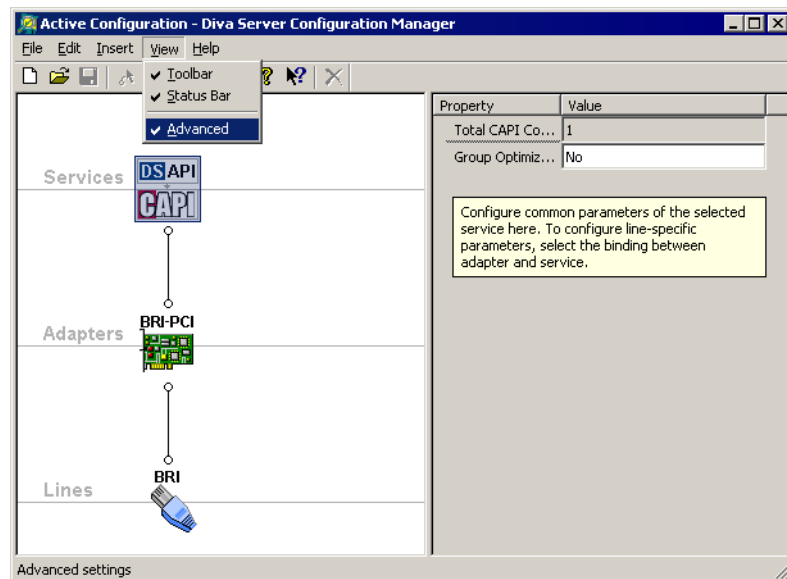
5. Check the selected the installation options. Then click on **Next**.

Up comes this dialog:

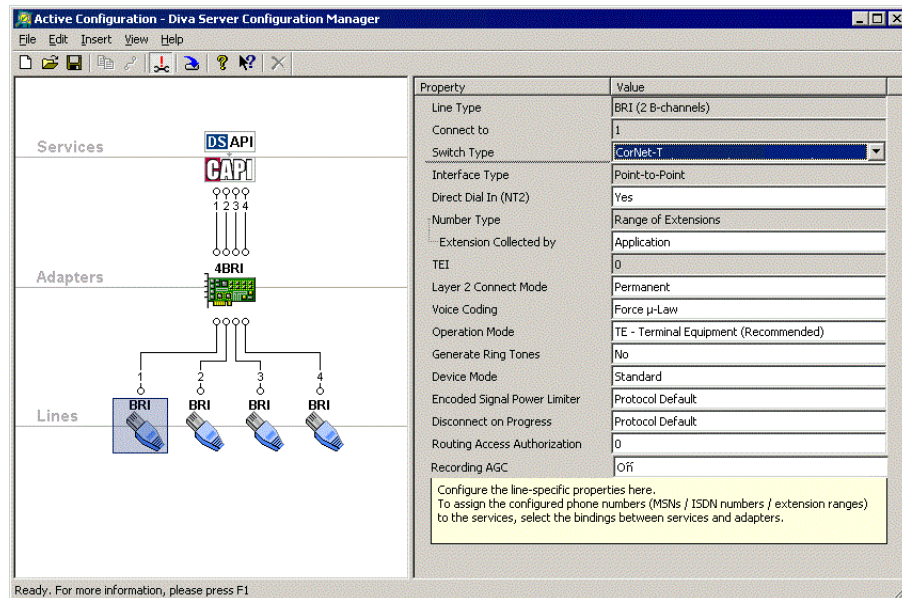


6. Deselect the **Restart your computer** option. Finally, click **Finish**.

The Eicon driver configuration program starts and the following dialog opens:

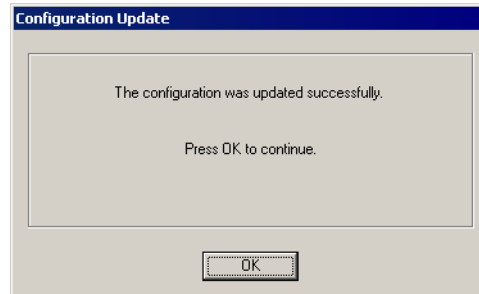


7. Open the **View** menu option and select the **Advanced** option.
8. **For a BRI interface** select a BRI icon and make the following settings in the fields of the dialog's right hand portion:
 - a) Click on the **Switch Type** field and select **CorNet-T**.
 - b) Click on the **Interface Type** field and select **Point-to-Point**.
 - c) Click on the **Direct Dial In** field and select **Yes**
 - d) Click on the **Number Type** field and select **Range of Extensions**.
 - e) Click on the **Extension Collected by** field and select **Application**.
 - f) Click on the **Layer 2 Connect Mode** field and select **Permanent**.
 - g) Click on the **Voice Coding** field and select **Force a-Law** (USA: μ -Law).
 - h) Click on the **Recording AGC** field and select **On**.
 - i) Repeat the steps **a** to **g** for each available BRI line.

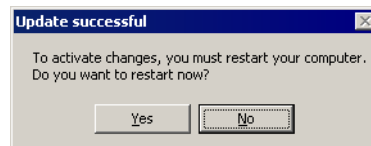


- j) Continue with step 9 on page 327.

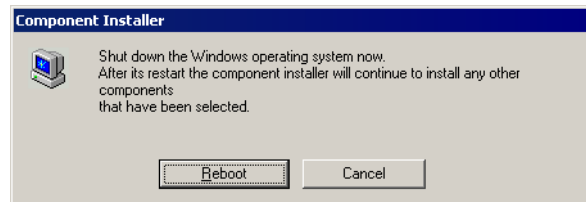
9. Open the **File** menu option and select the **Activate** option. This update may take several minutes.
10. After you settings have been successfully copied, the following dialog opens:



11. Click **OK**. Up comes this dialog:



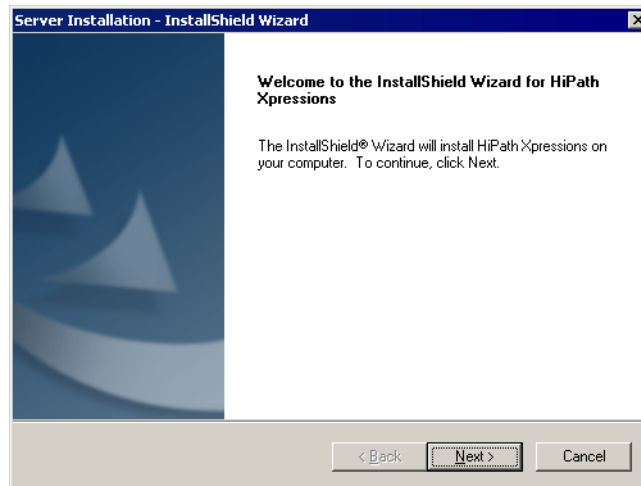
12. Click on **No**. **DO NOT REBOOT**.
13. Close the **Active Configuration** window. Up comes this dialog:



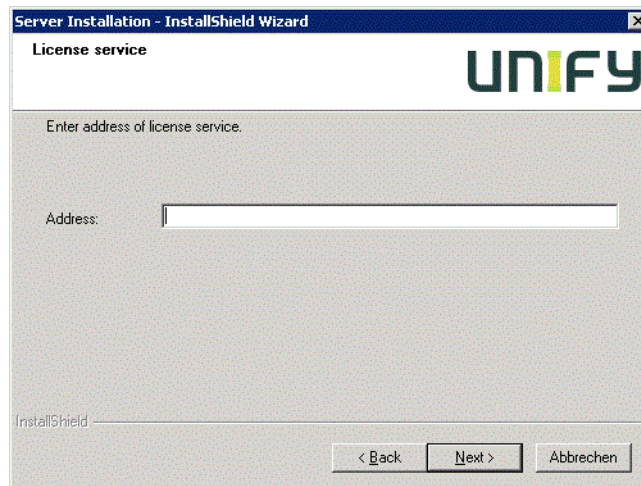
14. Now click **Reboot** to restart the system.

C.6.7 Install the Xpressions Components

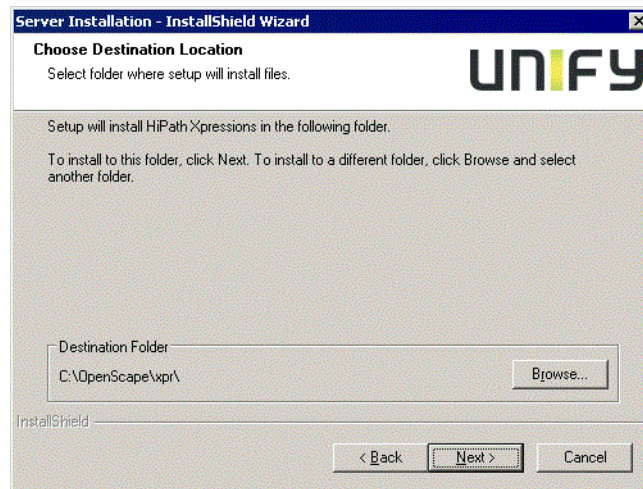
1. After rebooting, log on to the server computer with an administrator account.
The setup is continued and the following dialog opens:



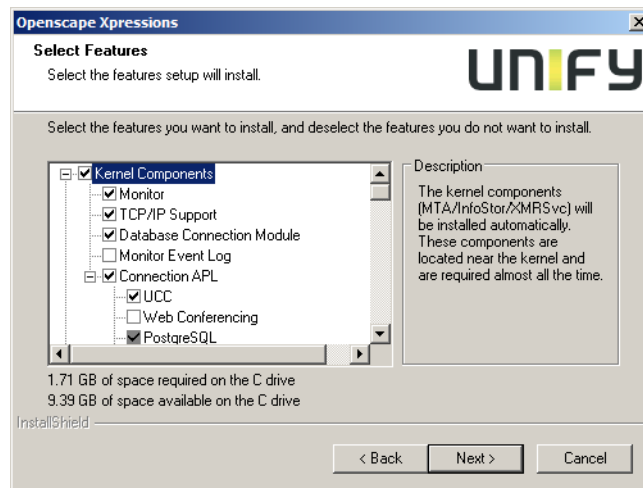
2. Click on **Next**. Up comes this dialog:



3. Enter the IP address of the computer on which the CLA runs. Then click on **Next**. Up comes this dialog:

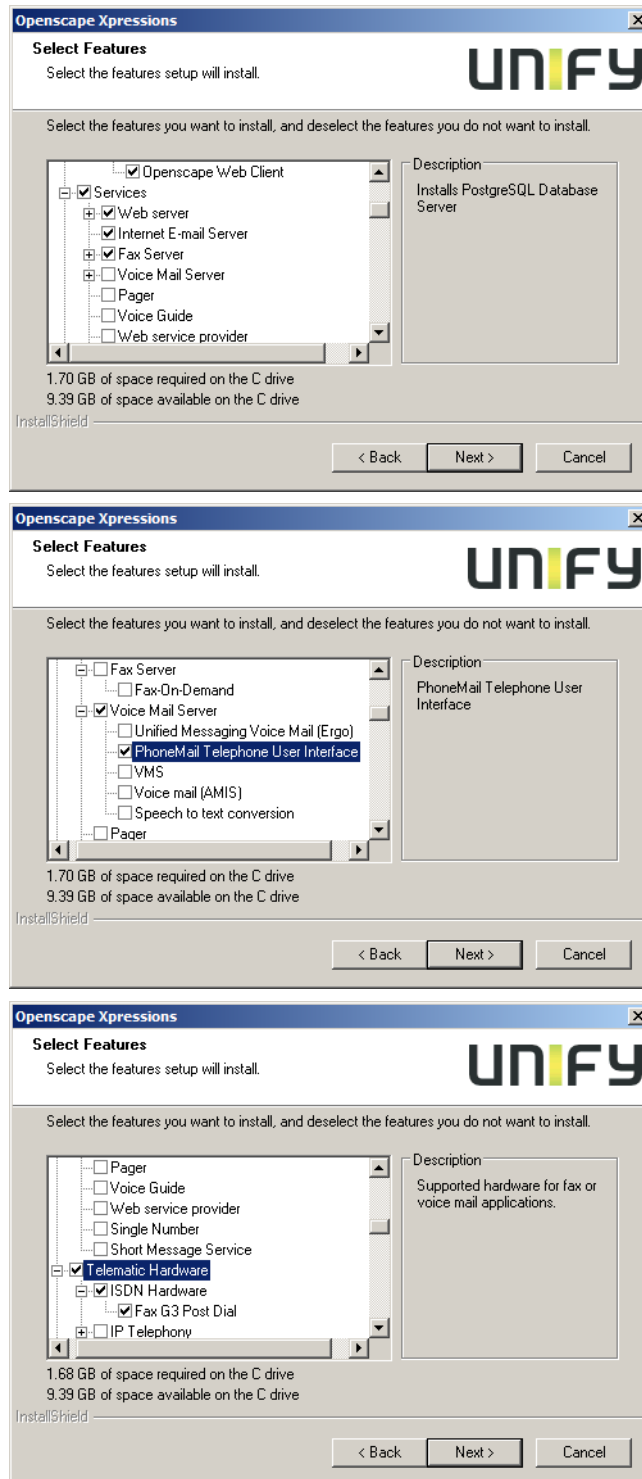


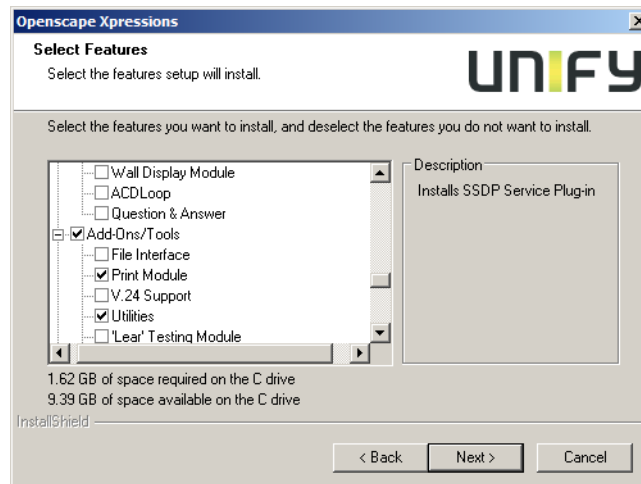
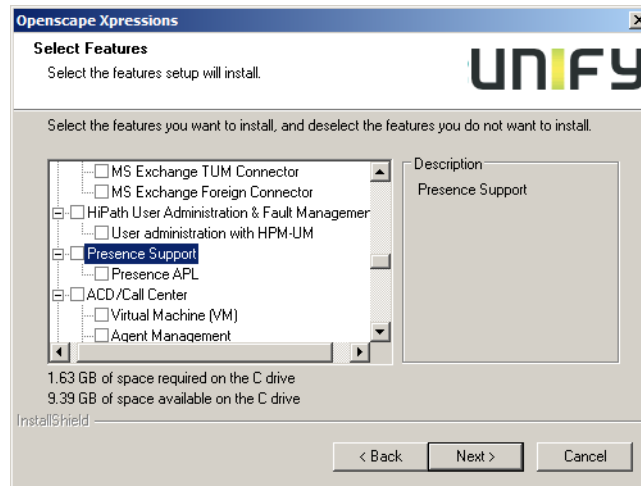
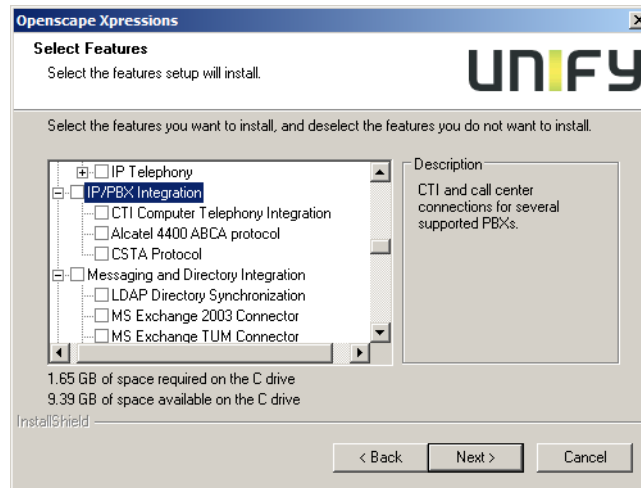
4. Check whether the defaulted setup target folder is on the largest available partition. If this is the case, click on **Next**. Otherwise use the **Browse...** button to select another target folder situated on the largest available partition. Check the customer's order (see [5 on page 243](#)) and select the components associated to the ordered options in this dialog (cf. the selected entries in following figures).



Configuring OpenScope Xpressions as Voice-only System

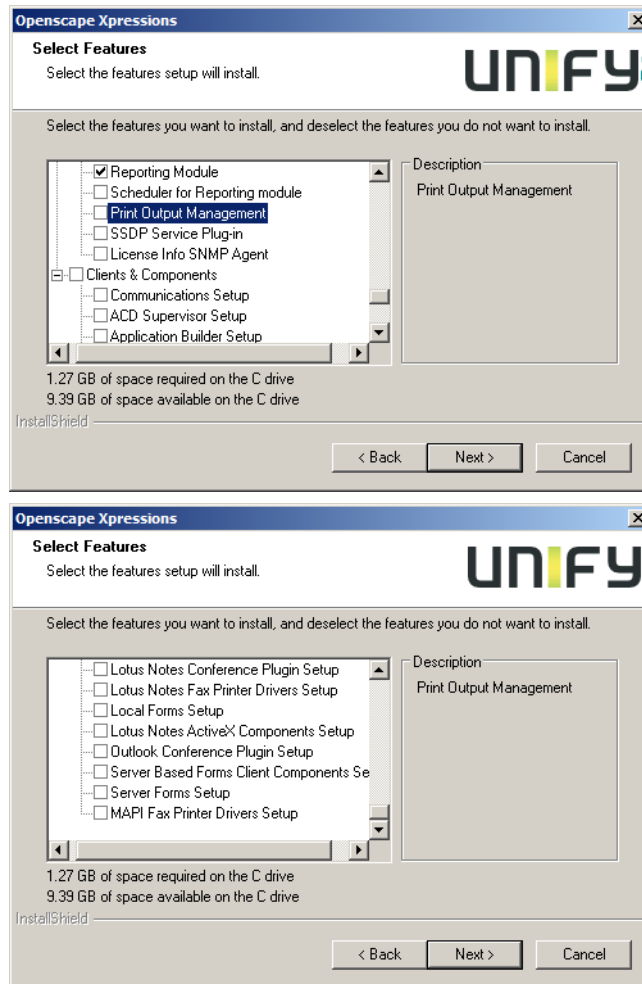
Hicom 300H/CorNet-T Installation



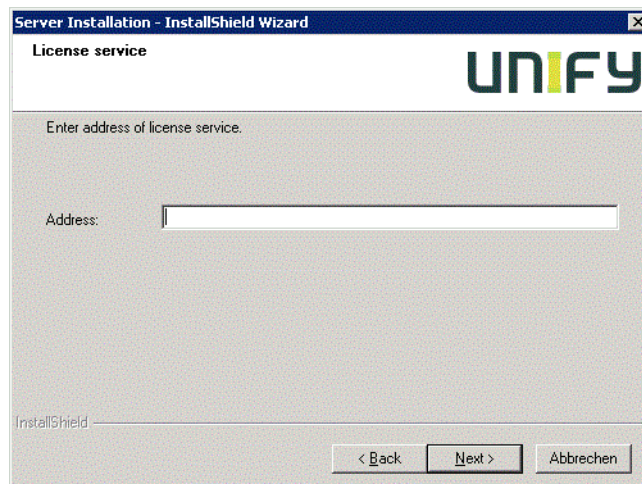


Configuring OpenScape Xpressions as Voice-only System

Hicom 300H/CorNet-T Installation



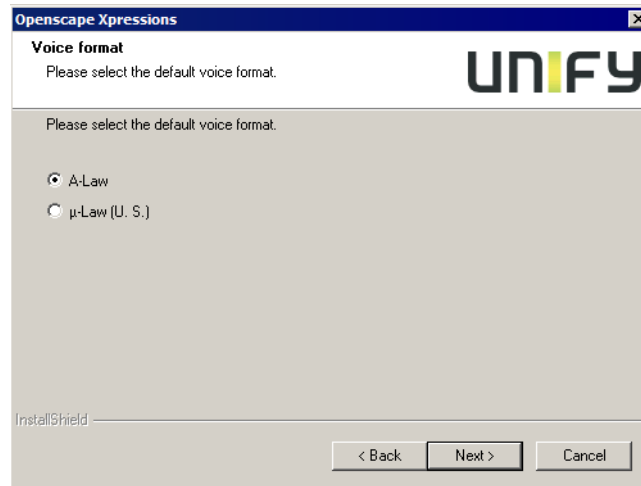
After selecting all licensed features, click on **Next**. Up comes this dialog:



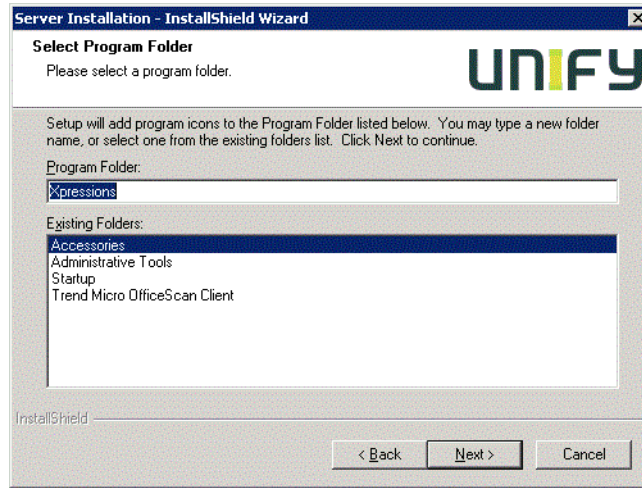
5. Click on **Next**.

NOTE: If desired, you may change the location of one of the folders to another drive. Make sure to use the largest available partition.

Up comes this dialog:



6. Select a default voice format. If you are in the U.S., select **µ-Law**. If you are in another country, select **A-Law**. Then click on **Next**. Up comes this dialog:



7. Click on **Next** to copy the program folder. Up comes this dialog:



8. Select the authentication type:

Login via the Windows User Account

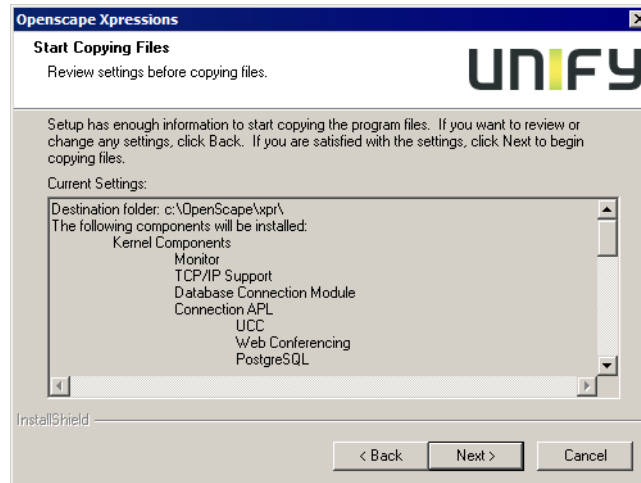
This is the standard method. If this method is applied, the user's Windows account is used for authentication against the XPR server. All password-specific functions in the XPR server are deactivated. After you have selected this option, the next installation step is to choose the Windows accounts to serve as XPR administrator or XPR postmaster (cf. [Section 4.5.6.1, "Login via the Windows User Account", on page 106](#)).

Login via XPR account (user name + password (PIN))

With this authentication method, user accounts for the XPR administrator and the XPR postmaster are created in the XPR database. It is still possible though to activate the authentication via the Windows user account for some

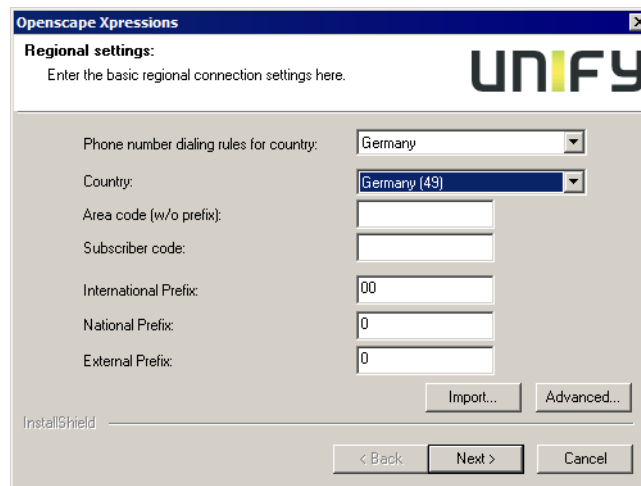
users in hindsight. In the next installation step you need to specify a name and password for the administrator and the postmaster of the XPR server each (cf. [Section 4.5.6.2, “Login via XPR Account”](#), on page 107).

Then click on **Next**. Up comes this dialog:



9. Check the listed options and click on **Next**. The copying process begins. A status dialog informs you about the installation progress.

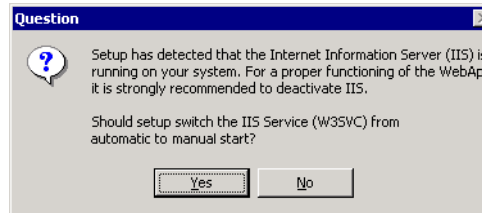
Up comes this dialog:



10. In the **Phone number dialing rules for country** field select the country in which the system is to be set up.
11. Enter the area code (without prefix) and the subscriber number. Then click on **Next**.
12. If the Internet E-mail server has been selected as option and the Windows Internet Information Server (IIS) has been installed and activated on the computer, the following dialog appears:

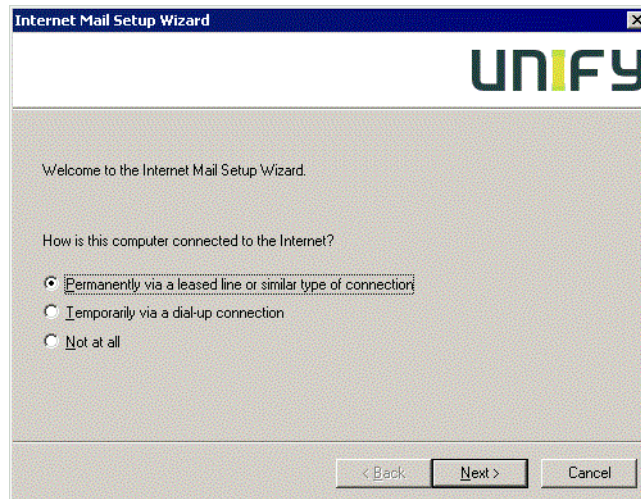
Configuring OpenScape Xpressions as Voice-only System

Hicom 300H/CorNet-T Installation

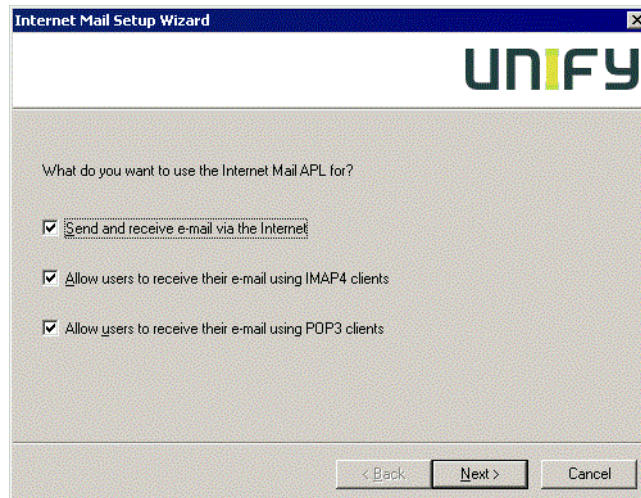


Confirm this dialog with **Yes**.

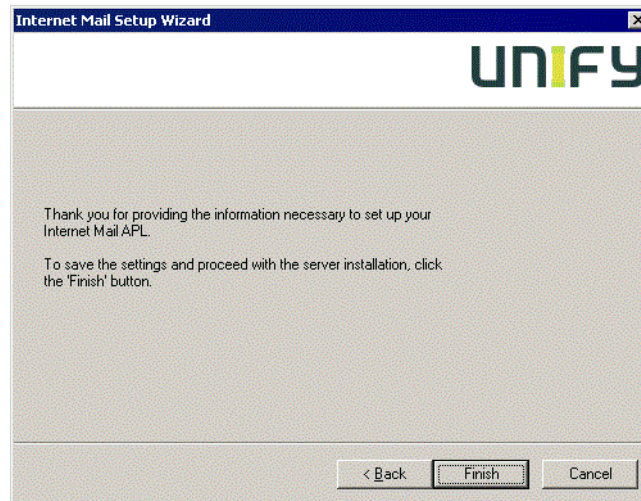
If the Internet Information Server has not been installed on the computer, the following dialog appears:



- a) Select the **Permanently via a leased line or similar type of connection** option, then click on **Next**. Up comes this dialog:

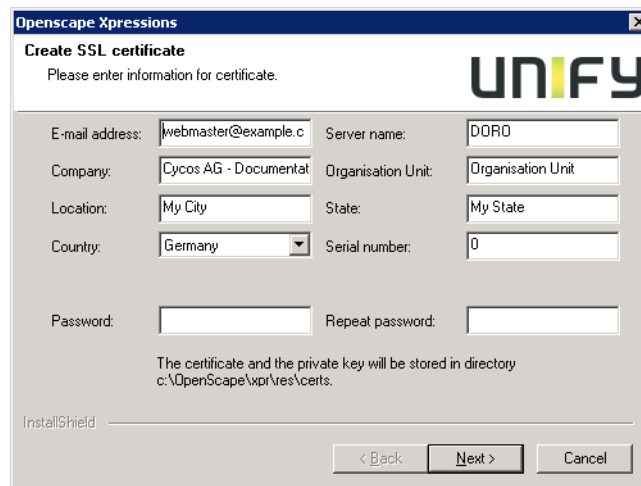


- b) Verify that **all options are selected** and click on **Next**. Up comes this dialog:



c) Click **Finish**. Up comes this dialog:

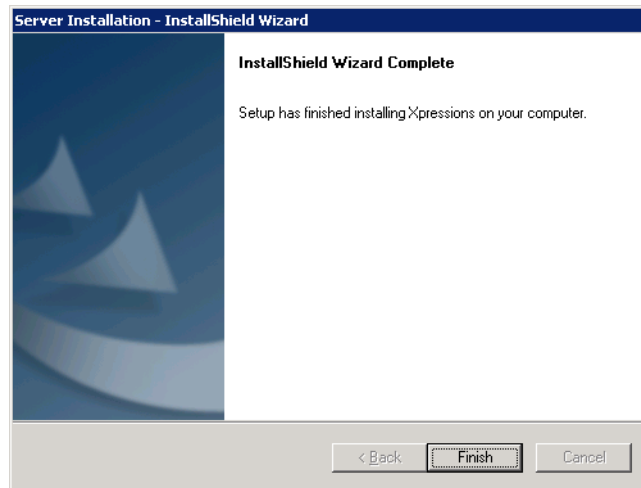
13. The SMTP APL setup is completed. Up comes this dialog:



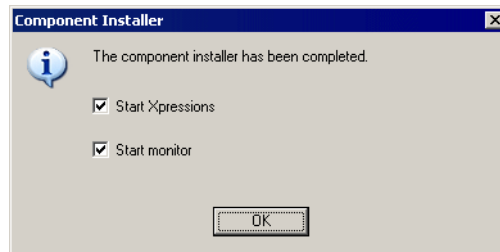
14. In the dialog's fields make the specifications that are to become elements of the certificate. In the **Password** field enter a sufficiently complex password and repeat this specification in the **Repeat password**:. Then click on **Next**.

IMPORTANT: 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.

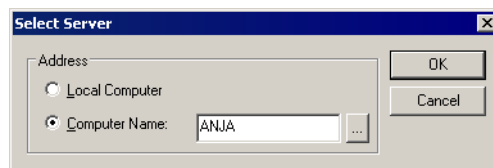
Up comes this dialog:



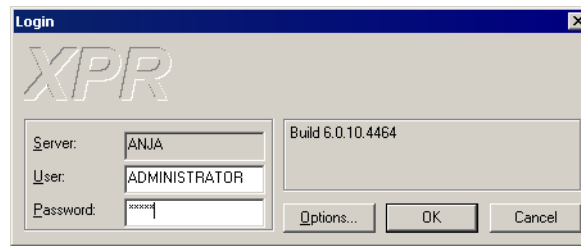
15. Click **Finish**. You may have to click **Finish** several times depending on the selected options. The server setup is thus complete.
16. The selected language packets and other components will now be installed. These installations occur automatically, so that you need not make any entries. As soon as all installations are complete, the following dialog appears:



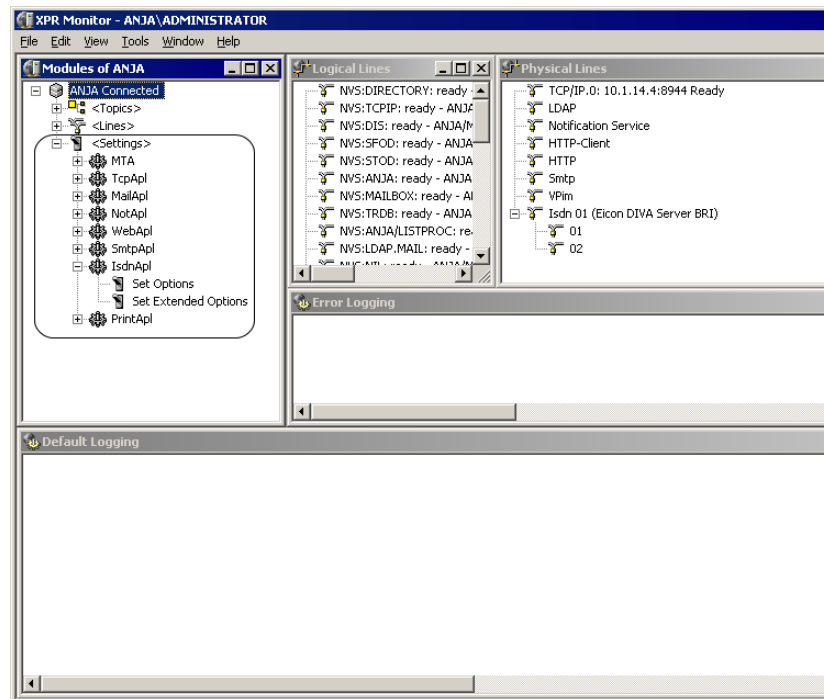
17. Select the options **Start HiPath Xpressions** and **Start monitor** and click on **OK**. Up comes this dialog:



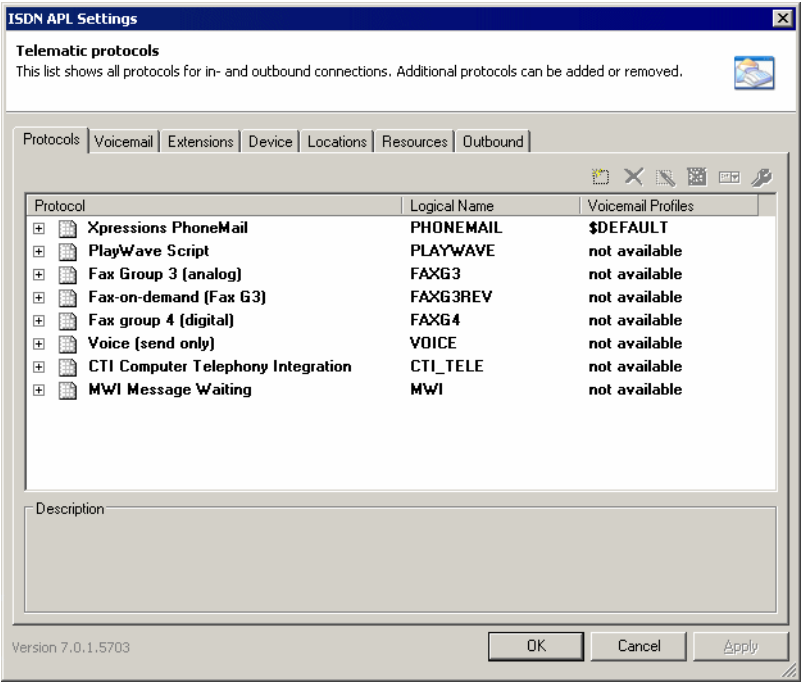
18. Enter or browse the Xpressions server name, then click **OK**. The monitor login dialog opens:



19. Log on to the XPR monitor as **Administrator**, then click on **OK**. The monitor opens:

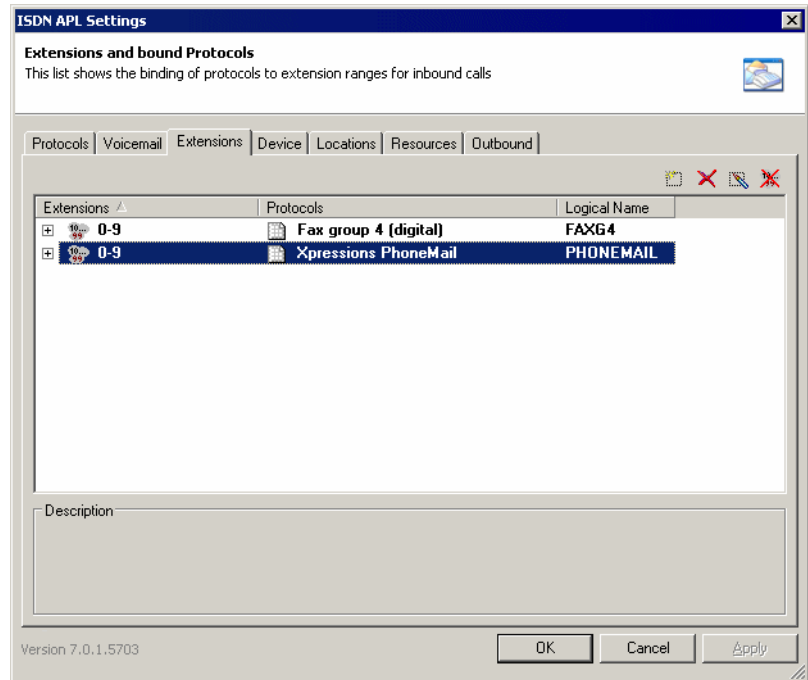


20. In the **Modules of <Xpressions Server>** window under **<Settings>** expand the **IsdnApi** entry and doubleclick **Set Extended Options**. Up comes this dialog:

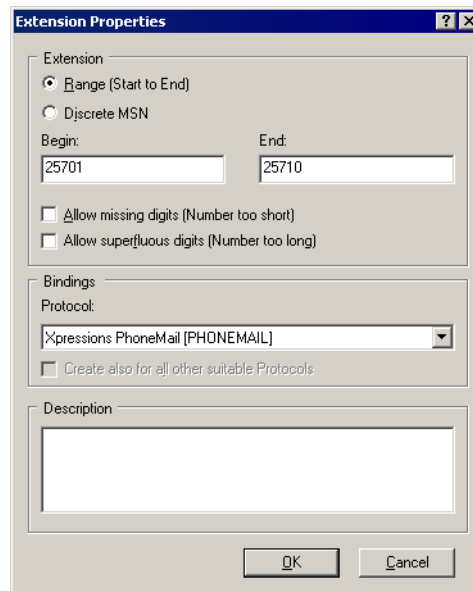


21. Check whether the **Protocols** tab shows all protocols displayed above. Verify that the *CTI_TELE*, *MWI*, *PHONEMAIL*, *PLAYWAVE*, and *VOICE* protocols are displayed at any rate.

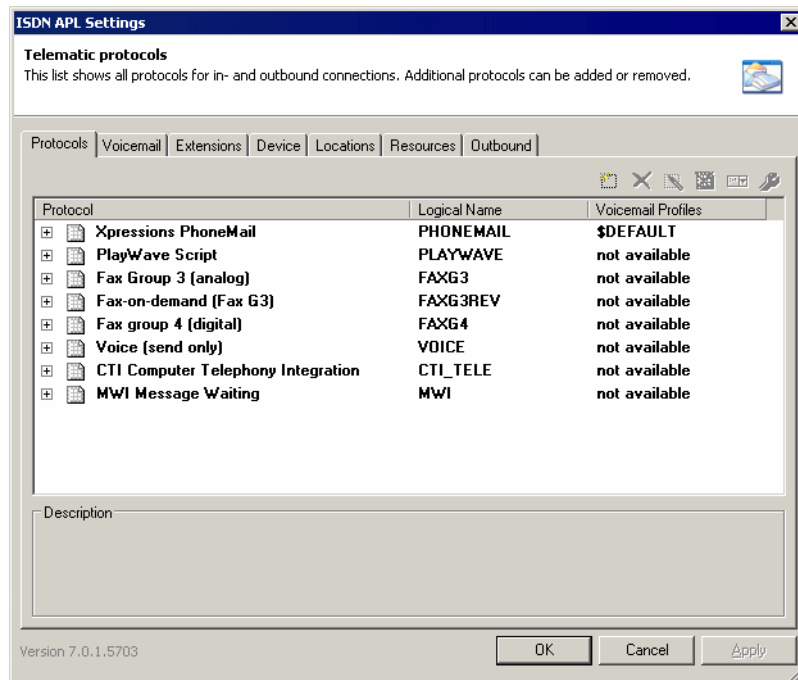
22. Switch to the **Extensions** tab, then double-click **Xpressions PhoneMail**.



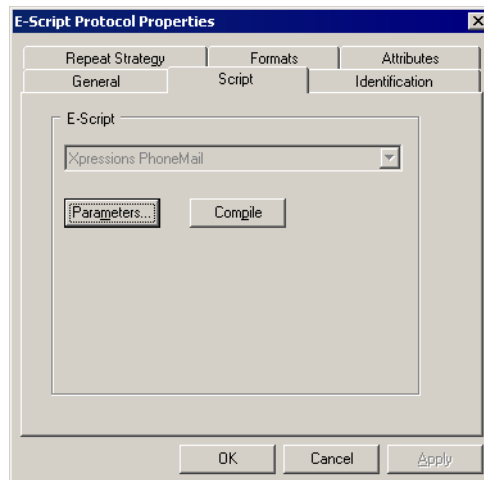
Up comes this dialog:



23. In the **Extensions** field enter the first and last digit only for the ACCESS NUMBERS, then click on **OK**. The dialog closes and you return to the following dialog:



24. Open the **Protocols** tab and doubleclick the **Xpressions PhoneMail** entry. Up comes this dialog:



25. Open the **Script** tab and click on the **Parameters** button. Up comes this dialog:

The dialog box is titled "Xpressions PhoneMail" and has tabs for General, Options, Settings, Addressing, and Customer. The "General" tab is selected. Under the "Service Access Numbers" section, there are six input fields with the following labels and values:

Label	Value
Direct Access:	25701
Guest/Forward Access:	25702
Callback Access:	25703
Fax Access:	25704
Transfer Access:	25705
Universal Access:	25706

At the bottom of the dialog are buttons for OK, Cancel, and Apply.

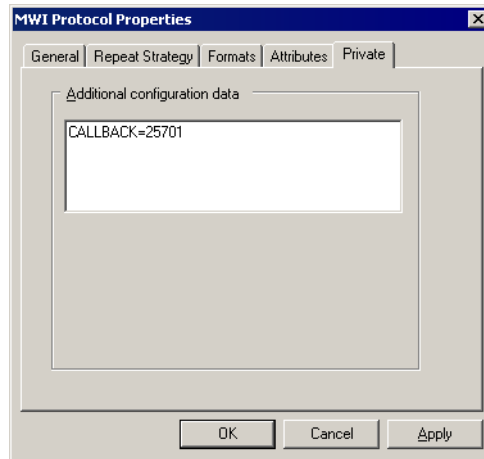
26. Enter the **Service Access Numbers** and click on **OK**.
27. Click on **OK** again to close the **E-Script Protocol Properties** window. You return to the following dialog:

The dialog box is titled "ISDN APL Settings" and has tabs for Protocols, Voicemail, Extensions, Device, Locations, Resources, and Outbound. The "Protocols" tab is selected. It displays a list of telematic protocols with their logical names and voicemail profiles.

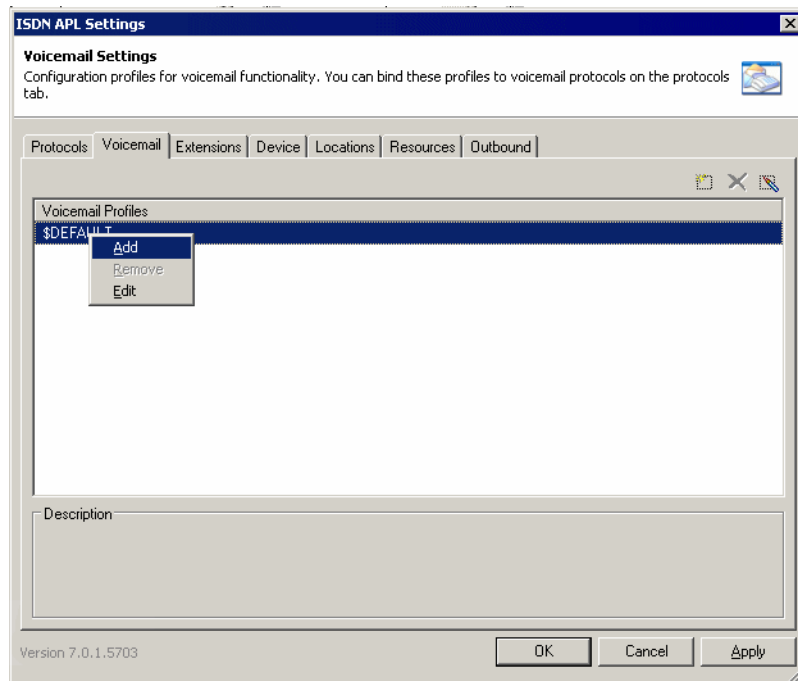
Protocol	Logical Name	Voicemail Profiles
Xpressions PhoneMail	PHONEMAIL	\$DEFAULT
PlayWave Script	PLAYWAVE	not available
Fax Group 3 (analog)	FAXG3	not available
Fax-on-demand (Fax G3)	FAXG3REV	not available
Fax group 4 (digital)	FAXG4	not available
Voice (send only)	VOICE	not available
CTI Computer Telephony Integration	CTI_TELE	not available
MWI Message Waiting	MWI	not available

Below the list is a "Description" field. At the bottom of the dialog are buttons for OK, Cancel, and Apply, and the version number "Version 7.0.1.5703" is displayed.

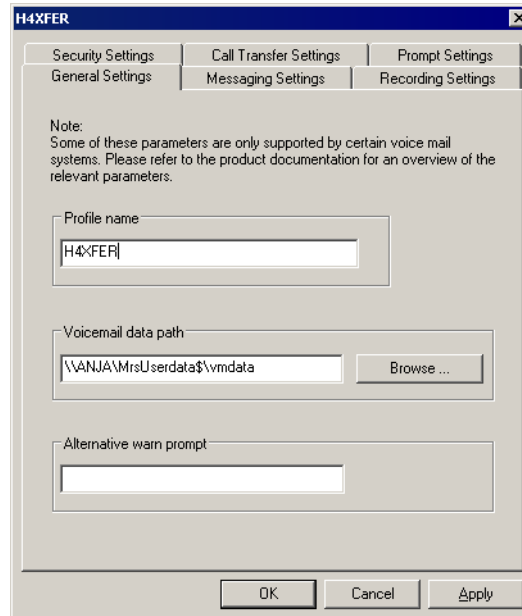
28. Open the **Protocols** tab and doubleclick the **MWI** entry. Up comes this dialog:



29. Open the **Private** tab, enter the PBX callback number and click on **OK**. Up comes this dialog:

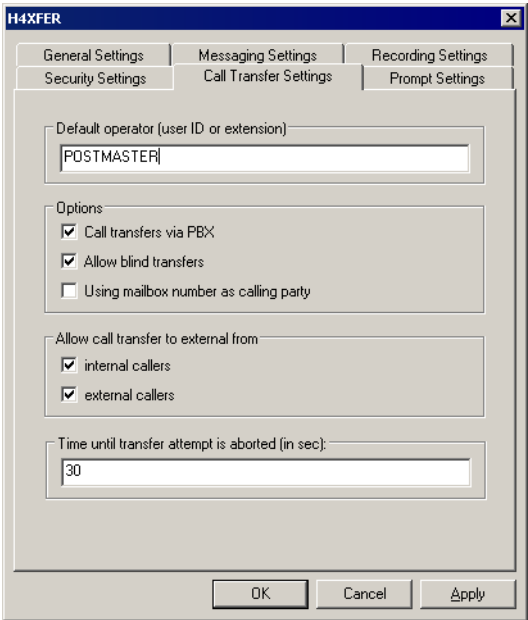


30. Open the **Voicemail** tab, click with the right mousebutton on the **\$DEFAULT** entry and select **Add** in the context menu. Up comes this dialog:

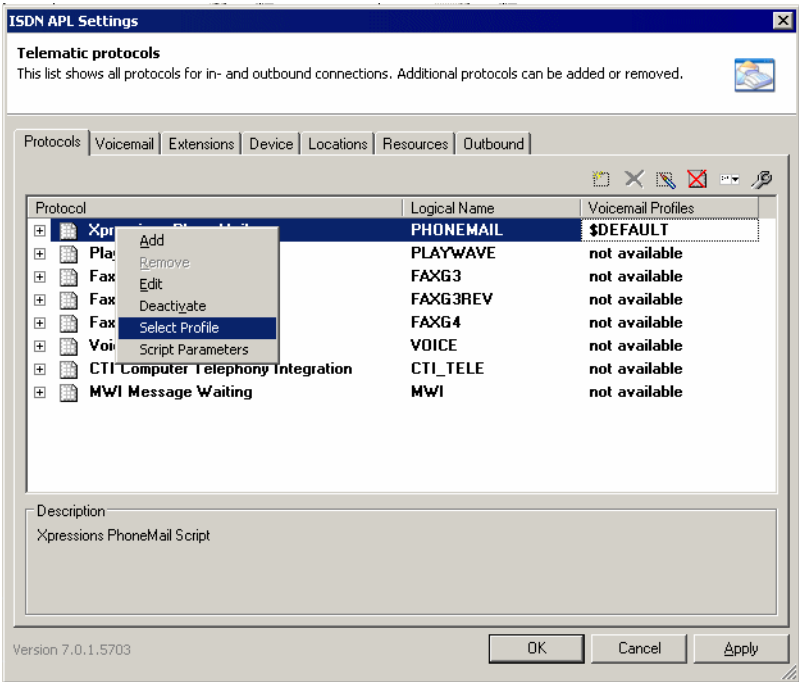


31. Open the **General Settings** tab and enter *H4XFER* in the **Profile name** field.
32. Open the **Call Transfer Settings** tab and,
33. If it does not already exist, enter the user ID or the extension of the **default operator**.
34. Select the **Allow blind transfers** option.

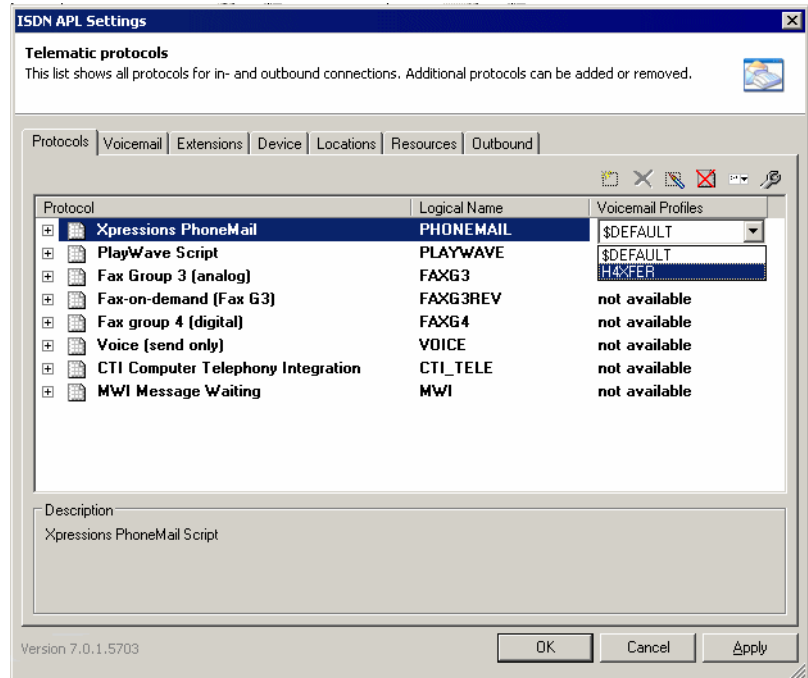
35. Verify that the **internal callers** and **external callers** options in the **Allow call transfer to external from** section are active.



36. Click on **OK** to close the profile configuration. You return to the following dialog:



37. Open the **Protocols** tab, click with the right mousebutton on the **Xpressions PhoneMail** entry and select **Select Profile** in the context menu.



38. Open the **Voicemail Profiles** pull-down menu and select **H4XFER**.
39. Click on **OK** to close the **ISDN APL Settings** window.
40. Proceed to [Section C.8, "System Test and Troubleshooting"](#).

C.7 PRI/Eicon Nortel Meridian QSIG Installation

This chapter describes the installation of a PRI interface using Dialogic DIVA server board(s) as well as the QSIG protocol on a Nortel Meridian PBX, Option 11, system release software 25 or later, hotfix G or later with QSIG features.

Interface	PBX	Line Card	PBX Card	Protocol	Max. no. of boards per server	Max. no of channels per session
PRI Connectivity						
T1/PRI	Nortel Meridian	Dialogic DIVA PRI		QSIG	3	68

C.7.1 Configuring the Nortel Meridian

This information will be added after a consultant determines the requirements.

C.7.2 Pre-installation Checklist

Perform the checklist as specified in [Section C.3.3, “Performing the Checklist”](#), on [page 243](#) and have info ready.

C.7.3 Activate the License

Read [Chapter 3, “Generating Licenses”](#) about licensing. Then make sure that

- a CLM and a CLA is available in the network
- you have the required license as XML file (cf. [Section 3.1, “Licensing Routine”](#), on page 38 and [Section 3.5, “Generating a License Key”](#), on page 41).

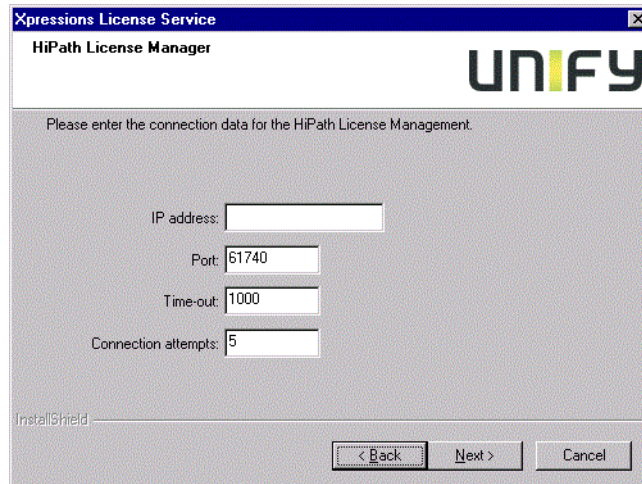
After you have obtained the license as XML file, import it into the CLM and transfer the license to the CLA that OpenScape Xpressions is to connect. Please refer to [Section 3.7, “Activating Licenses in the CLA”](#), on page 44.

If you need to obtain the license via the CLA, please read section 5 in the CLM online help. To open the help, click on the **Help** button in the CLM interface.

After successfully activating the license continue with [Section C.7.6, “Install the OpenScape Xpressions Software”](#), on page 354.

C.7.4 Install the License Service

1. Connect the XPR installation medium to the computer.
2. The license service installation starts. In the next dialogs click on **Next** until the following dialog opens:



3. In this dialog enter the IP address of the computer on which the CLA runs. Then click on **Next**.
4. In the following dialog click **Install**.
5. In the following dialog click **Finish**. The license service installation is thus complete.

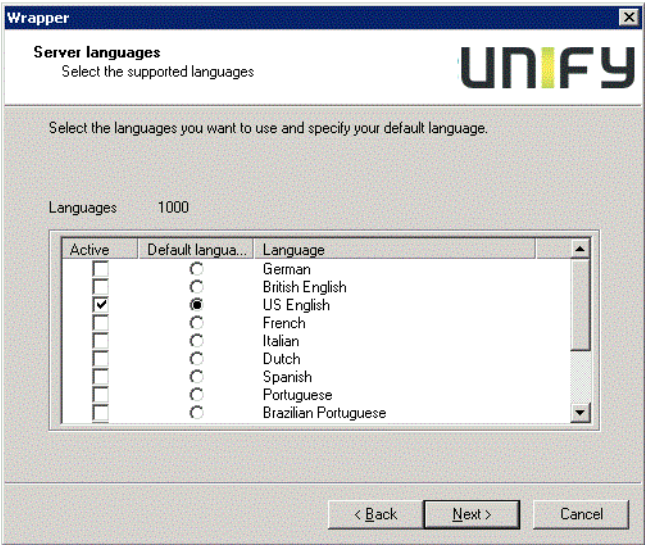
C.7.5 Server Name, Languages and Release Notes

1. After the license service installation, the following dialog opens:

2. Enter the server name and then click on **Next**. When you select the server name, heed the following points:
 - the name you enter here **cannot be modified any more**
 - the name must not contain blanks, special characters such as ;, !, %, &, ... , or German umlauts (ä, ö, ü).
 - you must not use names of logical XPR lines. For example: *PhoneMail*, *VMS*, *COM*, *CON*, *FAXG3*, *FAXG4*, *MWI*, *FOD*, *PlayWave* and *SMTP* will not be accepted.
 - If you want to connect the XPR server to another XPR server via a Remote System Link, the server name selected here must not exceed a length of 11 characters.

NOTE: Remote System Link is not compatible with [Crypt_Sec], it is designed to only work with [KRYPT].

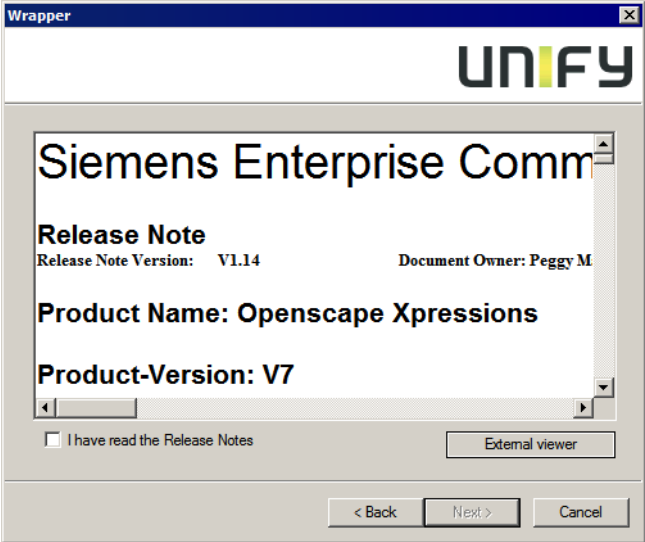
Up comes this dialog:



- In the **Active** column select the languages to be installed. Only select as many languages as licenses are available.

NOTE: You need to select at least one language in order to continue the installation.

- In the **Default language** column select the language that the XPR server is to use as default. You can specify only one language as default language.
- Click the **Continue** button. Up comes this dialog:



This dialog represents the `ReleaseNotes.rtf` file, which is found in the `XpressionsInstall` directory of the setup medium.

6. Please read the Release Notes. Via the **Open in external viewer** button you can open the corresponding file in the application that is registered in the operating system for the file type *RTF*.

7. Select the **I have read the Release Notes** check box. This activates the **Next** button.

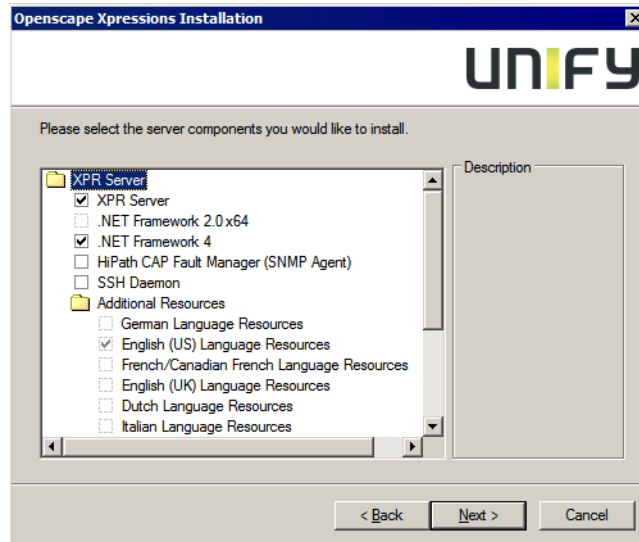
If you do not select the check box, the **Next** button stays inactive and you cannot continue the installation.

8. After you have read the Release Notes, click on **Next**.

The dialog for selecting the server components opens. Please continue reading in [Section C.4.5, "Install the OpenScape Xpressions Software"](#), on [page 250](#).

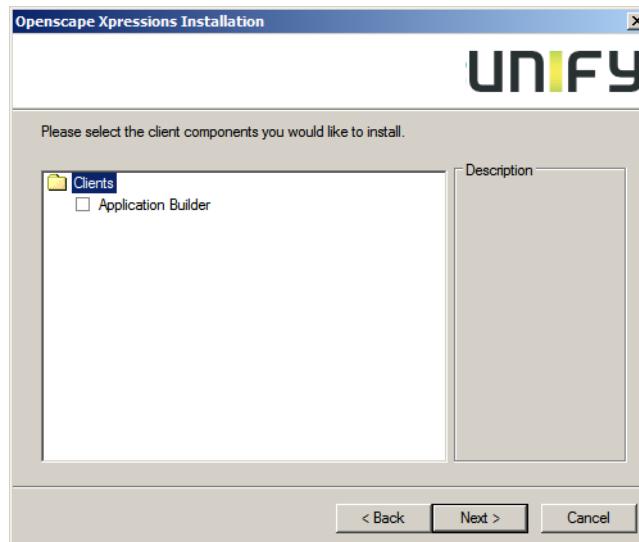
C.7.6 Install the OpenScape Xpressions Software

Up comes this dialog:

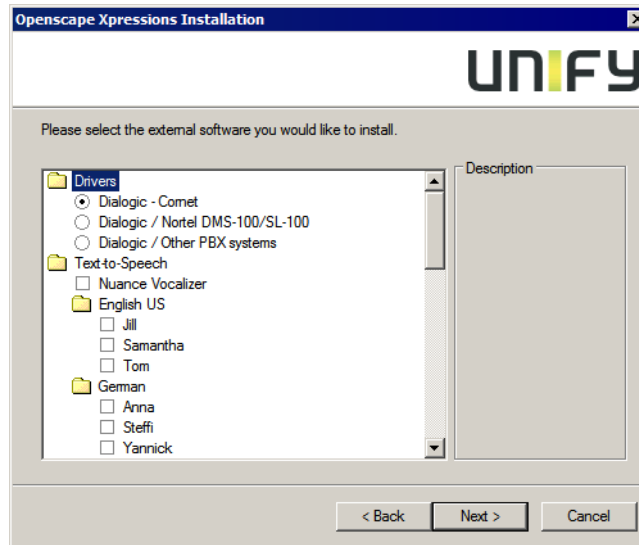


1. Select the **XPR server**. Then click on **Next**.

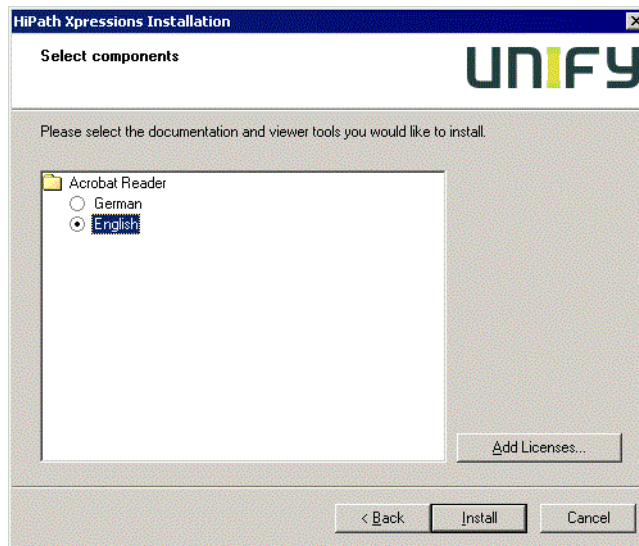
Up comes this dialog:



2. Click on **Next**. Up comes this dialog:



3. Select **Dialog / Nortel DMS-100/SL-100**. Then click on **Next**. Up comes this dialog:

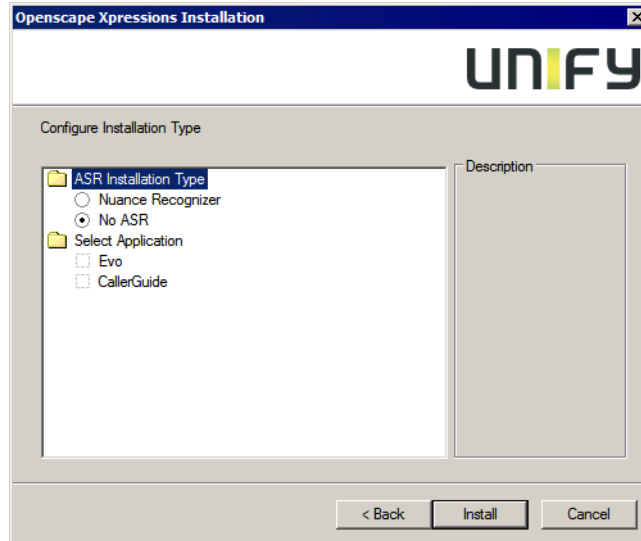


Configuring OpenScape Xpressions as Voice-only System

PRI/Eicon Nortel Meridian QSIG Installation

4. If you want to install the Acrobat Reader, select a language and click on **Install**. Otherwise click only on **Install** without making a selection.

If the customer has purchased an ASR license, the **Next** button appears instead of **Install**. When you click on **Next**, the following dialog opens:



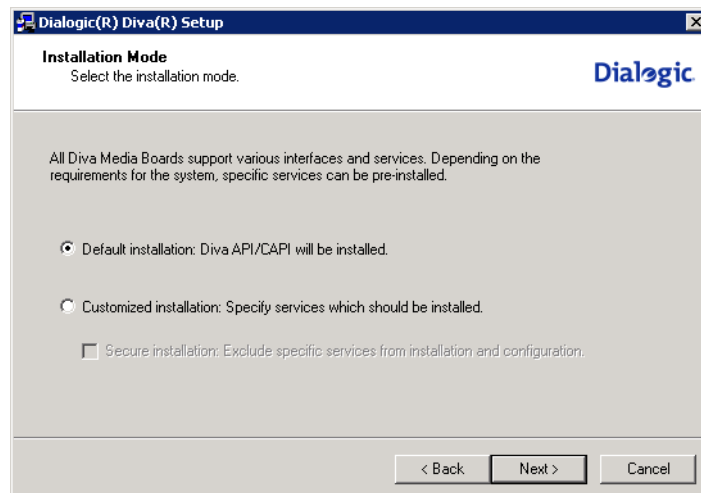
Select the ASR setup type and ASR applications. For further information please refer to [Section 4.3.11, "Installation Type for Automatic Speech Recognition"](#), on page 85. Then click **Install**.

C.7.7 Install the Dialogic DIVA Driver

1. Up comes this dialog:

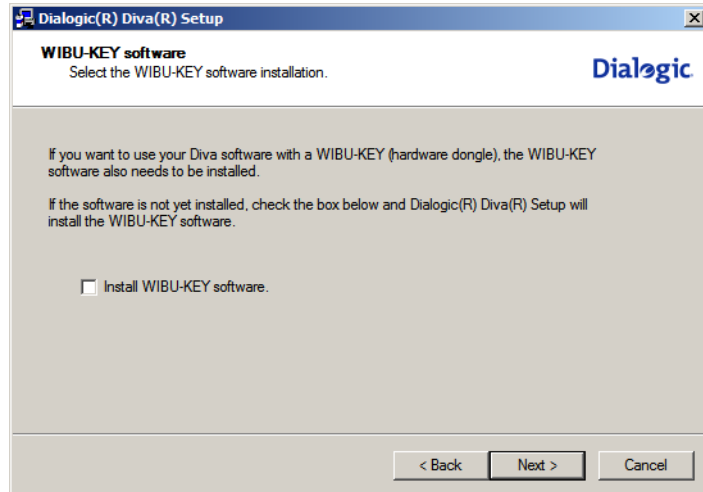


2. Click on **Next**. Up comes this dialog:



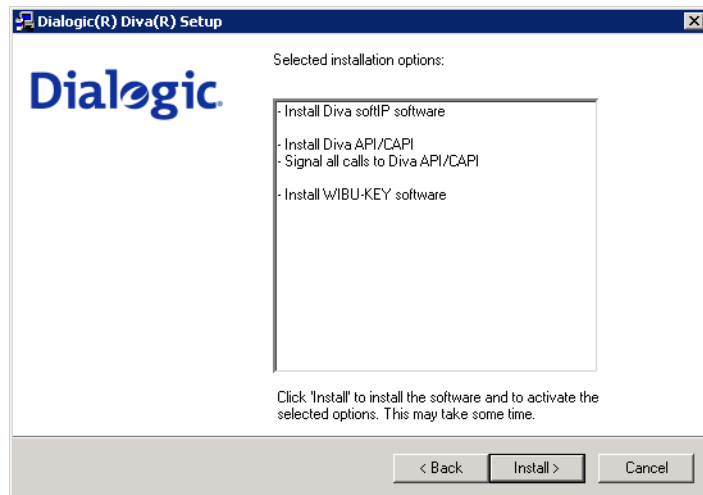
3. Select the option **Default installation: Diva API / CAPI will be installed.** Then click on **Next**.

Up comes this dialog:



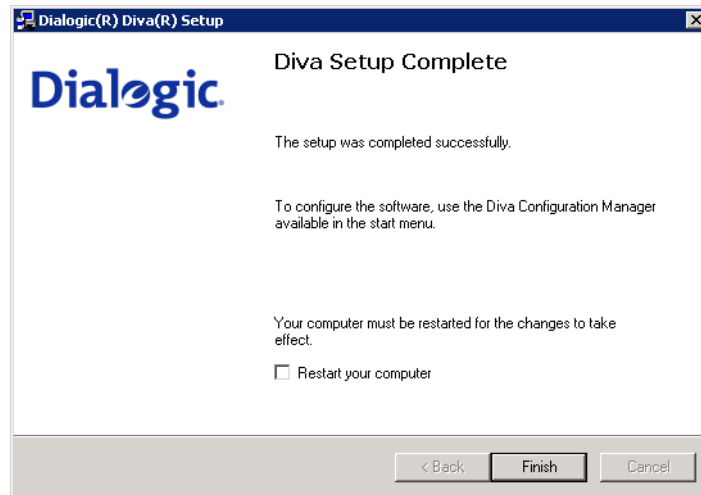
4. If you use WIBU-KEY, select the option **Install WIBU-Key software.** Then click on **Next**.

Up comes this dialog:



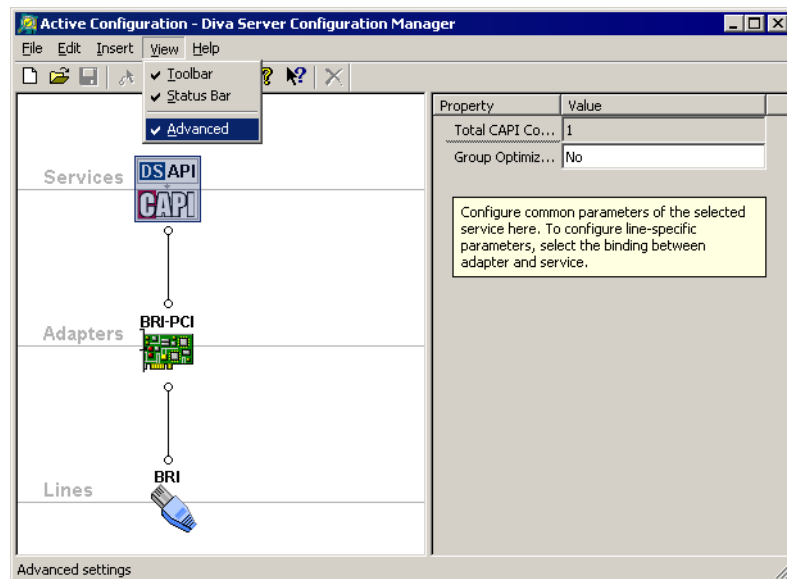
5. Check the selected the installation options. Then click on **Next**.

Up comes this dialog:



6. Deselect the **Restart your computer** option. Finally, click **Finish**.

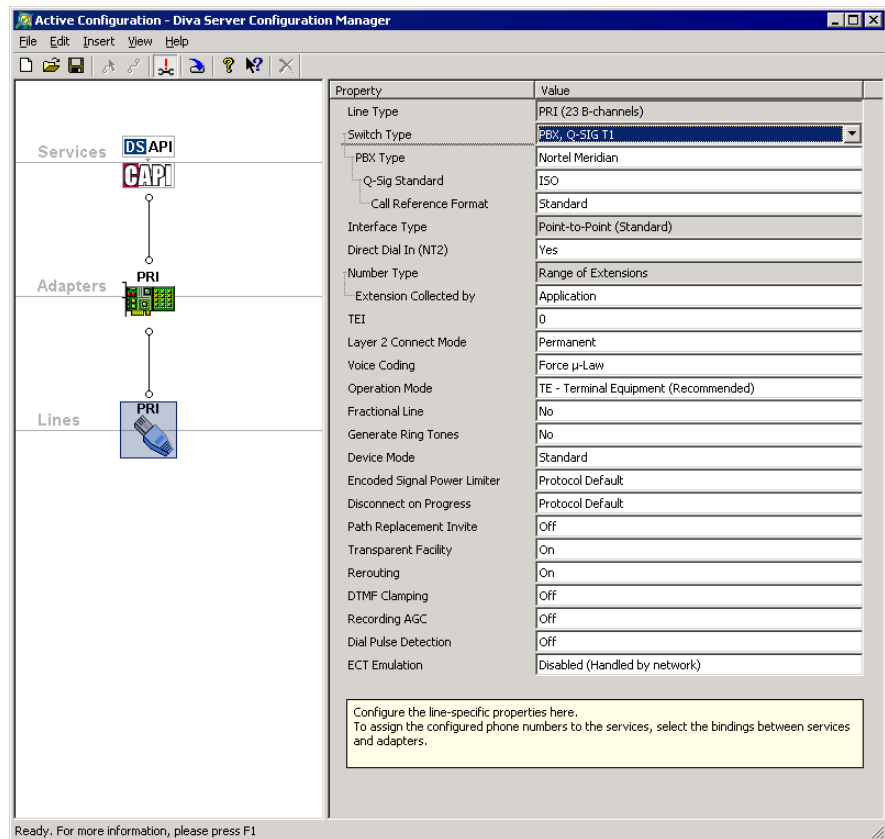
The Eicon driver configuration program starts and the following dialog opens:



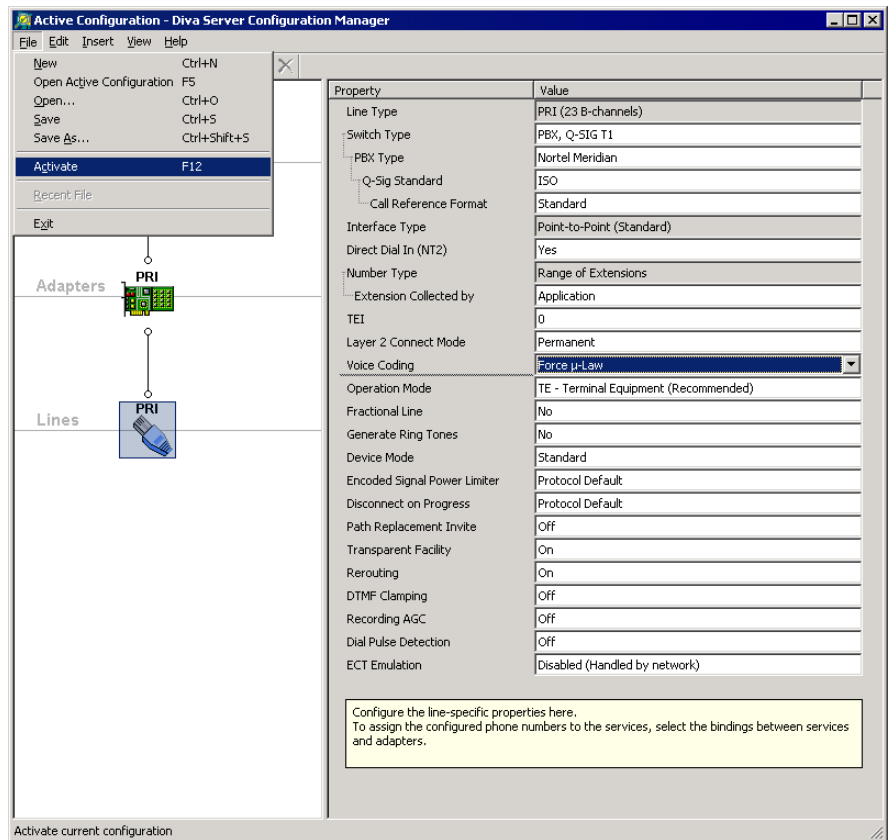
Configuring OpenScope Xpressions as Voice-only System

PRI/Eicon Nortel Meridian QSIG Installation

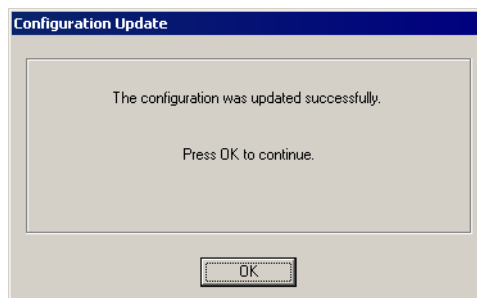
7. Open the **View** menu option and select the **Advanced** option.
8. **For a PRI interface** select a PRI icon and make the following settings in the fields of the dialog's right hand portion:
 - a) Click on the **Switch Type** field and select **PBX, Q-SIG T1**.
 - b) Click on the **PBX Type** field and select **Nortel Meridian**.
 - c) Click on the **Direct Dial In** field and select **Yes**
 - d) Click on the **Q-SIG Standard** field and select **ISO**.
 - e) Click on the **Call Reference Format** field and select **Standard**.
 - f) Click on the **Interface Type** field and select **Point-to-Point**.
 - g) Click on the **Number Type** field and select **Range of Extensions**.
 - h) Click on the **Extension Collected by** field and select **Application**.
 - i) Click on the **Layer 2 Connect Mode** field and select **Permanent**.
 - j) Click on the **Voice Coding** field and select **Force a-Law** (USA: μ -Law).
 - k) Click on the **Transparent Facility** field and select **On**.
 - l) continue to [9 on page 361](#).



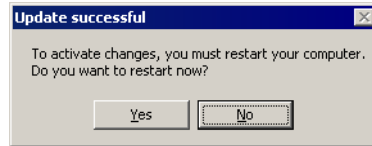
- Open the **File** menu option and select the **Activate** option. This update may take several minutes.



- After you settings have been successfully copied, the following dialog opens:

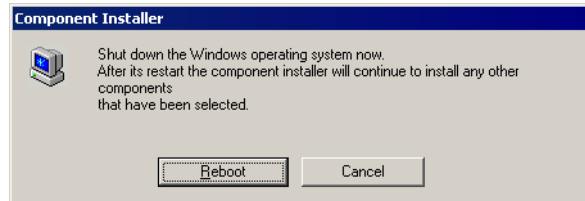


11. Click **OK**. Up comes this dialog:



12. Click on **No**. **DO NOT REBOOT**.

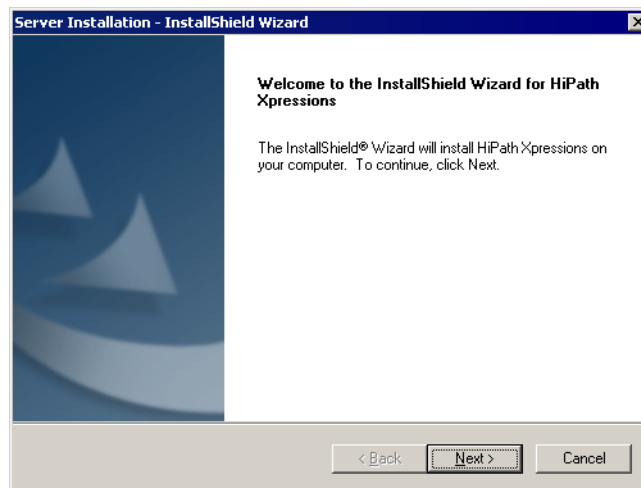
13. Close the **Active Configuration** window. Up comes this dialog:



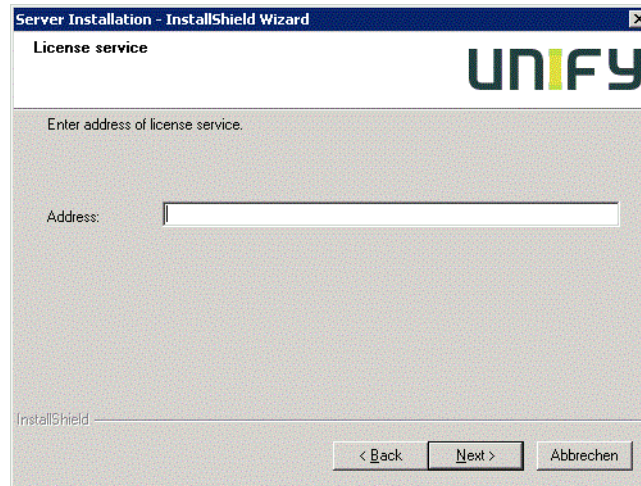
14. Now click **Reboot** to restart the system.

C.7.8 Install the Xpressions Components

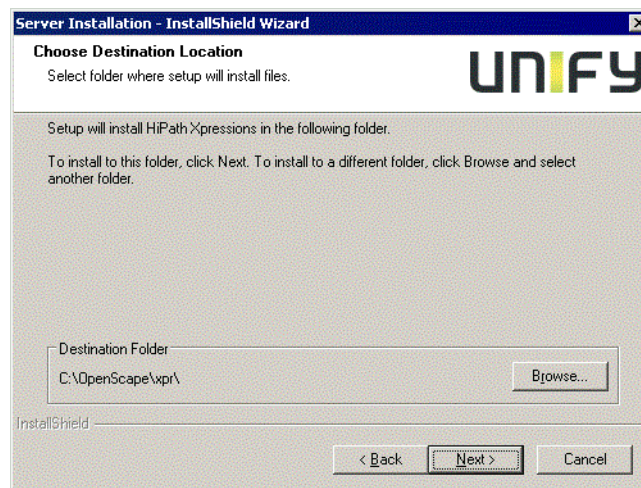
1. After rebooting, log on to the server computer with an administrator account. The setup is continued and the following dialog opens:



2. Click on **Next**. Up comes this dialog:



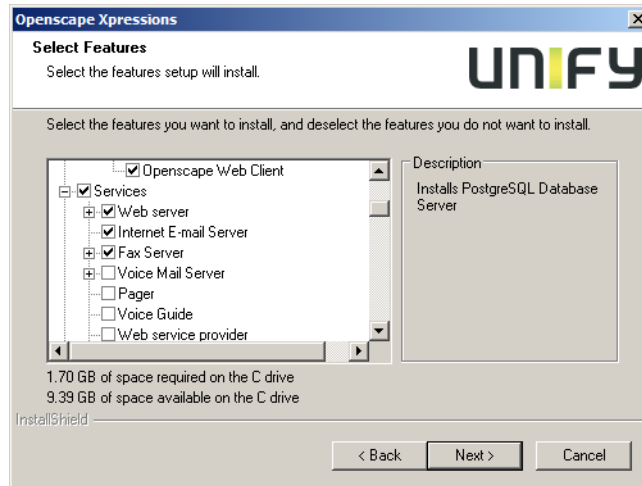
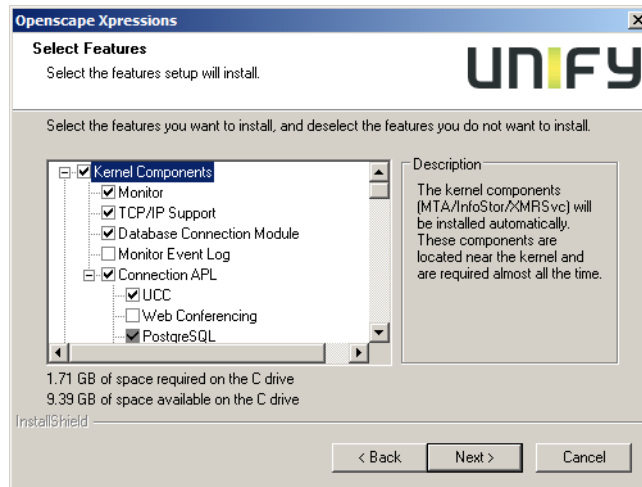
3. Enter the IP address of the computer on which the CLA runs. Then click on **Next**. Up comes this dialog:



Configuring OpenScape Xpressions as Voice-only System

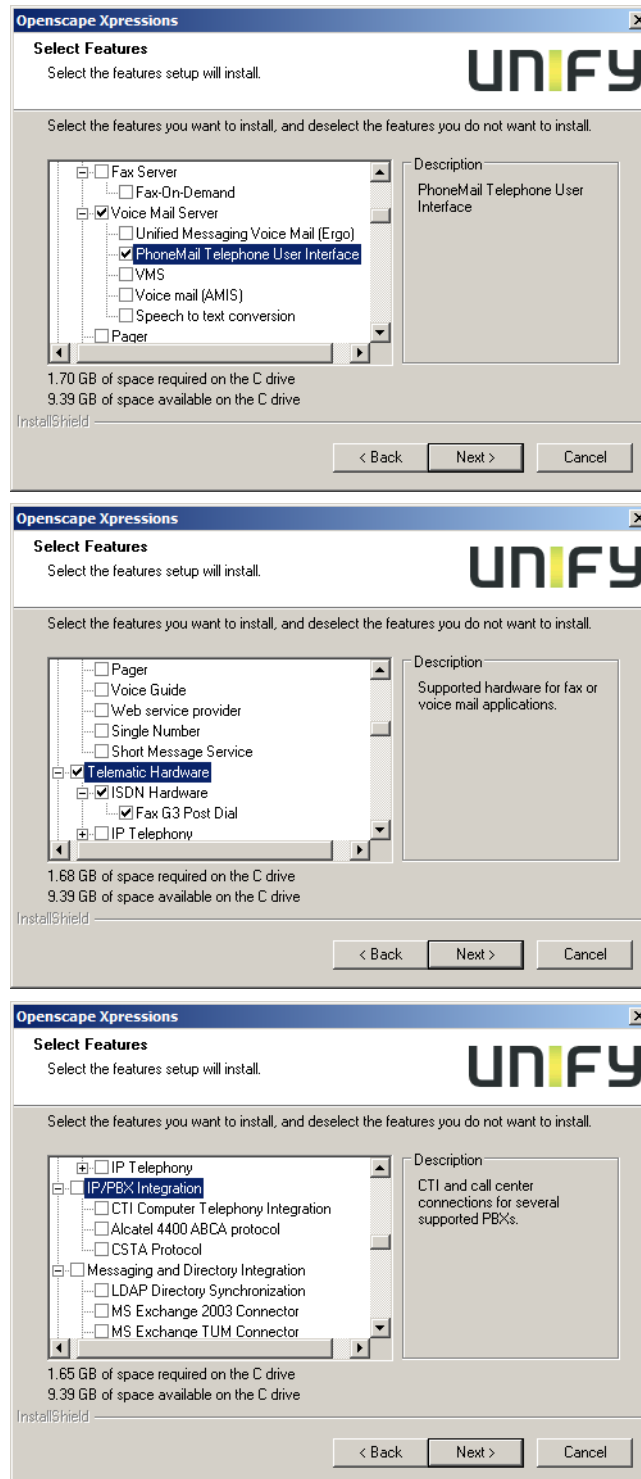
PRI/Eicon Nortel Meridian QSIG Installation

4. Check whether the defaulted setup target folder is on the largest available partition. If this is the case, click on **Next**. Otherwise use the **Browse...** button to select another target folder situated on the largest available partition. Check the customer's order (see [5 on page 243](#)) and select the components associated to the ordered options in this dialog (cf. the selected entries in following figures).

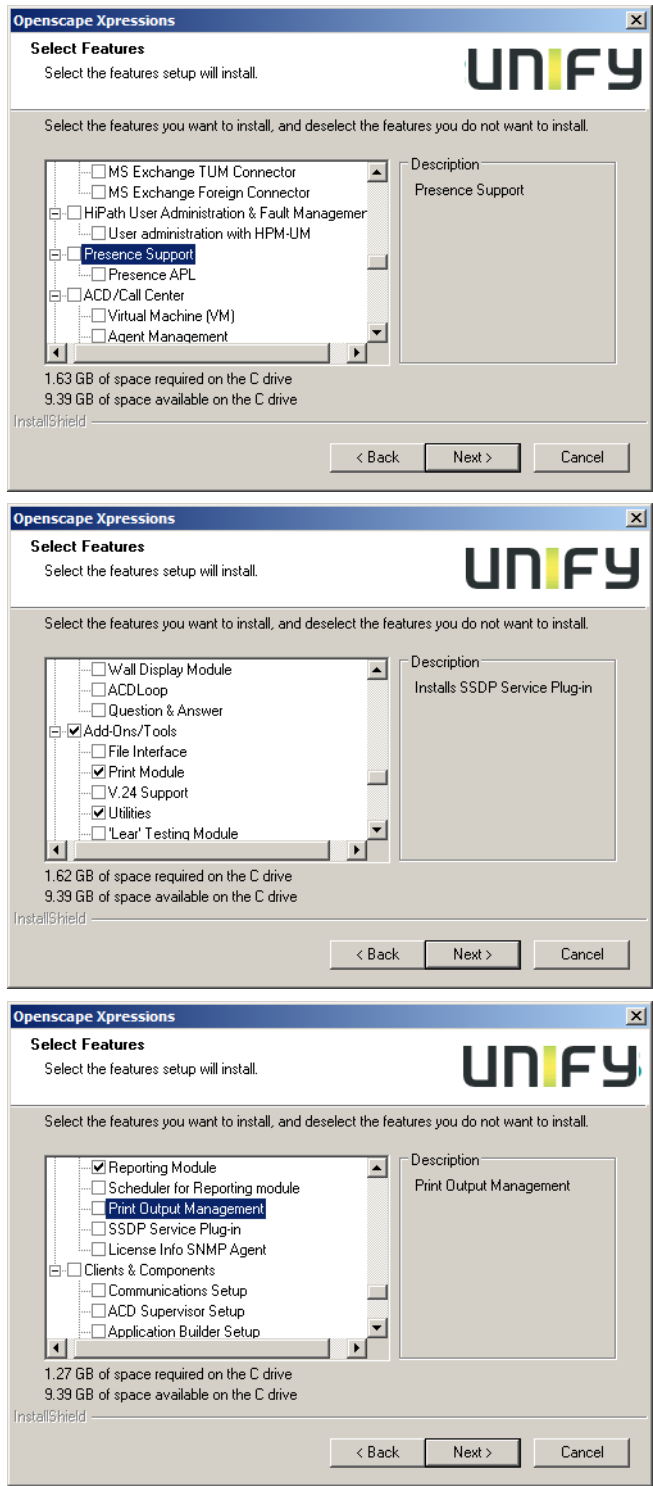


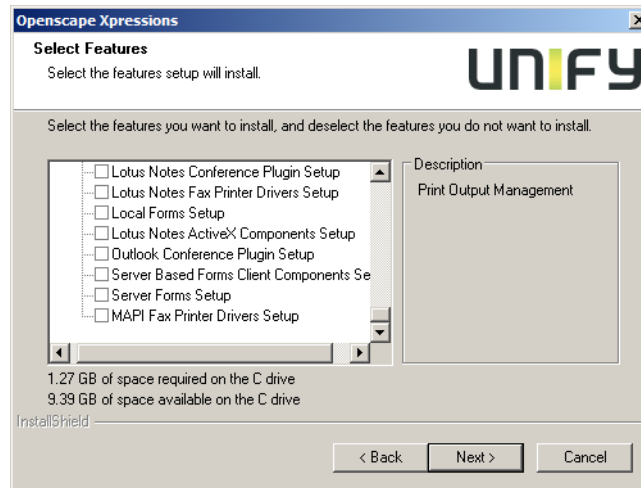
Configuring OpenScope Xpressions as Voice-only System

PRI/Eicon Nortel Meridian QSIG Installation

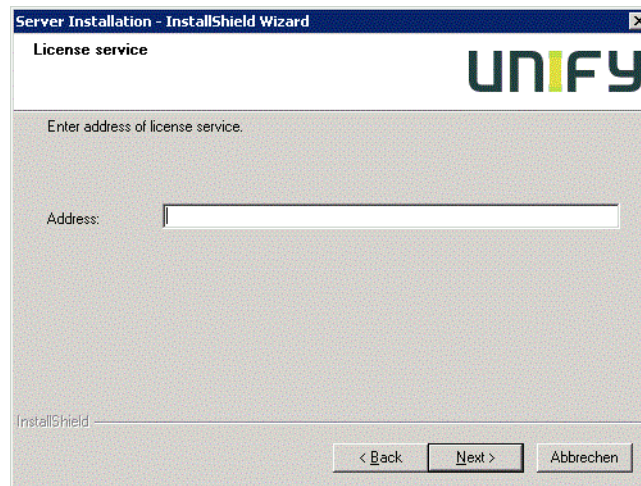


Configuring OpenScope Xpressions as Voice-only System
PRI/Eicon Nortel Meridian QSIG Installation





After selecting all licensed features, click on **Next**. Up comes this dialog:



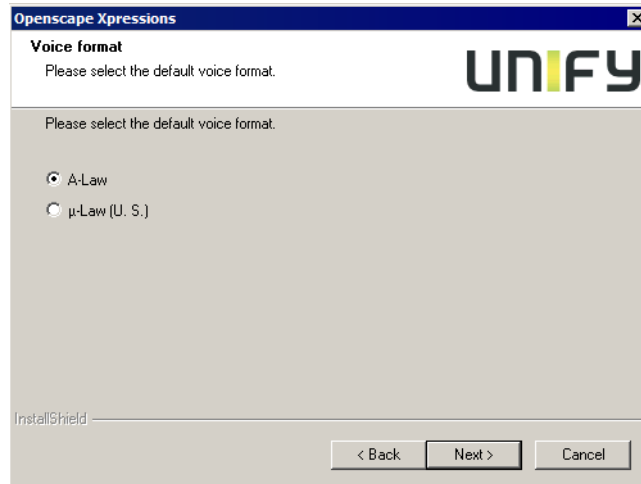
5. Click on **Next**.

NOTE: If desired, you may change the location of one of the folders to another drive. Make sure to use the largest available partition.

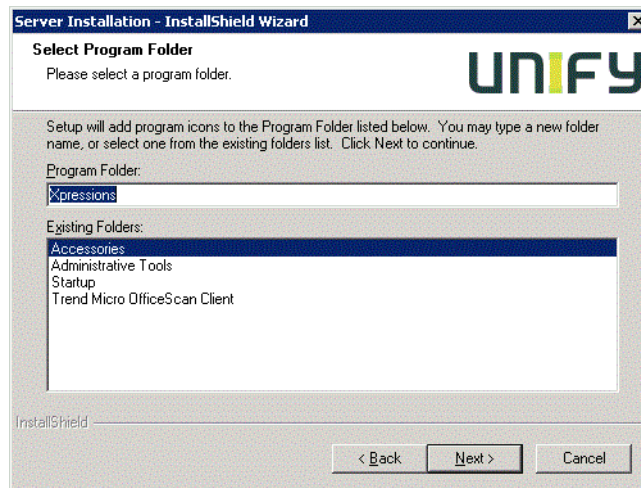
Up comes this dialog:

Configuring OpenScape Xpressions as Voice-only System

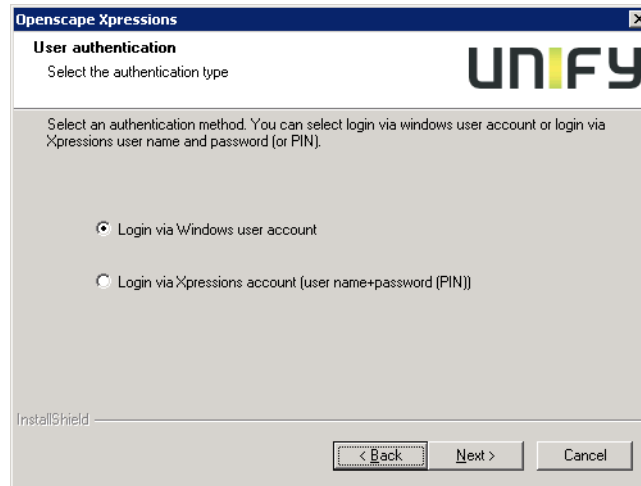
PRI/Eicon Nortel Meridian QSIG Installation



6. Select a default voice format. If you are in the U.S., select **μ-Law**. If you are in another country, select **A-Law**. Then click on **Next**. Up comes this dialog:



7. Click on **Next** to copy the program folder. Up comes this dialog:



8. Select the authentication type:

Login via the Windows User Account

This is the standard method. If this method is applied, the user's Windows account is used for authentication against the XPR server. All password-specific functions in the XPR server are deactivated. After you have selected this option, the next installation step is to choose the Windows accounts to serve as XPR administrator or XPR postmaster (cf. [Section 4.5.6.1, "Login via the Windows User Account", on page 106](#)).

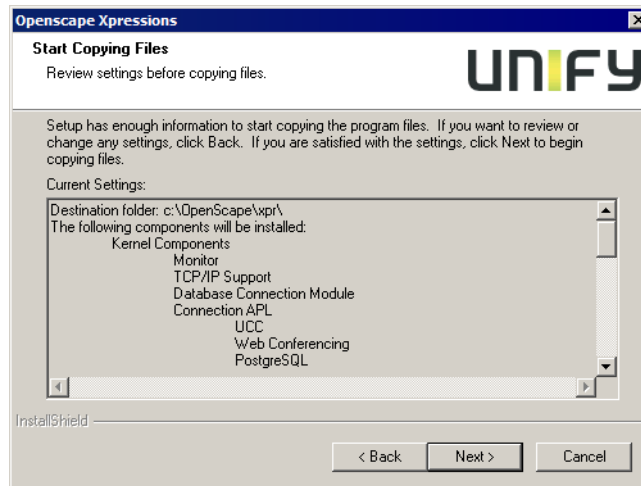
Login via XPR account (user name + password (PIN))

With this authentication method, user accounts for the XPR administrator and the XPR postmaster are created in the XPR database. It is still possible though to activate the authentication via the Windows user account for some users in hindsight. In the next installation step you need to specify a name and password for the administrator and the postmaster of the XPR server each (cf. [Section 4.5.6.2, "Login via XPR Account", on page 107](#)).

Then click on **Next**. Up comes this dialog:

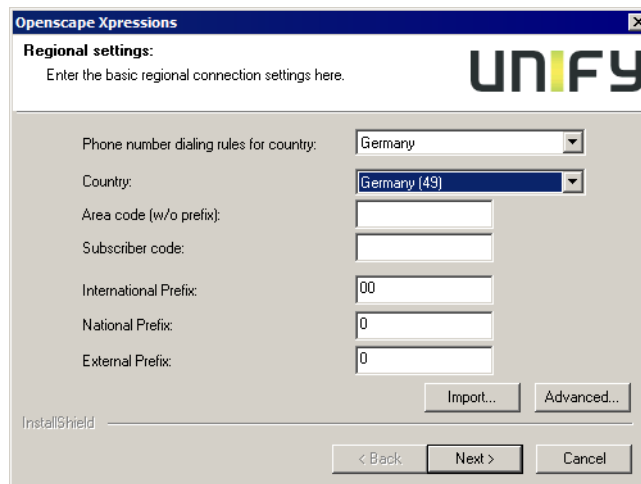
Configuring OpenScape Xpressions as Voice-only System

PRI/Eicon Nortel Meridian QSIG Installation

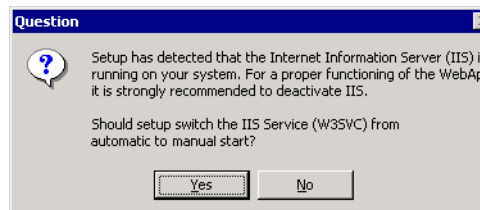


9. Check the listed options and click on **Next**. The copying process begins. A status dialog informs you about the installation progress.

Up comes this dialog:

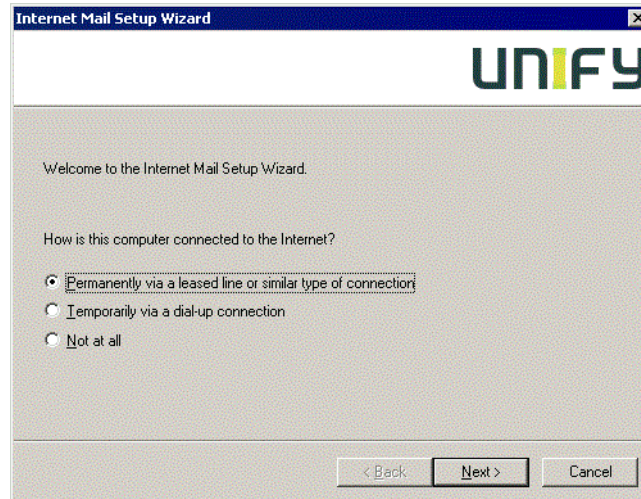


10. In the **Phone number dialing rules for country** field select the country in which the system is to be set up.
11. Enter the area code (without prefix) and the subscriber number. Then click on **Next**.
12. If the Internet E-mail server has been selected as option and the Windows Internet Information Server (IIS) has been installed and activated on the computer, the following dialog appears:

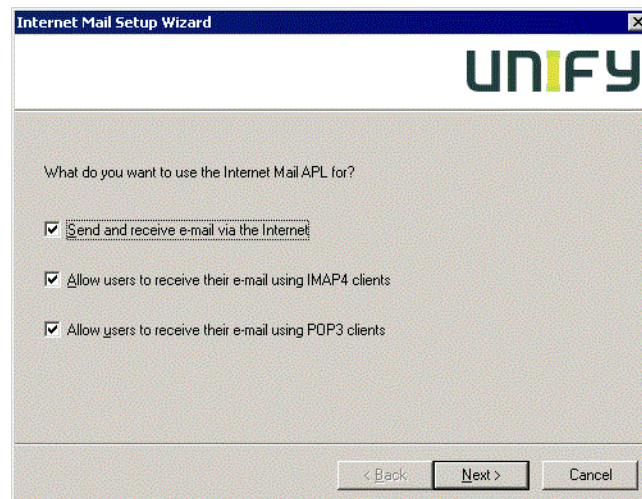


Confirm this dialog with **Yes**.

If the Internet Information Server has not been installed on the computer, the following dialog appears:



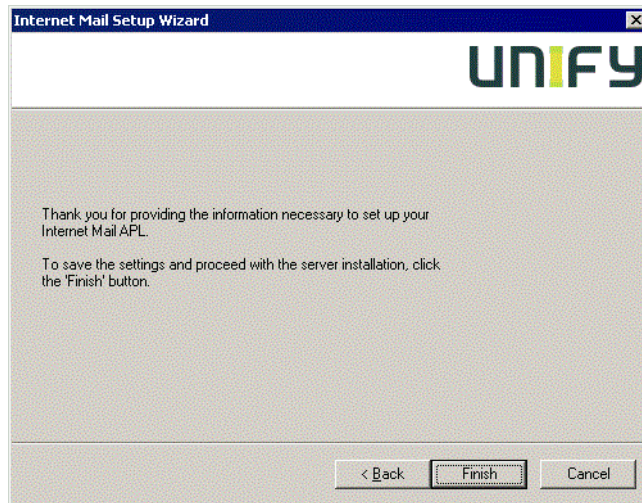
- a) Select the **Permanently via a leased line or similar type of connection** option, then click on **Next**. Up comes this dialog:



- b) Verify that **all options are selected** and click on **Next**. Up comes this dialog:

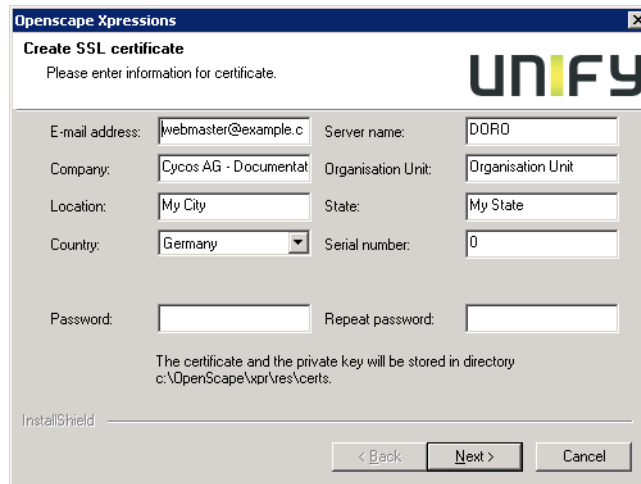
Configuring OpenScape Xpressions as Voice-only System

PRI/Eicon Nortel Meridian QSIG Installation



c) Click **Finish**. Up comes this dialog:

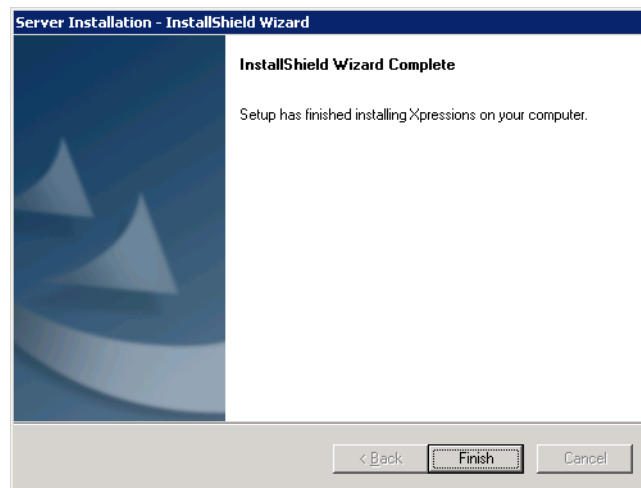
13. The SMTP APL setup is completed. Up comes this dialog:



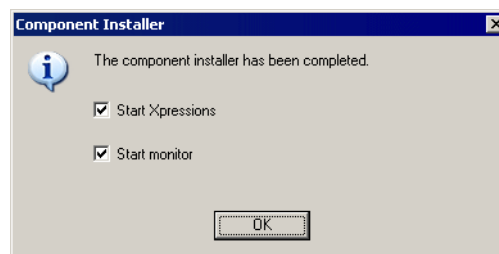
14. In the dialog's fields make the specifications that are to become elements of the certificate. In the **Password** field enter a sufficiently complex password and repeat this specification in the **Repeat password:**. Then click on **Next**.

IMPORTANT: 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.

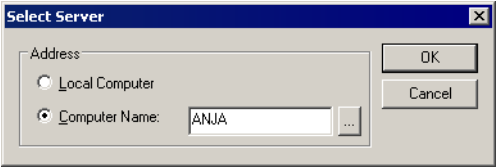
Up comes this dialog:



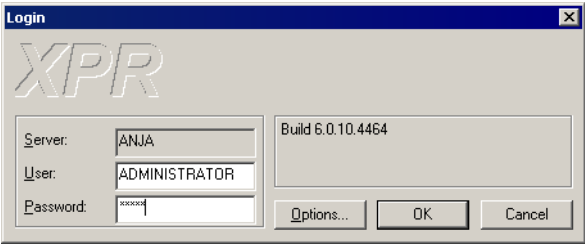
15. Click **Finish**. You may have to click **Finish** several times depending on the selected options. The server setup is thus complete.
16. The selected language packets and other components will now be installed. These installations occur automatically, so that you need not make any entries. As soon as all installations are complete, the following dialog appears:



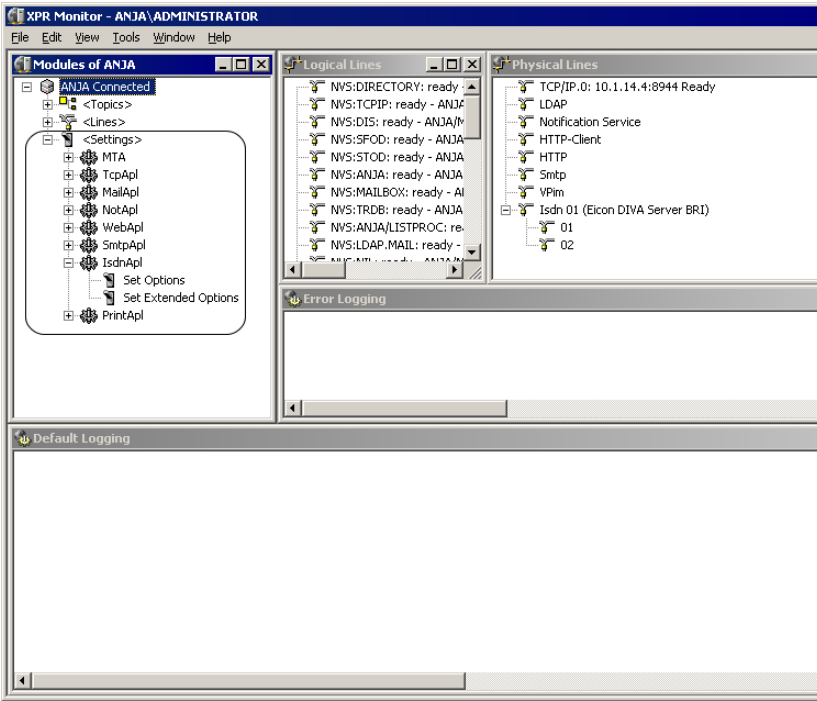
17. Select the options **Start HiPath Xpressions** and **Start monitor** and click on **OK**. Up comes this dialog:



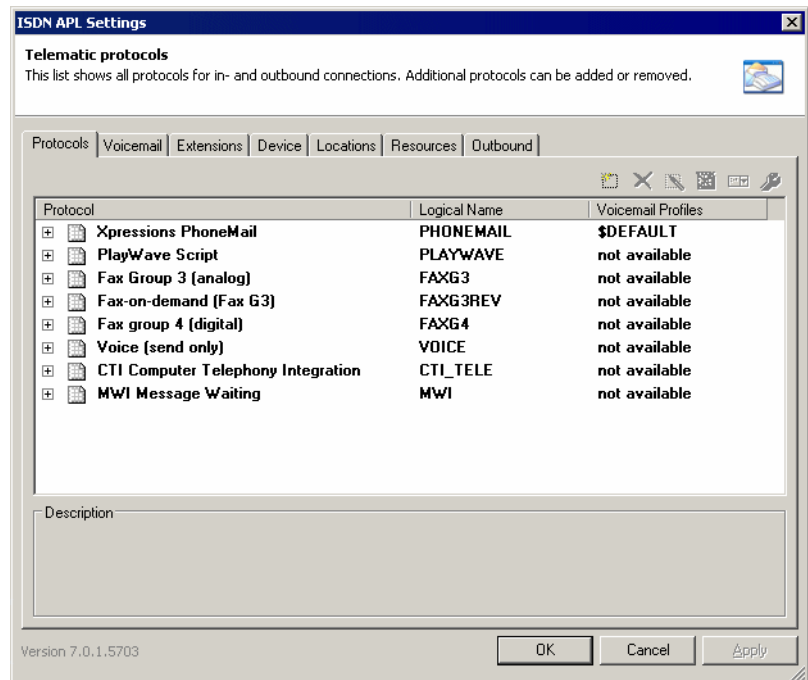
18. Enter or browse the Xpressions server name, then click **OK**. The monitor login dialog opens:



19. Log on to the XPR monitor as **Administrator**, then click on **OK**. The monitor opens:

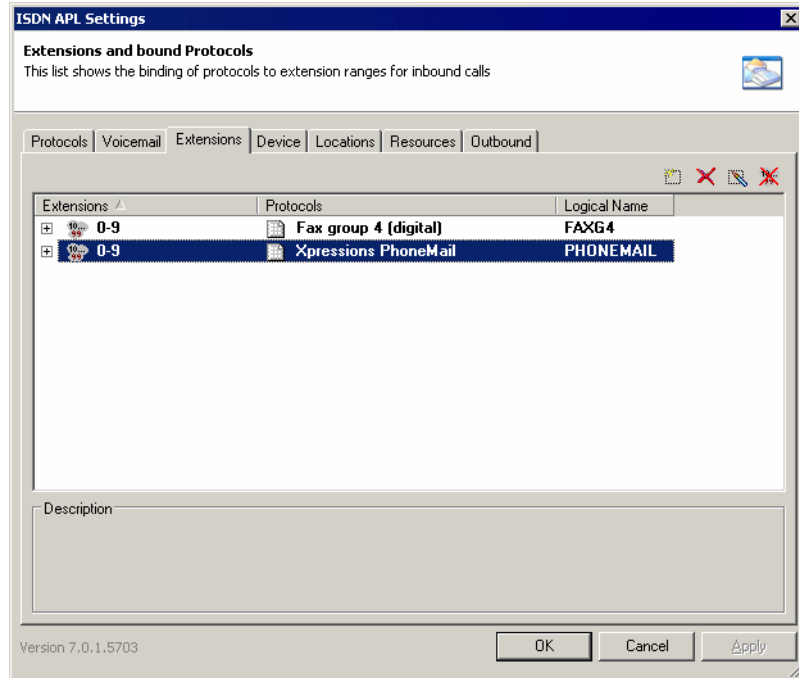


20. In the **Modules of <Xpressions Server>** window under **<Settings>** expand the **IsdnApl** entry and doubleclick **Set Extended Options**. Up comes this dialog:

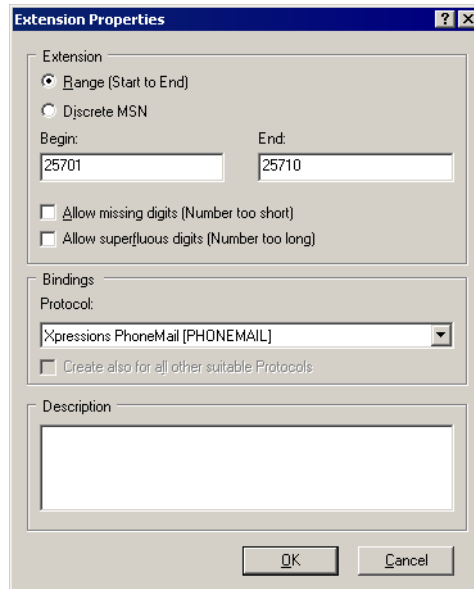


21. Check whether the **Protocols** tab shows all protocols displayed above. Verify that the *CTI_TELE*, *MWI*, *PHONEMAIL*, *PLAYWAVE*, and *VOICE* protocols are displayed at any rate.

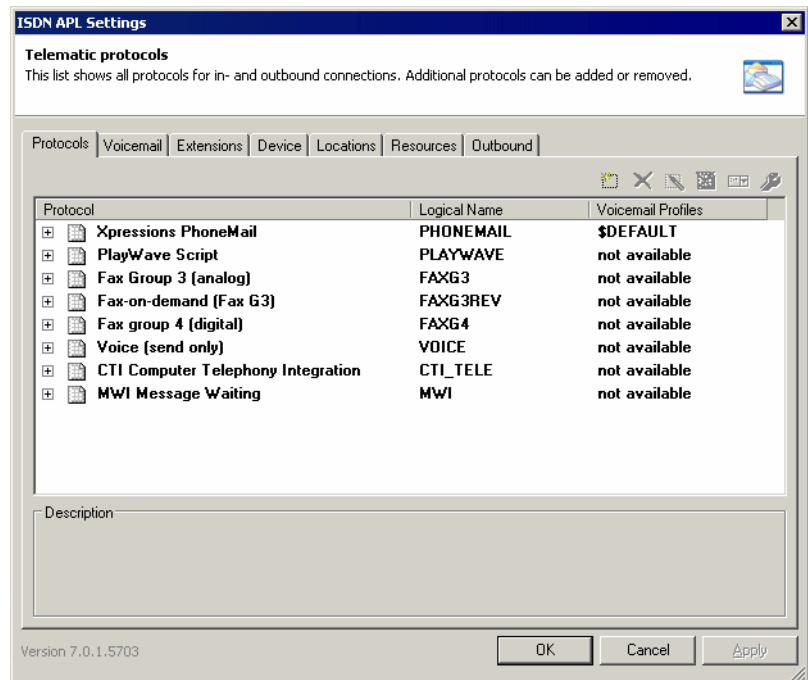
22. Switch to the **Extensions** tab, then double-click **Xpressions PhoneMail**.



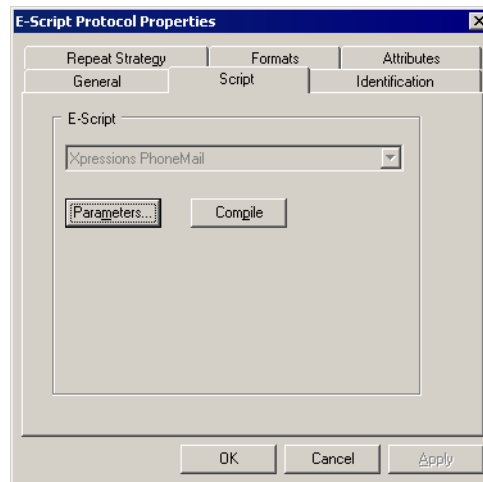
Up comes this dialog:



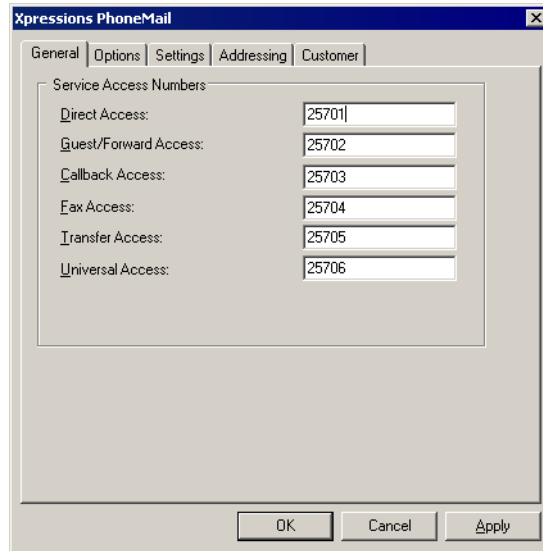
23. In the **Extensions** field enter the first and last digit only for the ACCESS NUMBERS, then click on **OK**. The dialog closes and you return to the following dialog:



24. Open the **Protocols** tab and doubleclick the **Xpressions PhoneMail** entry. Up comes this dialog:



25. Open the **Script** tab and click on the **Parameters** button. Up comes this dialog:

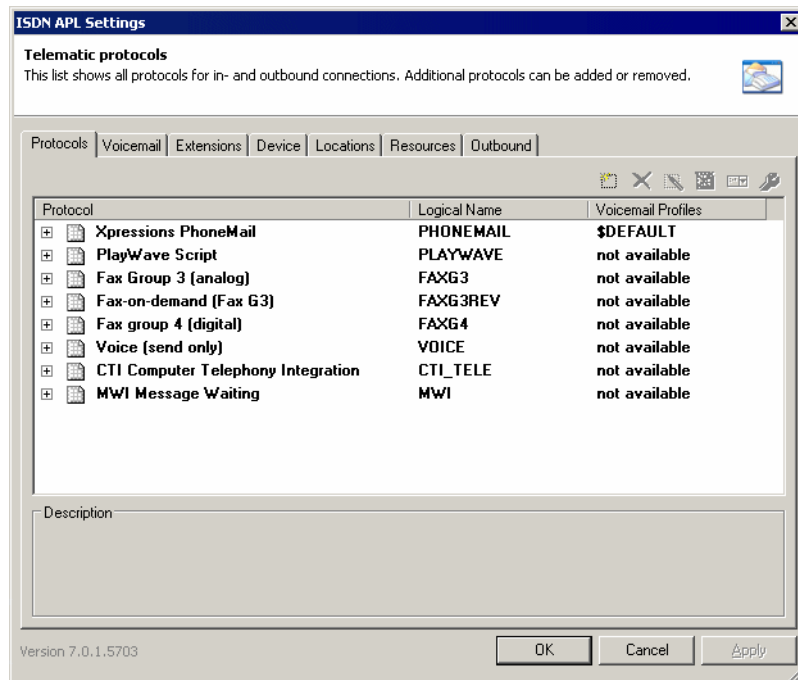


The dialog box is titled "Xpressions PhoneMail" and has tabs for General, Options, Settings, Addressing, and Customer. The "Settings" tab is selected. Under the "Service Access Numbers" section, there are six input fields with the following labels and values:

Label	Value
Direct Access:	25701
Guest/Forward Access:	25702
Callback Access:	25703
Fax Access:	25704
Transfer Access:	25705
Universal Access:	25706

At the bottom of the dialog are buttons for OK, Cancel, and Apply.

26. Enter the **Service Access Numbers** and click on **OK**.
27. Click on **OK** again to close the **E-Script Protocol Properties** window. You return to the following dialog:

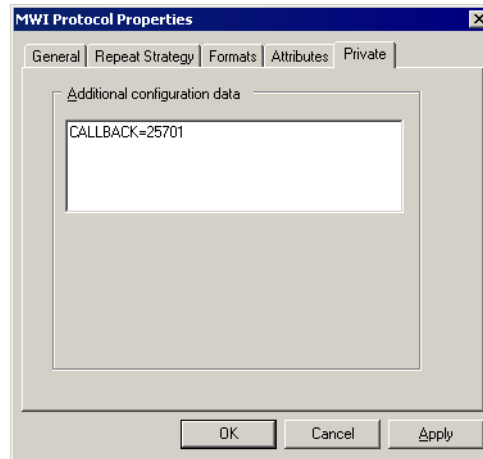


The dialog box is titled "ISDN APL Settings" and has tabs for Protocols, Voicemail, Extensions, Device, Locations, Resources, and Outbound. The "Protocols" tab is selected. Below the tabs is a table of protocols:

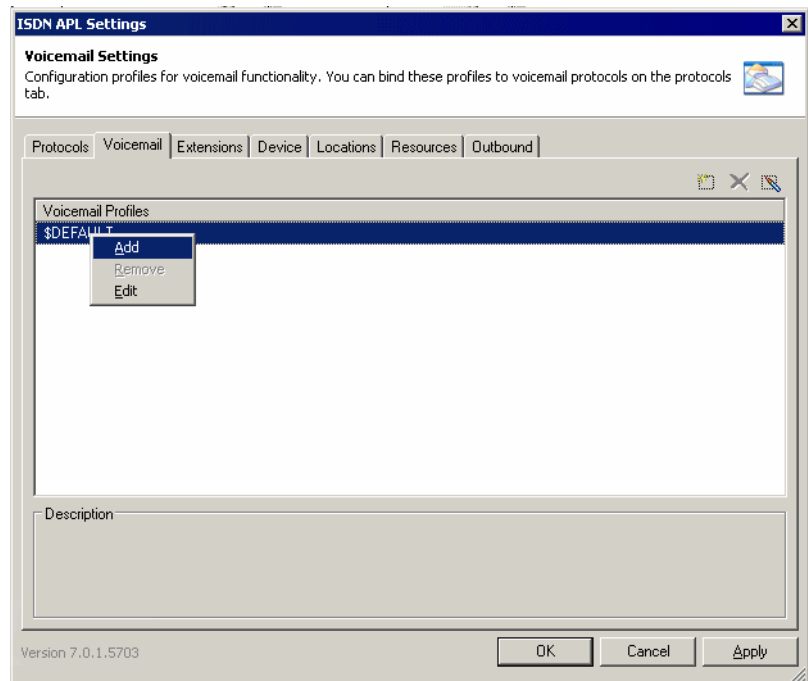
Protocol	Logical Name	Voicemail Profiles
Xpressions PhoneMail	PHONEMAIL	\$DEFAULT
PlayWave Script	PLAYWAVE	not available
Fax Group 3 (analog)	FAXG3	not available
Fax-on-demand (Fax G3)	FAXG3REV	not available
Fax group 4 (digital)	FAXG4	not available
Voice (send only)	VOICE	not available
CTI Computer Telephony Integration	CTI_TELE	not available
MWI Message Waiting	MWI	not available

Below the table is a "Description" field. At the bottom of the dialog are buttons for OK, Cancel, and Apply. The version number "Version 7.0.1.5703" is displayed in the bottom left corner.

28. Open the **Protocols** tab and doubleclick the **MWI** entry. Up comes this dialog:



29. Open the **Private** tab, enter the PBX callback number and click on **OK**. Up comes this dialog:



Configuring OpenScope Xpressions as Voice-only System

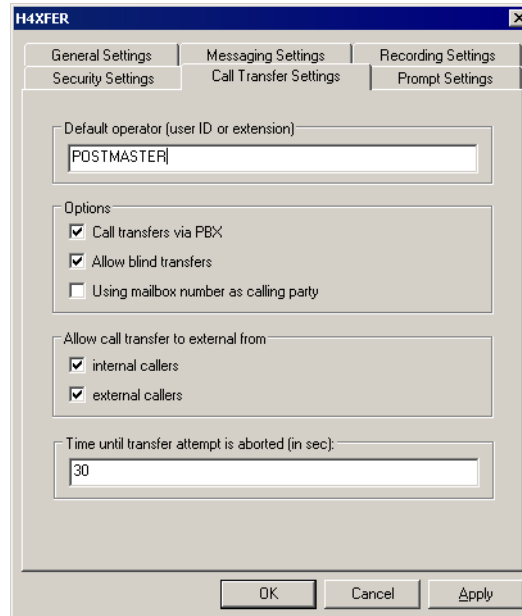
PRI/Eicon Nortel Meridian QSIG Installation

30. Open the **Voicemail** tab, click with the right mousebutton on the **\$DEFAULT** entry and select **Add** in the context menu. Up comes this dialog:

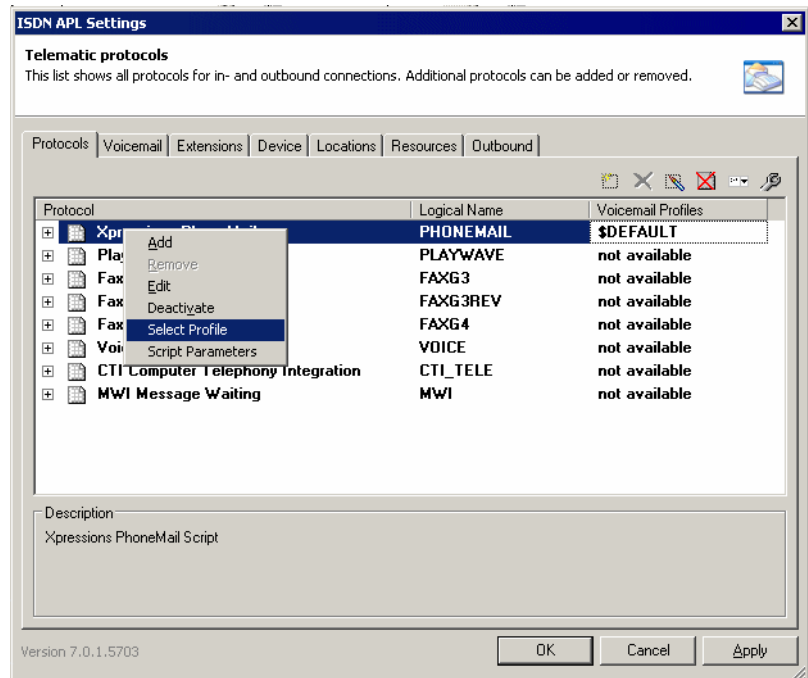
The screenshot shows a Windows-style dialog box titled "H4XFER". It has a tabbed interface with the following tabs: "Security Settings", "Call Transfer Settings", "Prompt Settings", "General Settings", "Messaging Settings", and "Recording Settings". The "General Settings" tab is currently selected. Inside the dialog, there is a "Note" section stating: "Note: Some of these parameters are only supported by certain voice mail systems. Please refer to the product documentation for an overview of the relevant parameters." Below the note, there are three main input areas: 1. "Profile name" with a text box containing "H4XFER". 2. "Voicemail data path" with a text box containing "\\ANJA\MrsUserdata\$\vmdata" and a "Browse ..." button to its right. 3. "Alternative warn prompt" with an empty text box. At the bottom of the dialog are three buttons: "OK", "Cancel", and "Apply".

31. Open the **General Settings** tab and enter *H4XFER* in the **Profile name** field.
32. Open the **Call Transfer Settings** tab and,
33. If it does not already exist, enter the user ID or the extension of the **default operator**.
34. Select the **Allow blind transfers** option.

35. Verify that the **internal callers** and **external callers** options in the **Allow call transfer to external from** section are active.



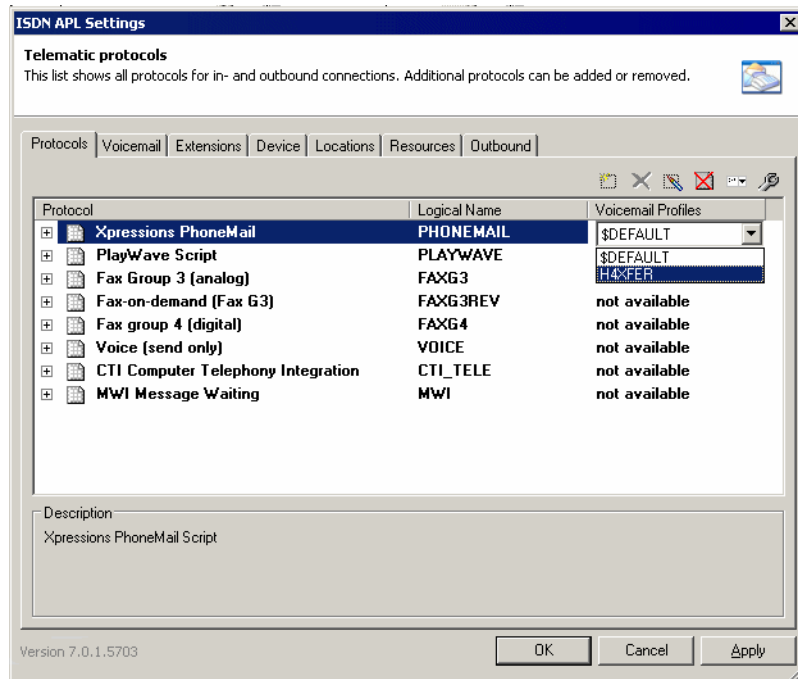
36. Click on **OK** to close the profile configuration. You return to the following dialog:



37. Open the **Protocols** tab, click with the right mousebutton on the **Xpressions PhoneMail** Entry and select **Select Profile** in the context menu.

Configuring OpenScope Xpressions as Voice-only System

PRI/Eicon Nortel Meridian QSIG Installation



38. Open the **Voicemail Profiles** pull-down menu and select **H4XFER**.
39. Click on **OK** to close the **ISDN APL Settings** window.
40. Proceed to [Section C.8, "System Test and Troubleshooting"](#).

C.8 System Test and Troubleshooting

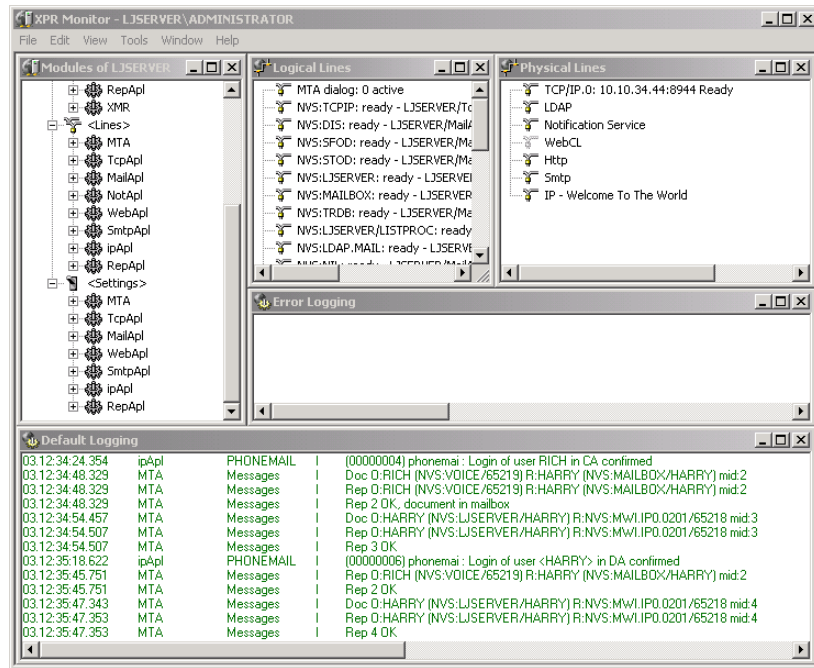
C.8.1 Create Test Users

NOTE: For detailed information about the creation of a user using the Web Assistant, please refer to the *OpenScape Xpressions Web Assistant* manual.

1. Open the **Web Assistant** and log on as **Administrator**.
2. Select the **User administration** entry in the **Server settings** menu.
3. Select the entry **Create new user** in the topmost pull-down menu and click the **Execute** button.
4. Enter the user's ID and voice number. Then click **Create**.
5. Enter a password in the **Password** field (for the GUI), and in the **PIN** field specify a PIN (for the TUI). Leave the other settings unchanged and click on **Save**.
6. Click on **Continue**.
7. Create another user. To do so, follow the steps [3](#) to [5](#).
8. Make sure that both new users are displayed in the **user list**
9. In the list of users click the **Postmaster** entry.
10. In the **Voicemail** field enter a valid extension for the postmaster, then click on **Save** and eventually on **Next**.
11. Test the system now (cf. [Section C.8.2, "Testing the System"](#), on page 384).

C.8.2 Testing the System

1. Place a test call to the new user created. Record a message and send the message to the user.
2. Check for proper MWI indication on the test phone.
3. Listen to the message. Then delete it.
4. Check that the MWI indication disappears.
5. In the **Default Logging** window, note these four distinct events have been logged accordingly.



6. Installation is working properly.

C.8.3 Troubleshooting Hints

Key tools used in troubleshooting:

1. Xpressions monitor
2. Windows Event Viewer
3. Services Window

C.8.3.1 Start-up Problems

- APLs configured incorrectly
- Missing E-scripts or incorrect E-scripts applied to the protocols
- Typos in the APL configuration
- Required services up and running or not up and running
- Failing integration cards
- Incorrect PBX settings
- Log-on privileges - Local and Domain
- Customer-provided server is incorrectly configured
- Missing Xpressions components - re-run the installation CD in a modify mode to verify components installed

C.8.3.2 Cannot Access Xpressions

PBX Systems Issues

- PBX configuration
- PBX card down
- Bad line to the PBX or cable defect

Xpressions Issues

- Insufficient voice ports
- Traffic load issues
- Defective integration card in Xpressions server
- Invalid user ID/server configuration
- Windows Server 2008 Local Admin privileges problems
- Active port availability through monitor
- Check all active ports of the XPR monitor
- Check Services window for activity or inactivity
- Check Event Log for integration/port trouble

C.8.3.3 TUI

- Cannot send/receive messages
- Callback extension not configured in APL
- User extension on configured in APL/User profile

C.8.3.4 MWI Light Indication

- MWI will not light due to the MWI protocol in the APL not being configured properly or the callback number was not entered in the script parameters.

D PBX Connection Variants for OpenScape Xpressions

This chapter describes the OpenScape Xpressions connections to the following telephone systems:

Hicom 300 / 300E (CorNet-N)	(Cf. Section D.1, "Connecting CorNet-N to Hicom 300/Hicom 300 E/H" , on page 388)
HiPath 3000 (CorNet-N)	(Cf. Section D.2, "Connecting HiPath 3000 (CorNet-N)" , on page 413)
HiPath 3000 (CorNet-IP)	(Cf. Section D.3, "Connecting HiPath 3000 (CorNet-IP)" , on page 432)
HiPath 4000 V6 and OpenScape 4000 V7 / V8	(Cf. Section D.4, "Connecting HiPath 4000 V6 and OpenScape 4000 V7 / V8" , on page 455)
OpenScape Voice V7 (SIP)	(Cf. Section D.5, "Connecting OpenScape Voice V7 (SIP)" , on page 496)
OpenScape Voice V8 (SIP)	(Cf. Section D.6, "Connecting OpenScape Voice V8 (SIP)" , on page 502)
OpenScape Voice V9 (SIP)	(Cf. Section D.7, "Connecting OpenScape Voice V9 (SIP)" , on page 502)
Alcatel OmniPCX Enterprise	(Cf. Section D.9, "Connecting an Alcatel OmniPCX Enterprise (OXE) via IP APL" , on page 508)
Mitel 3300 ICP	(Cf. Section D.10, "Connecting a Mitel 3300 ICP" , on page 515)

NOTE: Hicom 150 E/Office/H, 200 are no longer supported. Such systems are used and connected at one's own risk.

NOTE: Fax documents can be transmitted in the following ways:

- Via the ISDN APL (classic fax)
- By G.711 via the IP APL (fax as tones)
- By T.38 via the IP APL (fax as data)

G.711 and T.38 can be transmitted via the IP APL via H.323, SIP or CorNet-IP, but not via TAPI.

The IP APL with CorNet-IP **does not** support the following features:

- Digit-by-digit dialing information transmission (suffix dialing)

If case of a digit-by-digit dialing information transmission the first call sign received is already evaluated. If the dialing information is transmitted block-by-block, a received phone number is not further processed until the entire

PBX Connection Variants for OpenScape Xpressions

Connecting CorNet-N to Hicom 300/Hicom 300 E/H

phone number is received. The PBX must be set to either block-by-block or digit-by-digit dialing information transmission. In contrast, no settings need to be made in the IP APL.

- Callback if busy (CCBS; Completion of Calls to Busy Subscriber)

A caller who receives a busy sign from his/her callee can request this feature via his/her telephone's keypad before putting the phone down. When the previously busy callee puts his/her phone down, the caller's telephone is informed about this by a special ringtone. If the caller answers this return call by picking up the receiver, the callee is called again.

- Callback if no reply (CCNR; Completion of Calls on No Reply)

A caller whose call is not accepted can request this feature via his/her telephone's keypad before putting the phone down. When the callee puts the phone down the next time, the caller's telephone is informed about this by a special ringtone. If the caller answers this return call by picking up the receiver, he/she is reconnected to the desired callee.

- Hicom PIN

If you call the XPR server access number you need to enter a PIN for logging on. The HiCom-PIN feature means that you only need to perform this logon process once a day. In case of a second call you are logged on without being prompted to enter a PIN.

- Remote activation of a call diversion

Remote activation of a call diversion means that you, for example, call the access number of the XPR server TUI from your private phone to activate a call diversion to your own business phone by TUI.

D.1 Connecting CorNet-N to Hicom 300/Hicom 300 E/H

D.1.1 Introduction

This chapter describes all of the steps you need to carry out in order to optimally implement the OpenScape Xpressions product with its various configuration options in a customer environment with Hicom 300 and/or Hicom 300 E/H communication systems.

D.1.2 Connecting Hicom 300

The following two figures represent the major connecting options of the components Hicom 300 (E/H) and OpenScape Xpressions. There are two different scenarios:

- Case 1: S_2 connection to Hicom 300 (E/H) for voice, fax and Unified Messaging
- Case 2: S_0 connection to Hicom 300 (E/H) for voice, fax and Unified Messaging

D.1.2.1 Hardware/Software Requirements

Case 1: For the S_2 connection

In this case the physical connection between the OpenScape Xpressions product and the Hicom 300 and Hicom 300 E/H communication systems is set up via digital S_2 tie trunks with the CorNet-N networking protocol.

A free S_2 port on a DIUS2 module is therefore required for Hicom 300 systems.

A free S_2 port on either a DIUS2, DIUN2 or DIUN4 module is required for Hicom 300 E/H systems.

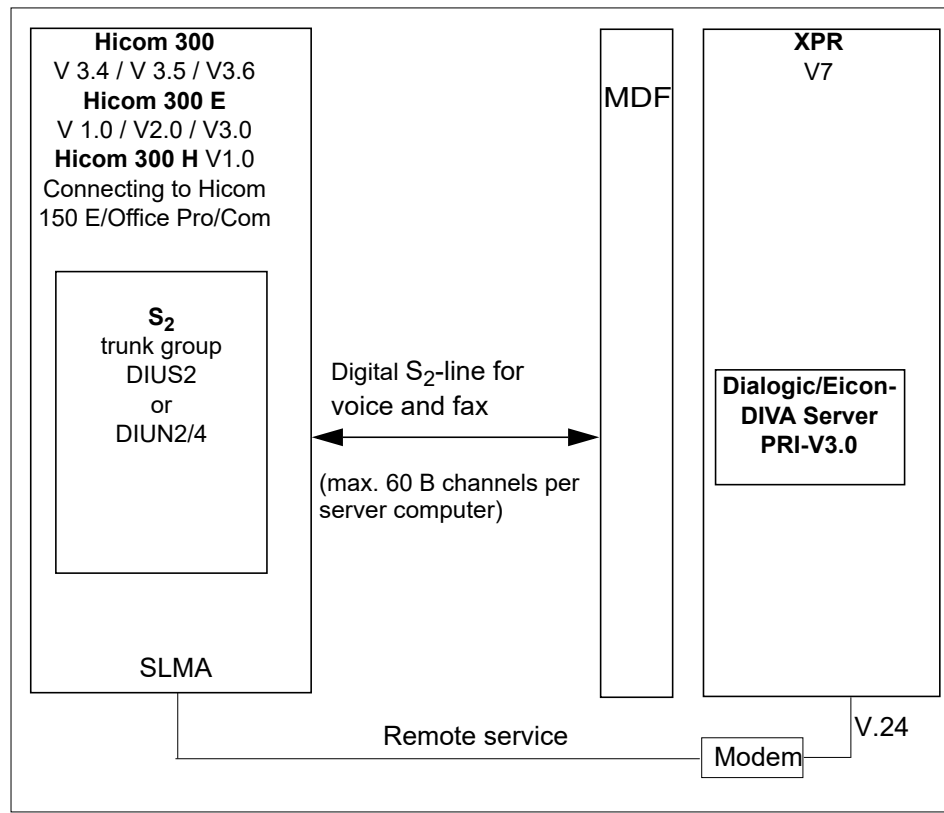
Hicom 300 systems running software version V3.4 SA11 and Hicom 300 E/H systems from version V1.0 or higher are supported. A specific software release is not required.

The licenses required for basic telephone and networking functions in the case of a Hicom 300 E/H are provided automatically by the configuration (L30220-Z622-A811/-L806/-L827).

The OpenScape Xpressions features (such as callback access) can be used from all telephone extensions in a digital Hicom 300 network running software version V3.4 or higher.

PBX Connection Variants for OpenScape Xpressions

Connecting CorNet-N to Hicom 300/Hicom 300 E/H



The Dialogic/Eicon DIVA Server PRI-V2.0 module is default-used for the S₂ connection to the Hicom on the OpenScape Xpressions side independently from the number of ordered B-channels for voice, fax and Unified Messaging operation.

Case 2: For the S₀ connection

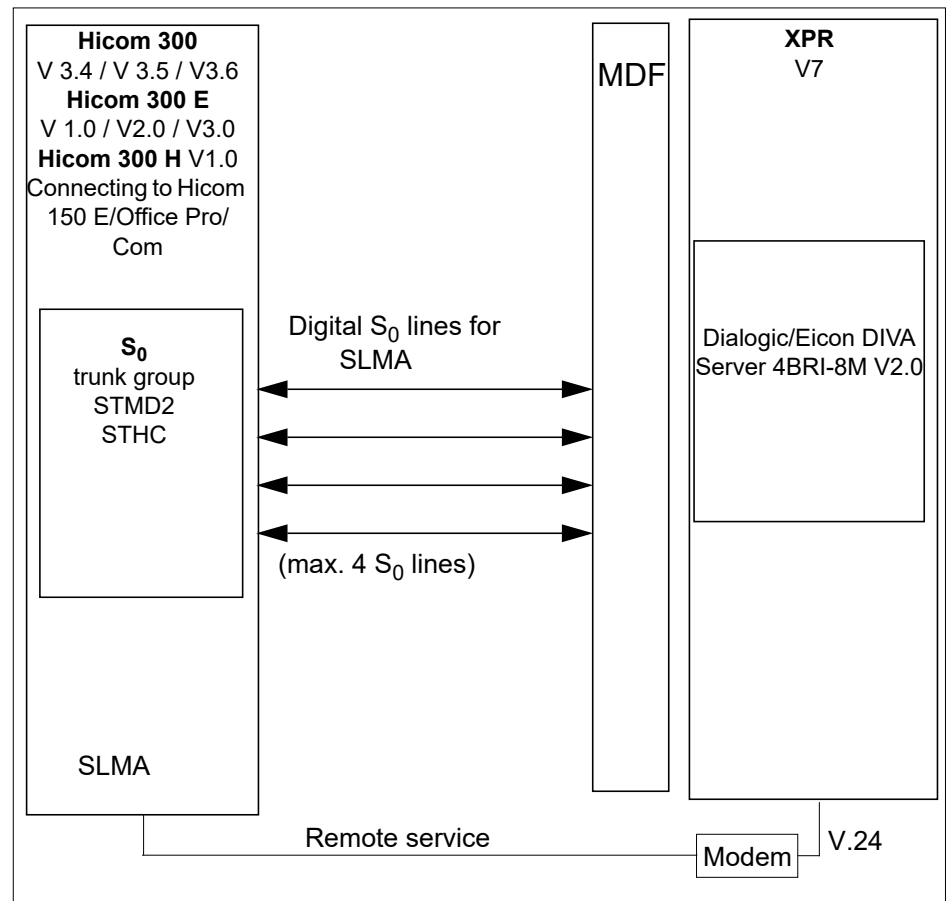
In this case, the physical connection between the OpenScape Xpressions product and the Hicom 300 and Hicom 300 E/H communication systems is set up via up to 4 digital S₀ cross connections with the CorNet-N (U.S.: CorNet-T) networking protocol.

Up to four free S₀ ports are required on an STMD module for Hicom 300 systems

Up to four free S₀ ports are required on an STMD, STMD2 or STHC module for Hicom 300 E/H systems.

PBX Connection Variants for OpenScape Xpressions

Connecting CorNet-N to Hicom 300/Hicom 300 E/H



Hicom 300 systems running software version V3.4 SA11 or higher and Hicom 300 E/H systems with version V1.0 or higher are supported in the case of the S₀ link.

The licenses required for basic telephone and networking functions in the case of a Hicom 300 E/H are provided automatically by the configuration (L30220-Z622-A811/-L806/-L827).

The OpenScape Xpressions features (such as callback access) can be used from all telephone extensions in a digital Hicom 300 network running software version V3.4 or higher.

Dialogic/Eicon DIVA Server BRI-2M-V2.0 / Dialogic/Eicon DIVA Server 4BRI-8M-V2.0 modules are always used on the OpenScape Xpressions side for the S₀ connection to the Hicom depending on the number of ordered (max. 8) channels.

D.1.2.2 OpenScape Xpressions Access Numbers

The selection of a OpenScape Xpressions application via the telephone user interface is generally made by analyzing the transmitted B user number (= access number). For fax applications, the B-user number can sometimes be used to directly address a mailbox.

For customized applications such as all Fax-on-Demand applications, for example, the required numbers can be selected from an assigned set of numbers.

Virtual numbers/users in Hicom 300 are not required for an S₀ or S₂ link with CorNet-N.

For standard messaging applications, on the other hand, a set of numbers is assigned logically rather than numerically. These are:

- **Forward access number**

CFW must be configured on this number for each individual user who has set fixed or variable call forwarding or who has set forward no answer to his/her mailbox in OpenScape Xpressions for all voice connections. This setting can be made either by the administrator (AMO ZIEL) or it can be made individually using the telephone.

For OpenScape Xpressions V7 the "Forward Access Number" is identical with the "Guest Access Number" and, based on the existence of a "Redirecting Number", the application decides itself whether a "Forwarding Case" or a real "Guest Access" call is involved.

- **Direct access number**

When a mailbox user in OpenScape Xpressions dials the direct access number, this user is given access to all of the OpenScape Xpressions telephone features following successful identification.

- **Guest access number**

When a person who does not have their own mailbox in OpenScape Xpressions dials the guest access number, this person is given access to a restricted selection of features compared to those available through direct access (for example, for leaving a message in any mailbox).

- **Callback access number**

The callback access number gives a mailbox owner in OpenScape Xpressions brief access (in comparison to direct access) to his/her new messages. The callback access number must be configured for the generic server mailbox in the Hicom 300 and is used implicitly with the Hicom function "New Message".

- **Fax access number**

The fax access number is the analogue of the forward access number but exclusively effective for the Fax Group 3 service. Creating a fax access number is not mandatory for all Hicom 300 configurations (see [Section D.1.4.3, “Fax Messaging Aspects”, on page 401](#)).

The number must be fixedly set as call rerouting target for all Hicom 300 subscribers allowed to use the fax service without having an individual fax device but merely a mailbox in OpenScape Xpressions.

The structure of all access numbers for OpenScape Xpressions must comply with certain rules for the Hicom 300.

First, however, comes a short definition of the terms “Open” and “Closed Numbering”.

Open numbering

Open numbering means that the single systems of a Hicom network are independently numbered. Each system has its own set of numbers. A number is therefore only unique within a single system. If a connection is established between two systems, the number must be prefixed by a route ID. When a number belonging to a user within the same system is dialed, the route ID for this system can also be dialed. During digit analysis, the system recognizes that the destination being dialed lies within the same system and ignores the route ID. Since the introduction of least cost routing, a number in international format can also be used.

Closed numbering

With closed numbering, all numbers are uniquely assigned network-wide. The network behaves like a large PBX.

Hicom with OpenScape Xpressions represent a combined system with closed and open numbering.

To minimize the administration effort in the Hicom or especially in Hicom networks the OpenScape Xpressions product is connected via CorNet-N according to the basic rules of open Hicom numbering. In order to minimize the administrative effort required in the Hicom or, more specifically, in Hicom networks, the connection of the OpenScape Xpressions product via CorNet-N is based on the basic rules of open Hicom numbering.

Example: For conventional five-digit closed Hicom numbering, the route ID could be 950, for example, and the last two digits could then be used for any OpenScape Xpressions applications. For example 10 for forward access, 11 for direct access and 20 for the first fax-on-demand application. The Hicom should be set up in a way that the route ID is not transmitted as well. Numbers of this type, for example 88, may also represent server mailboxes the numbers of which are unknown in the Hicom. In general, the Hicom 300 system will route all calls with numbers between 95000 and 95099 to OpenScape Xpressions. There is no fixed assignment of these numbers to the ports bought in OpenScape Xpressions.

D.1.2.3 General Notes for the Configuration with S₀/S₂ Connection

As outlined in [Section D.1.2.2, “OpenScape Xpressions Access Numbers”](#), OpenScape Xpressions is connected to the home-PBX Hicom 300 via a route ID; e. g. by means of open numbering. A Hicom 300 can always only be connected via S₀ or S₂ interface.

IMPORTANT:

Please note that the current version V7 of OpenScape Xpressions only supports Hicom nets with closed numbering. This means that for larger networks, a separate OpenScape Xpressions server is required for each subnet with closed numbering. Multiple OpenScape Xpressions servers can then be networked together via RSL as a project-specific solution.

When dealing with voice, fax and data communication via Hicom 300/300 E, note that this Hicom system is not transparent against the various services but allows individual settings for each single service; e. g. different call reroutings for a single phone number only depending on the service. The resulting consequences are considered in more detail in [Section D.1.4.3, “Fax Messaging Aspects”](#), on page 401.

The charges detail recording for outgoing connections from OpenScape Xpressions e.g. into the public network is realized by the Hicom PBX that includes the trunk interfaces. In such cases, OpenScape Xpressions ensures that the mailbox user incurring the charges is always entered as the A user of the connection. In such cases, OpenScape Xpressions ensures that the mailbox user bearing the charges is always entered as the A user of the connection.

Incoming calls for a user who has forwarded to OpenScape Xpressions can be recorded by number by the Hicom 300 call charge registration function.

The OpenScape Xpressions telephone user interface consistently uses in homogeneous Hicom 300 networks and with connecting OpenScape Xpressions via CorNet-N interface the character and display transmission via D-channel while e. g. from outside or specific telephone devices MFV characters are used.

The attendant consoles on the Hicom 300 V3.5 or E V1.0 or higher can also use the features of OpenScape Xpressions directly.

In the case of the S₀ and S₂ connection, the OpenScape Xpressions MWI is completely integrated in the Hicom 300 mailboxes and is available throughout the entire network via CorNet. If new messages are available, a user can be directly connected to the relevant mail server (callback access).

In contrast with Hicom VMS, TCS or FMS connection or integration over S₀, the message waiting indication for the Hicom 300 is restart-tolerant in the case of OpenScape Xpressions with an S₀/S₂ connection.

D.1.2.4 Integration Features through the Use of CorNet-N

The **CorNet-N** protocol, specific for the Unify GmbH & Co. KG, allows using the following features for the connection of OpenScape Xpressions to Hicom 300/300 E via S_0 or S_2 :

- Phone number of the caller
- Called user's number
- Transfer of the services (voice, Fax G3, data,...)
- Exchange of end system skills by means of classmarks
- Information transfer relating to external/internal call
- Transfer of the basis for call forwarding (fixed/variable CFW) or forwarding no answer (CD) or forwarding on busy
- Transfer of the number of the user who was originally called in the case of call forwarding (CFW)/forwarding no answer (CD) (number of the forwarder)
- Consultation via only one connection (log. remote transfer)
- Server control via keypad within a digital Hicom 300 network
- Connection-associated user signaling via telephone display
- Setting or deleting the message waiting indication (MWI) by assigning a B-channel

D.1.2.5 Configuration of the S_0/S_2 Interfaces to OpenScape Xpressions

The connection of the OpenScape Xpressions server to the systems Hicom 300/300 E/300 H is performed via an ISDN S_0 or S_2 connection as subsystem and with the tie line.

A S_2 connection on the Hicom side therefore requires a module DIUS2, DIUN2 or DIUN4 with a free S_2 port or in case of the S_0 connection a module STMD, STMD2 or STHC with up to 4 free S_0 ports.

On the OpenScape Xpressions side an Dialogic/Eicon DIVA Server PRI-V2.0/3.0 is used for physically coupling the Hicom based on S_2 . For the S_0 coupling, modules of type Dialogic/Eicon DIVA Server BRI-2M-V2.0 or Dialogic/Eicon DIVA Server 4BRI-8M-V2.0 are used on the OpenScape Xpressions side.

The wiring is in 4-wire format via the main distribution frame (MDF). On the OpenScape Xpressions side, an RJ-48C jack with a special pin layout is required for the S_2 connection. Standard RJ-45 jacks are used for the S_0 -connection.

PBX Connection Variants for OpenScape Xpressions

Connecting CorNet-N to Hicom 300/Hicom 300 E/H

The number of B-channels ordered on the OpenScape Xpressions side must at any rate be identically configured on the Hicom side. All tie trunk B-channels are combined to a trunk group used in both directions. Therefore we recommend to configure a linear (non-cyclic) trunk group usage and to define an adverse starting point for both sides to minimize possible call collisions. Specific configurations such as connecting a OpenScape Xpressions server with two different trunk modules or even Hicom systems (e. g. for security reasons) requires special optimizations.

OpenScape Xpressions V7 with integrated Dialogic/Eicon boards supports the services *Voice* and *Fax G3*; 64 KBit data transparent is not supported.

AMO	Essential AMO Parameters	Significance/Notes
DIMSU	TYP=CC, ... TYP=LTG, ...	Define dimensioning data SWU
COT	COTNO= <i>new</i> DFNN= NO LWNC= NO NLCH= YES NLHT= YES CFOS= YES	Class of Trunk for correct charge recording in Hicom 300 and correct routing for music-on-hold while recoupling Programing the call rerouting possible for other subscribers
COP	COPNO= <i>new</i>	Class of Parameter
WABE	CD= DAR=TIE	Defines digit analysis
BUEND	BUNUM= <i>new</i> NAME="OpenScape Xpressions" ANZ=30 RESERV=N	Combination of lines into groups
BCSU	TYPE=DIU LTG= LTU= SLOT=	Configuration of LTU modules
REFTA	PEN= PRIO=0 BLOCK=N READYASY=N	Edits the reference clock tables
LWPAR	TYPE=DIUS2 QUAL=ON	Parameterizes the loadware (with S ₂ connection <i>only</i>)
TDCSU	OPT=NEWU PEN= COTNO= COPNO= ...	Configures digital lines (per S ₀ /S ₂ port)
LODR	ODR= CMD= <i>ECHO/END</i>	Administration of LCR routings

AMO	Essential AMO Parameters	Significance/Notes
LDAT	LROUTE= LSVC=ALL TGRC= ODR=	LCR routing
LDPLN	LDP= LRTE=	Sets up a sample dialing plan for LCR
RICHT	MODE= <i>LRTENEW/PM</i> LRTE= LSVC= NAME="OpenScape Xpressions"/ "New messages" IDX= SAN=	Defines routes/server numbers

D.1.2.6 Hicom 300 and Hicom 300-E/H Connection Differences

The scope of Hicom 300 CorNet-N features is identical for all Hicom 300 versions from V3.4 SA11 as well as for Hicom 300 E / H from V1.0.

The STMD2 and DIUN2 modules can be implemented in Hicom 300 E V1.0 or higher.

The DIUN4 and STHC modules can only be implemented in Hicom 300 E V3.0 or H V1.0 or later.

A DIUS2 or STMD module is required for all older Hicom 300 systems up to V3.6.

D.1.3 Configuring MWI and Remote Service Access

D.1.3.1 Message Waiting Indication

Message Waiting Indication for all Hicom 300 network subscribers normally occurs via the CorNet-N interface. It is set up using the AMOs SCSU, WABE and ZIEL. The mailbox lamp set in this way is not restart-tolerant in the case of Hicom 300.

To enable the callback access to the subscriber mailboxes in the S_0 configuration, a permanent CFW to the callback access number must be set up in OpenScape Xpressions for the analog port (see also the example).

D.1.3.2 Remote Service Access

The "Remote Service Access for OpenScape Xpressions" feature requires – if desired by the customer – an analog port at the Hicom 300, Hicom 300 E/H for connecting a modem. There are no special settings for this port, it must be released for outgoing and incoming traffic (AMOs SCSU and WABE).

D.1.4 Configuring Hicom 300 Users and Services

D.1.4.1 General Aspects

Some Hicom features that modify the behavior of a user connection can only be used systemwide, and, in the case of Hicom 300 systems, not on a user-specific basis. This includes the feature *forwarding on busy* for voice connections and Fax G3 connections.

In the central Hicom system data (AMO ZAND), the AMO parameter setting CONANS = YES/NO can be used to specify whether or not forwarding on busy is to apply generally. Furthermore, the additional parameter setting COBUSY = YES/NO can be used to specify whether forwarding on busy is to be applied only to calls from the central office (=YES) or generally. If these presets have been made, some "Classes of Service" must be defined and assigned to the single subscribers by means of AMO COSSU, TYPE=COS and parameter DVCE = ..FWDBSY.

NOTE:

For Hicom 300 users who have activated the call-waiting/camp-on feature, Busy is never signaled on the interface to OpenScape Xpressions; Forwarding no answer is signaled instead.

Similar settings are also required for calls to fax devices and group fax numbers. Keep in mind that the descriptions in the previous section are eventually also valid for fax since many fax calls are still signaled from analog devices as voice call. The basic setting "Forward on Busy = YES" and the definition of one or more classes of service, which are assigned exclusively to fax devices or other fax numbers, is therefore advised.

Calls for these fax numbers can be forwarded to an individual user's fax mailbox, to an overflow mailbox or to a stand-by device.

For fax connections signaled under the ISDN service Fax Group 3, it may also be necessary or advisable to make CO interface settings via AMO COT ; parameter COTPAR = ..FAX1&FAX2.. All calls recognizable as fax are then routed to an

alternative number or overflow mailbox also in the busy and vacant case (e. g. no paper). For calls signaled as voice (e. g. from the analog network), the central and individual settings for the voice service must be performed as well.

When connecting over 'Consultation hold on same line', the COTPAR=...KLHT... must be set for the interface to the server in order to feed music-on-hold through the connected Hicom to the party on hold.

So that via OpenScape Xpressions the call forwarding of a subscriber can be modified in the Hicom, the COT parameter AUAT must be set.

The parameters LWNC (line without node number) and DFNN (use default node number of trunk) in the COT to the XPR server must **not** be set so that the call detail recording can cleanly determine the paying party. If LWNC is not set in this case, the Hicom system prevents looping. Since this loop is absolutely authorized in the server interaction (fax transmission and fax forwarding back to the server), the KSLP parameter (no loop check) can be set.

For Hicom 300 network configurations with internal subscribers outside the home PBX of OpenScape Xpressions note that the mailbox access must be configured per Hicom 300 system via AMO RICHT with parameter ART=PM. Also note that with all cross connections by the parameter TSCS in the AMO COT the transmission of message waiting indication reports via temporary signaling connections is enabled.

So that privacy users can check their mailboxes, the following administration steps must be performed in the Hicom:

- In AMO WABE, determine or configure the digit analysis result for **Call line identification on**, e. g. **33
- In AMO RICHT prefix the **PM for OpenScape Xpressions** entry with the digit analysis result, e. g. 12345 -> **3312345

Enter the latter number in the MWI protocol at the DIgApl under **Private** or at the ISDN Apl as callback number under **Parameter**. These settings deactivate the phone number suppression for the MWI feature.

AMO	Essential AMO Parameters	Significance/Notes
ZAND	COBUSY=YES/NO CONANS=YES/NO	Central Hicom 300 system data
COT	PAR=...FAX1&FAX2 PAR=...TSCS... PAR=...NLHT	Class of Trunk (for CO interface) Class of Trunk (for all tie trunks) Class of Trunk (for server connection)
COSSU	TYPE=COS DVCE=...FWDBSY...	Defines the class of service
RICHT	MODE=PM IDX= FAXO= SAN=	Makes entry in service access table (per Hicom in the network)

AMO	Essential AMO Parameters	Significance/Notes
CTIME	FAXOFLPM=	Defines the fax intercept centrally

D.1.4.2 Voice Messaging Aspects

As mentioned in [Section D.1.2.2, "OpenScape Xpressions Access Numbers"](#), the different voice applications in OpenScape Xpressions are selected by specific phone numbers.

The so-called "Forward Access" allows access to the answering machine feature of a subscriber for any caller; while the "Callback Access" allows the mailbox owner to access his/her new messages in the mailbox.

The OpenScape Xpressions marketing aims at assigning a mailbox for voice to all standard Hicom telephone users and at having "Fixed CFW" set up – but not activated – on the forward access number of OpenScape Xpressions when the system is delivered.

By activating and deactivating the fixed call forwarding, the subscriber can then toggle between the fixed forwarding to the box and a temporal call forwarding to the box.

The Hicom 300 feature "Variable CFW" is not required for forwarding calls to OpenScape Xpressions, but can instead be used for the temporary forwarding of calls on an individual basis.

Using the Hicom 300 LM feature "forwarding on busy" should depend on the individual customer scenario. If, for example, the customer is operating in a predominantly digital ISDN environment in which the callback feature is used frequently, it may be useful not to have the function for forwarding to the answering machine on busy activated.

The setting up of forwarding on busy for CO calls (not internal calls) is still recommended as the default for voice messaging (CONANS=YES and COBUSY= YES).

The above basic settings are also recommended for teleworking.

For specific voice subscriber configurations with e. g. several assigned telephones or a stationary telephone and a mobile DECT telephone it is useful to configure only one mailbox for the subscriber's main device which records the messages in all cases. To do this, it is generally necessary to combine the telephones in a hunt group with an overflow to "PhoneMail" or "Voicemail", specifying the mailbox number.

For executive-secretary configurations the standard recommendation is: call rerouting/call forwarding to the mailbox of the first (originally) addressed subscriber (AMO CHESE).

If a OpenScape Xpressions mailbox is available we recommend not to use the Hicom 300 feature “Station Forced Busy” for all Hicom 300 subscribers.

AMO	Essential AMO Parameters	Significance/Notes
ZIEL	TYPE=FWD SRCNO= SI=VOICE DESTNOF=	Assigns destination numbers

D.1.4.3 Fax Messaging Aspects

There are numerous ways to set up fax messaging services in the OpenScape Xpressions configuration together with Hicom 300. The most important aspects are explained below together with their effects on Hicom administration.

1. Support for fax devices configured on the Hicom 300

A distinction can be made between two device types:

- a) [Fax devices assigned to a single person.](#)
- b) [Fax devices used by more than one person.](#)

2. Hicom users without a separate fax device but with a separate international fax number

For this group you can choose from the following administration types:

- a) Administration of fax numbers exclusively in OpenScape Xpressions
see: [Users with a separate fax number, administration in OpenScape Xpressions only.](#)
- b) Administration in Hicom 300 and OpenScape Xpressions
see: [Users with a separate fax number, administration in the Hicom PBX and in OpenScape Xpressions.](#)

3. Hicom users without a separate fax device or a separate international fax number (because it is chargeable) but who are granted fax authorization by means of a fax code plus a telephone number.

See: OpenScape Xpressions

See [Users without a separate fax number, with fax authorization by means of a code](#)

Fax devices assigned to a single person

Demand is increasing among mailbox owners in OpenScape Xpressions who have a personal fax device (number e. g. 47011) for improved protection of information or for the option of electronic access to fax information and its editability.

PBX Connection Variants for OpenScape Xpressions

Connecting CorNet-N to Hicom 300/Hicom 300 E/H

- 1a Case 1)

In this case we recommend setting up a fax mailbox with the number of the original fax device (47011) on the OpenScape Xpressions side and programming fixed call forwarding to the fax access number on the server which then assigns calls to the desired mailbox.

NOTE:

This solution requires the redirected number being transmitted to the server when the connection is set up.

- 1a Case 2))

The next best solution involves setting up a fax mailbox on the server under an additional internal server number, which may exceed the standard length in the network under some circumstances. On the Hicom side, CFW must then be set up on this »Mailbox Number«, prefixed by the route ID for the server; for example, 950 47011. This user's business card will still bear the fax number 47011 and the number 95047011 need only be specified by the user when accessing the server.

NOTE:

The solution 1a Case 2) must be implemented if no redirected number is transmitted when the connection is set up.

Fax terminal IDs and sender numbers are always based on the fax device number, in this case 47011.

Fax devices used by more than one person

Fax devices shared by a number of different Hicom users generally have an increased communications security requirement; for example, in cases where phones are busy or faulty.

We therefore recommend to set up one mailbox in OpenScape Xpressions for each fax device in accordance with the procedure explained in 1a Case 1) or 1a Case 2) and that received fax documents are, depending on the situation or according to an intelligent algorithm, delivered to the original device or to an alternative fax device (refer to the *XPR Administrator Manual* for an example). Fax calls in the public network do not generally come from a mailbox of this type.

For this configuration it is necessary to perform the Hicom-300 settings that are relevant for the fax service as described in [Section D.1.4.1, "General Aspects", on page 398](#). This applies in particular to the settings for the fax intercept for "Busy" and "Available" in the AMO COT for the CO interface.

Because a majority of external fax calls are still signaled as "Voice" (even in the ISDN), it is necessary to set forwarding on busy centrally for voice and to configure the fax devices affected centrally by means of COS. It is also necessary to set forwarding no answer (CD) by means of "Fixed CFW not activated" in order to cover all possible cases.

AMO	Essential AMO Parameters	Significance/Notes
ZIEL	TYPE=FWD SRCNO= SI=FAX DESTNOF=	Assigns destination numbers
ACTDA	TYPE=STN CD= FEATCD=FWD SIFWD=FAX	Update user features

Users with a separate fax number, administration in OpenScape Xpressions only

The advantage of solution 2a) lies in the fact that administration of all users in the fax service is restricted to the server. This also means that e. g. temporary call forwarding to a real fax device via Hicom administration is not possible.

The fax numbers for all mailboxes begin with the configured route ID for the server; for example, 950, and a complete fax mailbox number would be 95012.

The number of required fax mailboxes is entered in the Hicom 300 numbering plan, with the result that only one or two digits may be permitted for the OpenScape Xpressions route ID. The maximum number of digits specified for extensions in the Hicom 300 network (for example, 5) must not be exceeded by fax numbers consisting of the route ID plus the local internal server extension number if the extensions are to be contactable internationally.

The fax number defined only on the server should also be included in the user's fax code so that the user's fax number can be transmitted correctly to partners. Because fax numbers defined in this way are unknown in the Hicom, the user's telephone number must be entered in the CostInfo field of their administration so that it will be used as the calling party number for outgoing calls in the public network, thereby enabling correct call charge registration by Hicom 300.

Users with a separate fax number, administration in the Hicom PBX and in OpenScape Xpressions

Solution 2b) is of particular interest for customers who are already using group fax numbers, who want uniform administration for voice and fax, or who want to use the Hicom features that they are familiar with for the Fax Group 3 service

Setup on the Hicom side comprises the following stages:

The definition of an individual fax number for each affected Hicom 300 user ((AMO WABE), the assignment of this fax number as a group fax number to the telephone number of the relevant user (AMO RUFUM) and the assignment of any physical fax

PBX Connection Variants for OpenScape Xpressions

Connecting CorNet-N to Hicom 300/Hicom 300 E/H

device to the phone number (AMO TGER), as well as the definition of the forwarding destination for fax (AMOs ZIEL and ACTDA) mean that every Hicom 300 user is also capable of receiving fax documents in international traffic.

In OpenScape Xpressions there are two methods available for setting up these mailboxes. Different destination numbers must be set for fax call forwarding in the Hicom, depending on which of these two types is chosen.

- Case 1:

The route ID for OpenScape Xpressions and the first digit(s) of group fax number for the Hicom lie in a OpenScape Xpressions fax number range (see OpenScape Xpressions manual *System Administration*, subject **Extension ranges for DigApl or ISDNapl**). The relevant fax mailbox is set up in international format with the group fax number. The fax code is defined in exactly the same way, as the numbers represent valid fax numbers. This means that the call charges can be assigned correctly for outgoing fax connections. For incoming traffic, fax CFW to this mailbox number, prefixed with the route ID, must be set up in the Hicom. In order for the call number addressed by the Hicom to be now recognized as a mailbox number, the route ID must be removed from the destination number that is transmitted. This is generally done in the MTA, whereby all fax numbers with the route ID are replaced with the fax numbers without the route ID (for more information on routing rules, see the Administrator Manual). This is not necessary if the Hicom is configured in such a way that the route ID is not transmitted.

- Case 2:

Fax call forwarding in the Hicom is based on the fax access number (see the OpenScape Xpressions *System Administration* manual). For this configuration, the redirecting number that corresponds to the telephone number to which the dialed group fax number was assigned must now be analyzed in OpenScape Xpressions. This means that the fax mailbox must also be set up with the voice number. Call charge assignment is thus ensured for outgoing calls. In order to be able to address users correctly, their group fax number must still be set in the fax code for this mailbox.

AMO	Essential AMO Parameters	Significance/Notes
WABE	CD= DAR=FAXNO	Definition of the group fax number
TGER	STNO= FAXNO=	Assigns user devices
RUFUM	TYPE=COMB FAX1= FAX2=	Telephone number conversion
ZIEL	TYPE=FWD SRCNO= SI=FAX DESTNOF=	Assigns destination numbers

AMO	Essential AMO Parameters	Significance/Notes
ACTDA	TYPE=STN CD= FEATCD=FWD SIFWD=FAX	Update user features

Users without a separate fax number, with fax authorization by means of a code

This Hicom 300-specific case, which requires a fax code (AMO WABE), can only be handled by a suitable Hicom administration (AMO ZIEL and ACTDA) working with OpenScape Xpressions. Each of these fax users is assigned a fax number made up of the fax code plus the individual telephone number. This fax number functions securely within the Hicom 300 network and can often be used for calls from the public network.

To ensure that users can be reached using a fax code, they must be assigned an (arbitrary) physical fax device (AMO TGER). Fax CFW is based on the fax access number as in 2b) and the fax mailbox is set up with the same number as the voice mailbox. This ensures that call charges are always assigned.

Given that Hicom users without a separate fax number will seldom receive fax documents from the public network, the fax code should either be a central fax number (device or mailbox, e.g. 33333) or the specific personal telephone number (e.g. 47011) including the fax code (e.g. 68), which can be used more successfully in an ISDN environment.

In other words, variant 1: "49 89 722 33333" or variant 2: "49 89 722 68 47011". The business card for such a user should contain both fax addresses, starting with variant 2 and followed by variant 1.

AMO	Essential AMO Parameters	Significance/Notes
WABE	CD= DAR=FAX	Definition of the fax code
TGER	STNO= FAXNO=	Assigns user devices
ZIEL	TYPE=FWD SRCNO= SI=FAX DESTNOF=	Assigns destination numbers
ACTDA	TYPE=STN CD= FEATCD=FWD SIFWD=FAX	Update user features

D.1.4.4 Aspects of e-mail Access via Telephone

This is based on the same principle as direct access and callback access (see [Section D.1.2.2, “OpenScape Xpressions Access Numbers”](#) or [Section D.1.4.2, “Voice Messaging Aspects”](#)).

D.1.5 Settings for special (Fax) Applications

D.1.5.1 Fax-On-Demand Applications

All customized configurable fax-on-demand applications require no user-specific settings in the Hicom 300, Hicom 300 E/H. They are addressed directly by number.

D.1.6 Appendix: Hicom 300 AMO Batch Examples

In the following you find:

[/* Batch example for DIUS2 connection from OpenScape Xpressions to Hicom 300 V3.5](#)

[/* Batch example for DIUS2 connection from OpenScape Xpressions to Hicom 300 E V2.0](#)

[/* Batch example for DIUS2 connection from OpenScape Xpressions to Hicom 300 E V3.0](#)

[/* Batch example for STMD connection from OpenScape Xpressions to Hicom 300 V3.0](#)

[/* Batch example for STMD connection from OpenScape Xpressions to Hicom 300 V3.4](#)

/* Batch example for DIUS2 connection from OpenScape Xpressions to Hicom 300 V3.5

```
CHANGE-LWPAR:DIUS2,2,COP-
PER,S2,ON,Y,16,0,D5,10,10,Y,Y,DF,N,0,255,N,N;

ADD-COSSU:,35,TA&TNOT-
CR&CDRATN&CDRSTN&CDRINT&CDRS&CDRC,,,,,,,,,;

CHANGE-COSSU: COS,35,,TA&TNOTCR&SUBCAL&CDRINT&CDRSTN&CDRIND;

ADD-COT:30,TIE&NLCR&TSCS&CATR&NLRD&AOCC&CDRO&CDRD&DTNI&CFOS;

ADD-COP:11,,TA,TA;

ADD-BCSU:DIU,1,1,79,Q2096-X200,0,,,,;

ADD-BUEND:36,"DIU-XPR-1",30,N,0;

ADD-TDCSU:NEW,1-01-079-0,30,11,0,0,35,1,1,"DIUS2-XPR
",0,CORNV33,1,N,
,
0,,,,,,,,,31,MANY,930,0,1,1,EMP-
TY,21,1,S2CONN,36,CIR,1&&30,N,1,Y,2;

ADD-LODR:2,,,ECHO,1;

ADD-LODR:2,,,ECHO,2;

ADD-LODR:2,,,END;
```

PBX Connection Variants for OpenScape Xpressions

Connecting CorNet-N to Hicom 300/Hicom 300 E/H

```
ADD-RICT:LRTENEW,21,ALL,"DIUS2-XPR ",36,930,,,,,"",,,,,;
",36,930,,,,,"",,,,,;

ADD-WABE:930,,,TIE,N,,,,,,,;

ADD-LDAT:21,ALL,1,,36,2,1,,1,EMPTY,WCHREG,,NONE,1,4;

ADD-LDPLN:930-X,,21,1,;

ADD-RICT:PM,3,,,930802,"PUI NTSRV405";

/* Batch example for DIUS2 connection from OpenScape Xpressions
to Hicom 300 E V2.0

CHANGE-LWPAR:DIUS2,9,COP-
PER,S2,ON,Y,16,0,D5,10,10,Y,Y,DF,N,0,255,N,N;

ADD-COSSU:,10,TA&TNOTCR,TA&TNOTCR;

ADD-COT:10,TIE&TSCS&AOCC&DTNI&NLRD&NLCD&NLHT&NLCH&CFOS;

ADD-COP:10,,TA,TA;

ADD-BCSU:DIU,1,1,109,"Q2096-X200",0,,,,,0;

ADD-BUEND:3,"S2_1_ZUM_XPR",30,N,0,*1_ZUM_",30,N,0,*;

ADD-TDCSU:NEW,1-01-109-0,10,10,0,0,,1,1," ",0,CORNV33,1,N,
0,,,,,,,,,31,MANY,,0,1,1,EMP-
TY,10,1,N,S2CONN,3,CIR,1&&30,N,1,Y,9;

ADD-LODR:2,,,ECHO,1;

ADD-LODR:2,,,ECHO,2;

ADD-LODR:2,,,END;

ADD-RICT:LRTENEW,937,ALL,"S2_1_ZUM_XPR ",3,937,,,,,"",,,,,;

ADD-WABE:937,,,TIE;

ADD-LDAT:937,ALL,,3,2,1,;

ADD-LDPLN:937-X,,937,1,;

EINRICHTEN-RICT:PM,1,,,937802,"OpenScape Xpressions 937";
```

Note:

- In LWPAR the quality control parameter "qual=ON" must be set (CRC4).
- In networked systems, the tie lines between the systems must show the TSCS parameter in "COT", which permits network-wide MWI message notification. Make sure that the parameter is set for the routes system A->B and B->A:
Furthermore, the route (PM) to OpenScape Xpressions must be defined in each system. In the above example, the number is structured as follows:

```
937/930 => Tie trunk number to OpenScape Xpressions
802     => Access number to the OpenScape Xpressions "Callback Access"
```

/* Batch example for DIUS2 connection from OpenScape Xpressions to Hicom 300 E V3.0

```

ADD-COT:169,COTN&BSHT&BLOC&ATRS&NLCR&TSCS&NL-
HT&NLCH&NLRD&LIND&NTON&CFOS;

ADD-COP:169,,TA,TA;

ADD-COSSU:,169,TA&TNOTCR&CDRSTN&CDRC&MB&COSXCD&VCE&NOANSA&FWDN-
WK&MSN&FWDECA;

CHANGE-COSSU:169,,TA&TNOTCR&FAX&BASIC&INTWOR&OFTFS&MSN;

CHANGE-COSSU:169,,TA&TNOTCR&TTX&BASIC&INTWOR&OFTFS&MSN;

CHANGE-COSSU:169,,TA&TNOTCR&BASIC&VSM&MSN;

CHANGE-COSSU:169,,TA&TNOTCR&BASIC&INTWOR&DSM&MSN&CDRSTN&MUL-
TRA;

ADD-BUEND:169,"XPRESSIONS",30,N,0,*,0;

0ADD-TDCSU:NEW,1-02-115-
0,169,169,0,0,169,1,1,"DH2108",0,CORNV33,1,N,0,,
49,819,6635,,,,,,,,10,MANY,1-10-169,0,1,4,EMP-
TY,169,5,N,,,,,16,8,
S2CONN,169,CIR,1&&30,N,1,Y,0;

ADD-RICHT:LRTENEW,169,ALL,XPRESSIONS,169,1-10-
169,NO,YES,FIX,FTEXT,DTMF-NACHWAHL,PP300,NO,NO,;

ADD-LODR:169,,,ECHO,2;

ADD-LODR:169,,,NPI,ISDN,INTERNAT;

ADD-LODR:169,,,END;

ADD-LDAT:169,ALL,,,169,169,1,,,,,169,;

ADD-WABE:6400,,,TIE;

ADD-LDPLN:6400-2XXXX,,169,1,; /* not normally needed

ADD-RICHT:PM,2,,,64009,XPRESSIONS;

ADD-LDPLN:6400-X",,169,1,;

ADD-KNFOR:1-10-169,ISDN,INTERNAT,USERNSCR,SEND1,SEND1,YES;

```

/* Batch example for STMD connection from OpenScape Xpressions to Hicom 300 V3.0

```

ADD-COT:169,COTN&BSHT&BLOC&ATRS&NLCR&TSCS&NL-
HT&NLCH&NLRD&LIND&NTON&CFOS;

ADD-COP:169,,TA,TA;

ADD-COSSU:,169,TA&TNOTCR&CDRSTN&CDRC&MB&COSXCD&VCE&NOANSA&FWDN-
WK&MSN&FWDECA;

CHANGE-COSSU:169,,TA&TNOTCR&FAX&BASIC&INTWOR&OFTFS&MSN;

```

PBX Connection Variants for OpenScape Xpressions

Connecting CorNet-N to Hicom 300/Hicom 300 E/H

```
CHANGE-COSSU: COS, 169,, TA&TNOTCR&TTX&BASIC&INTWOR&OFTFS&MSN;
CHANGE-COSSU: COS, 169,, TA&TNOTCR&BASIC&VSM&MSN;
CHANGE-COSSU: COS, 169,, TA&TNOTCR&BASIC&INTWOR&DSM&MSN&CDRSTN&MUL-
TRA;
ADD-BUEND: 169, "XPRESSIONS          ", 4, N, 0, *, 0;
ADD-TDCSU: NEW, 1-06-079-5, 169, 169, 1, 0, 169, 1, 1, "DH2108          ", 0,
"CORNV33", 1, N, 0,, 49, 819, 7000,,,,,,,,, 31, MANY, 1-10-169, 0, 1, 1, EMP-
TY,
169, 9, N,,,,,,,,, 16, 8, SOCONN,, Y, 169, CIR, Y, X, 0, N;
ADD-RICHT: LRTENEW, 169, ALL, XPRESSIONS, 169, 1-10-
169, NO, YES, FIX, FTEXT, DTMF-NACHWAHL, PP300, NO, NO, ;
ADD-LODR: 169,,, ECHO, 2;
ADD-LODR: 169,,,, NPI, ISDN, INTERNAT;
ADD-LODR: 169,,, END;
ADD-LDAT: 169, ALL,,, 169, 169, 1,,,,, 169, ;
ADD-WABE: 6400,,, TIE;
ADD-LDPLN: 6400-2XXXX,, 169, 1, ; /* not normally needed
ADD-RICHT: PM, 2,,, 64009, XPRESSIONS;
ADD-LDPLN: 6400-X", , 169, 1, ;
ADD-KNFOR: 1-10-169, ISDN, INTERNAT, USERNSCR, SEND1, SEND1, YES;
```

/* Batch example for STMD connection from OpenScape Xpressions to Hicom 300 V3.4

```
#01 Adding WABE;
ADD-WABE: 934,,, TIE, N;
#02 Adding COT
ADD-COT: 100, TIE&NLCDR&NLCDR&DTNI;
#03 Adding COP
ADD-COP: 100,, TA, TA;
#03 Adding COS
ADD-COSSU: , 48, TA&TNOTCR&CDRATN&CDRSTN&CDRINT&CDRS&CDRC;
CHANGE-COSSU: COS, 48,, TA&TNOTCR&SUBCAL&CDRINT&CDRSTN&CDRIND;
#04 Adding the trunk group to OpenScape Xpressions
ADD-BUEND: 80, "XPR ON NTSERVER ", 16, N, 0 ;
#06 Adding the lines (STMD module must already be set up in BC-
SU)
```

PBX Connection Variants for OpenScape Xpressions

Connecting CorNet-N to Hicom 300/Hicom 300 E/H

```
ADD-TDCSU:NEW,1-03-103-4,100,100,0,0,48,1,1,"
",0,CORNV33,
1,N,0,,49,30,383927,00,0,,,,,31,MANY,853,0,1,1,EMP-
TY,1,1,S0CONN,,Y,80,ASC,
Y,Y,0,N;

ADD-TDCSU:NEW,1-03-103-5,100,100,0,0,48,1,1,"",0,
CORNV33,1,N,0,,49,30,383927,00,0,,,,,31,MANY,853,0,1,1,EMP-
TY,1,1,S0CONN,,Y,
80,ASC,Y,Y,0,N;

ADD-TDCSU:NEW,1-03-103-6,100,100,0,0,48,1,1,"",0,
CORNV33,1,N,0,,49,30,383927,00,0,,,,,31,MANY,853,0,1,1,EMP-
TY,1,1,S0CONN,,
Y,80,ASC,Y,Y,0,N;

ADD-TDCSU:NEW,1-03-103-7,100,100,0,0,48,1,1,"",0,
CORNV33,1,N,0,,49,30,383927,00,0,,,,,31,MANY,853,0,1,1,EMP-
TY,1,1,S0CONN,,
Y,80,ASC,Y,Y,0,N;

#07 Adding the route

ADD-RICHT:LRTENEW,24,ALL,"XPR ON NTSERVER",80,853,YES,,FIX,DIG-
IT,"XPR INPUT",,,,,;

#08 Adding the dial plan

ADD-LODR:1,,,ECHO,2;

ADD-LODR:1,,,END;

ADD-LDAT:24,ALL,1,,80,1,1,,1,EMPTY,WCHREG,,NONE,1,4;

ADD-LDPLN:934-X,,24,1,;

#09 Adding DAR MBON MBOFF to WABE

ADD-WABE:**7,,,MBON;

ADD-WABE:**8,,,MBOFF;

#10 Adding an analog port for a modem

ADD-WABE:2105,,,STN;

ADD-SCSU:2105,,ANATE,0,0,1,1,1,1,1,1;

#11 Adding the destination for the Output key ('VMX Mailbox')

Option a) (recommended)

ADD-WABE:3147,,,STN;

ADD-SC-
SU:3147,,ANATE,0,0,1,1,1,1,1,1,,0,NO,,,,,,,,,VAR,,,,,,,,,"",,
,,FLOAT,,,NO,;

ADD-SA:VCE,3147,,,CYC,8,"NTSRV404";

ADD-ZIEL:EVMTAB,DSZINT,3147
```

PBX Connection Variants for OpenScape Xpressions

Connecting CorNet-N to Hicom 300/Hicom 300 E/H

```
ADD-ACTDA:STN,3147,FWD,,934802;
```

Option b) (without display as regards mail box entry)

```
ADD-ZIEL:EVMTAB,DSZINT,934802;
```

D.2 Connecting HiPath 3000 (CorNet-N)

D.2.1 Introduction

This chapter describes measures required for ideal usage of the OpenScape Xpressions product with its different configuration options in a customer environment with a HiPath 3000 communication system.

D.2.2 Connecting to HiPath 3000

D.2.2.1 Hardware/Software Requirements

The OpenScape Xpressions product is physically connected to the HiPath 3000 communications system via digital S_0 tie trunks with the CorNet-N networking protocol, which is specific for Unify GmbH & Co. KG.

Up to four free S_0 ports are required on a STMD or STLS module for the telecommunication system.

For the max. 4 S_0 connections, modules by Dialogic/Eicon (one 4BRI-8M) are used on the OpenScape Xpressions side.

D.2.2.2 OpenScape Xpressions Access Numbers

Selection of a OpenScape Xpressions application via the telephone user interface is generally made by analyzing the transmitted B user number (called party number). For some applications, the B user number is also used to address a mailbox.

For customized applications such as all Fax-on-Demand applications, for example, the required numbers can be selected from an assigned set of numbers.

Virtual numbers/users are generally not required for the S_0 link with CorNet-N.

For standard OpenScape Xpressions messaging applications, a set of numbers is assigned logically rather than numerically. These are:

- **Forward access number**
The forward access number is used as the destination in the call destination list being created for the users.

PBX Connection Variants for OpenScape Xpressions

Connecting HiPath 3000 (CorNet-N)

- **Direct access number**
When a mailbox user in OpenScape Xpressions dials the direct access number, this user is given access to all of the telephone features of OpenScape Xpressions.
- **Guest access number**
When a person who does not have their own mailbox in OpenScape Xpressions dials the guest access number, this person is given access to a restricted selection of features compared with those available through direct access (for example, for leaving a message in any mailbox).
- **Callback access number**
The callback access number gives a mailbox owner in OpenScape Xpressions brief access (without identification) directly to his/her new messages.
- **Fax access number**
The fax access number is similar to the forward access number, but applies only to the Fax Group 3 service. Using a central fax access number is not possible.

The structure of all access numbers for OpenScape Xpressions must follow very specific rules. These rules are explained by means of examples below.

First let us present a short definition of the terms "open" and "closed numbering".

Open numbering

With open numbering the users of the individual systems of a Hicom network are numbered independently of one another. Each system has its own set of numbers.

A number is therefore only unique within a single system. If a connection is established between two systems, the number must be prefixed by a route ID. When a number belonging to a user within the same system is dialed, the route ID for this system can also be dialed. During digit analysis, the system recognizes that the destination being dialed lies within the same system and ignores the route ID.

Closed numbering

With closed numbering, all numbers are uniquely assigned network-wide. With this type of numbering the system functions like a single large PBX.

Hicom together with OpenScape Xpressions uses a combined system of open and closed numbering.

To minimize the administration effort in the Hicom or especially in Hicom networks the OpenScape Xpressions product is connected via CorNet-N according to the basic rules of open Hicom numbering. This means that a separate route ID is defined for the tie trunk to OpenScape Xpressions and that, consequently, all numbers that begin with this ID are automatically assigned to the server (as network nodes) and are basically unknown to the HiPath 3000.

Various aspects on addressing with OpenScape Xpressions access numbers

The following typical conditions should be assumed:

- The range of call numbers assigned should reach from 1234-100 to 1234-299 for approximately 120 users; i.e. 3-digit numbering is used internally.
- The tie code for OpenScape Xpressions should be 19, with the result that all numbers from 1234-19xxx to 1234-19yyy (possibly with additional dial digits) are assigned to the server.
- A range of these extension numbers, for example from 90 to 99, should be used for the internationally addressable applications direct access, guest access, callback access and various Fax-On-Demand applications.
- The tie trunk for OpenScape Xpressions consisting of 1 to 4 S₀ interfaces should (despite open numbering) be configured so that the tie code (in this case 19) is not transmitted in the CorNet-N.

D.2.2.3 Further Notes

The charges detail recording for outgoing connections from OpenScape Xpressions e.g. into the public network is realized by the Hicom PBX that includes the trunk interfaces. In such cases, OpenScape Xpressions ensures that the mailbox user incurring the charges is always entered as the A user of the connection. If the mailbox numbers managed in OpenScape Xpressions do not match the extension numbers known, a valid extension number must be entered in the CostInfo field for these mailboxes so that charges incurred by this mailbox can be correctly assigned.

The PC attendant console can also directly access the OpenScape Xpressions features by means of DTMF dialing.

D.2.2.4 Integration Features through the Use of CorNet-N

The **CorNet-N** protocol, specific for Unify GmbH & Co. KG, allows using the following features for the connection of OpenScape Xpressions to HiPath 3000 with S₀ boards by Dialogic/Eicon:

- Caller's number (A user)
- Callee's number (B user)
- Exchange of end system skills by means of classmarks
- Information transfer relating to external/internal call
- Transfer of the basis for call forwarding (fixed/variable CFW) or forwarding no answer (CD) or forwarding on busy

PBX Connection Variants for OpenScape Xpressions

Connecting HiPath 3000 (CorNet-N)

- Transfer of the number of the user who was originally called in the case of call forwarding (CFW)/forwarding no answer (CD) (number of the forwarder)
- Controlling the server via DTMF
- Setting or deleting the message waiting indication (MWI) by assigning a B-channel

D.2.2.5 Configuring S₀ Interfaces to OpenScape Xpressions

The OpenScape Xpressions server is linked via max. 4 ISDN-S₀ connections as subsystem with the CorNet-N tie trunk protocol.

Therefore a digital cross-traffic module is required on the Hicom side.

On the OpenScape Xpressions side one Dialogic/Eicon 4BRI-8M module is used for the physical link with the Hicom.

The B-channels on the OpenScape Xpressions side must be configured/released in exactly the same number on the Hicom side.

OpenScape Xpressions V7 supports only the *voice* and *Fax G3* services; transparent 64-Kbit user data is not supported.

For the administration of the tie trunk OpenScape Xpressions using Hicom Assistant, subsystem operation (with a separate number block) must be set up. All B-channels must be combined in a linear hunt group. The route ID is handled in the least cost routing.

Consultation connections are not supported for OpenScape Xpressions V7.

D.2.3 Configuring Message Waiting Indication and Remote Service Access

D.2.3.1 Message Waiting Indication

The message waiting indication is enabled for all users in a Hicom 150 network using Dialogic/Eicon BRI-2M or 4BRI-8M boards via the CorNet-N interface. A port of type PhoneMail must be set up in the Hicom in this case. This port does not have to exist physically.

D.2.3.2 Remote Service Access

For the “Remote Service Access for OpenScape Xpressions” feature an analog port is required at the HiPath 3000 for connecting a modem (if so desired by the customer). There are no special settings for this port, it must be released for outgoing and incoming traffic.

D.2.4 Configuring Participants

D.2.4.1 General Aspects

Neither voice nor fax terminal devices require central system settings. All of the required settings, in particular those for forwarding, can be made for each Hicom user using Hicom Assistant and in part using the telephone.

D.2.4.2 Voice Messaging Aspects

Fixed call forwarding, call forwarding no answer when available and, if required, call forwarding on busy for OpenScape Xpressions must be set individually for each Hicom 150 user's telephone.

NOTE:

Using the "forwarding on busy" feature should depend on the individual customer scenario. If, for example, the customer is operating in a predominantly digital ISDN environment in which the callback feature is used frequently, it may be useful not to activate the function for forwarding to the answering machine on busy.

For specific voice user configurations with, for example, multiple telephone assignments or a stationary telephone and a mobile unit, setting up a single mailbox for the main user telephone is recommended, whereby this telephone then records all messages. To do this, it is generally necessary to combine the telephones in a hunt group with an overflow to "OpenScape Xpressions", specifying the mailbox number. Another possibility is to configure a second mailbox that defines the first mailbox as a referral (STAND-IN).

For executive/secretary configurations the recommended default is: call forwarding/call forwarding no answer to the mailbox of the first addressed user.

OpenScape Xpressions applications such as Direct Access or Guest Access are, on the other hand, addressed directly and the required mailbox number or call number must be entered manually by the remote user using DTMF suffix dialing.

D.2.4.3 Aspects of e-mail Access via Telephone

This is based on the same principle as direct access and callback access (see [Chapter D, "OpenScape Xpressions Access Numbers"](#) or [Chapter D, "Voice Messaging Aspects"](#)).

D.2.5 Settings for special (Fax) Applications

D.2.5.1 Fax-On-Demand Applications

None of the customer-specifically configurable Fax-on-Demand applications requires user-specific settings in the HiPath 3000.

D.2.6 Examples

D.2.6.1 Example Configuration HiPath 3000

Setting up the S₀ Tie Lines for Connecting OpenScape Xpressions

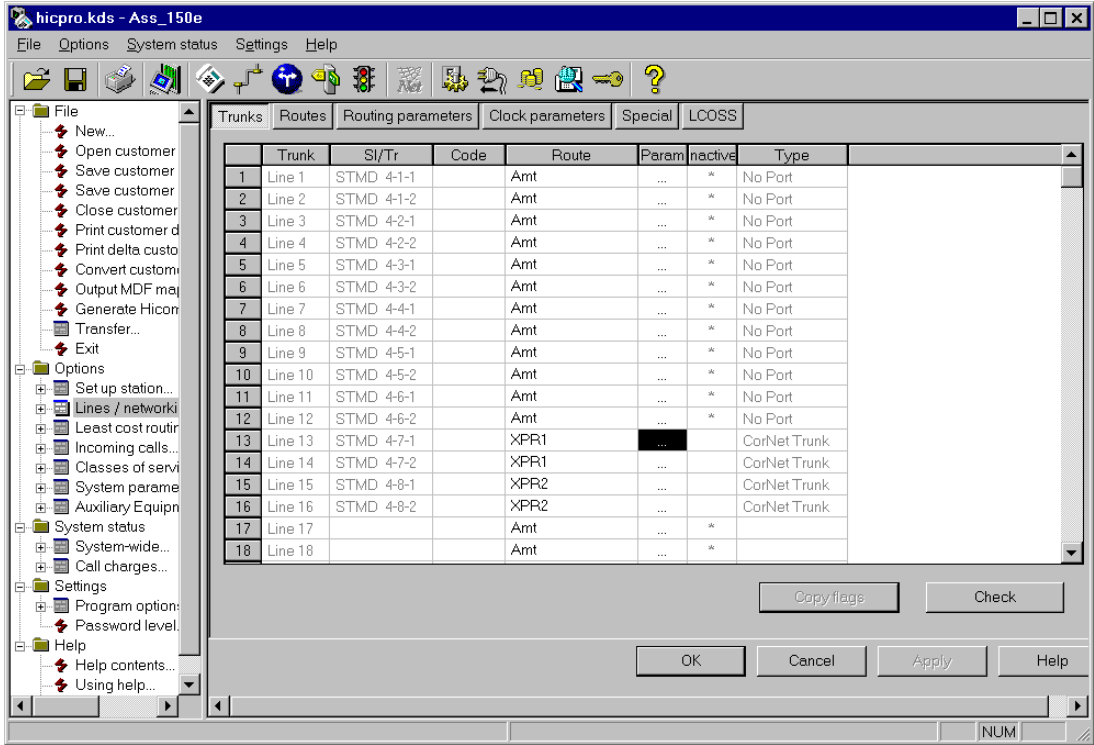
The description below explains how CorNet-N tie lines between Hicom Office / HiPath 3000 and OpenScape Xpressions are configured. The screenshots refer to HiPath 3000. Deviations from the Hicom Office are described in the text. An STMD or STLS module set up with the correct number of free ports is required.

NOTE:

In Hicom 150 H or later the protocol "S0/S2 CorNet-N variant2 master (Xpressions) direct" has been introduced in the tie trunk for OpenScape Xpressions. This enables the B-channels to be released for switching operations via OpenScape Xpressions. The "-nopbxswitch" parameter must NOT be set in this case.

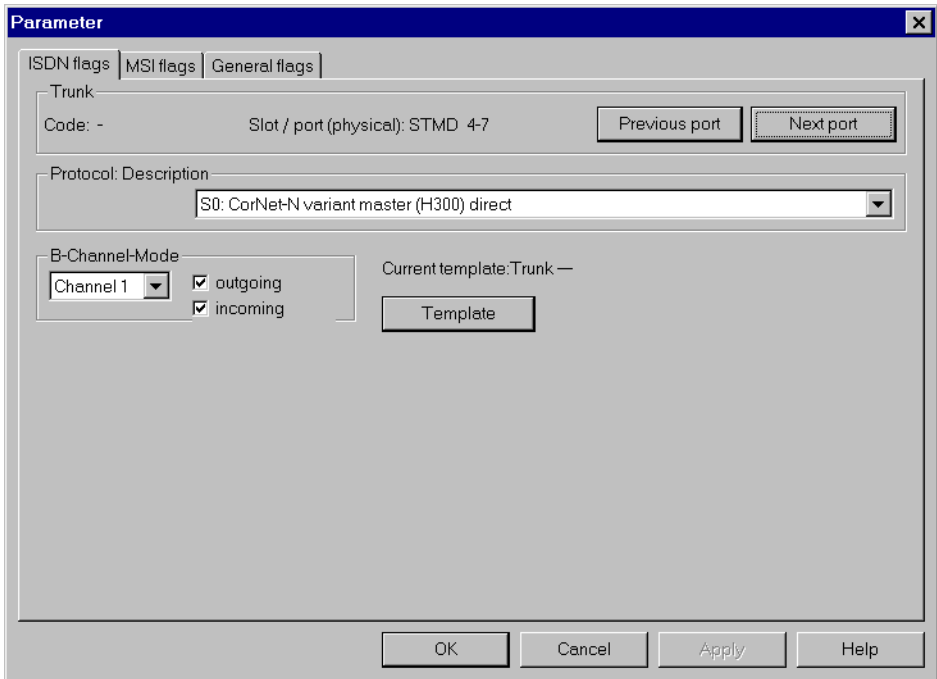
PBX Connection Variants for OpenScope Xpressions
Connecting HiPath 3000 (CorNet-N)

Options > Lines / networking > Trunks > Parameter (for all tie lines to OpenScope Xpressions)



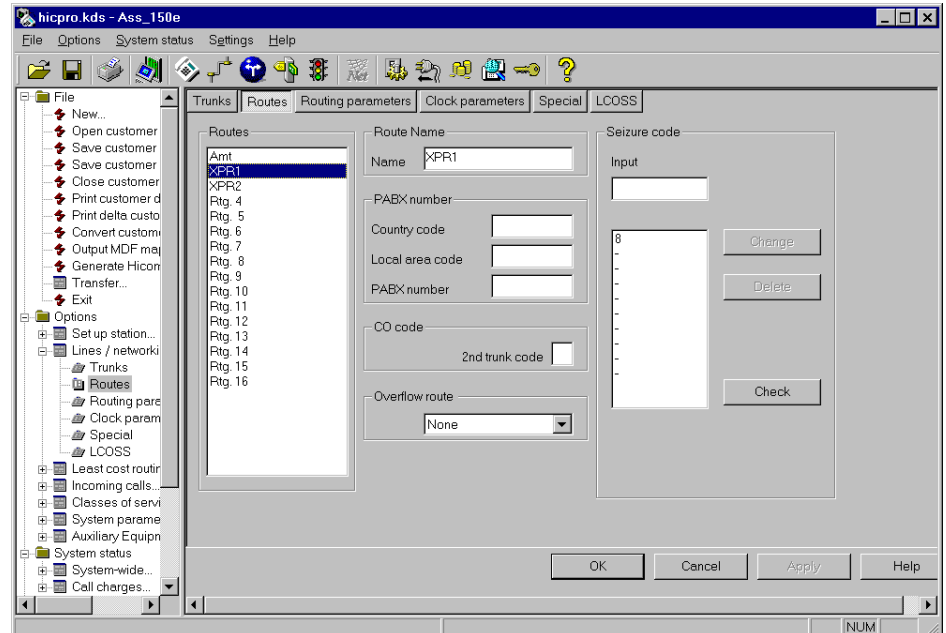
CorNet-N Master Direct (H300) - for Hicom Office 1.0

CorNet-N Version2 Master Direct Xpressions - for HiPath 3000



Options > Lines / networking > Routes (for the route to OpenScape Xpressions)

It is not necessary to enter a route code here. This is done as part of the LCR entries. The PBX number should be entered in the direction of the OpenScape Xpressions system. This means that all call information can be sent to international destinations.



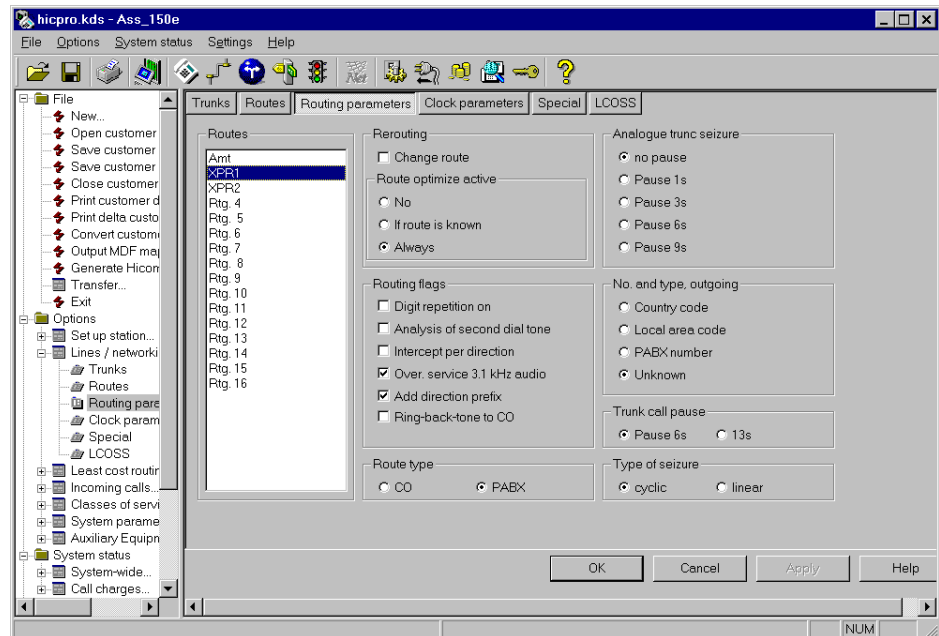
PBX Connection Variants for OpenScope Xpressions

Connecting HiPath 3000 (CorNet-N)

Options > Lines / networking > Routing parameters

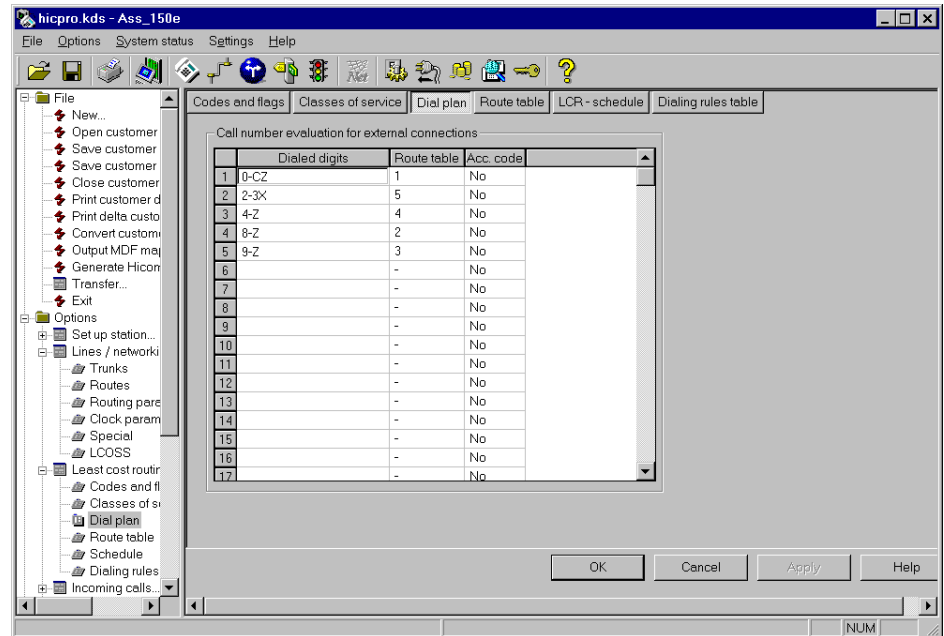
Type of seizure - cyclic (for fail-safe capacity)

Route type - PABX



Options > Least cost routing > Dial plan**Dialed digits** - code for tie trunk with "-Z" (random suffix)**Route table** - reference to the relevant route table**NOTE:**

If LCR has not been enabled so far, the access code must be checked as well.



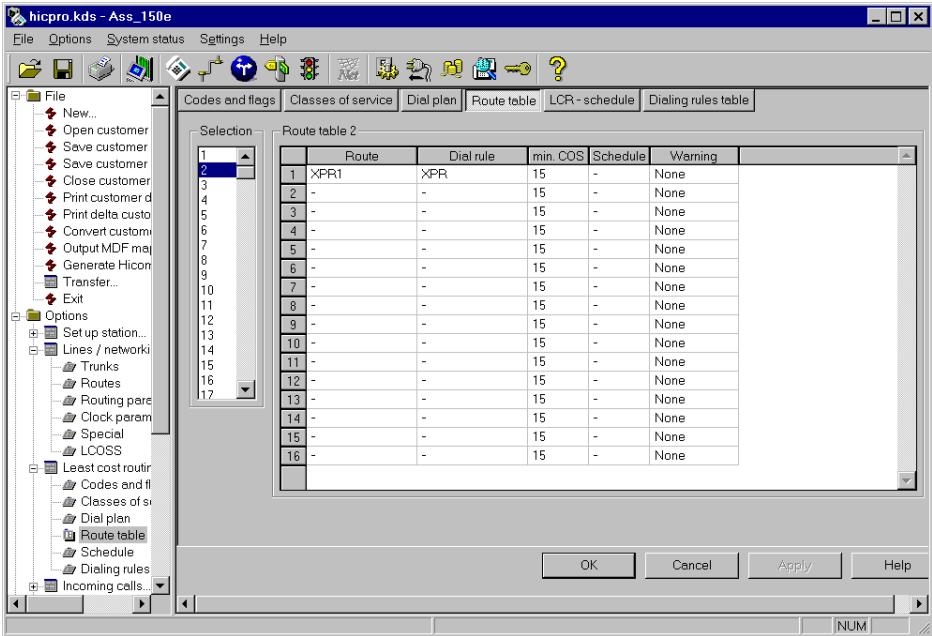
PBX Connection Variants for OpenScope Xpressions
Connecting HiPath 3000 (CorNet-N)

Options > Least cost routing > Route table

Selection - select the appropriate route table

Route - indicate the route to OpenScope Xpressions

Dial rule - indicate new dialing rule



Options > Least cost routing > Dialing rules table

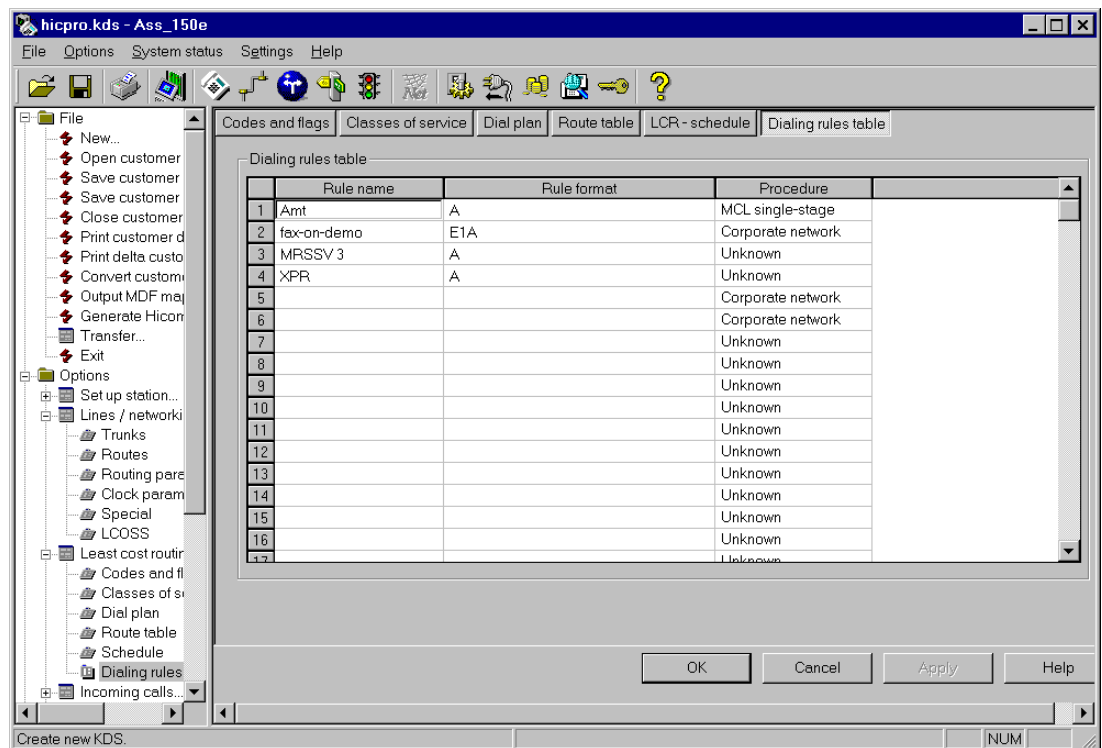
Rule name - specify appropriate rule name

Rule format - A = Only the suffix is passed to OpenScape Xpressions; E1A = tie trunk code and the suffix are forwarded to OpenScape Xpressions.

Procedure - Corporate network

NOTE:

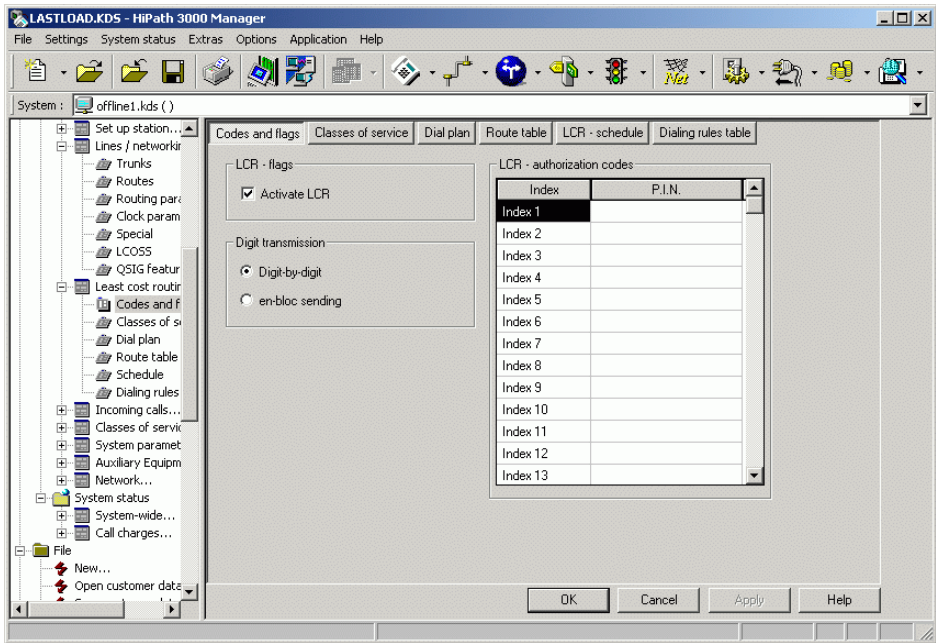
The rule format settings depend on the settings made in the ISDN APL/ DLG APL Apl of the OpenScape Xpressions system!



PBX Connection Variants for OpenScope Xpressions
Connecting HiPath 3000 (CorNet-N)

Options > Least cost routing > Codes and flags

Activate LCR (if not yet activated).



Configuring Call Forwarding no Answer with Dummy User

A dummy user is set up as the call forwarding no answer destination, whereby this dummy user receives an external CFW to the forward access number of OpenScape Xpressions. Call forwarding is implemented via a phone which allows "Associated Dialing/Services" (feature code *83). The user must be of the type answering machine.

Options > Set up station...

Set up station: Parameter

Flags | **Station Type** | ISDN flags

Station
No. 41 Call no.: 200 Name: pseudo 200

Previous station Next station

CMI

Mobile code :

Logged on:

Company abbreviation :

System family :

PP family :

Extension Type

☐ Standard

☐ Phone Mail (Callno. 5 digits)

☐ Phone Mail (Callno. 6 digits)

☒ Answer Machine

☐ Fax

☐ Loudspeaker

☐ External MOH

☐ P.O.T MW LED

☐ Station with pulse dialing

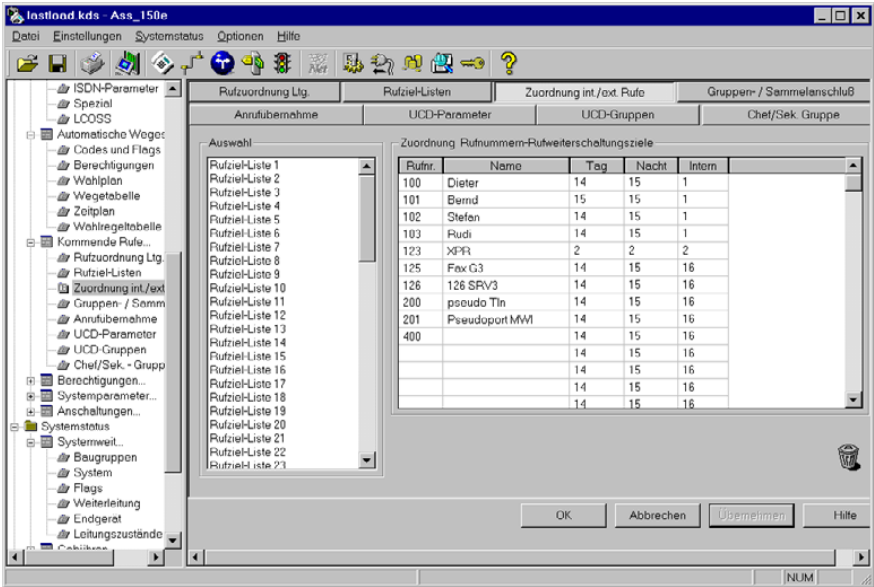
Lock Code

Reset

OK Cancel Apply Help

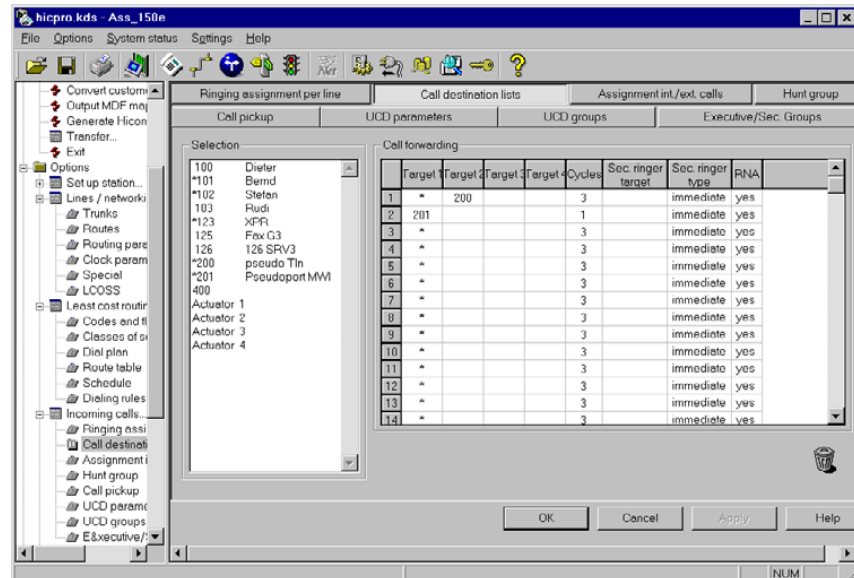
PBX Connection Variants for OpenScope Xpressions
Connecting HiPath 3000 (CorNet-N)

Options > Incoming calls > Assignment int./ext. calls



The users are assigned call destination lists for the various calls. Separate call destination lists are created for forwarding to OpenScope Xpressions. For call forwarding no answer for internal calls, the users are assigned call destination list 1, for example.

Options > Incoming calls > Call destination lists

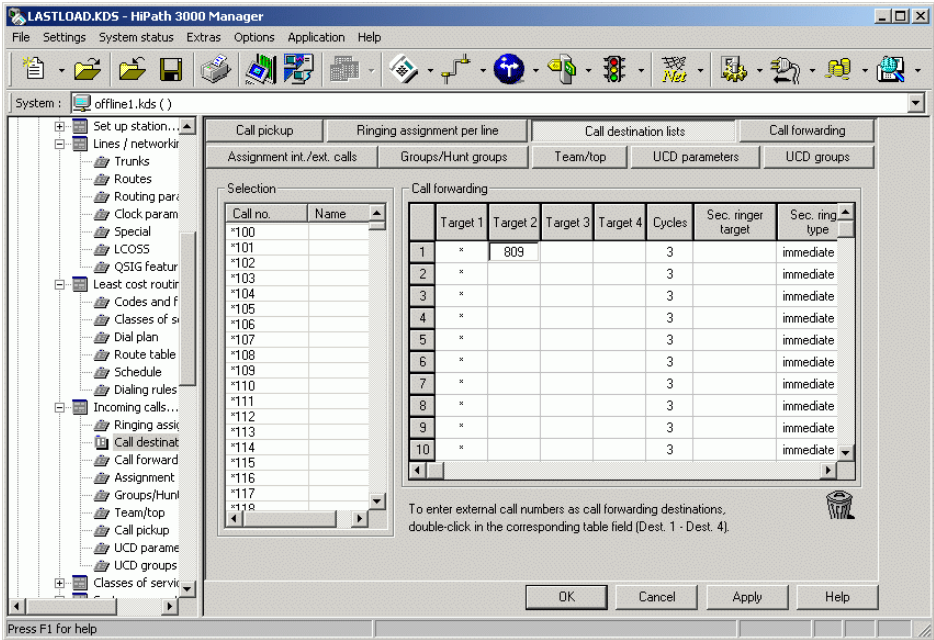


Call destination list 1 contains the previously created dummy number as the second destination. Call forwarding no answer is implemented for a user through the fixed forwarding of this number to OpenScape Xpressions.

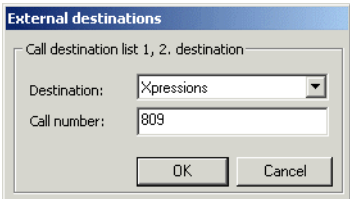
Configuring Call Forwarding no Answer without Dummy User

It is possible to directly refer to a cross direction from a call destination list. This simplification means that the dummy subscriber is no longer needed.

Options > Incoming calls > Call destination lists



By double-clicking the appropriate destination you can select the direction and store the call number directly in the ensuing dialog box.



Procedure for "Check Phonemail" (callback to the Callback Access of OpenScape Xpressions):

Requirements in the HiPath:

The Phone Mail (Callno. 5 digits) extension type is assigned to a subscriber PEN (without module access). The associated services function diverts this port from an authorized extension to the callback access of OpenScape Xpressions.

In older systems calls have to be routed via an additional dummy number accessed from a call destination list, as the callback function ignores call forwarding.

Options > Set up station > Parameter > Station Type

Select **Phone Mail 5-digit number**.

NOTE:

Although multiple Phonemail terminals can be set up in the HiPath 3000, callbacks are always performed via the first logical port.

Set up station: Parameter

Flags | **Station Type** | ISDN flags

Station
No. 24 Call no.: 123 Name: XPR

Previous station Next station

CMI
Mobile code :
Logged on:
Company abbreviation :
System family :
PP family :

Extension Type
☐ Standard
☒ Phone Mail (Callno. 5 digits)
☐ Phone Mail (Callno. 6 digits)
☐ Answer Machine
☐ Fax
☐ Loudspeaker
☐ External MOH
☐ P.O.T MW LED
☐ Station with pulse dialing

Lock Code
Reset

OK Cancel Apply Help

D.3 Connecting HiPath 3000 (CorNet-IP)

IMPORTANT: This example of a connection to a HiPath 3000 via CorNet-IP is to serve solely as guiding line. In a "real-life" environment, adjust the line parameters, code numbers, IP addresses etc. to your environment's conditions. If you configure the example on a HiPath 3000 in a "real-life" environment, please be definitely sure to save the current HiPath 3000 settings beforehand.

This example requires:

- An XPR server with installed IP APL, as well as the protocols **Fax Group 3 (FAXG3)** and **Xpressions PhoneMail**. You find information about the XPR server setup in the OpenScape Xpressions *Server Installation* manual.
- An installed Manager E (at least version HA620B.50.071) via which the configuration of the HiPath 3000 can be evaluated, modified and transferred to the PBX. You find information about the HiPath Manager E installation in the administrator documentation for the HiPath 3000/5000 Manager E.
- You should know how to operate the Manager E. In this example we will not deal with operating the Manager E in detail. You find information about the HiPath Manager E operation in the administrator documentation for the HiPath 3000/5000 Manager E.

The following settings will be used in this example of connecting a HiPath 3000 via CorNet-IP:

- Code numbers 83-XXXX for fax (E2 will be transmitted only). The dial plan is called E2A.
- Code numbers 88-XX for PhoneMail (everything will be transmitted). The dial plan is called E1A.
- The XPR server has the IP address 192.168.22.101.
- The HG gateway has the IP address 192.168.22.230.
- In the XPR server a phone number length of 4 digits will be set.

The HiPath 3000 is connected to the XPR via an HG1500 module. The hardware used, for example an STMI card, and the loadware used determine the number voice channels and other HG1500 features.

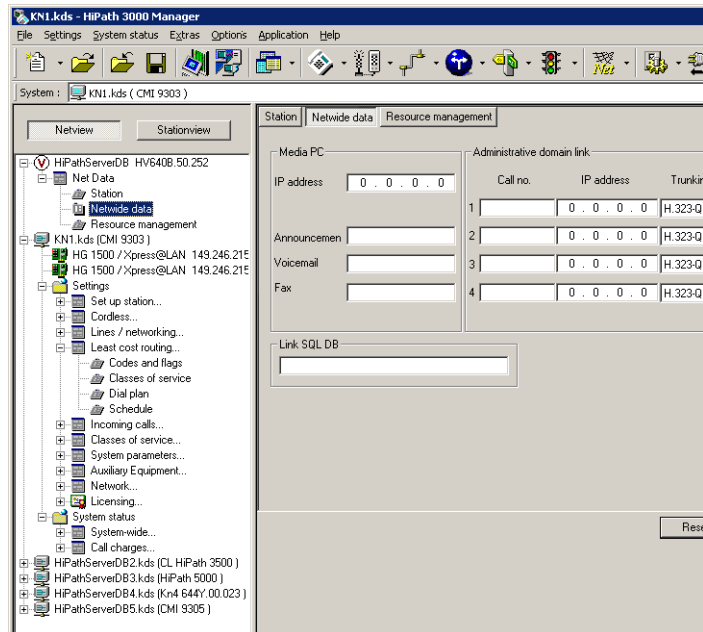
D.3.1 Configuration in the Manager E

First, we will take care of all required Manager E configuration steps. Proceed as follows:

1. Start the Manager E and transmit the KDS from the system to the PC:
 - a) In the Manager E open the menu option **File > Transfer**.
 - b) Enter the log-on information and click on **System > PC**.
 - c) Confirm the log-on information and wait until the transmission is complete.
 - d) Click on **OK** and subsequently on **Close**.
2. If you want to connect the XPR server to a HiPath 5000 Real-Time Services Manager (RSM), execute the following substeps in addition.

The RSM is used as central administration unit in an IP networking of HiPath 3000 systems. By creating a single-system image all nodes involved can be centrally managed. HiPath 5000 RSM is a platform for the central provision of applications and enables their use by all stations of the IP networking. Please obtain detailed information from the service manual *HiPath 3000/ 5000 V7 IP Systems*.

- a) Open in the manager E the page **Netwide data > Netwide data**.



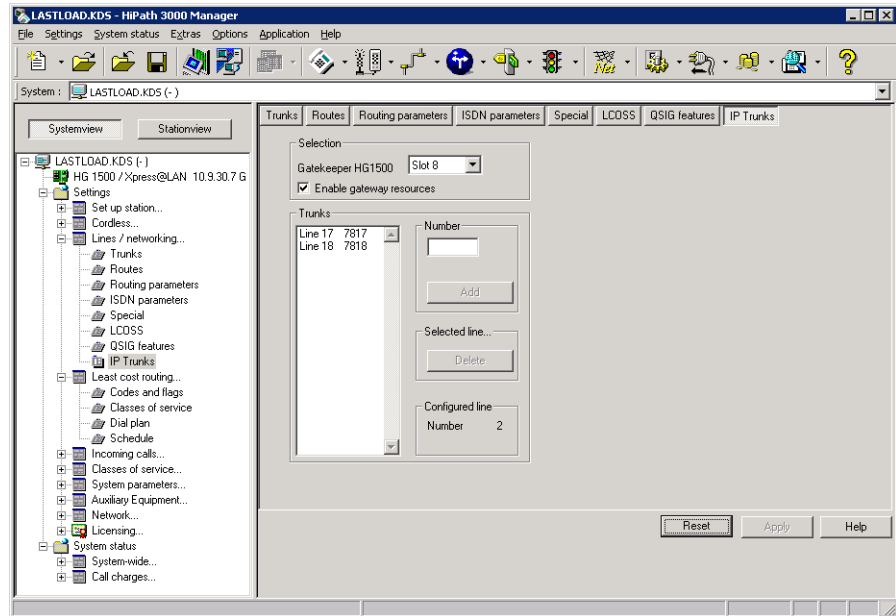
- b) In the **IP address** field of the **Media PC** section enter the XPR server IP address. In this way the XPR server is made known as node.
- c) Enter the tie-trunk number in the **Voicemail** field.

These substeps are the same for HiPath 3000 V5, V6 and V7.

PBX Connection Variants for OpenScope Xpressions

Connecting HiPath 3000 (CorNet-IP)

3. In the Manager E open the **Lines/networking > IP Trunks** page for configuring IP lines.



In the **Gatekeeper HG1500** field of the **Selection** section select the slot of the HG1500.

The IP APL is only released for access to an HG module. tick the **Enable gateway resources** checkbox.

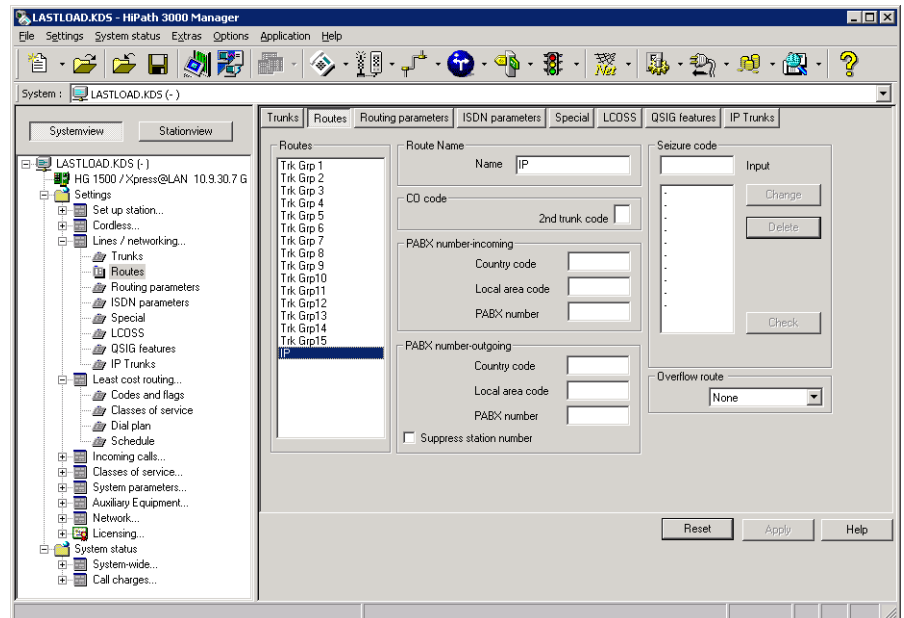
IMPORTANT: If one or both of these settings are modified, the HG1500 must be rebooted, since it is only informed about being the signaling gateway during the booting process. A signaling gateway receives more data, for example call routing data, from the HiPath 3000, so that you can only view routing information from a signaling gateway in the web-based management under **Explorer > Voice Gateway > PBX > Routing**.

You can start rebooting the HG1500 module via the **Reboot** button situated bottom left in the web-based management. The browser needs to be closed then so that it empties its cache and does not display obsolete data of the HG1500 module.

In the **Number** field enter the number of lines that you want to use as IP lines. For our example we take two lines.

Then click **Apply**.

4. Open the **Lines/networking > Routes** page to define a route.



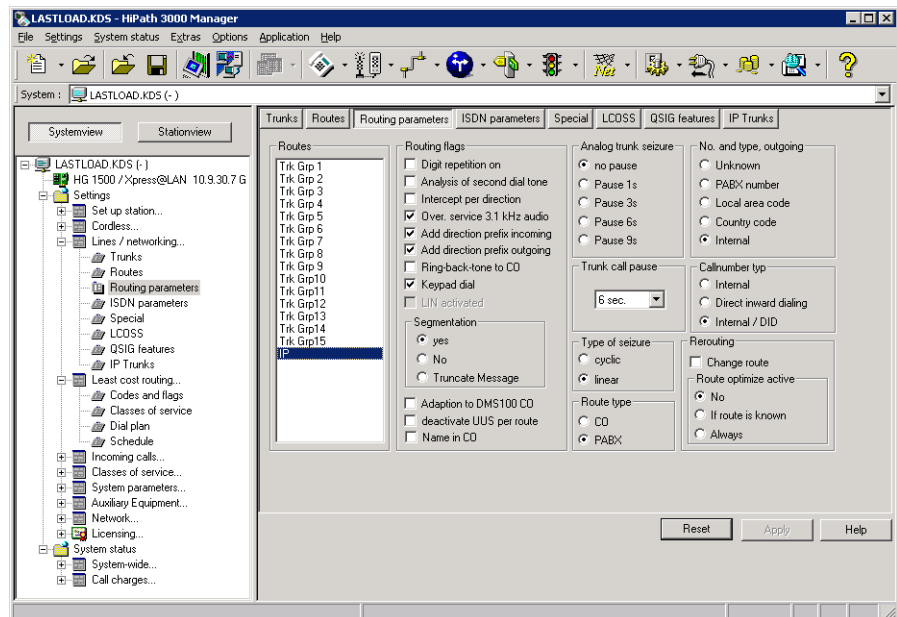
In our example we name the route **IP**. In the **Routes** section select the desired direction and enter the name **IP** in the **Name** field of the **Route Name** section.

Then click **Apply**.

PBX Connection Variants for OpenScope Xpressions

Connecting HiPath 3000 (CorNet-IP)

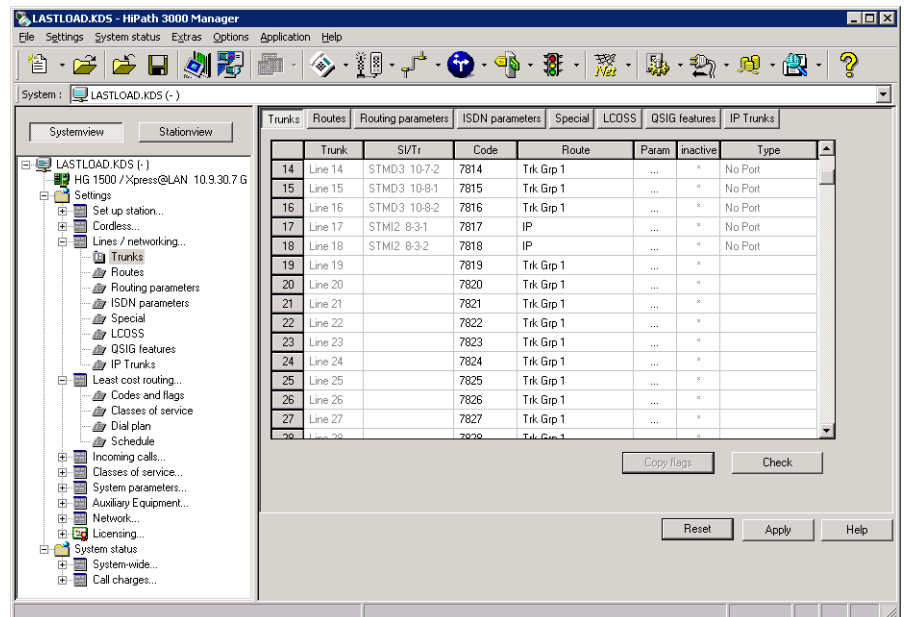
- On the **Routing parameters** page set the direction parameters for the direction just named.



For the example copy the settings from the figure. Make sure that the **IP** entry is selected in the **Routes** list, so that you edit the direction you defined in the previous step.

Then click **Apply**.

6. Open the **Trunks** page to assign the lines configured in step 3 the direction defined in step 4.



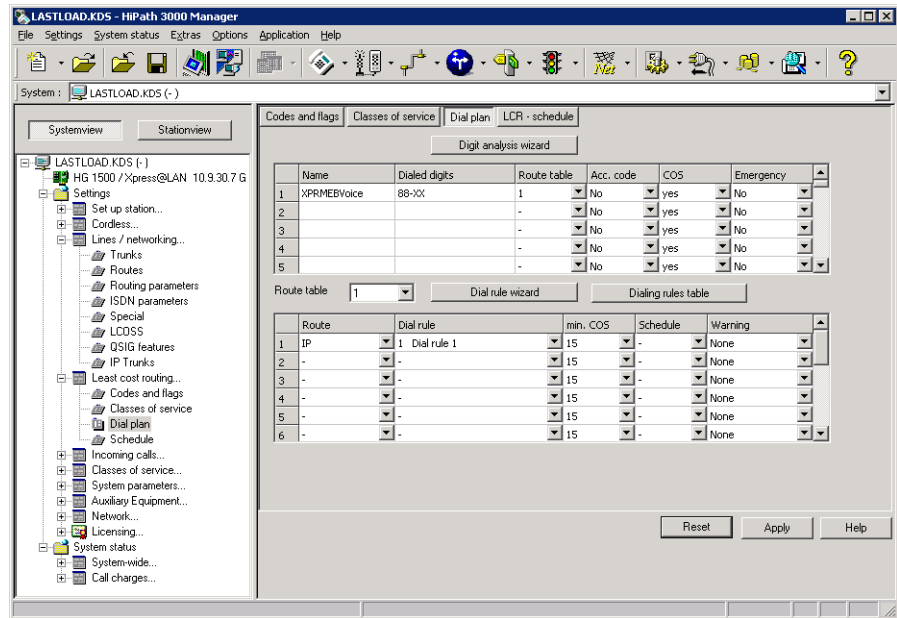
In the list, look for the lines configured in step 3 and select for both lines in the **Route** column the direction **IP**, which you have defined in step 4.

Then click **Apply**.

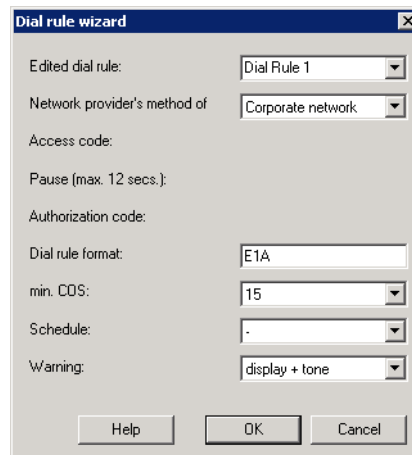
PBX Connection Variants for OpenScope Xpressions

Connecting HiPath 3000 (CorNet-IP)

7. Open the **Dial plan** page to configure the code number for PhoneMail.



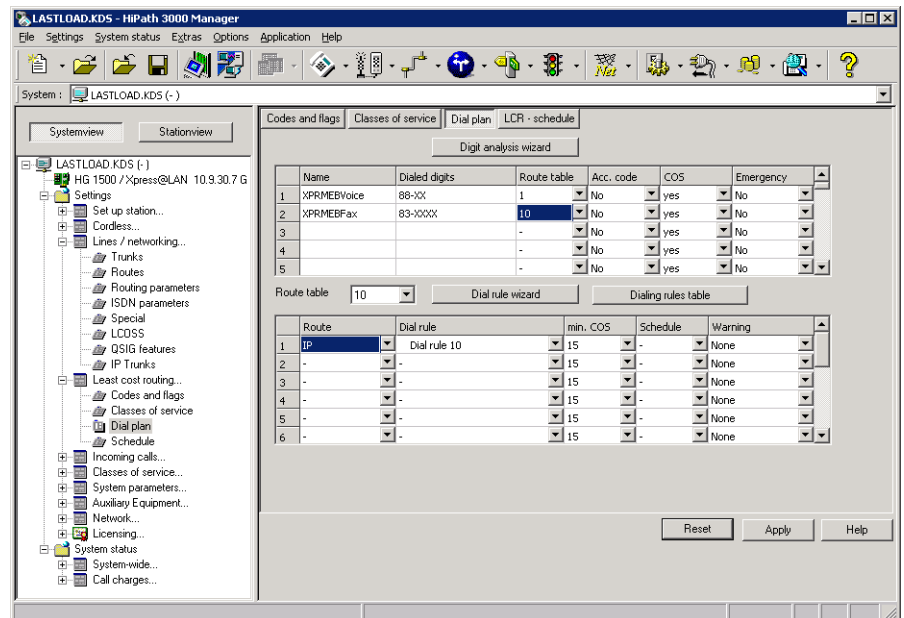
- a) Specify a dial rule. Set this dial rule analog to the following figure:



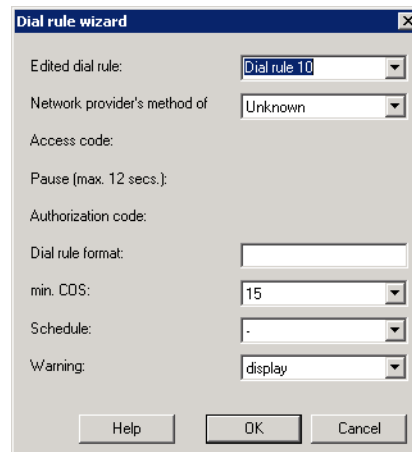
- b) In route table 1 set the *IP* route in the **Route** column and in the **Dial rule** column set the *Dial rule 1* just created.
- c) Then, set in the section on top of this the phone number analysis as follows:
 - **Name:** XPRMEBVoice
 - **Dialed digits:** 88-XX
 - **Route table:** 1
 - **Acc. code:** No
 - **COS:** yes

- **Emergency:** No

8. Configure the code number 83 for fax.



- a) First specify a dial rule here as well. Set this dial rule analog to the following figure:



- b) In route table 1 set the *IP* route in the **Route** column and in the **Dial rule** column set the *Dial rule 10* just created.
- c) Then, set in the section on top of this the phone number analysis as follows:

- **Name:** XPRMEBFax
- **Dialled digits:** 83-XXXX
- **Route table:** 10

PBX Connection Variants for OpenScape Xpressions

Connecting HiPath 3000 (CorNet-IP)

- **Acc. code:** No
- **COS:** yes
- **Emergency:** No

9. Click on **Apply**.

10. Transfer the changed KDS to the HiPath 3000.

The configuration of the example on the HiPath 3000 is thus complete.

D.3.2 Configuration in the HG1500

Now we need to configure the voice gateway in the HG 1500, i.e. set nodes and routing. The HG 1500 administration interface is operated via a browser.

NOTE: So that the HG1500 administration interface can be used, a Java Runtime environment must be installed on the computer.

Proceed as follows:

1. In the Manager E system view click on the **HG1500/ ...** option. Confirm the question for SSL according to your conditions. Subsequently, the administration interface opens in the standard browser.
2. Enable the write access for the administration interface configuration. First click on the footer once to activate the Java Applet contained therein and then click the **write access** icon.



3. In the main navigation click in the header of the administration interface the **Explorers** link. The Explorer navigation opens at the left margin.
4. In the Explorer navigation click the **Voice Gateway** option. A Java Applet starts with which the voice gateway configuration can be edited.
5. In the Java Applet open the **PBX > Nodes** folder.
6. Add a new node.
 - a) Click on the **Nodes** folder with the right mousebutton and select the **Add PBX Node** option in the context menu.
 - b) Assign a number to the new node, for our example number 1.
 - c) Then click **Apply**.
7. Select the new node in the **PBX > Nodes** list. The node settings are shown. Set the following options:
 - a) Click with the right mousebutton on the new node and select the **Edit IP Addresses** option.
 - b) Enter the XPR server IP address in the **HXG Gatekeeper Board 1 - IP Address** field. For our example this is 192.168.22.101.
 - c) Make sure that the **Alive Monitoring** checkbox is disabled.
 - d) Click on **Apply**.
8. Set the codecs for the example:

PBX Connection Variants for OpenScape Xpressions

Connecting HiPath 3000 (CorNet-IP)

- a) Click with the right mousebutton on the node and select the Edit Codecs option.
- b) Perform the following settings:

Codec	Priority	Voice Activity Detection (VAD)
G.711 A-Law	Priority 1	Off
G.711 μ -law	Priority 7	Off
G.723	Priority 4	Off
G.729	not used	Off
G.729A	Priority 3	Off
G.729B	not used	On
G.729AB	Priority 2	On

9. Enter the code number for the *Voice* service in the routing:
 - a) Click on the **Routing** entry with the right mousebutton and select the **Add Call Address** option.
 - b) Select under **Node Number** the node you have defined in step 6. In our example this is node 1.
 - c) In the **call address** field enter the phone number that we have intended for the *Voice* service and defined in the dial plan for PhoneMail (cf. [Section D.3.1, "Configuration in the Manager E"](#), step 7). In our example this is the phone number 88.
 - d) In the **Service** drop-down menu select the **Voice** option.
 - e) Click on **Apply**.
10. Enter the code number for the *Fax* service in the routing:
 - a) Click on the **Routing** entry with the right mousebutton and select the **Add Call Address** option.
 - b) Select under **Node Number** the node you have defined in step 6. In our example this is node 1.
 - c) In the call address field enter the phone number that we have intended for the *Fax* service and defined in the dial plan for Fax (cf. [Section D.3.1, "Configuration in the Manager E"](#), step 8). In our example this is the phone number 83.
 - d) In the **Service** drop-down menu select the **Fax** option.
 - e) Click on **Apply**.
11. Make sure that DTMF is activated in the parameters for H.323:

- a) Underneath the **Voice Gateway** folder click with the right mouse button on the **H.323 Parameters** option and select the **Edit H.323 Parameters** option.
 - b) Select the **User Input for DTMF Outband Signaling** check box.
 - c) Click on **Apply**.
12. Make sure that DTMF is also activated in the payload settings:
- a) In the Explorer navigation click the **Payload** link.
 - b) Click on the **HW Modules** folder with the right mousebutton and select the **Edit DSP Settings** option.
 - c) Select the **DTMF Outband Signaling** check box.
 - d) Click on **Apply**.
13. Transfer the modified settings to the HG1500. Click on the disk icon with the red background in the footer for this purpose.



IMPORTANT: When using T.38 or G.711 verify that no HG logging is active. This also applies for HG3550.

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.

The IP APL uses as error correction: **t38UDPRedundancy**.

The configuration of the example on the HG1500 is thus complete.

D.3.3 Configuration in the XPR Server

The site, as well as the extension range for the protocols PhoneMail and FaxG3 must now be configured in the XPR server.

1. Open the XPR monitor and log in as administrator.
2. In the **Modules of <server name>** dialog open the **ipApl** entry and doubleclick **Set Extended Options**.
3. The **IP APL Settings** dialog opens.

PBX Connection Variants for OpenScape Xpressions

Connecting HiPath 3000 (CorNet-IP)

4. Open the **Devices** tab and doubleclick the **H.323 Protocol Stack /HiPath CorNet-IP** entry. The configuration dialog opens.

The screenshot shows a configuration window titled "H.323 Protocol Stack / HiPath CorNet-IP". Inside, there's a "Device Settings" section with the subtitle "Configuration related to Channels". Below this are tabs for "Device", "Streaming", "Fax", and "QoS", with "Device" being the active tab. The "Device" section contains several input fields: "Number of physical channels:" (empty), "Number of built-in Fax G3 channels:" (set to 0), "Gateway address:" (empty), "Gatekeeper" section with "IP address:" (empty), "Registration E.164 address:" (empty), and "Registration H323 name:" (empty). Below these are radio buttons for "Default" (selected), "Intel PIMG", "HiPath 3000 >= V5.0", and "HiPath 4000 >= V2.0". There's a checkbox for "H323 Trace" (unchecked) and a text field next to it. The "Fake IDs" section has "Fake caller ID:" and "Fake called ID:" fields. Below that is a section for "Intel PIMG access numbers:" with a text field. At the bottom are two dropdown menus: "Type Of Number for outgoing calls:" (set to "Unknown") and "Numbering plan for outgoing calls:" (set to "Unknown"). At the very bottom are "OK", "Cancel", and "Apply" buttons.

5. Under **Number of physical channels** enter the number of channels that was configured in the HiPath. For the example this is two channels.

6. In the **Number of built-in Fax G3 channels** field you enter the maximum number of channels that may be available for a fax transmission. The difference between the **Number of physical channels** and **Number of built-in Fax G3 channels** fields is the number of channels exclusively available for voice transmission.

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.

The IP APL uses as error correction: **t38UDPRedundancy**.

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.

7. Enter under **Gateway address** the HG1500 IP address. This HG1500 is used for outgoing calls. Outgoing calls can be the following:
- Notification calls
 - MWI (Message Waiting Indication)
 - Monitored call forwarding

The IP APL is only released for access to one HG module.

IMPORTANT: If you make an entry in the **Gateway address** field, the fields in the **Gatekeeper** section must be empty.

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.

8. If you want to connect the IP APL with a H.323 gatekeeper, specify in the **Gatekeeper – IP address** field the IP address of the relevant H. 323 gatekeeper. We assume here that an operable network connection exists between the XPR server and the relevant gatekeeper.

IMPORTANT: By gatekeeper we understand here a real H.323 gatekeeper and no signaling gateway (see step 7 on page 445).

IMPORTANT: If you make an entry in the **Gatekeeper** section the **Gateway address** field must be empty.

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 as of software version 5.0 (Unify GmbH & Co. KG)
- HiPath 4000 as of software version 2.0 (Unify GmbH & Co. KG)

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.

9. The **H323 Trace** checkbox 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 SysWow64 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.

10. 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 **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.

11. Click on the **Streaming** tab.

PBX Connection Variants for OpenScape Xpressions
Connecting HiPath 3000 (CorNet-IP)

H.323 Protocol Stack / HiPath CorNet-IP

Streaming Settings

Configuration related to Streaming, Codec and DTMF

Device

Streaming

Fax

QoS

Streaming

Packet size (msec): 20

First RTP Port: 29100

Codec

☒ G.711a

☒ G.711μ

☐ G.729AB

DTMF Settings

☒ DTMF via RFC 2833

☒ DTMF via signalling messages

☒ In-Band DTMF Detection for G.711

OK

Cancel

Apply

12. 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.

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.

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.

NOTE: The value set here must also be set in the HG module of the PBX for all codecs the checkboxes of which you have activated in the **Codec** section. Enter this in the **Frame size** field via Internet browser. In version 7 of the module you find this field under **Explorers > Voice Gateway > Voice Gateway > Codec Parameters > Codec**.

13. 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 240 ports. Only modify the default value if problems with other programs that use the same port arise.

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>+240

14. In the **Codec** range you select the codecs that can be used for the communication. Available are **G.711A**, **G.711 μ** 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

Because 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

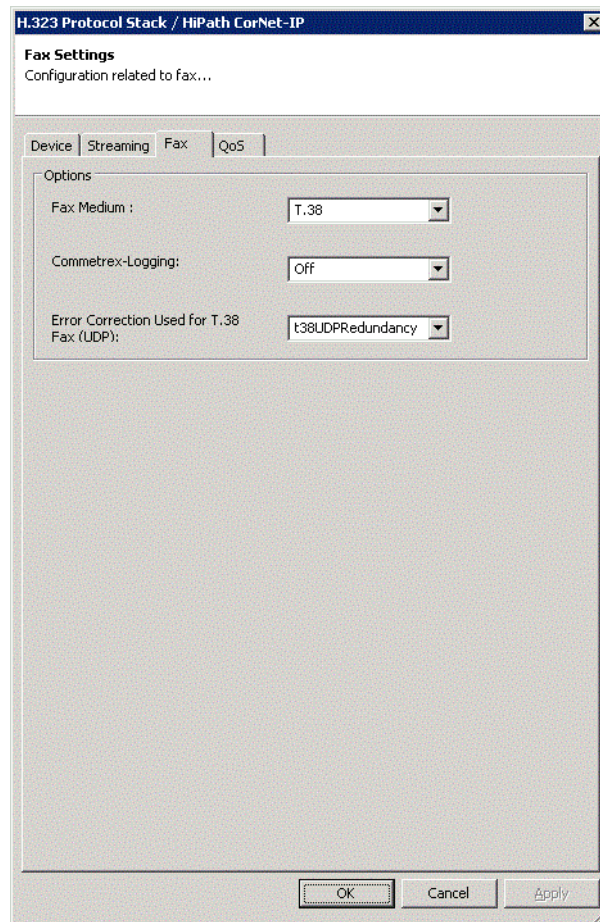
In the *DTMF Settings* section you specify how the IP APL processes DTMF signals. The following options are available:

- 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.

15. Click on the **Fax** tab.



16. 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.

17. 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 `\SysWow64\` under the name `trm*.log`. They may consist of text and also binary files. You cannot evaluate the log files yourself but need to send them to the company Commetrex.

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.

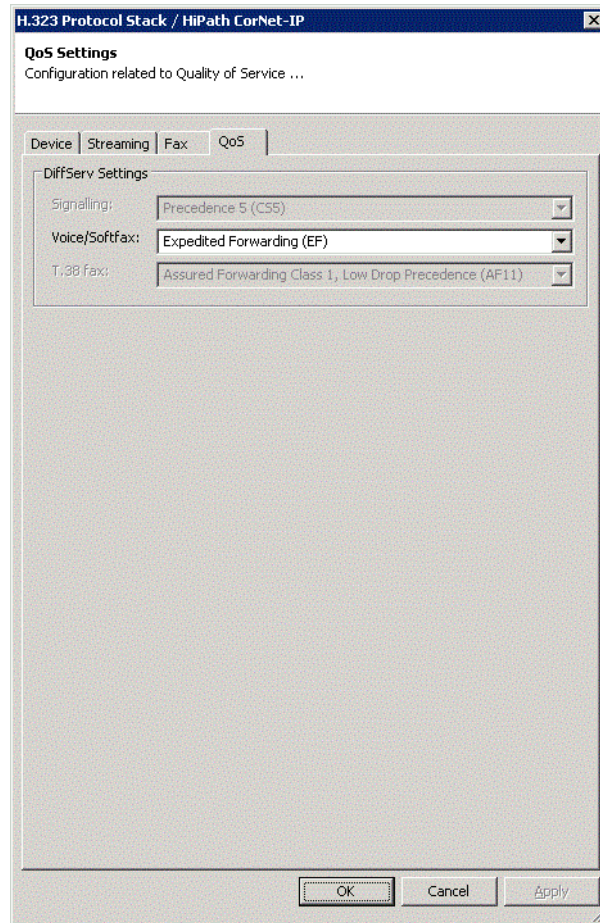
Therefore, activate logging only for the period in which you actually need it for the error search.

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.

18. Click on the **QoS** tab.



19. 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.

20. Click on **OK**.

PBX Connection Variants for OpenScape Xpressions

Connecting HiPath 3000 (CorNet-IP)

21. Open the **Extensions** tab.
22. Define the extension ranges for the protocols PHONEMAIL and FAX:
 - a) Click on the **Add** button above the list.
 - b) Enter value 3000 in the **Start** field and value 3010 in the **End** field.
 - c) In the **Bindings** drop-down menu select the **Fax Group 3 (FAXG3)** option.
 - d) Click on **OK**.
 - e) Click the **Add** button once more.
 - f) Enter value 8881 in the **Start** field and value 8886 in the **End** field.
 - g) In the **Bindings** drop-down menu select the **Xpressions PhoneMail** option.
 - h) Click on **OK**.
23. Enter the service access numbers for the PhoneMail protocol.
 - a) Doubleclick the **Xpressions PhoneMail** entry on the Protocols tab. The properties dialog of the protocol opens.
 - b) Open the **Script** tab and click on **Parameters....**
 - c) Enter the following numbers:

Service access	Number
Direct Access	8881
Guest/Forward Access	8882
Callback Access	8883
Fax Access	8884
Transfer Access	8885
Universal Access	8886t
 - d) Click on **OK**.
24. Close the IP APL settings dialog with **OK**.

Configuration in the XPR server is thus complete and the example operable.

D.4 Connecting HiPath 4000 V6 and OpenScape 4000 V7 / V8

NOTE: As of version 7, “HiPath 4000” is named “OpenScape 4000”.

For normal HiPath 4000 LTU connections and normal HiPath 4000 IPDA connections, use CorNet-IP as described in section [Section D.4.1, “CorNet-IP”](#), on page 455.

For HiPath 4000 SoftGate connections, use SIP as described in [Section D.4.2, “SIP”](#), on page 457.

D.4.1 CorNet-IP

IMPORTANT: PCI slots with ISDN boards of the Unify GmbH & Co. KG have been sold for new installations of a HiPath 4000 up to version V5. A HiPath 4000 with this hardware can be upgraded to hardware for HiPath 4000 V6 or OpenScape 4000 V7 by adding a DSCXL-V2 board. A connection from the XPR server to hardware upgraded in this way supports CorNet-IP and SIP, but no SIP-Q. This section describes how to connect this hardware.

IMPORTANT: If your hardware for HiPath 4000 V6 or OpenScape 4000 V7 is completely new, a purely server-based solution is on hand (VoIP switch). This hardware does not include any ISDN boards. It has been sold as of HiPath 4000 V6 R0. **This hardware supports SIP but no CorNet-IP and SIP-Q.** This section describes how to connect this hardware.

IMPORTANT: We **do not** recommend to connect a HiPath 4000 V6 **R0** via **SIP**. If you wish to use SIP, we recommend an upgrade of the HiPath 4000 to V6 **R1**, OpenScape 4000 V7 or later.

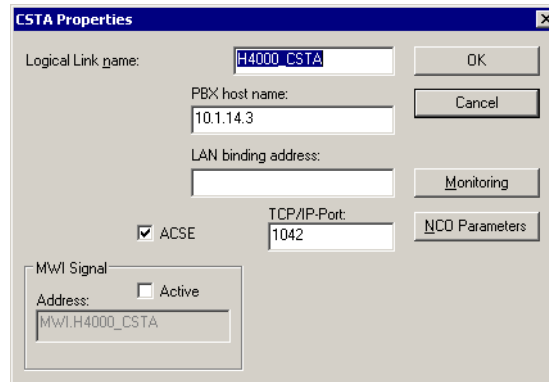
Connecting a HiPath 4000 V6 or OpenScape 4000 V7 differs only in one point from connecting a HiPath 4000 V4.0:

1. Start the XPR monitor.
2. Open the **Modules of <XPR server name>** window.
3. Doubleclick on **CtiApl**.
4. Doubleclick on **Edit Settings**.

PBX Connection Variants for OpenScope Xpressions

Connecting HiPath 4000 V6 and OpenScope 4000 V7 / V8

5. Doubleclick the HiPath 4000 V6/OpenScope 4000 V7 entry.



The screenshot shows the 'CSTA Properties' dialog box. It contains the following fields and controls:

- Logical Link name:** A text box containing 'H4000_CSTA'.
- PBX host name:** A text box containing '10.1.14.3'.
- LAN binding address:** An empty text box.
- TCP/IP-Port:** A text box containing '1042'.
- ACSE:** A checked checkbox.
- MWI Signal:** A section containing an 'Active' checkbox (unchecked) and an 'Address' text box containing 'MWI.H4000_CSTA'.
- Buttons:** 'OK', 'Cancel', 'Monitoring', and 'NCO Parameters'.

6. Activate the **ACSE** (Association Control Service Element) checkbox.
7. Click on **OK**.

D.4.2 SIP

IMPORTANT: PCI slots with ISDN boards of the Unify GmbH & Co. KG have been sold for new installations of a HiPath 4000 up to version V5. A HiPath 4000 with this hardware can be upgraded to hardware for HiPath 4000 V6 or OpenScape 4000 V7 by adding a DSCXL-V2 board. A connection from the XPR server to hardware upgraded in this way supports CorNet-IP and SIP, but no SIP-Q. This section describes how to connect this hardware.

IMPORTANT: If your hardware for HiPath 4000 V6 or OpenScape 4000 V7 is completely new, a purely server-based solution is on hand (VoIP switch). This hardware does not include any ISDN boards. It has been sold as of HiPath 4000 V6 R0. **This hardware supports SIP but no CorNet-IP and SIP-Q.** This section describes how to connect this hardware.

IMPORTANT: We **do not** recommend to connect a HiPath 4000 V6 **R0** via **SIP**. If you wish to use SIP, we recommend an upgrade of the HiPath 4000 to V6 **R1**, OpenScape 4000 V7 or later.

Execute the following steps to connect a HiPath 4000 V6 or OpenScape 4000 V7 to XPR.

NOTE: The following steps describe the procedure for HiPath 4000 V6. The steps for OpenScape 4000 V7 are analog.

1. Install and configure the HiPath 4000 V6 according to the instructions given in the setup guide *HiPath 4000 V6, Installation*, for example.
2. To configure SIP trunks, follow the instructions given in the service documentation *HiPath 4000 V6, Volume 4 - IP Solutions*, section *Native SIP Trunking*.

This trunk configuration also contains configuring the Common gateway.

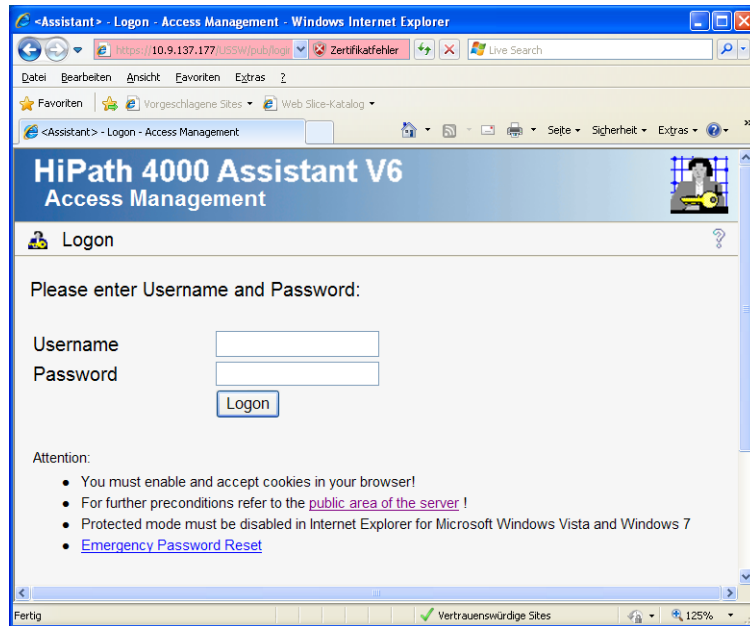
PBX Connection Variants for OpenScope Xpressions

Connecting HiPath 4000 V6 and OpenScope 4000 V7 / V8

You need to execute the following steps in addition:

3. Enter the following address in a browser to open the web-based manager of the HiPath 4000 V6.

`https://<IP address of the HiPath 4000 V6>`

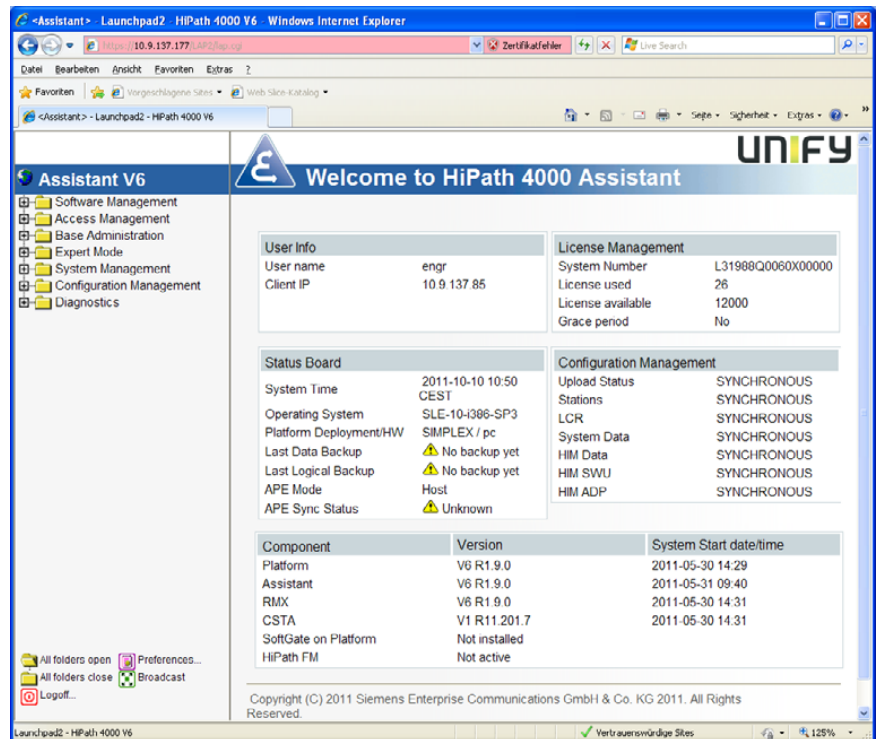


4. Verify that the browser complies with all requirements listed on this page.

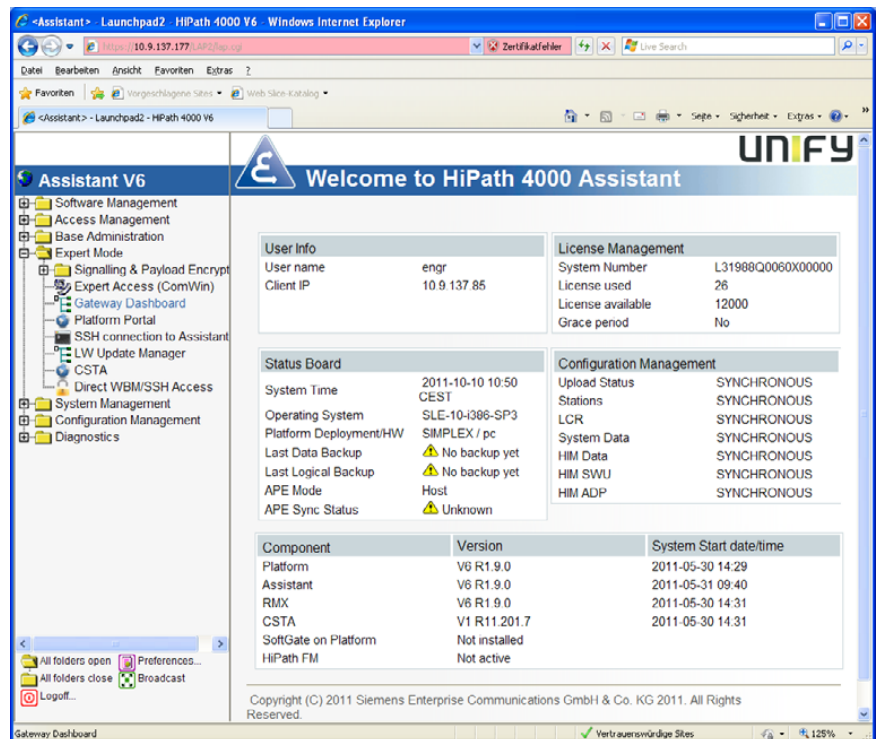
PBX Connection Variants for OpenScope Xpressions

Connecting HiPath 4000 V6 and OpenScope 4000 V7 / V8

5. Enter the user name and password and click on **Login**.



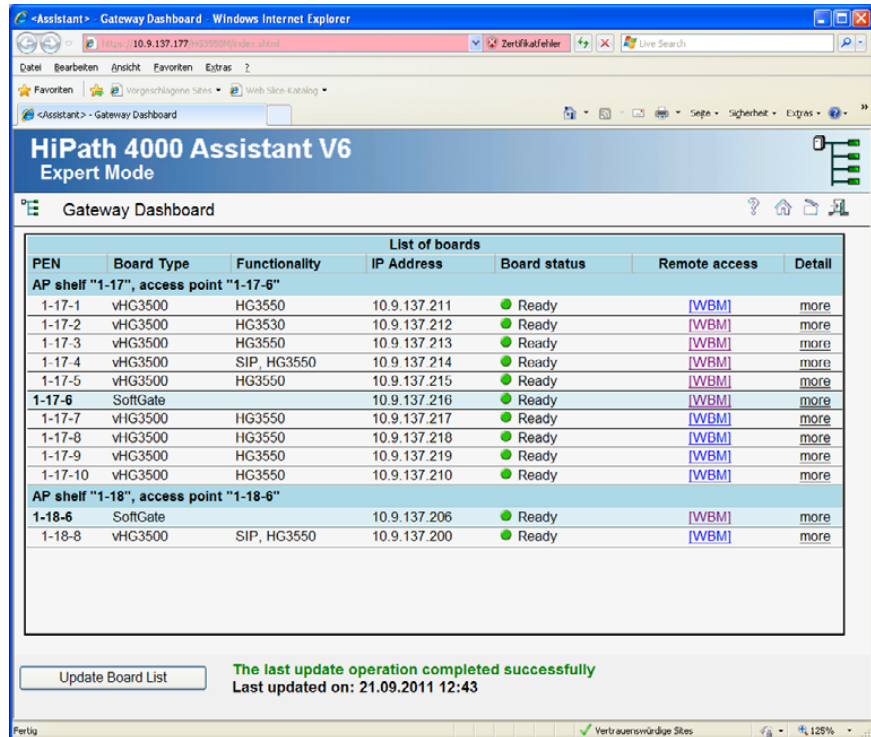
6. Open in the navigator **Expert Mode > Gateway Dashboard**.



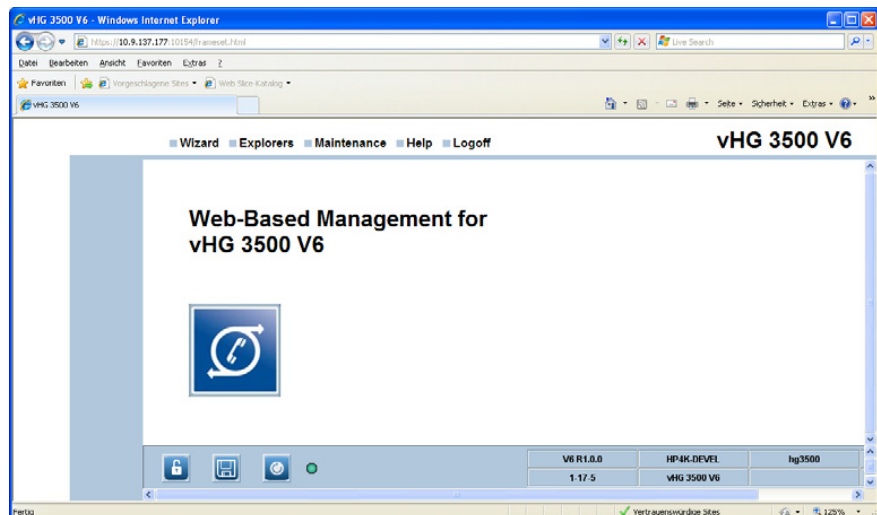
PBX Connection Variants for OpenScope Xpressions

Connecting HiPath 4000 V6 and OpenScope 4000 V7 / V8

7. Doubleclick Gateway Dashboard.

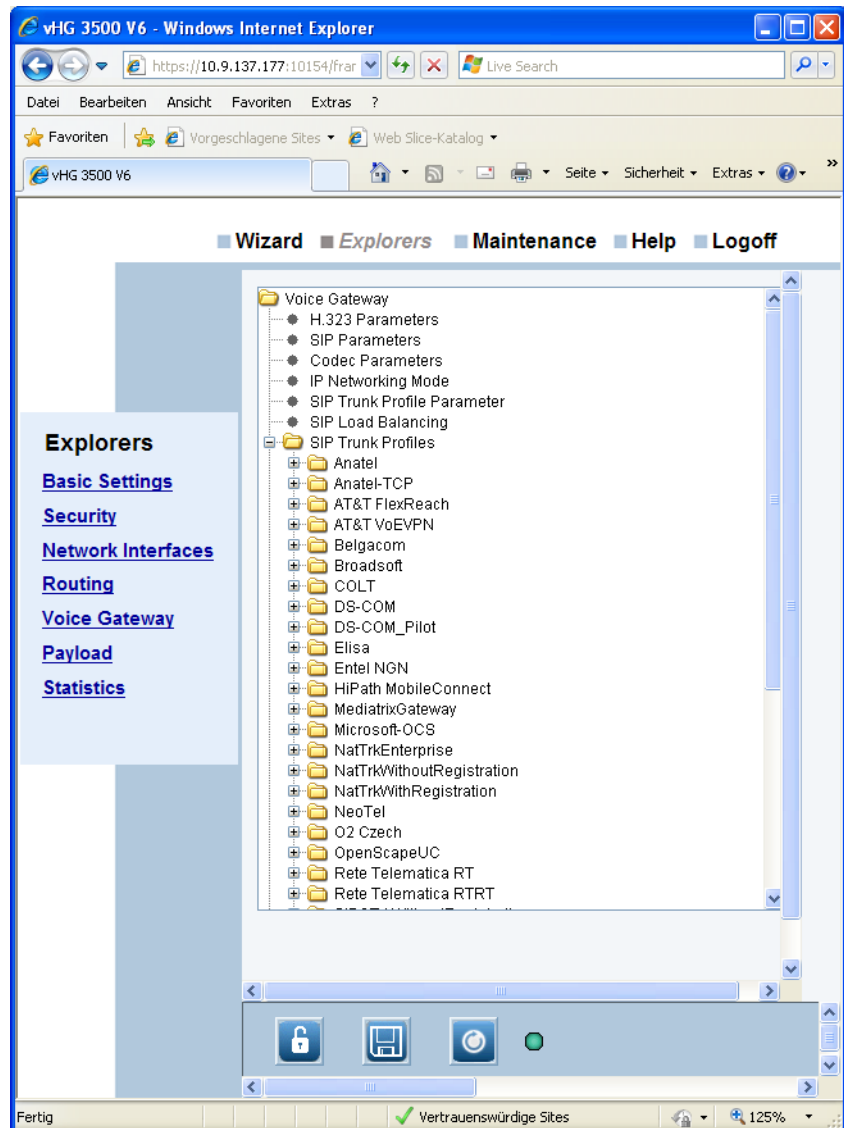


8. In the Remote access column, click on the entry of the gateway used for connecting the HiPath 4000 V6 to XPR.



9. Click on **Explorers**.

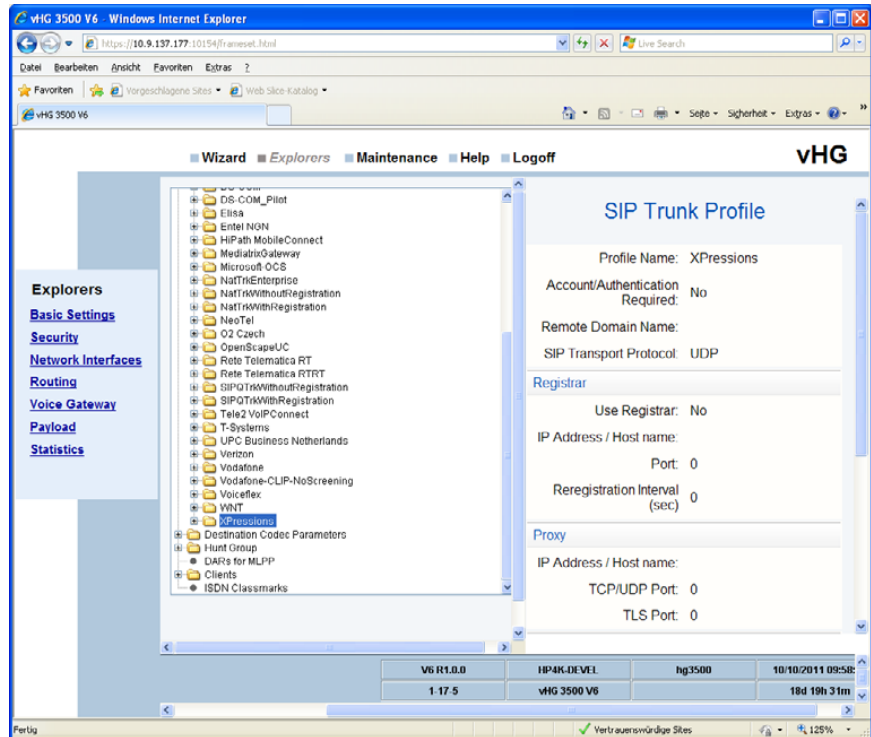
10. Click on **Voice Gateway**.



PBX Connection Variants for OpenScope Xpressions

Connecting HiPath 4000 V6 and OpenScope 4000 V7 / V8

11. Open **SIP Trunk Profiles > Xpressions**.



12. Rightclick **Xpressions** and select **Modify**.

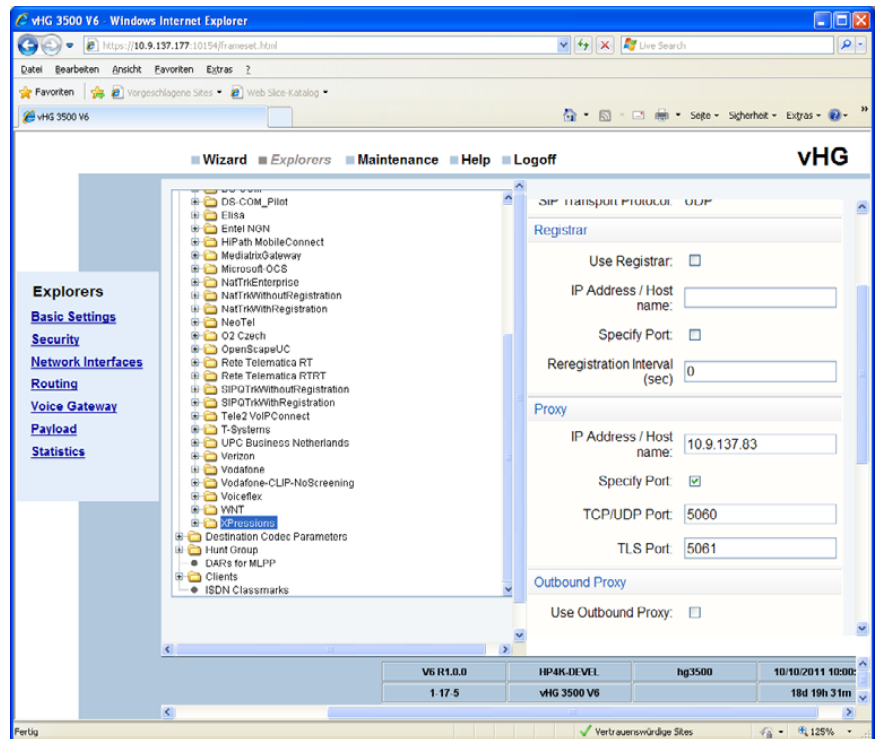
13. Scroll down the right-hand section until you see the **Proxy** group.

14. In the **IP Address/Host name** field, enter the IP address of the computer on which the OpenScope Xpressions is installed.

PBX Connection Variants for OpenScope Xpressions

Connecting HiPath 4000 V6 and OpenScope 4000 V7 / V8

15. Value 5060 is used for the TCP/UDP port and value 5061 for the TLS port by default. If you use other port numbers, activate the **Specify Port** check box and enter your values.

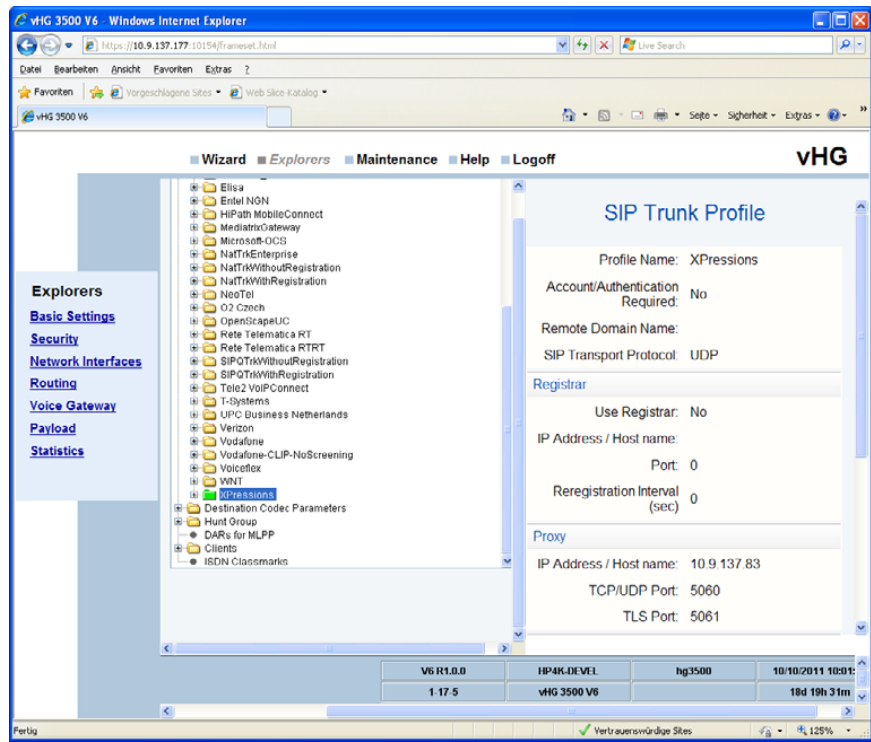


16. Click on the **Apply** button.

PBX Connection Variants for OpenScope Xpressions

Connecting HiPath 4000 V6 and OpenScope 4000 V7 / V8

17. In the navigator, rightclick Xpressions and select **Activate**. After its activation the **Xpressions** folder is green.

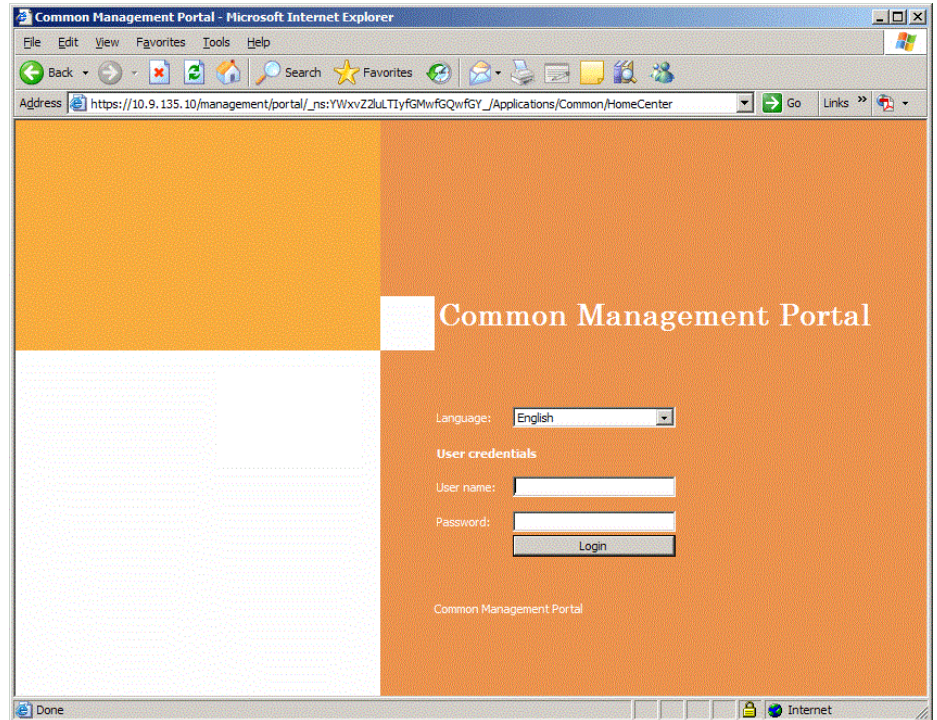


18. Beneath the navigator, click on the disk icon to save the entries.



D.4.2.1 Start

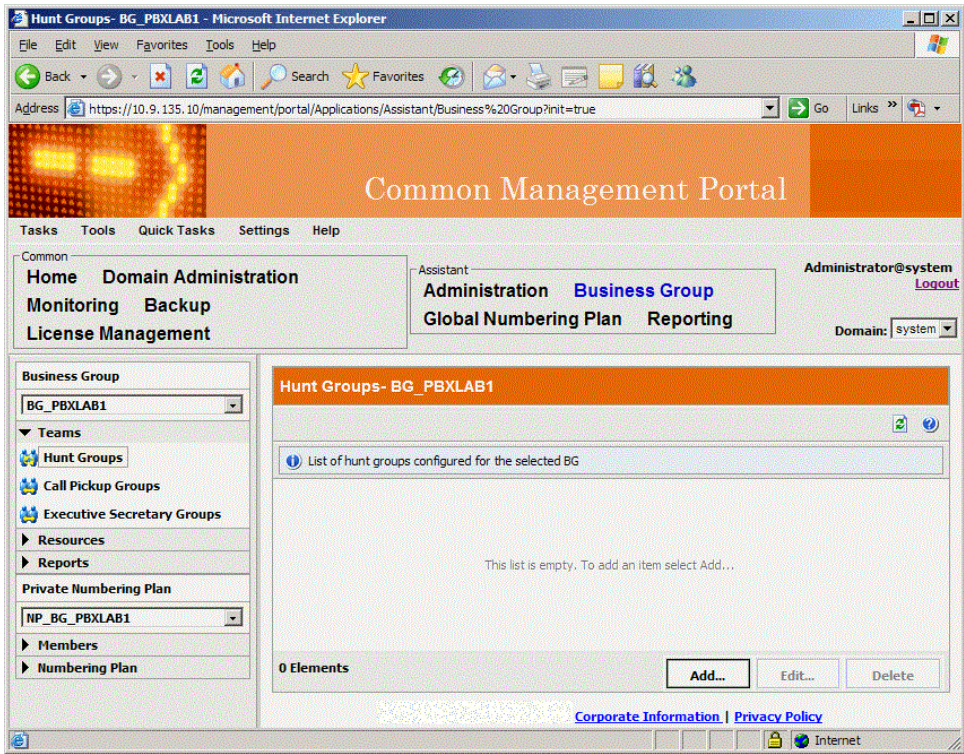
Open the address <https://<IP address of the HiPath 8000 V3.0>/management> in a browser.



Enter the user name and password and push the **Login** button.

PBX Connection Variants for OpenScope Xpressions
Connecting HiPath 4000 V6 and OpenScope 4000 V7 / V8

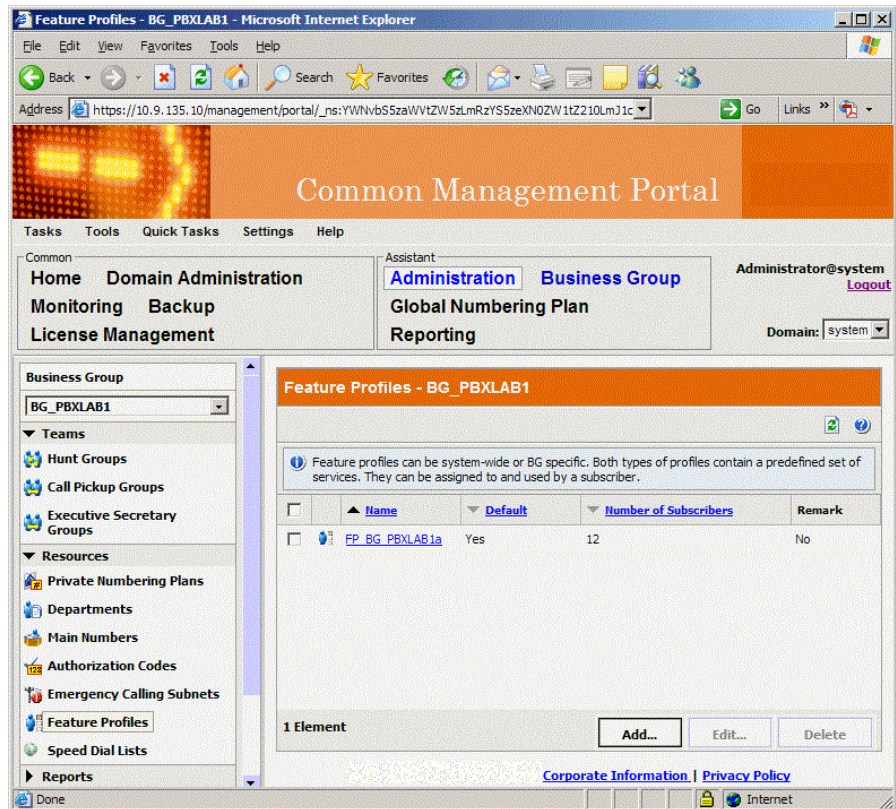
Click on the **Business Group** button.



D.4.2.2 Creating a Feature Profile

For each access number in the XPR IP APL, for example number for Direct Access, Forward Access or Callback Access, a subscriber must be created. The creation of a feature profile is suitable for an efficient assignment of properties to several subscribers.

Expand the **Resources** category on the left hand side and click on **Feature Profiles**.



Click the **Add...** button.

PBX Connection Variants for OpenScope Xpressions

Connecting HiPath 4000 V6 and OpenScope 4000 V7 / V8

https://10.9.135.10 - PopUp - Microsoft Internet Explorer

Add Feature Profile:BG_PBXLAB1

Here you can modify the current configuration of the services contained in this feature profile.

General Services

Identification

The default Feature Profile is used for the creation of a Subscriber.

Name:

Remark:

Default: ☐

Done Internet

In the **Name** field enter the name of the feature profile.

Activate the **Default** checkbox.

Click the **Services** tab.

PBX Connection Variants for OpenScape Xpressions

Connecting HiPath 4000 V6 and OpenScape 4000 V7 / V8

https://10.9.135.10 - Add Feature Profile:BG_PBXLAB1 - Microsoft Internet Explorer

Add Feature Profile:BG_PBXLAB1

Here you can modify the current configuration of the services contained in this feature profile.

General | **Services**

Services

A checkmark in a green dot on the left of a service indicates that the service is subscribed and activated.
Services may be mutually exclusive.
Attention: selecting one service may cause another service to be deactivated automatically by the tool.

Call Forwarding

Services	Subscribe
☐ Busy	No
☐ Enhanced	No
☐ No Reply	No
☐ Remote Activation	No
☐ Connected line identification presentation	No
☐ Selective	No
☐ Unconditional	No
☐ Usage Sensitive Variable	No
☐ Voice Mail	No
☐ Call Forwarding Internal/External	No

OK Cancel

Set, for example, the value of the fields

- **Voicemail,**
- **Called Name Delivery,**
- **Called Number Delivery,**
- **Caller ID, Connected Line Identification,**
- **Malicious Call Trace,**
- **Name Delivery,**
- **Outgoing CID Suppression,**
- **CSTA,**
- **Call Hold** and
- **Call Transfer**

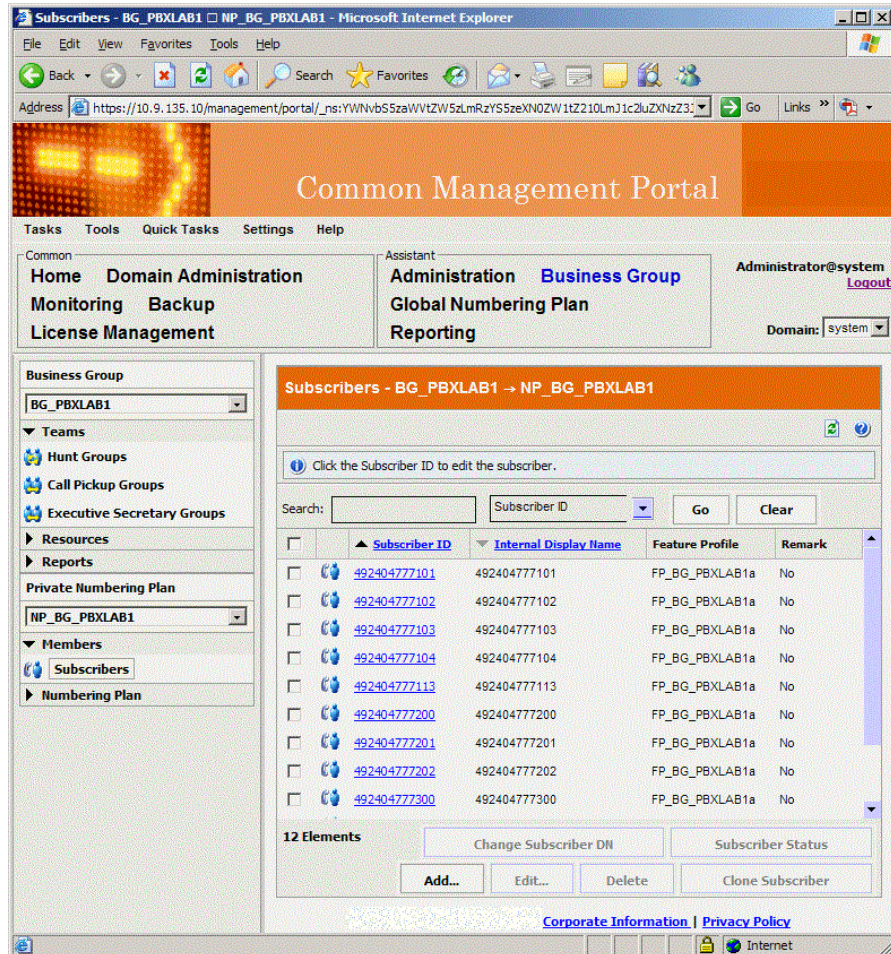
to Yes. Behind the **CSTA** field select the value *Type 1*.

Click on **OK**.

D.4.2.3 Creating a Subscriber

For each access number in the XPR IP APL, for example number for Direct Access, Forward Access or Callback Access, a subscriber must be created. The creation of a feature profile is suitable for an efficient assignment of properties to several subscribers.

Expand the **Members** category on the left hand side and click on **Subscribers**.



Click the **Add...** button.

PBX Connection Variants for OpenScape Xpressions

Connecting HiPath 4000 V6 and OpenScape 4000 V7 / V8

https://10.9.135.10 - Subscriber:BG_PBXLAB1 - - Microsoft Internet Explorer

Subscriber:BG_PBXLAB1 -

Subscriber Description

General User SIP Advanced Hunt Groups Keyset Services

Private Numbering Plan

Choose the PNP for this subscriber

Numbering Plan: NP_BG_PBXLAB1 (Default) ...

Subscriber

Add the basic information for this subscriber.

Remark:

Office Code: +49 (2404) 777 ...

Extension: ...

Internal Display Name:

Unicode Internal Display Name:

External Display Name:

Unicode External Display Name:

Call Pickup Group: ...

Routing

These optional attributes are used in the numbering plans for routing purposes (call originator attributes).

Class Of Service: ...

OK Cancel

Done Internet

Assign a value to the **Numbering Plan** and **Office Code** field if this has not already been done automatically.

Assign a value to the **Extension** field by pushing the button next to this field.

If required, enter a value in the fields **Internal Display Name**, **Unicode Internal Display Name**, **External Display Name** and **Unicode External Display Name**.

Click on the **SIP** tab.

PBX Connection Variants for OpenScape Xpressions

Connecting HiPath 4000 V6 and OpenScape 4000 V7 / V8

The screenshot shows a web browser window with the address bar displaying "https://10.9.135.10 - Subscriber:BG_PBXLAB1 - Microsoft Internet Explorer". The page title is "Subscriber:BG_PBXLAB1 -". Below the title bar, there is a "Subscriber Description" section with a user icon. The main navigation tabs are "General", "User", "SIP", "Advanced", "Hunt Groups", "Keyset", and "Services". The "SIP" tab is selected. The "Phone" section contains the following fields and options:

- Name:** A text input field.
- Type:** A dropdown menu set to "Dynamic".
- Transport Protocol:** A dropdown menu set to "UDP".
- IP Address:** A text input field.
- Port:** A text input field.
- SIP Phone:** A text input field containing "Executive Secretary Configuration".
- Associated Proxy Device:** A text input field with a dropdown arrow.

Below the "Phone" section, there is a "Remote Phone" section with a message: "Additional SIP phones of the current subscriber are displayed below. Clicking on the IP address will redirect you to the phone's administration. The link 'phone status' will display the main characteristics of the phone." Below this message, it says "0 Elements" and "This list is empty.".

The "Security" section contains the following fields:

- Realm:** A text input field.
- User Name:** A text input field.
- Password:** A text input field.

At the bottom right of the form, there are "OK" and "Cancel" buttons. The browser's status bar at the bottom shows "Done" and "Internet".

Assign value *Static* to the **Type** field.

Assign value *UDP* to the **Transport Protocol** field.

Enter the XPR server IP address in the **IP Address** field and value *5060* in the **Port** field.

Click on the **Services** tab.

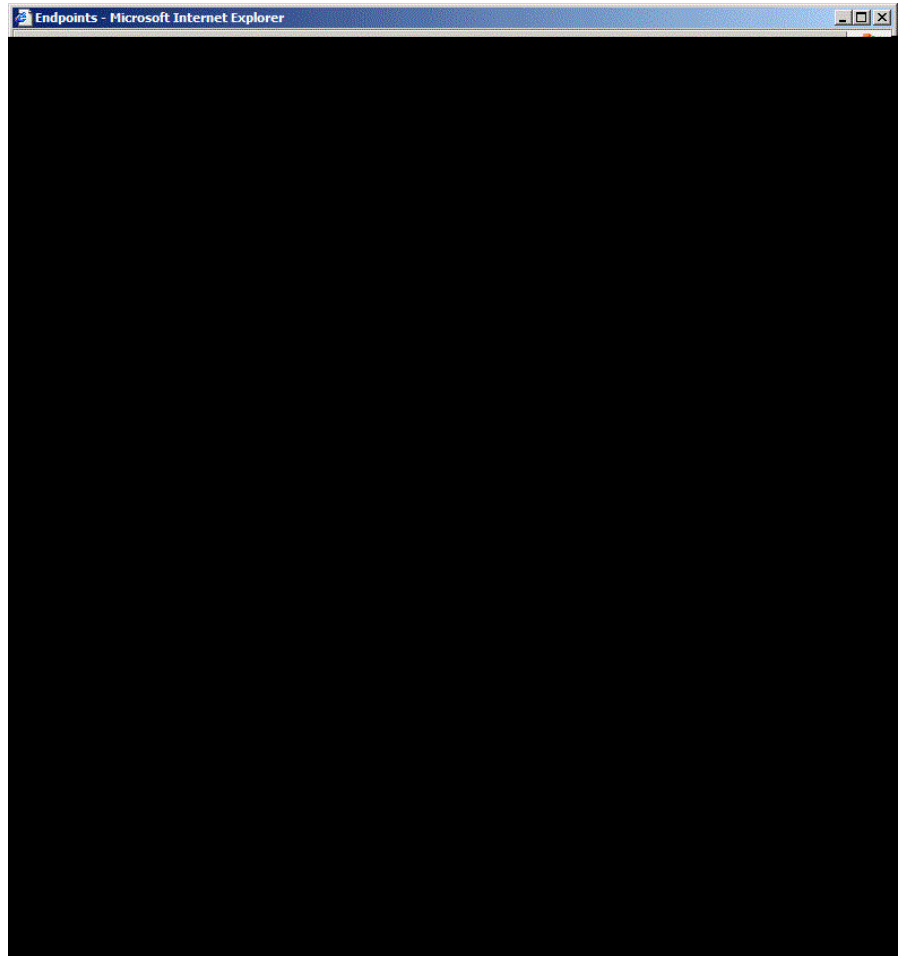
If required, assign a value to the **Feature Profile** field by pushing the button next to this field. The services fields will be allocated with the values set in the feature profile.

Click on **OK**.

D.4.2.4 Endpoint Configuration

When creating a subscriber, an endpoint is automatically created as well, which needs to be configured.

Expand the **Numbering Plan** category on the left hand side and click on **Endpoints**.



Click on the endpoint that was automatically created upon the creation of a subscriber.

Activate the checkboxes **Trusted Device** and **Registered** and push the **OK** button.

D.4.3 Configuration of the HiPath 8000 V3.0 via NMC and SMC

In the following we will provide a general overview of the configuration of a connection between an XPR server and a HiPath 8000 V3.0. You find detailed instructions and descriptions in the following HiPath 8000 V3.0 manuals:

- Configuration and Administration using NetManager NMC
- Configuration and Administration using CLI
- Subscriber Account/Services Administration using NetManager SMC

Before it is possible to establish a connection between the XPR server and HiPath 8000 V3.0 the following requirements must be met:

1. The HiPath 8000 V3.0 administration is managed via the NMC and the SMC client. To install the connection between the XPR server and HiPath 8000 V3.0, accounts with sufficient privileges are required on the SMC as well as on the NMC.
2. A dialing plan (E.164¹ or private) must exist in order to access the XPR server.
3. The office codes and the connected home dial numbers must have been already entered with the help of the Home DN Managers in the NMC.
4. If an SIP authentication has been configured for clients, the XPR server must become a permanent entry in the NMC for an outcall (e.g. voice mail output via telephone). Otherwise the outcall will be refused due to the lacking authorization. Proceed as follows:
 1. In the NMC open the **Signaling Manager** and thereunder the **SIP** entry.
 2. Open the **Provisioning** tab.
 3. Open the **HTTP Authentication** tab.
 4. Open the **Digest** tab.
 5. Select the **Enable Authentication** option.

1. Standard for Carrier Dialing Plan (see HiPath 8000 V3.0 documentation)

5. Open the **Realms** tab and select the entry that contains the XPR server IP address. Then click the **Modify** button on the right margin. Up comes this dialog:

The screenshot shows a 'Modify Realm' dialog box. It has a title bar with the text 'Modify Realm' and a close button. The dialog contains the following fields and controls:

- ID Type:** A dropdown menu with 'IP Address' selected.
- ID:** Four separate input boxes containing the values '139', '23', '49', and '149'.
- Trusted Entity:** A checkbox that is checked.
- Local Realm:** An empty text input field.
- Local Username:** An empty text input field.
- Local Password:** An empty text input field.
- Confirm Local Password:** An empty text input field.
- Remote Realm:** An empty text input field.
- Remote Username:** An empty text input field.
- Remote Password:** An empty text input field.
- Confirm Remote Password:** An empty text input field.
- Buttons:** 'OK', 'Cancel', and 'Help' buttons at the bottom right.

1. Select the **Trusted Entity** option and click the **OK** button.
2. In the NMC window click the **Apply** button.

D.4.3.1 Configuration of the basic Voice Mail Number

To install the XPR server on the HiPath 8000 V3.0, the following steps are necessary.

1. Define the numbers home DN's that are to be assigned to the XPR server.
2. Create this number with the help of the Home DN Managers in the NMC (menu **Tools** -> **Home DN Manager**).
3. Create the business group lines (BGL) that are linked to the home DN's. Therefore connect to the HiPath 8000 V3.0 and start the SMC client.
4. Select **New BGL** and **Create BGL** and enter the following information for the BGL:

Description	Value
Connection Information	SIP Phone
Registration Type	static
Transport Type	UDP
Address	<i>IP address of the XPR server</i>
Port	5060
Register	Select yes (the XPR server does not register automatically)
VOIP: Echo Cancellation	Select Disabled

5. After the BGLs have been created, the XPR numbers must exist as SIP endpoints.

NOTE: For a connection between HiPath 8000 V3.0 and an XPR server a connection via E.164 should be preferred. In such a case, the HiPath 8000 V3.0 always provides normalized numbers to the XPR server.

D.4.3.2 Forwarding to OpenScape Xpressions for a HiPath 8000 V3.0 Subscriber

The following steps are required to activate the *Call Forward on Busy and No-Answer* feature:

1. Log on the HiPath 8000 V3.0 via the SMC client.
2. Select the Business Group (BG) of the subscriber for whom *Call Forward on Busy and No-Answer* shall be activated.
3. On the **New BGL** tab select the Business Group Line (BGL) for which *Call Forward on Busy and No-Answer* shall be activated.
4. Select the **BGL Services** tab.
5. Under the **Call Forward** feature you will find a **voice mail** option. Click the yellow arrow to open the configuration possibilities.
6. Set the following options:
 - Option **Operation** to **Subscribed**.
 - Select the **Activate** option.
 - Enter the value for the ringing tone duration in seconds.
 - Option **Voice mail number** to the normalized Forward Access Number of the XPR server.
7. Click the **Submit** button.

Call Forward on Busy and No-Answer should now be active for the subscriber in the HiPath 8000 V3.0.

NOTE: You can use a *Business Group Feature Profile* in a HiPath 8000 V3.0 to configure this feature. Such a profile can then be applied to several BGLs, so that not each single subscriber must be configured individually. You find further information about configuring a Business Group Feature Profile in the HiPath 8000 V3.0 documentation.

D.4.4 IP APL Configuration

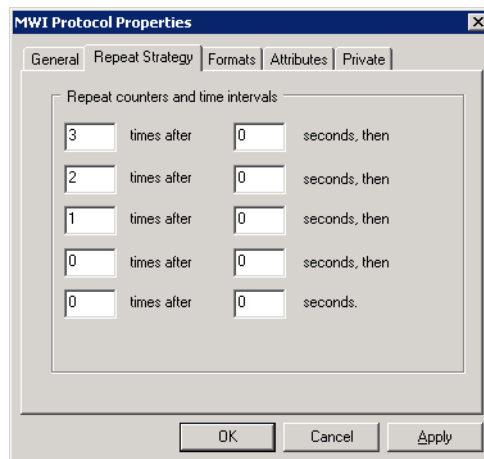
IMPORTANT: To configure the IP APL, an XPR server and the IP APL must already have been installed.

So that the connection of the HiPath 8000 V3.0 to the XPR server works correctly, the XPR server IP APL must now be configured. This includes the MWI protocol configuration (cf. [Section D.4.4.1, “Configuring the MWI Protocol”, on page 478](#)) and the activation of the SIP device (cf. [Section D.4.4.2, “Activating the SIP Device”, on page 479](#)).

D.4.4.1 Configuring the MWI Protocol

To support MWI, the *Message Waiting Indication* protocol must be implemented in the IP APL. Proceed as follows:

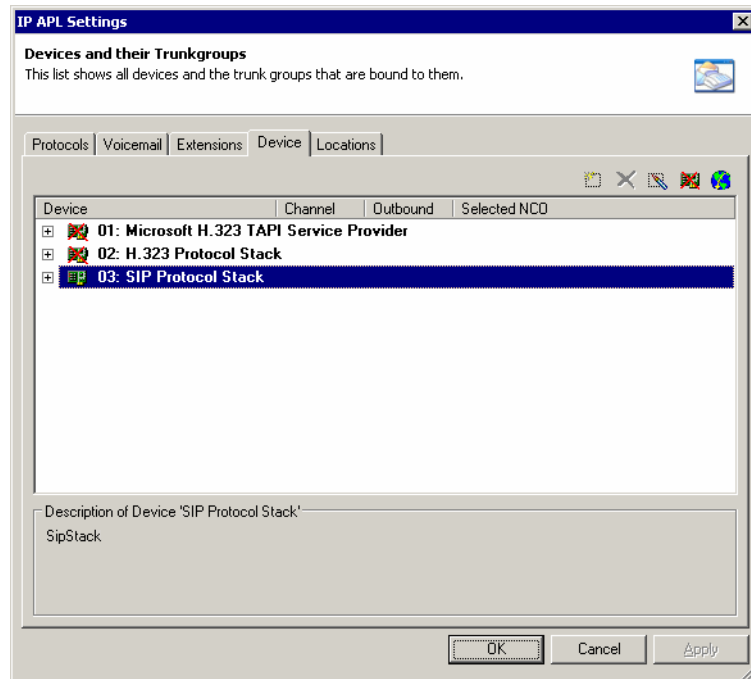
1. In the modules window of the XPR monitor select the **IpApl > Set Options** menu item.
2. Add the *Message Waiting Indication* protocol on the **Protocols** tab of the configuration dialog.
3. Open the configuration dialog for the *Message Waiting Indication* and switch to the **Repeat Strategy** tab.



4. Set all MWI protocol settings to value **0**.
5. Copy the settings with the **OK** button.

D.4.4.2 Activating the SIP Device

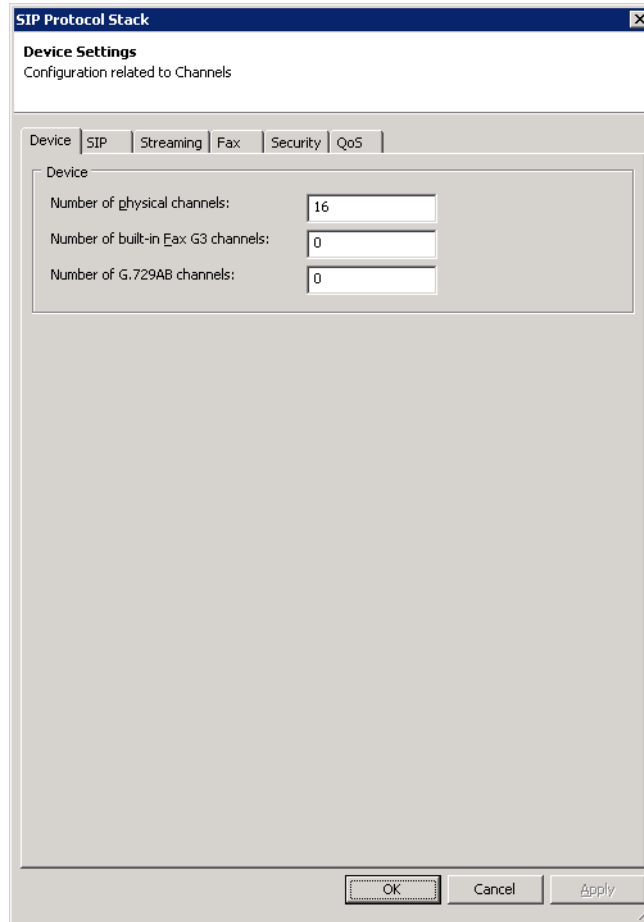
1. In the modules window of the XPR monitor select the **IpApl > Set Options** menu item.
2. In the **IP APL Settings** dialog switch to the **Device** tab.



3. Activate the *SIP Protocol Stack* device with the **activate** icon in the toolbar.

IMPORTANT: In an IP APL, only one device may be activated at a time. Therefore, make sure that all devices, except for the SIP Protocol Stack, are deactivated.

4. Open the SIP device configuration dialog with a doubleclick on the *SIP Protocol Stack* device.



The following fields correspond to those for the H.323 device (cf. [Section D.3.3, “Configuration in the XPR Server”, on page 443](#)).

- **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.

5. 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.

6. Click on the **SIP** tab.

The screenshot shows the 'SIP Protocol Stack' configuration window with the 'SIP Settings' tab selected. The window title is 'SIP Protocol Stack'. Below the title bar, it says 'SIP Settings' and 'Configuration related to Addresses, Action and Transport'. There are five tabs: 'Device', 'SIP', 'Streaming', 'Fax', 'Security', and 'QoS'. The 'SIP' tab is active. The 'SIP Options' section has three radio buttons: 'SIP Proxy IP Address' (selected), 'SIP Proxy DNS Name', and 'Own IP Address'. The 'SIP Proxy IP Address' field shows '10 . 12 . 14 . 16' and '5060'. The 'SIP Proxy DNS Name' field is empty. The 'Own IP Address' field shows '10 . 12 . 14 . 20' and '5060'. The 'Action' section has two radio buttons: 'Act as SIP Trunk' (selected) and 'Act as SIP User'. The 'Own SIP user name' field is empty. The 'Transport' section has three radio buttons: 'UDP' (selected), 'TCP', and 'TLS'. At the bottom are 'OK', 'Cancel', and 'Apply' buttons.

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 a HiPath 8000 cluster, the SIP proxy must be defined via its complete cluster name – example:

HiPath8000.Alsdorf.com.

For further information please refer to the *OpenScape Xpressions Server Administration* manual.

7. 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.

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

PBX Connection Variants for OpenScape Xpressions

Connecting HiPath 4000 V6 and OpenScape 4000 V7 / V8

- for the options TLS (see below) with value 5061.
8. 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 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 voicemail protocol.

9. With the **UDP**, **TCP** and **TLS** options you define which protocol the IP APL is to use for the SIP communication with the gateway.

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: If you select the **TLS** option here, you need to perform additional security settings via the **Security** tab.

10. Click on the **Streaming** tab.

The screenshot shows the 'SIP Protocol Stack' configuration window with the 'Streaming' tab selected. The window title is 'SIP Protocol Stack'. Below the title bar, the 'Streaming Settings' section is visible, with the subtitle 'Configuration related to Streaming, Codec and DTMF'. The 'Streaming' tab is active, showing settings for 'Packet size (msec)' set to 30, 'First RTP Port' set to 29100, and 'First T.38 Port' set to 12500. The 'Codec' section shows checkboxes for 'G.711a' (checked), 'G.711µ' (checked), and 'G.729AB' (unchecked). The 'DTMF Settings' section shows checkboxes for 'DTMF via RFC 2833' (checked), 'DTMF via SIP INFO Messages' (checked), and 'In-Band DTMF Detection for G.711' (checked). At the bottom of the window are 'OK', 'Cancel', and 'Apply' buttons.

SIP Protocol Stack

Streaming Settings
Configuration related to Streaming, Codec and DTMF

Device | SIP | **Streaming** | Fax | Security | QoS

Streaming

Packet size (msec): 30

First RTP Port: 29100

First T.38 Port: 12500

Codec

☒ G.711a ☒ G.711µ ☐ G.729AB

DTMF Settings

☒ DTMF via RFC 2833
☒ DTMF via SIP INFO Messages
☒ In-Band DTMF Detection for G.711

OK Cancel Apply

11. 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.

12. 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 240 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> + 240**

IMPORTANT: The port ranges for RTP and T.38 (see below) must not clash.

13. 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 120 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 T.38 Port**> to <**First T.38 Port**>+120

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.

14. 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.

15. 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

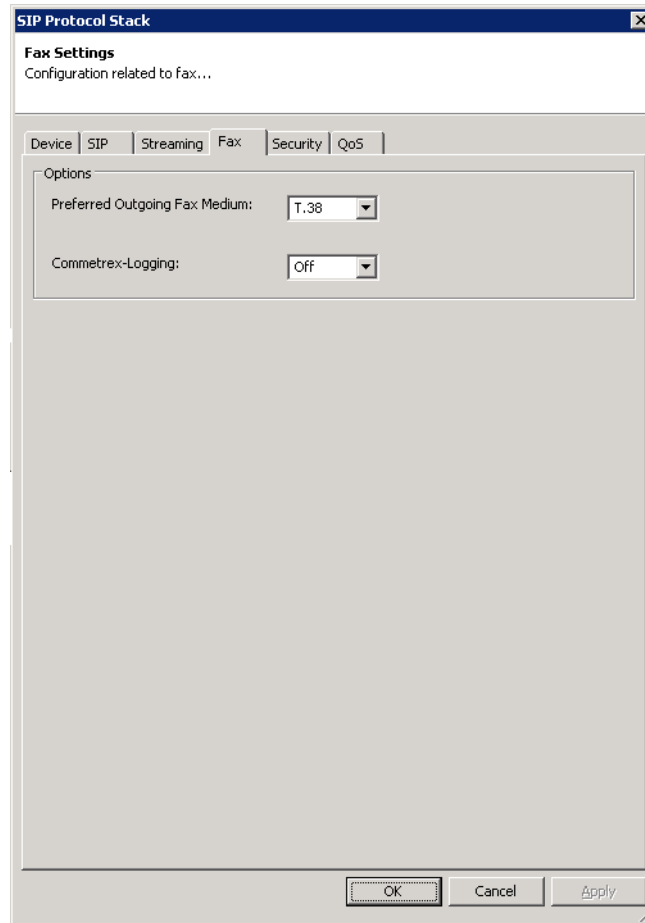
All three options are activated by default.

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 simultaneously transfers a DTMF tone out-of-band and in-band 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.

16. Click on the **Fax** tab.



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.

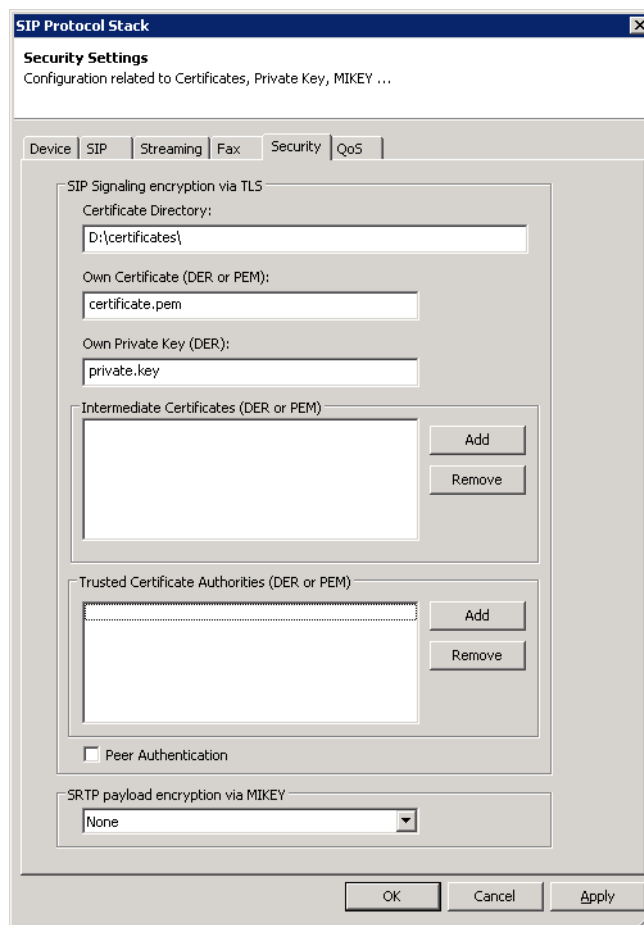
IMPORTANT: Sending and receiving of fax messages may cause disturbances in the IP APL if heavy fax traffic and the execution of maintenance script jobs coincide.
Therefore, perform maintenance script jobs at times when you do not expect heavy fax traffic – e.g. at night. If the described problem arises just the same, reduce the priority for the automatic XPR server maintenance.

17. In the **Preferred Outgoing Fax Medium** field you specify whether fax messages are sent via G.711 or T.38.

18. 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 `\SysWow64\` 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.

19. Click on the **Security** tab.



The screenshot shows the 'SIP Protocol Stack' window with the 'Security Settings' tab selected. The window title is 'SIP Protocol Stack' and the subtitle is 'Security Settings Configuration related to Certificates, Private Key, MIKEY ...'. The 'Security' tab is active, showing fields for 'Certificate Directory' (D:\certificates\), 'Own Certificate (DER or PEM)' (certificate.pem), 'Own Private Key (DER)' (private.key), and 'Intermediate Certificates (DER or PEM)' with 'Add' and 'Remove' buttons. Below these is 'Trusted Certificate Authorities (DER or PEM)' with 'Add' and 'Remove' buttons. A 'Peer Authentication' checkbox is unchecked. At the bottom, 'SRTP payload encryption via MIKEY' is set to 'None'. 'OK', 'Cancel', and 'Apply' buttons are at the bottom right.

You need to employ TLS to encode the SIP-based communication between XPR server and the connected PBX. To this the IP APL requires a corresponding client certificate.

20. 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.
21. 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.
22. 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.
23. 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.
24. 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.
25. 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.
26. If the RTP-based communication between XPR server and RTP terminal device is to be encrypted, an individual key must be exchanged for each RTP connection via the MIKEY protocol. 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.

PBX Connection Variants for OpenScope Xpressions

Connecting HiPath 4000 V6 and OpenScope 4000 V7 / V8

Your selection in the **MIKEY** field defines whether the MIKEY, and thus the SRTP protocol, is used between XPR server and terminal device. If you select the **Profile 0** option here, MIKEY, and at the same time also the SRTP protocol, is activated. The **None** option deactivates the MIKEY and SRTP protocol.

IMPORTANT: The MIKEY protocol 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.

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.

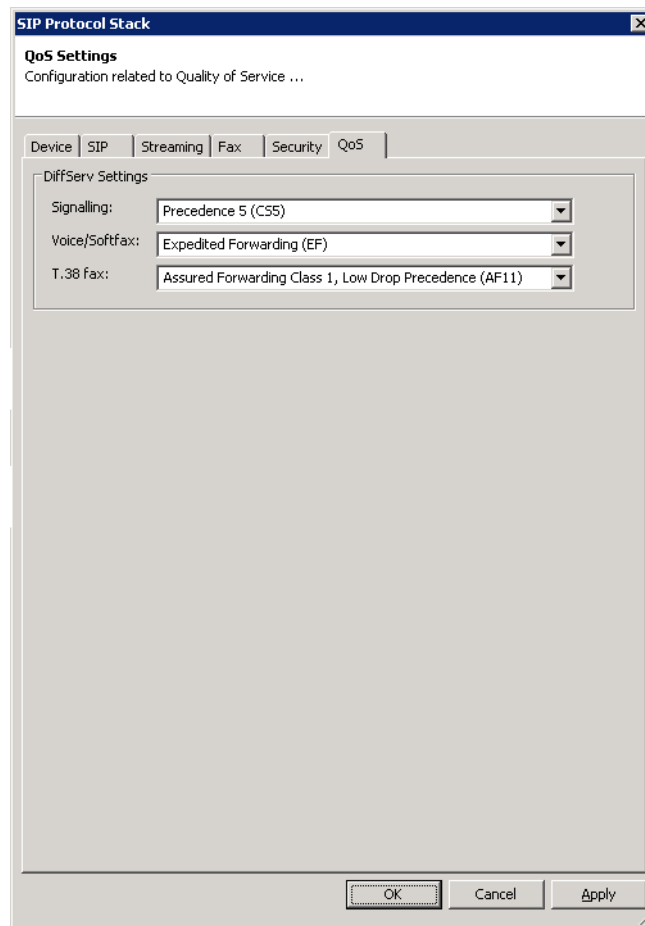
27. Click on the **QoS** tab.

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.

28. Copy the performed settings with the **OK** button.

D.4.4.3 Settings in the Server Location

You need to perform the following settings in the server location. Proceed as follows:

1. Start the XPR monitor, open the **Advanced Settings** dialog of the telematics APL and in there the **Locations** tab.
2. Doubleclick the location.
3. Add the following variables with the corresponding values in succession:
 - **TypeOfNumber** with the value *International*

PBX Connection Variants for OpenScape Xpressions

Connecting HiPath 4000 V6 and OpenScape 4000 V7 / V8

- **UseTypeInternational** with the value *True*
- **HiPath8000** with the value *True*

Proceed as follows:

- a) Click in the **Variables** section with the right mousebutton and select the **Add** option.
 - b) Click on the dotted button next to the **New variable** entry.
The **Variable selection** dialog opens.
 - c) Open the branch **Client specific > Telematic APLs** and select the **TypeOfNumber** variable. Afterwards, click on **OK**.
 - d) Click in the **Variables** section to assign a value to the new variable.
 - e) Select for the **TypeOfNumber** variable the value according to the above list.
 - f) Perform the steps **a** to **e** analog for the other two variables. Assign the corresponding value from the above list to these two variables.
4. Click on **OK** to save the new variables.
 5. Click on **OK** to save the location modifications.

D.4.5 Setting up MWI on Optipoint 410/420/600 SIP Phones

Two settings have to be modified to set up MWI on Optipoint 410/420/600 SIP phones:

- Defining a keyset for voice mail messages
- A number that is dialed when the voice mail keyset is pushed

D.4.5.1 Defining the Keyset for Voice Mail Messages

Proceed as follows:

1. Open the web interface of your SIP phone.
2. Under the **Administrator Settings** menu select the option **Function key assignments**.
3. Select a keyset under **Phone key assignments** and click the **Edit** button.
A window opens in which you can assign a function to the keyset.
4. Select the **Messages** or **Voice Messages** option and click the **Save changes** button.

Afterwards, the LED belonging to the keyset will always flash when new messages are available.

D.4.5.2 Definition of a Number to be dialed for a Keyset

Proceed as follows:

1. Open the web interface of your SIP phone.
2. Under the **Administrator Settings** menu select the option **System Information**.
3. Under **Miscellaneous** in the **voice mail number** field, enter the callback access number of the XPR server.

D.4.6 Configuring the Alternate Feature with optiPoint 410/420

NOTE: To configure this feature you need the IP address and the administrator password of the optiPoint telephone. If you do not have such data, please consult the network administrator.

So that the alternate feature can be used with the optiPoint 410/420 in case of a connection to the HiPath 8000 V3.0, two settings must be performed via the Web-interface of the telephone.

Auto reconnect

How to perform this setting:

1. Open the Web-interface of the telephone and accept the certificate with **Yes**.
2. Click the **Administration** link in the header.
3. Enter the administrator password in the **Password** field and click on **Login**.
4. Open the **SIP features** menu option.
5. Make sure that the **Auto reconnect** option is not selected. If the option is selected, the associated feature is disabled.
6. If you have made a modification, click on **Submit** at the bottom margin of the page. Otherwise you can close the page again.

Auto reconnect - CTI

How to perform this setting:

1. Open the Web-interface of the telephone and accept the certificate with **Yes**.
2. Click the **Administration** link in the header.
3. Enter the administrator password in the **Password** field and click on **Login**.
4. Open the **Feature Access** menu option.
5. Make sure that the **Auto reconnect - CTI** option is selected in the **Status** column.
6. If you have made a modification, click on **Submit** at the bottom margin of the page. Otherwise you can close the page again.

D.4.7 DTMF Digits on the XPR Server

DTMF digits can be transferred between the XPR server and a connected party in three different ways:

1. By means of *RTP Event Packets* (RFC2833), with the pushed digit being transferred within an RTP packet. This is the most common way, since optipoint phones support RFC2833. This is also called *Outband DTMF Sending*.
2. Via an audio DTMF tone inside the RTP packet (inband). This way is used when the DTMF packet comes from outside via a gateway. If this gateway supports *Outband DTMF*, this option should be used.
3. Via a DTMF digit in a SIP INFO message.

D.4.8 T.38 Calls for HiPath 8000 V3.0

T.38 calls for the HiPath 8000 V3.0 are configured via the BGL or in the Endpoint Profile (EPP). EPPs are used for trunking solutions.

D.4.9 Differences between small Enterprise and big Network Solutions

The main difference between the usage of the XPR server in a small or large enterprise is in the position of the XPR server inside the numbering environment. You have to decide where to logically locate the XPR server:

- inside a single BG serving only one BG
- inside a single BG serving more than one BG
- outside the BGs serving several BGs
- etc.

Therefore we recommend to sum up all numbers belonging to the XPR server in a separate BG.

D.5 Connecting OpenScape Voice V7 (SIP)

D.5.1 Configuring the OpenScape Voice V7

In the following we will describe the configuration of an OpenScape Voice V7 for connecting an XPR. The CMP is used for this purpose. UDP will be deployed as transport protocol for SIP.

NOTE: Even if TLS (Transport Layer Security) is to be used as transport protocol instead of UDP, the connection is configured as endpoint (SIP trunk) and not as Business Group Line (BGL). Certificates must be checked.

Under **Configuration > OpenScape Voice > Global Translation and Routing > Endpoint Management > Endpoints** you need to select and open the endpoint.

On the **SIP** tab you need to select TLS in the **SIP Signaling** section under **Transport Protocol** and enter 5061 in the **Port** field.

You cannot use TLS for OpenScape 8000 versions older than V7.

D.5.1.1 Requirements

Settings in the XPR

1. Start the XPR monitor.
2. In the **Modules** window click on the extended settings of the Telematic APL.
3. Select the **Locations** tab.
4. Set the variables:
 - **HP8000** to value *true*,
 - **TypeOfNumber** to value *International* and
 - **UseTypeInternational** to value *true*.
5. In the **Modules** window click on the extended settings of the NOT APL.
6. Click on the **Internal Settings** tab.
7. Activate the **Signal any change of box** check box.

Settings in the OpenScape Voice V7

We assume that a business group and a numbering plan have already been created.

Settings in the internet browser

Enable your browser to allow pop-ups in general or at least for the OpenScape Voice V7 Internet address.

1. Click on **Tools > Internet Options** in the Internet Explorer.
2. Select the **Privacy** tab.
3. Deactivate the **Turn on Pop-up Blocker** checkbox in the **Pop-up Blocker** section.

NOTE: If you want to restrict pop-ups to specific Internet addresses only, enable the **Turn on Pop-up Blocker** checkbox in the **Pop-up Blocker** section. Click on the **Settings** button. Enter the Internet address of the OpenScape Voice V7 in the first field. Confirm the entry with the **Add** button. Click on **Close**.

4. Click on **OK**.

D.5.1.2 CMP Login

1. Open the address `https://<IP address of the OpenScape Voice V7>/` management in a browser.
2. Enter the user name and password.
3. Confirm the entry with **Login**.

D.5.1.3 Creating an Endpoint Profile

The XPR server is introduced to the OpenScape V7 as endpoint (SIP trunk). Since an endpoint needs an endpoint profile, it will be created first.

1. Select **Configuration > OpenScape Voice > Business Group > Profiles > Endpoint**.
2. Click the **Add...** button.
3. In the **Name** field enter a name for the endpoint profile and click on **Save**.
4. Select the **Services** tab.
5. Set the value of the field **Call Transfer** to Yes.
6. Click on **Save**.

D.5.1.4 Creating an Endpoint

In this step the XPR server will be introduced to the OpenScape Voice V7 as endpoint.

1. Select **Configuration > OpenScape Voice > Business Group > Members > Endpoints**.
2. Click on **Add...**
3. In the **Name** field of the **General** tab enter the name of the endpoint. It must comprise at least 6 characters.
4. Click on the button behind the **Profile** field.
5. Click the radio button in front of the endpoint profile to be assigned to this endpoint. Click on **OK**.

OpenScape Voice users have call forwarding activated. If an external or internal call is not answered, the call is forwarded to the XPR. The caller has the option to leave a message for the called subscriber or to be routed out of the XPR and forwarded to a new destination. If the caller decides to be routed out of the XPR and forwarded to a new destination, the call cannot be rerouted to the XPR independently from the forwarding configuration.

If this behavior is not wanted, and a forwarding back to the XPR should be possible for an endpoint, the following requirement must be complied with:

- The check box **Accept Billing Number** must be activated on the **Attributes** tab of the endpoint configuration.
1. Select the **SIP** tab.
 2. Set the type to **Static**.
 3. In **Endpoint Address**, enter the IP address of the XPR server.
 4. In the **Security** section, add this IP address as **Trusted by clicking on Add....**
 5. Configure the Realm attributes and click **OK**
 6. As **Transport protocol**, select **UDP**. The value in the **Port** field is automatically reset. Port 5060 is used for UDP.
 7. Click on **Save**.

D.5.1.5 Creating a Destination

So far, the XPR server has only been introduced to the OpenScape Voice V7 as endpoint. In the following steps a destination will be created and a route assigned to it. Via a numbering plan, the route is assigned to the above created and XPR server representing endpoint.

1. Select **Configuration > OpenScape Voice > Business Group > Destinations and Routes > Destinations**.
2. Click on **Add....**
3. In the **Name** field enter a name and click on the **Save** button.

After you have created this destination you need to set the destination's properties that could not be set during the creation.

4. Click on the created destination.
5. Select the **Routes** tab. Click on **Add....**
6. Enter a number in the **ID** field.
7. Click on the button behind the **SIP Endpoint** field.
8. Select the radio button of a numbering plan and click on **OK**.
9. Select the radio button in front of the above created endpoint. Confirm the selection with **OK**.
10. Click on **OK**.

D.5.1.6 Creating a Prefix Access Code

The prefix access code defines which incoming calls are routed to the XPR server.

IMPORTANT: Only users of the same business group can use the prefix access code.

1. Select **Configuration > OpenScape Voice > Business Group > Translation > Prefix Access Codes**.
2. Click the **Add...** button.
3. Enter a value in the **Prefix Access Codes** field. Only digits and the characters '#', '*' and '+' are allowed. All incoming calls that correspond to this phone number plan and meet further conditions are routed to the XPR server.
4. Enter values in the **Minimum Length** and **Maximum Length** fields according to your requirements.

NOTE: For example, enter value 4 in the **Prefix Access Codes** field, 3 in the **Minimum Length** field and 3 in the **Maximum Length** field. All three-digit phone numbers beginning with 4, thus from 400 to 499, are routed to the XPR server.

5. Select *Off-net Access* in the **Prefix Type** field.
6. Select *International* in the **Nature Of Address** field.
7. Select *E.164 Destination* in the **Destination Type** field.
8. Click on **Save**.
9. Select **Translation > Destination Codes**.
10. Click on **Add...**
11. In the **Destination Code** field, select the Prefix Access Code previously created.
12. Click on the button behind the **Destination Name** field.
13. Select the radio button of a destination name and confirm with **OK**.
14. Click on **Save**.

D.5.1.7 Creating a Feature Profile

To perform MWI with the OpenScape Voice V7, you need to take the following steps.

1. Select **Configuration > OpenScape Voice > Business Group > Profiles > Feature**.
2. Click on **Add....**
3. In the **Name** field enter a name for the feature profile.
4. Activate the **Default** checkbox.
5. Select the **Features** tab and select **Call Forwarding to Voice Mail** and **One Number Service** from the **Feature** drop down menu.
6. Click on **Add...**
7. Click on **One Number Service**
8. Set the value of the **One Number Service** field to *Inbound And Outbound*.
9. Click on the button behind the **VoiceMail** field.
10. Click **OK**.
11. Click on **Call Forwarding to Voice Mail**
12. Enable the **Activate** checkbox.
13. Enter a phone number in the **Voice Mail Number** field.
14. In the **Ring Duration** field enter the period in seconds that is to pass until a call is forwarded to the voice mailbox.
15. Click **OK**.
16. If normalized phone numbers are forwarded for MWI, `Srx/Main/MwiNatureOfAddress` must be set to 2.
17. For this purpose, log on to the OpenScape Voice V7 by SSH, for example by using the `puTTY` tool.
18. Switch to the user `srx` with the `su - srx` command.
19. Start the CLI with the `startCLI` command.
20. Log on as `sysad`.
21. Enter "98" for the Expert Mode.
22. Enter

```
confModifyParameter "Srx/Main/MwiNatureOfAddress" "2"
for setting the new value.
```

D.6 Connecting OpenScape Voice V8 (SIP)

Configuring an Open Scape Voice V8 (SIP) corresponds to configuring an Open Scape Voice V7 (SIP). Please continue reading from [Section D.5, “Connecting OpenScape Voice V7 \(SIP\)”](#), on page 496.

D.7 Connecting OpenScape Voice V9 (SIP)

Configuring an Open Scape Voice V9 (SIP) corresponds to configuring an Open Scape Voice V7 (SIP). Please continue reading from [Section D.5, “Connecting OpenScape Voice V7 \(SIP\)”](#), on page 496.

D.8 IPSec Configuration

This chapter provides information about the following topics:

- [Using IPSec](#)
- [Configuring IPSec for CSTA Connections](#)

D.8.1 Using IPSec

During Operation, OpenScape Xpressions and OpenScape Voice exchange sensitive data with the help of the CSTA protocol. Always make sure to protect such data from unauthorized access.

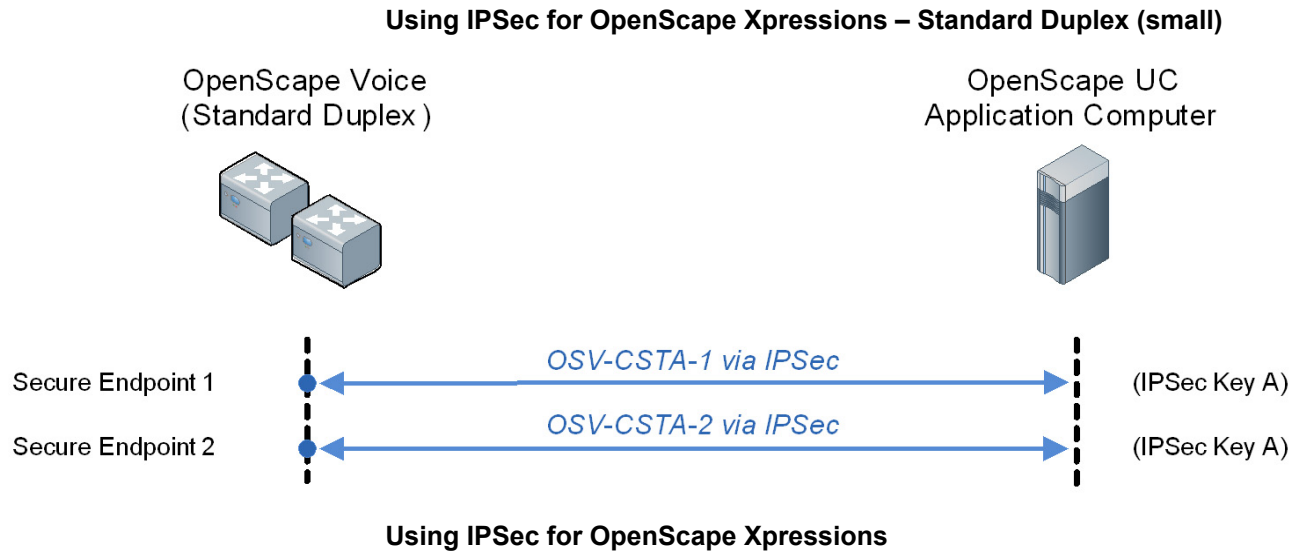
The most simple way to achieve this is operating all involved systems in a common, protected sub-network. This is in particular possible for Integrated Simplex.

If you operate the various system components in different or even unprotected sub-networks, communication between these components must be encrypted. We recommend IPSec for this purpose. This protocol establishes connection tunnels between the involved systems. Data transmitted through such a connection tunnel is encrypted by IPSec and consequently protected from unauthorized access.

To use IPSec tunnels in OpenScape Voice, a so-called secure end point is configured there for each tunnel. A target system and an IPSec key is assigned to such an end point.

NOTE: If OpenScape Voice shall use several IPSec tunnels to a common target system, the same key must be configured in for the associated secure end points in OpenScape Voice.

The computer systems of OpenScape Xpressions are configured for IPSec with the help of a configuration file.



D.8.2 Configuring IPSec for CSTA Connections

To encrypt the CSTA connections between OpenScape UC Application and OpenScape Voice using IPSec you need to execute the following configuration steps:

- [Configuring OpenScape Voice for IPSec-based CSTA Connections](#)
- [Configuring OpenScape Xpressions for IPSec-based CSTA Connections](#)

D.8.2.1 Configuring OpenScape Voice for IPSec-based CSTA Connections

Encrypting the CSTA communication between OpenScape Voice and OpenScape Xpressions by IPSec requires configuring IPSec in OpenScape Voice.

NOTE: You need to execute the configuration steps for OpenScape Voice (Standard Duplex) on one of the two system nodes only. All settings are automatically transmitted from the configured system node to the second system node.

Start the configuration

How to configure IPSec for OpenScape Voice:

1. Start the RTP Command Line Interface (startCLI) on one of the OpenScape Voice (Standard Duplex) nodes and log in there as **sysad**.
2. Select:

Main Menu >**Application-level Management >****Network Element Security Management >****Secure End Point Device Security Management**

3. Create a secure end point for the IP address of the first CSTA interface of OpenScape Voice.

Example:

```
Selection (default: 3): 1
Secure End Point Name <Max Length 63 (max length: 63)> (default: ): <unique name for the CSTA end point>
Description <Max Length 63 (max length: 63)> (default: ):
FQDN <Max Length 63 (max length: 63)> (default: ):
Remote IP Address < (max length: 15)> (default: ): <IP addr. of the XPR computer>
Remote NetMask < (max length: 15)> (default: ): <sub-network mask>
Remote Port <0 = All Ports>:
Local Host < (max length: 32)> (default: ): <csta_ip_alias_1>
Local Port <0 = All Ports>:
IPsec Profile Name <Max Length 63 (max length: 63)> (default: ): IPSEC_ESP
IKE Profile Name <Max Length 63 (max length: 63)> (default: ): IKE_SHA_WIN
Key Generation Method <1 = automatic, 2 = user input> (default: 1): 1
Key Length in Bytes (default: 16):
Do you want to execute this action? <y/n> (default: yes):

Operation successful
```

NOTE: If you do not specify an IP address but the associated fully qualified host name under `Local Host`, you need not modify the IPSec configuration in the event that the IP address of the relevant interface changes at a later date.

The fully qualified host names for CSTA are defined for OpenScape Voice in `/etc/hosts`. They read by default `csta_ip_alias_1` and `csta_ip_alias_2`.

4. Determine the key used for the tunnel of the first CSTA interface. To do so, display the settings of the just created end point as shown in the following example.

Example:

PBX Connection Variants for OpenScape Xpressions

IPSec Configuration

```
Selection (default: 3): 4
Secure End Point Name <Max Length 63 (max length: 63)> (default: ): <name of the created CSTA end point>
Do you want to execute this action? <y/n> (default: yes): y
Total Number of SecEndPts Retrieved : 1
Name: Ext_Asst
Description:
FQDN:
Remote IP Address: <Ext_Asst_IP_Address>
Remote NetMask: 255.255.255.255
Remote Port : 0
Local Host: bond_node_alias
Local Port: 0
IPsec Profile: IPsec_ESP
IKE Profile: IKE_SHA
Key Gen Method: Automatic
Key Type: Hex
Key Length: 16

Key: 7aa88aecd7f40699884b75795fbf9354
```

5. Note down the **Key**: output.
6. Create a secure end point for the second CSTA interface of OpenScape Voice. Because the relevant IPSec tunnel will later lead to the same application computer as for the first end point, you need to use the same key – the one you just noted down. Proceed as shown in the following example:

Example:

```
Selection (default: 3): 1
Secure End Point Name <Max Length 63 (max length: 63)> (default: ): <unique name for the CSTA end point>
Description <Max Length 63 (max length: 63)> (default: ):
FQDN <Max Length 63 (max length: 63)> (default: ):
Remote IP Address < (max length: 15)> (default: ): <IP addr. of the UC application computer>
Remote NetMask < (max length: 15)> (default: ): <sub-network mask>
Remote Port <0 = All Ports>:
Local Host < (max length: 32)> (default: ): <csta_ip_alias_2>
Local Port <0 = All Ports>:
IPsec Profile Name <Max Length 63 (max length: 63)> (default: ): IPSEC_ESP
IKE Profile Name <Max Length 63 (max length: 63)> (default: ): IKE_SHA_WIN
Key Generation Method <1 = automatic, 2 = user input> (default: 1): 2
Key Length in Bytes (default: 16): <key of the first CSTA end point>
Do you want to execute this action? <y/n> (default: yes):

Operation successful
```

You have now configured IPSec for the CSTA connection in OpenScape Voice.

D.8.3 Configuring OpenScape Xpressions for IPSec-based CSTA Connections

Encrypting the CSTA communication between OpenScape Voice and OpenScape Xpressions by IPSec requires configuring IPSec on the application computer of OpenScape Xpressions.

NOTE: The configuration will be described for Windows Server 2008 R2 only.

How to configure IPSec for the application computer:

1. Open Start > Control Panel > Administrative Tools > Windows Firewall with Advanced Security.
2. Click on **Connection Security Rules** in the left-hand section.
3. Click on **Connection Security Rules** with the right mouse button and select **New Rule...** from the context menu.

The **New Connection Security Rule Wizard** dialog opens.

4. Select rule type **Server-to-server** and click on **Next**.
5. Specify for endpoint 1 the IP address on which OpenScape Xpressions operates. Specify the IP address of OpenScape Voice for endpoint 2. Then click on **Next**.
6. Specify the authentication requirements. Select entry **Request authentication for inbound and outbound connections** and click on **Next**.
7. Select **Advanced** and click on **Customize....**
8. Click on **Add**. Enter the key you have assigned on OpenScape Voice under **Preshared key (not recommended)**.
9. Confirm your input with **OK**. Close the dialog with **OK**. Click on **Next** to perform the next settings.
10. Adopt the set profiles and click on **Next**.
11. Assign a name to the **Connection Security Rules** and provide an optional description, then click on **Finish**.

D.9 Connecting an Alcatel OmniPCX Enterprise (OXE) via IP APL

IMPORTANT: Please note that the connection of the Alcatel OmniPCX via SIP is currently only released for project-specific installations.

If the following installation is to occur via a remote desktop, please be **absolutely** sure to heed the notes in [Section 4.1.2, "Installation via Remote Desktop Connection"](#), on page 51.

The Alcatel OmniPCX is connected to the XPR server via the IP APL and the SIP protocol. The following is a description of the conceptional connection and the detailed configuration tasks of this solution.

D.9.1 Connection Concept

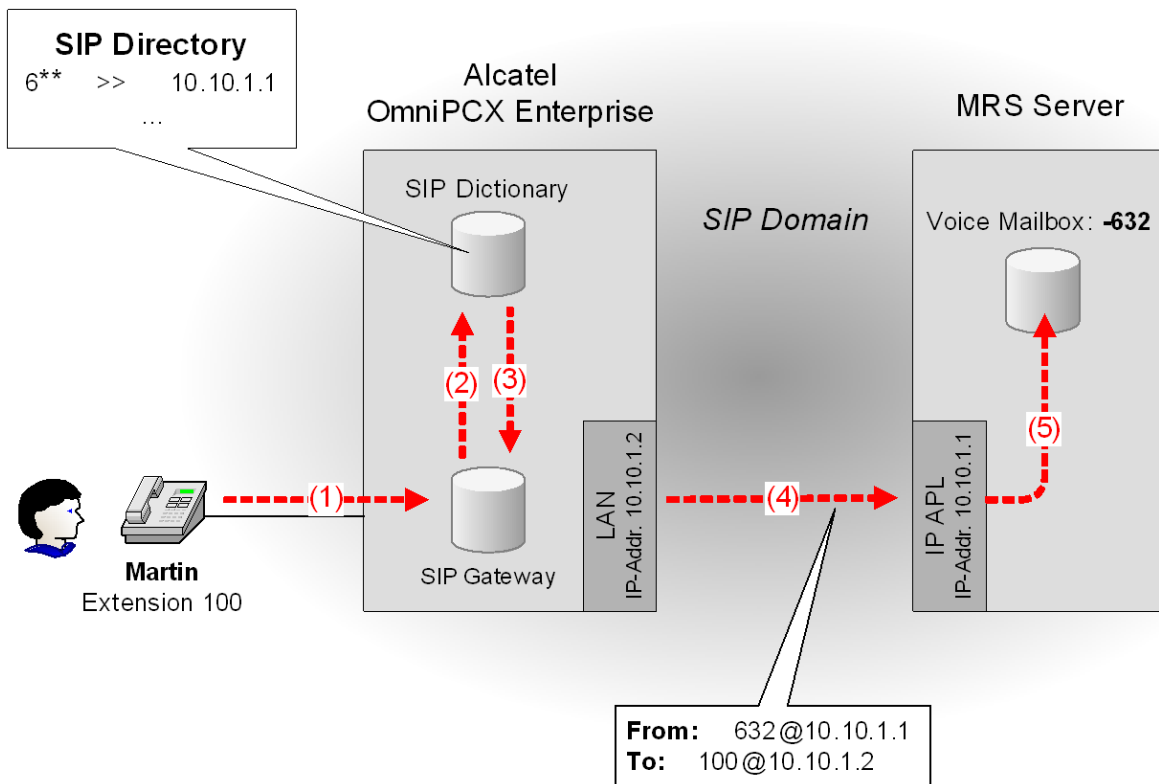
The PBX and the XPR server form one SIP domain. In this domain the Alcatel OmniPCX operates as SIP Proxy server.

The realization of this connection concept requires the following configuration steps:

- [Alcatel OmniPCX Enterprise Configuration](#)
- [IP APL Configuration](#)

Let us first contemplate two simple examples of the general connection functioning:

Connection setup from the PBX to the XPR server



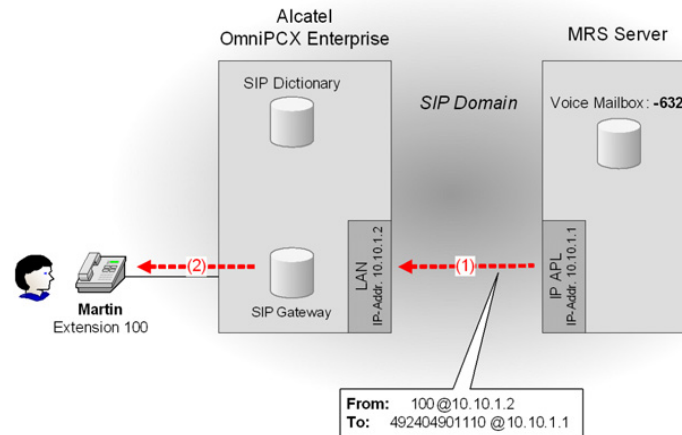
User *Martin* calls the XPR server voice mailbox with the phone number 632 from this telephone with the extension number 100. The routing is performed via the following SIP-relevant steps:

1. *Martin* dials the phone number 632. On grounds of its user configuration, the PBX recognizes this extension as representing an external user. Therefore, it forwards the connection request to the SIP Gateway within the PBX.
2. The SIP Gateway must resolve the involved phone numbers to SIP-conform addresses. For this purpose, it sends a corresponding request to the internal SIP dictionary.
3. The SIP dictionary contains the information that all triple digit connection requests displaying a 6 at the first position are to be forwarded to the IP address 10.10.1.1.
4. From this information and the dialed phone number the SIP Gateway generates the target address 632@10.10.1.1. Furthermore, it generates the originator address 100@10.10.1.2 from its own IP address and from the extension of user *Martin*.
5. The IP APL generates the destination number 632 from the transferred SIP addresses and the originator number 100.

PBX Connection Variants for OpenScape Xpressions

Connecting an Alcatel OmniPCX Enterprise (OXE) via IP APL

Connection setup from XPR server to PBX



The IP APL sets up a connection to the telephone device with the phone number *100*. This is e.g. required for the transmission of MWI notifications or for the playback of voice mails at a telephone. The routing is performed via the following SIP-relevant steps:

1. The MTA of the XPR server sends an MWI notification to the telephone with number *100* via the IP APL. The IP APL forms the destination address *100@10.10.1.2* and the originator address *492404901110@10.10.1.2*. The address portion *492404901100* of the originator address results from the setting **Own SIP user name** of the IP APL configuration (cf. [IP APL Configuration](#) on [page 510](#)).
2. The SIP Gateway of the PBX generates the target number *100* from the transferred SIP addresses and the display *492404901110* for the originator information displayed on the telephone.

D.9.1.1 Alcatel OmniPCX Enterprise Configuration

Please contact your system administrator for the Alcatel Omni PCX Enterprise configuration.

D.9.1.2 IP APL Configuration

So that the Alcatel Omni PCX Enterprise connection to the XPR server works correctly, the XPR server IP APL must now be configured. Proceed as follows:

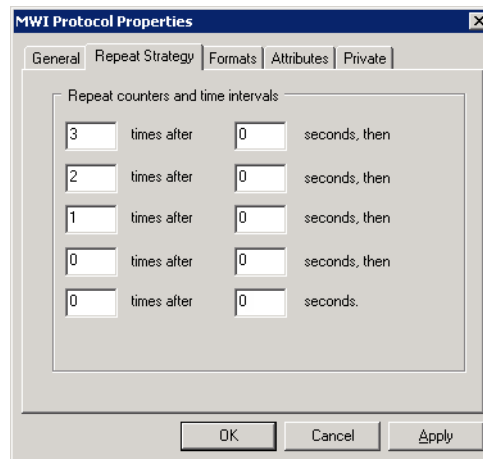
IMPORTANT: The following step-by-step instructions suppose that the XPR server including the IP APL have already been installed and are working correctly.

1. In the modules window of the XPR monitor select the **IpApl > Set Options** menu item.

Configuring the MWI protocol

To support MWI, the *Message Waiting Indication* protocol must be implemented in the IP APL. Proceed as follows:

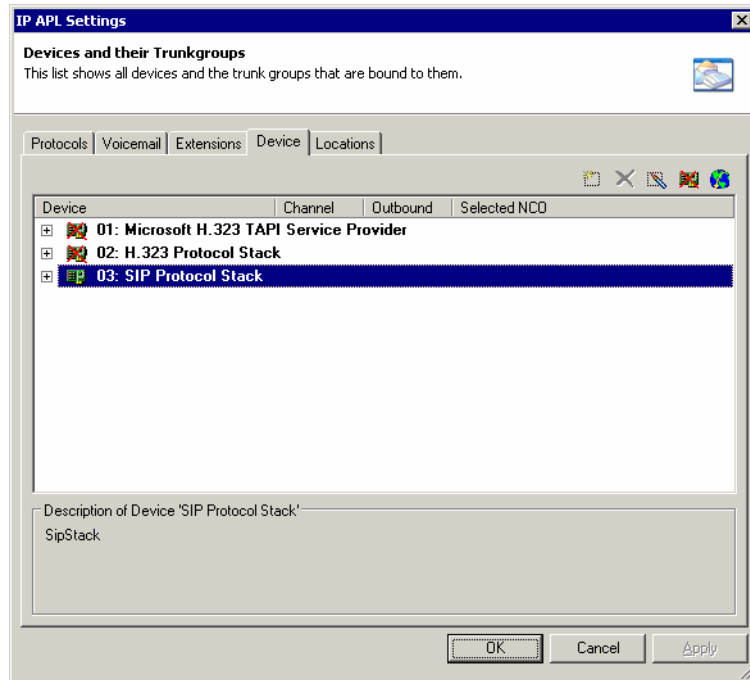
2. Add the *Message Waiting Indication* protocol on the **Protocols** tab of the configuration dialog.
3. Open the configuration dialog for the *Message Waiting Indication* and switch to the **Repeat Strategy** tab.



4. Set all MWI protocol settings to value **0**.
5. Copy the settings with the **OK** button.

Activating the SIP device

6. In the **IP APL Settings** dialog switch to the **Device** tab.



7. Activate the *SIP Protocol Stack* device with the **activate** icon in the toolbar.

IMPORTANT: In an IP APL, only **one** device may be activated at a time. Therefore, make sure that all devices, except for the SIP Protocol Stack, are deactivated.

PBX Connection Variants for OpenScape Xpressions

Connecting an Alcatel OmniPCX Enterprise (OXE) via IP APL

- Open the SIP device configuration dialog with a doubleclick on the *SIP Protocol Stack* device.

Properties of SIP Protocol Stack

Device

Number of physical channels: 16

Number of built-in Fax G3 channels: 0

Number of G.729AB channels: 0

Gateway address: 10 . 12 . 13 . 10

Gateway SIP Port: 5060

Own address: 10 . 12 . 13 . 11

Own SIP Port: 5060

☐ UDP ☒ TCP ☐ TLS

First RTP Port: 29100

Own SIP user name: 100

Packet size (msec): 30

Codec

☒ G.711 ☐ G.729AB

DTMF Settings

☒ DTMF via RFC 2833

☒ DTMF via SIP INFO Messages

☒ In-Band DTMF Detecti

Security OK Cancel

- In the **Number of physical channels** field specify the number of parallel communication connections to be possible between XPR server and PBX.
- In the **Gateway address** field enter the IP address under which the SIP Gateway service can be reached in the PBX.
- In the **Own address** field enter the IP address under which the IP APL is to be addressed.
- From the **UDP**, **TCP** and **TLS** options select the protocol that you want to use for connecting the PBX.

NOTE: If you select the **TLS** option here, you need to perform additional security settings via the **Security** button. You find information about this in the OpenScape Xpressions Server Administration manual.

- In the **Own SIP user name** field enter the phone number that is configured in the XPR server for directly accessing (Direct Access) the voice mail protocol. For example, the extension 500.

PBX Connection Variants for OpenScape Xpressions

Connecting an Alcatel OmniPCX Enterprise (OXE) via IP APL

14. In the **Codec** section specify the voice codecs the IP APL is to use for the RTP communication with terminal devices.

15. Copy the settings with the **OK** button.

The XPR-OmniPCX integration is now operative.

D.10 Connecting a Mitel 3300 ICP

NOTE: Connecting a Mitel 3300 ICP is released only project-specifically.

In this paragraph the connection of a Mitel 3300 ICP PBX to XPR with the help of the IP APL will be described.

The Mitel ICP3300 PBX does not dispose of IP-based tie trunks. Therefore virtual telephones (so-called soft phones) are configured in the PBX and summed up in a hunt group. The PBX communicates with the IPAPL via the virtual telephones. The IPAPL regards the virtual telephones as TAPI lines.

If Mitel users want to listen to their voice mail, they dial the hunt group number and a connection to the voice mail is established via one of the virtual telephones of the hunt groups. The user then enters their voice mail number and can listen to their voice mails.

D.10.1 Configuration of the Mitel 3300 ICP PBX

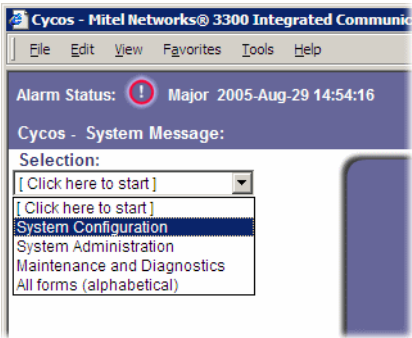
The configuration includes the configuration of the virtual telephones and the hunt group configuration. It will be performed with the help of the web-based Mitel 3300 ICP administration interface.



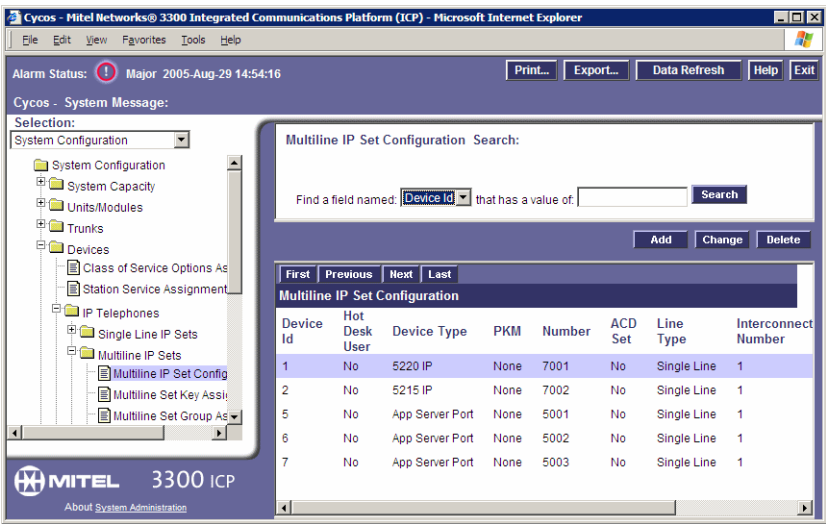
D.10.1.1 Configuring virtual Telephones

The virtual telephones must be configured in the Mitel 3300 ICP. Proceed as follows:

- 1. Select the **System Administration Tool** on the main page of the administration tool. The following page will be displayed:



- 2. Select the menu option **System Configuration**.
- 3. Open the **Devices > IP-Telephones > Multiline IP Sets > Multiline IP Set Configuration** in the selection list. The following page opens that lists all IP telephones that have already been configured.



4. Click on the **Add** button. The following page opens in which virtual IP telephones can be added to the configuration.

5. Enter the desired number of virtual telephones in the **Enter the number of records to add** field.
6. In the **Device Type** field select **5020 IP**.
7. Enter the number of the first virtual telephone in the first field of the line **Number:**. Then enter the size of the steps the number of virtual telephones is to be increased with in the second field of the line **Number:**.
8. Click the **Save** button at the end of the page.

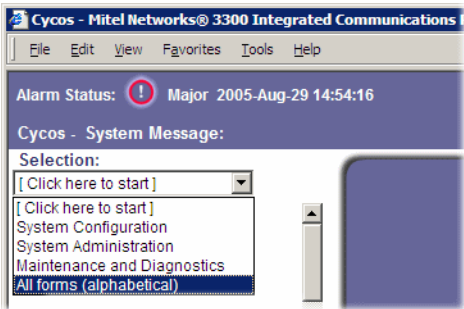
The new virtual telephones are created. With the settings in the figure in step 4 on page 517 30 new telephones are created the number range of which starts with 6000 and ends with 6029.

The virtual telephone configuration in the Mitel 3300 ICP is now completed. Now configure the hunt group as described in the following section.

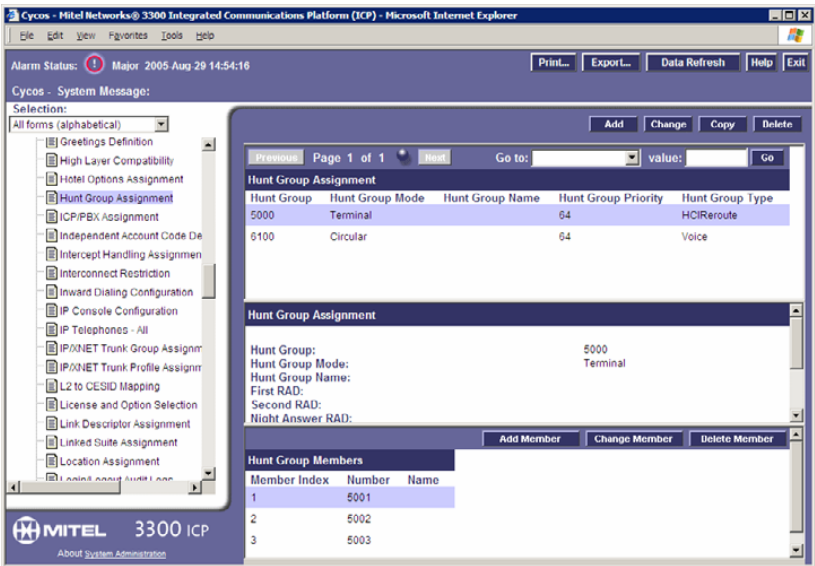
D.10.1.2 Hunt Group Configuration

Proceed as follows to sum up the virtual telephones that have been created in [Section D.10.1.1, “Configuring virtual Telephones”, on page 516](#):

- 1. Select the **System Administration Tool** on the main page of the administration tool. The following page will be displayed:



- 2. Select the menu option **All forms (alphabetical)**.
- 3. Browse to the entry **Hunt Group Assignment** in the list on the left hand side and select it. The following page opens:



4. Click the **Add** button. The following page opens:

Range Programming -- Web Page Dialog

Add Range Programming - Hunt Group Assignment Help

This form allows you to add one or more records.

1. Enter the number of records to add:

2. Define the Add Range Programming Pattern:

Field Name	Value to Add	Increment by
Hunt Group:	6100	
Hunt Group Mode:	☐ Terminal ☒ Circular	-
Hunt Group Name:		-
First RAD:		
Second RAD:		
Night Answer RAD:		
Hunt Group Priority:		
First Threshold:		

Preview Save Cancel

5. Enter the number of hunt groups you would like to create in the **Enter the number of records to add:** field.
6. Enter a name for the new hunt group in the **Hunt Group** field, e.g. 6100.
7. In the line **Hunt Group Mode:** select the **Circular** option.
8. Click **Save** to save the new hunt group.
9. Make sure that the new hunt group is selected in the list. Click the **Add Member** button to add the new virtual telephones that have already been created to the new hunt group. Up comes this dialog:

Range Programming -- Web Page Dialog

Add Range Programming - Hunt Group Members Help

This form allows you to add one or more records.

1. Enter the number of records to add:

2. Define the Add Range Programming Pattern:

Field Name	Value to Add	Increment by
Number:	6000	1
Name:		-

Preview Save Cancel

10. Enter the number of the newly created virtual telephones in the **Enter the number of records to add:** field

PBX Connection Variants for OpenScape Xpressions

Connecting a Mitel 3300 ICP

11. Enter the same values that you have used when creating the virtual telephones in step 7 on page 517 in the line **Number**:

12. Click **Save** to save the hunt group.

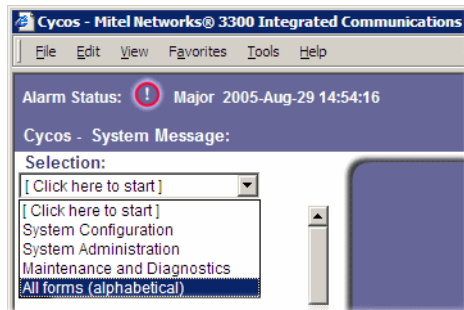
The hunt group configuration is now complete. Now continue with the assignment of the class of service.

D.10.1.3 Class of Service (COS) Assignment

The virtual telephones must be recognized as TAPI lines by the IPApI. Therefore the correct COS must be configured for the virtual telephones.

Proceed as follows:

1. Select the **System Administration Tool** on the main page of the administration tool.
2. Select the menu option **All forms (alphabetical)**.



- Browse to the entry **Station Service Assignment** in the list on the left hand side and select it. The following page opens that lists the different COS of all installed telephones:

Number	Intercept Number	Class of Service - Day	Class of Service - Night1	Class of Service - Night2	Class of Restriction - Day	Class of Restriction - Night1	Class of Restriction - Night2
5001	1	1	1	1	1	1	1
5002	1	1	1	1	1	1	1
5003	1	1	1	1	1	1	1
5004	1	1	1	1	1	1	1
6000	1	4	4	4	4	4	4
6001	1	4	4	4	4	4	4
6002	1	4	4	4	4	4	4

- Select an entry for a virtual telephone and click the **Change** button at the top of the page. The following page opens:

Field Name	Change action	Value to change	Increment by
Number:	-	5001	-
Intercept Number:	Change to	1	
Class of Service - Day:	Change to	4	
Class of Service - Night1:	Change to	4	
Class of Service - Night2:	Change to	4	
Class of Restriction - Day:	Change to	4	

- Change all COS (Day, Night1, Night2, Restriction) to the same value. Select a value that is exclusively used by the virtual telephones for this.

PBX Connection Variants for OpenScope Xpressions

Connecting a Mitel 3300 ICP

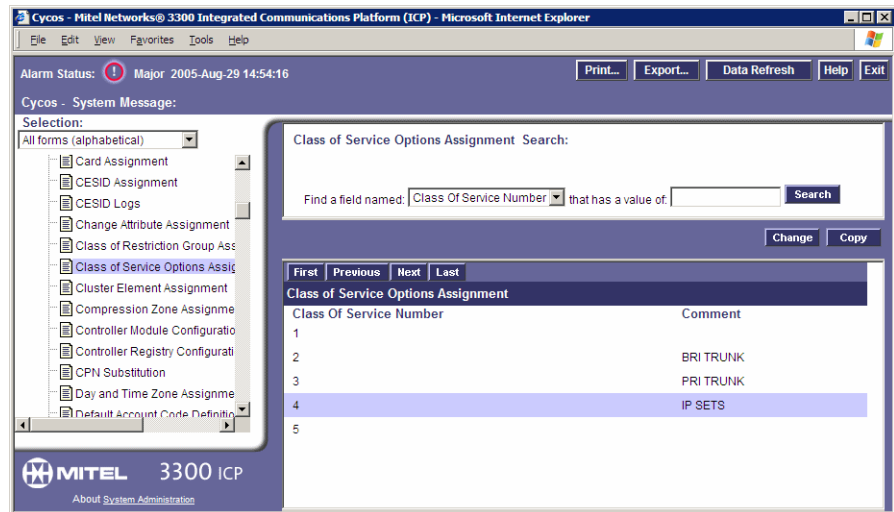
6. Perform step 4 and step 5 for all virtual telephones.

Now the COS must be configured so that the virtual telephones are considered as TAPI lines. Proceed as follows:

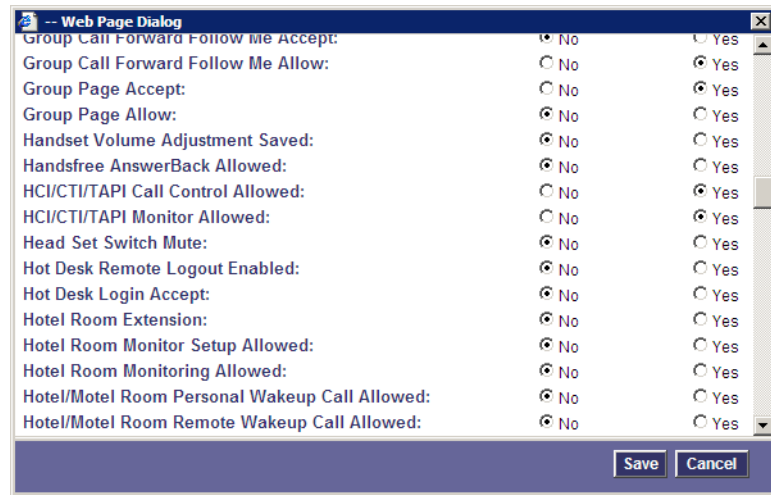
1. Select the **System Administration Tool** on the main page of the administration tool.
2. Select the menu option **All forms (alphabetical)**.



3. Browse to the entry **Class of Service Options Assignment** in the list on the left hand side and select it. The following page opens that lists all existing COS.



4. Select the COS you have used for the virtual IP telephones.
5. Click on **Change**. The following page opens in which the COS properties can be changed.



Property	No	Yes
Group Call Forward Follow Me Accept:	☐	☒
Group Call Forward Follow Me Allow:	☐	☒
Group Page Accept:	☐	☒
Group Page Allow:	☒	☐
Handset Volume Adjustment Saved:	☒	☐
Handsfree AnswerBack Allowed:	☒	☐
HCI/CTI/TAPI Call Control Allowed:	☐	☒
HCI/CTI/TAPI Monitor Allowed:	☐	☒
Head Set Switch Mute:	☒	☐
Hot Desk Remote Logout Enabled:	☒	☐
Hot Desk Login Accept:	☒	☐
Hotel Room Extension:	☒	☐
Hotel Room Monitor Setup Allowed:	☒	☐
Hotel Room Monitoring Allowed:	☒	☐
Hotel/Motel Room Personal Wakeup Call Allowed:	☒	☐
Hotel/Motel Room Remote Wakeup Call Allowed:	☒	☐

Save Cancel

6. Browse to the entries **HCI/CTI/TAPI Call Control Allowed** and **HCI/CTI/TAPI Monitor Allowed** and set both to **Yes**. Then click **Save**.

Now the Mitel 3300 ICP configuration for the connection to XPR is complete.

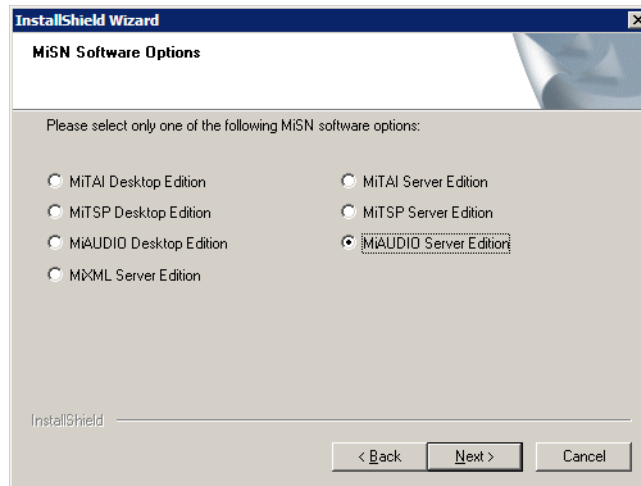
D.10.2 XPR Configuration

For the Mitel 3300 ICP connection the Tapi Service Provider (TSP) delivered by Mitel and the MiAUDIO Server Edition must be installed on the XPR side.

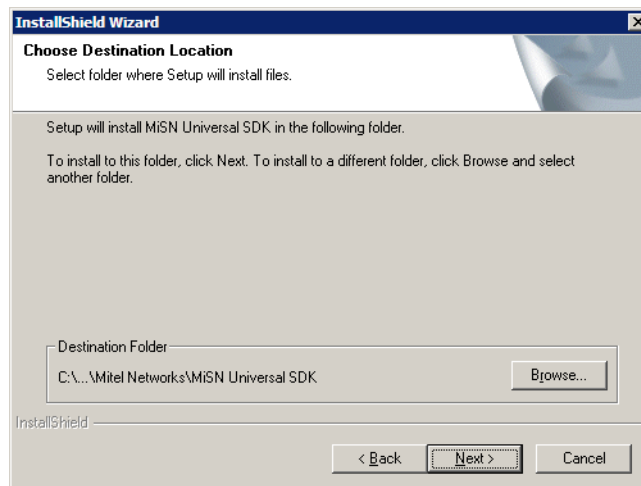
D.10.2.1 Installation/Configuration of Mitel Tapi Service Provider (TSP) and MiAUDIO Server Edition

Proceed as follows:

1. Start the TSP setup delivered by Mitel. A welcome dialog is displayed that you confirm with **Next >**.
2. Confirm the license agreement by clicking **Yes**. Up comes this dialog:

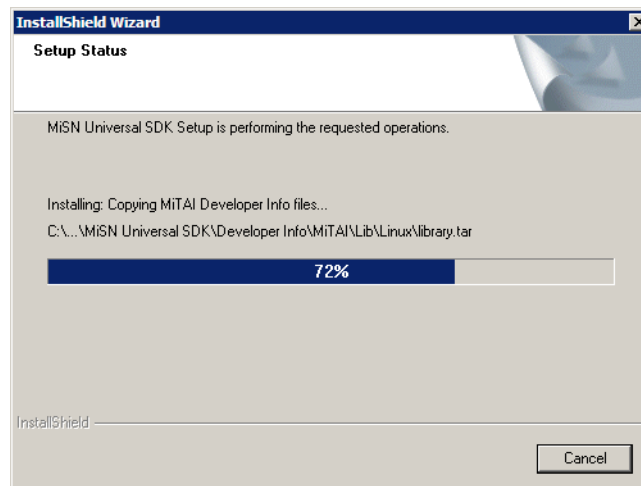


3. Select the **MiAUDIO Server Edition** option and click **Next >**. Up comes this dialog:

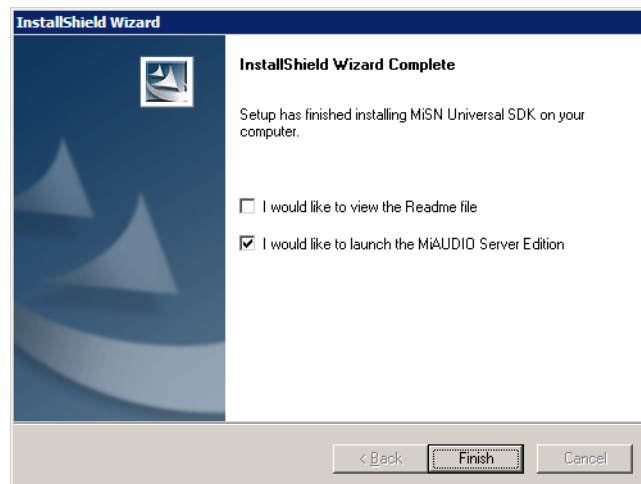


4. Select an installation path via the **Browse...** button or accept the default path which is a good choice. Then click on **Next**.

The installation routine now copies files and installs the software on the system. Up comes this dialog:



After the copy and installation process have been finished, the following dialog is displayed:



5. Select the **I would like to launch the MiAUDIO Server Edition** option and click on **Finish**. The installation routine for the MiAUDIO Server Edition starts.

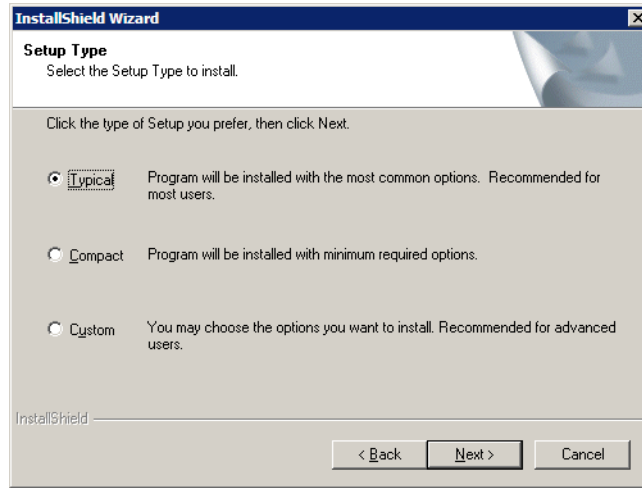
You can have the `Readme.txt` file displayed, that documents amongst others changes to the previous version. Therefore select the **I would like to view the Readme file** option.

6. Confirm the welcome dialog with **Next**.

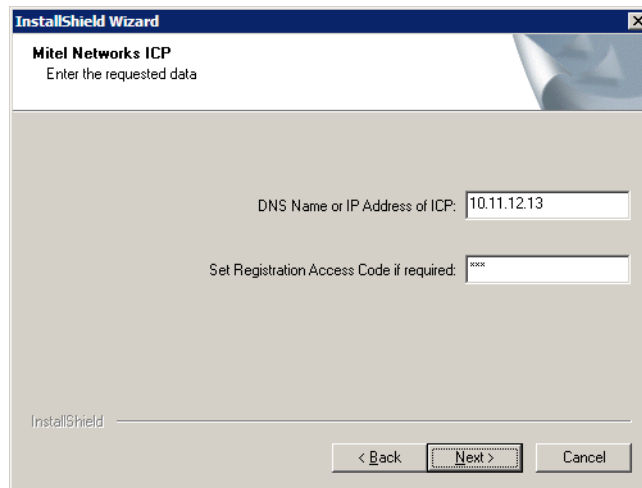
PBX Connection Variants for OpenScape Xpressions

Connecting a Mitel 3300 ICP

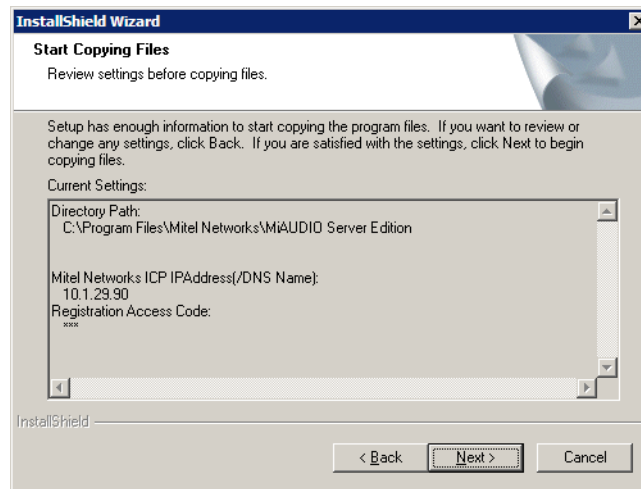
7. Select an installation directory via the **Browse...** button or accept the default path which is a good choice. Then click on **Next >**. Up comes this dialog:



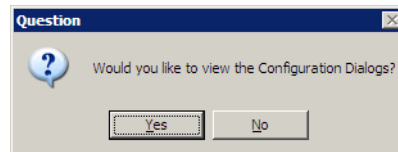
8. Select the **Typical** option and then click **Next >**. Up comes this dialog:



9. Insert the IP address of the Mitel PBX in the **DNS name or IP address of ICP** field and then click **Next >**. Up comes this dialog:



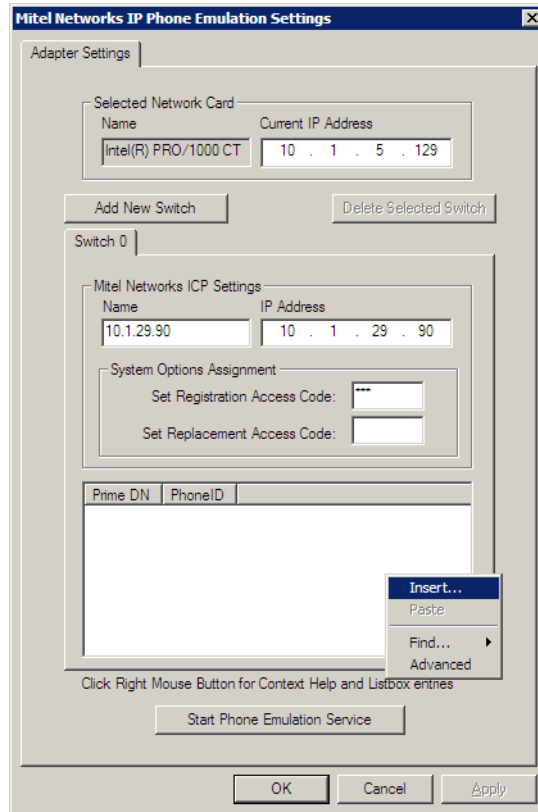
10. Check your settings and then click **Next >**. Via the **< Back** button you will come to the previous dialogs in order to change incorrect settings if necessary.
11. After the installation has been completed, the following dialog is displayed:



PBX Connection Variants for OpenScape Xpressions

Connecting a Mitel 3300 ICP

12. Click the **Yes** field to start the MiAUDIO Server Edition configuration. Up comes this dialog:



13. With the right mouse button click in the list field and select the menu option **Insert....**

14. Enter all numbers of the virtual IP telephones successively. Each newly entered telephone is symbolized by a red icon.

Mitel Networks IP Phone Emulation Settings

Adapter Settings

Selected Network Card

Name	Current IP Address
Intel(R) PRO/1000 CT	10 . 1 . 5 . 129

Add New Switch Delete Selected Switch

Switch 0

Mitel Networks ICP Settings

Name	IP Address
10.1.29.90	10 . 1 . 29 . 90

System Options Assignment

Set Registration Access Code:

Set Replacement Access Code:

Prime DN	PhoneID	ReasonCode	ICP[0]	ICP[1]
6200	000			
6201	001			
6202	002			
6203	003			
6204	004			

Click Right Mouse Button for Context Help and Listbox entries

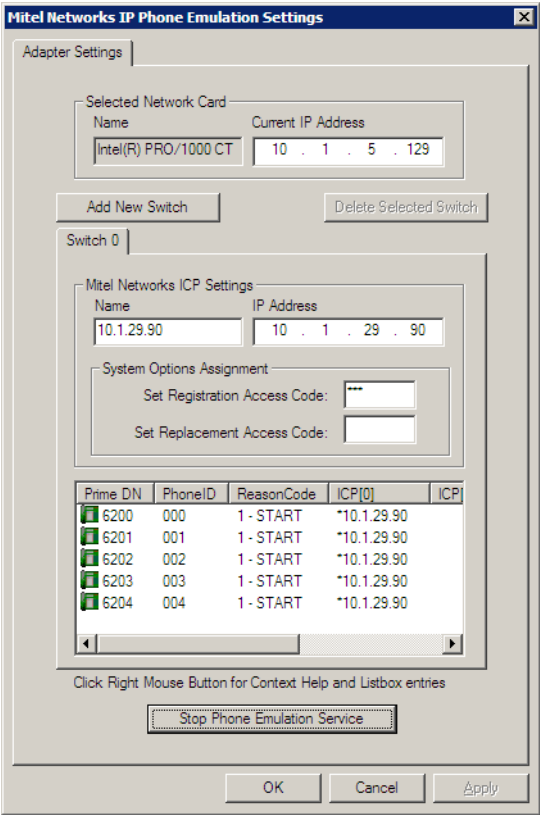
Start Phone Emulation Service

OK Cancel Apply

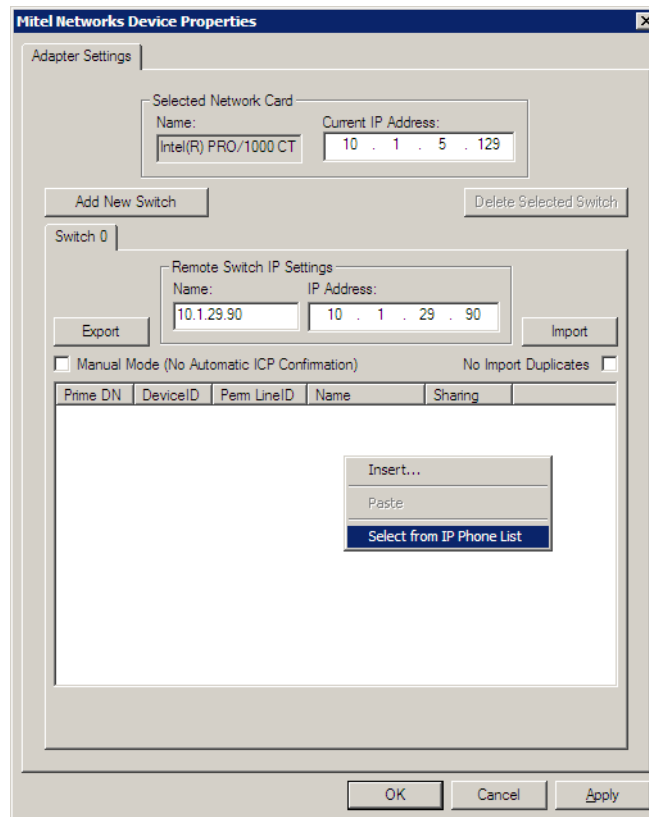
NOTE: The dialog is displayed in the advanced view that provides detailed information in the field. You will receive this view by selecting the **Advanced** option in the context menu of the right mouse button.

15. After you have entered all virtual telephones, click the **Start Phone Emulation Service** button.

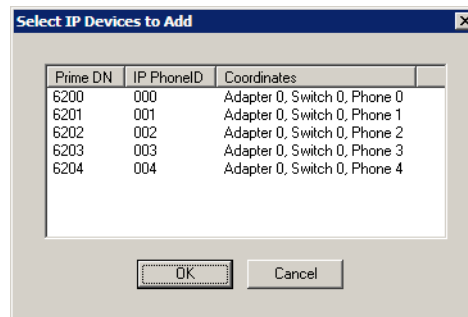
As soon as the service starts, all virtual IP telephones are represented by a green icon.



16. Click on **OK**. The following dialog opens in which the virtual telephones are configured that are to be monitored and controlled by the CTIAPL:



17. With the right mouse button click in the list field and select the menu option **Select from IP Phone list**. Up comes this dialog:



PBX Connection Variants for OpenScape Xpressions
Connecting a Mitel 3300 ICP

18. Select all virtual IP telephones before clicking **OK**. The selected IP telephones are displayed in the list field and flagged with a yellow icon.

Prime DN	DeviceID	Perm LineID	Name	Sharing	PhoneID
6200	000	25258			000
6201	001	25249			001
6202	002	25250			002
6203	003	25251			003
6204	004	25252			004

19. Click on **Apply**. If the entered devices really are IP telephones, they will be confirmed. Then click the **OK** button.
20. Click on **Finish**.

The Mitel TSP and the wave driver have now been installed and configured. The computer operating system must now be configured to activate the wave driver. Please refer to [Section D.10.2.3, “Activating Wave Drivers”, on page 533](#).

D.10.2.2 Mitel TSP configuration at a later Time

Proceed as follows to change the Mitel TSP configuration at a later time.

1. Click **Start > Settings > Control Panel > Phone and Modem Options**.
2. Open the **Advanced** tab and select the Mitel Networks TAPI Service Provider entry.
3. Click the **Configure...** button.

NOTE: If the configuration cannot be opened, read section [Section D.10.3, "Problems with the Mitel TSP configuration at a later time"](#), on page 534.

D.10.2.3 Activating Wave Drivers

Proceed as follows to activate wave drivers in the system:

1. Click on **Start > Settings > Control Panel > System**.
2. Open the **Hardware** tab.
3. Click the **Device Manager** button.
4. Open **Sound, video and game controllers** and double-click the **Mitel Networks IP Wave Driver** entry.
5. Select the **Use this device (enable)** entry under **Device usage**.

D.10.2.4 Usage of the Mitel TSP with the IPApI

The IPApI must be configured as follows so that it uses the Mitel TSP:

1. Start the XPR monitor.
2. Open the extended IPApI settings.
3. Open the **Devices** tab and activate the **Mitel TSP** entry via the right mouse button.
4. Click on **OK**.

The IPApI configuration is now complete.

D.10.3 Known Problems

Problems with the Mitel TSP configuration at a later time

If the retroactive change of the Mitel TSP configuration failed, since the corresponding DLL crashed, the following workaround might solve the problem:

1. Click **Start** > **Run...** and enter `mmc` to start the Microsoft Management Console.
2. Open the menu option **File** and select the **Add/Remove Snap-in...** option.
3. Click the **Add...** button.
4. Add the telephony service and then click **OK**.
5. Perform the steps listed in [Section D.10.2.2, “Mitel TSP configuration at a later Time”, on page 533](#) again.

D.10.4 MWI

Message Waiting Indication for a real telephone cannot be set via a TAPI line for a virtual IP telephone. For this, the Mitel SDK is used. MWI is directly set/deleted with the help of the Mitel SDK bypassing the TAPI lines.

D.10.4.1 MWI via IPApI

Proceed as follows to realize the MWI functionality via the IPApI:

1. Open the registry database of the computer the XPR server is running on.
2. Open the key
`HKLM/Software/Wow6432Node/PP-COM/MRS/IpApl/Devices`
3. Underneath this key, search for the device that contains the value **Mitel TSP** in the **name** key.
4. For this device, enter the string `GW=` in the **Private** key and the PBX IP address.
Example: `GW=11.22.33.44`
5. Restart the IPApI.

E Connecting OpenScape UC Application

E.1 Connecting OpenScape-Xpressions via Trusted Transfer Mode

Connecting OpenScape-Xpressions means that the OpenScape UC Application is connected to the PhoneMail on an OpenScape Xpressions server. This supplements the Unified Messaging features of PhoneMail with the Unified Communications features of OpenScape UC Application.

The Unified Communications features of the OpenScape UC Application are integrated in the user interface of PhoneMail, so that the user does not realize which application enables the respective feature. The user seems to be working with a Unified Communications system centrally providing all available features.

Working method

If the user selects a Unified Communications feature enabled by OpenScape UC Application in PhoneMail, the XPR server forwards the call to the voice portal user access. The user is automatically identified and the user menu that associates the feature is announced.

From the technical point of view, the XPR server transfers information to OpenScape UC Application with the call. The XPR server encodes the information in the originator number of the forwarded call and uses the Trusted Transfer Mode (TTM) phone number format for the encoding.

E.1.1 Connecting OpenScape-Xpressions with the HiPath 4000 V6

The following sections describe the configuration steps required for connecting an OpenScape-Xpressions in combination with the HiPath 4000 to the OpenScape UC Application. Furthermore, we provide information about restrictions on this solution.

NOTE: The basic HiPath 4000 and OpenScape UC Application configuration is excluded from the description. You find a detailed configuration guide in the product documentation.

E.1.1.1 Trusted Transfer Mode with the HiPath 4000

The HiPath 4000 is connected to the XPR server (A) via an ISDN line via the Cornet NQ protocol (ISDN APL). A direct SIP connection (IP APL) from the XPR server (A) to the OpenScape Voice exists in parallel.

When executing the Trusted Transfer Mode, the OpenScape Voice is addressed via the HiPath 4000 by means of the ISDN APL. The OpenScape Voice transfer the information to the OpenScape UC Application using an SIP connection. The return call from the OpenScape UC Application occurs via the parallel SIP connection to the XPR server (A). Once the direct SIP connection is known, it is used as communication path from then on.

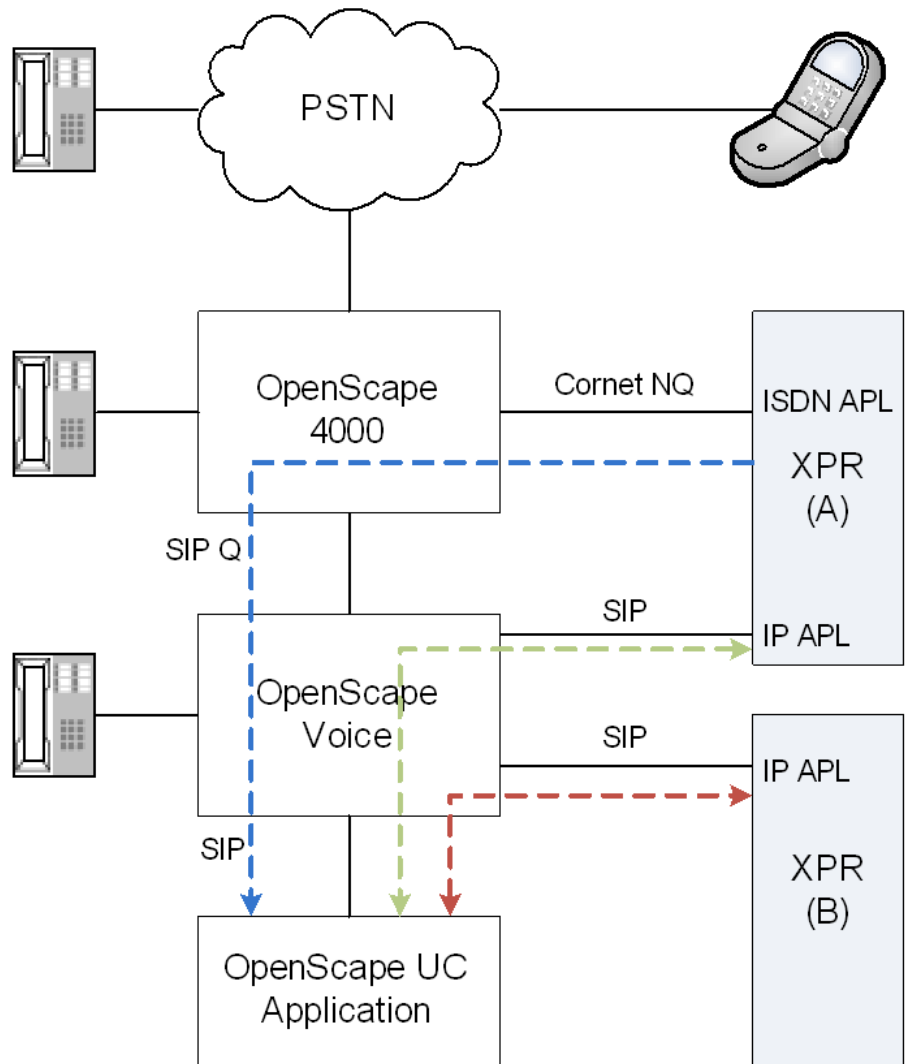
NOTE: The PhoneMail protocol is connected to the ISDN- and IP APL. The MWI protocol is deactivated within the IP APL.

Several XPR servers can be connected to the OpenScape Voice, as is exemplified by the XPR server (B). In case of this solution, a second entity must have been created in the Voice Portal.

The following flow chart illustrates the structure of the OpenScape UC Application connection:

Connecting OpenScape UC Application

Connecting OpenScape-Xpressions via Trusted Transfer Mode



Software versions used

For the information in this documentation applies:

- All steps described for the XPR refer to software version V7.
- All steps described for the HiPath 4000 apply from software version 6.

NOTE: For the time being the Trusted Transfer Mode has only been approved for usage at OpenScape Voice.

Restrictions

When connecting OpenScape-Xpressions, please heed the following:

Connecting OpenScape UC Application

Connecting OpenScape-Xpressions via Trusted Transfer Mode

- After the return from the voice portal, the display texts are no longer shown, since the XPR is connected to the OpenScape Voice via the IP APL instead of the ISDN APL.
- The start character in the TTM originator number must not be removed by the PBX or a gateway between XPR server and OpenScape UC Application.

E.1.2 Trusted Transfer Mode Configuration

E.1.2.1 Requirements

The following privileges must have been granted to the user in the Web Assistant:

- Trusted transfer mode

Proceed as follows:

1. Log on to the Web Assistant as administrator.
2. Open the user management.
3. Open the data of the user whose privileges you want to customize. To do this, click on the underlined USER ID in the user bar.

The user's data are displayed.

4. Tick off the check box in the **Voice Portal** line.
5. Click the **Edit** button in the **Privileges** line.

All available privileges are listed.

6. Tick off the check box in the **Permit** column for the following privileges:

- Trusted Menu privilege
- Trusted Transfer Mode.

7. Click on **Apply** to save your settings.

The privileges have been assigned.

E.1.2.2 Configuring the PhoneMail Script

Licenses

The system requires for the Trusted Transfer Mode an additional IP APL with the following licenses:

- SIP Channel Addon

- VoIP Channel

Configuring the IP APL

1. Log on to the XPR server.
2. Open the XPR monitor.
3. Select the **IPApI>Edit Settings** entry.

The **IPApI Settings** dialog opens.

4. Click in the list on **Xpressions PhoneMail**.
5. Open the **Customer** tab in the **Xpressions PhoneMail** dialog.
6. Enter **-ttm** in the **Parameter** field.
7. In the **Xpressions PhoneMail** dialog the **OpenScape** is now available. Open the **OpenScape** tab.

The screenshot shows the 'Xpressions PhoneMail' dialog box with the 'OpenScape' tab selected. The 'OpenScape Integration' section is expanded, showing a checked checkbox for 'OpenScape integration by Trusted Transfer Mode'. Below this, there are several input fields: 'Remote Trusted-Domain cal number' (5210), 'Remote Trusted-Domain ID' (49), 'Local Trusted-Domain ID' (49), 'Calling number schema' (p*%1\$2%2\$1%3\$4%4\$4%5\$2%6\$1), and 'Calling number Maximum Length' (17). At the bottom right are 'OK', 'Cancel', and 'Apply' buttons.

8. Enter the numbering plan.

NOTE: Please obtain detailed information about the numbering plan from chapter Telematic APL in the XPR Server Administration manual.

9. Verify that the specifications under **Remote Trusted-Domain ID** and **Local Trusted-Domain ID** are identical.

Connecting OpenScape UC Application

Connecting OpenScape-Xpressions via Trusted Transfer Mode

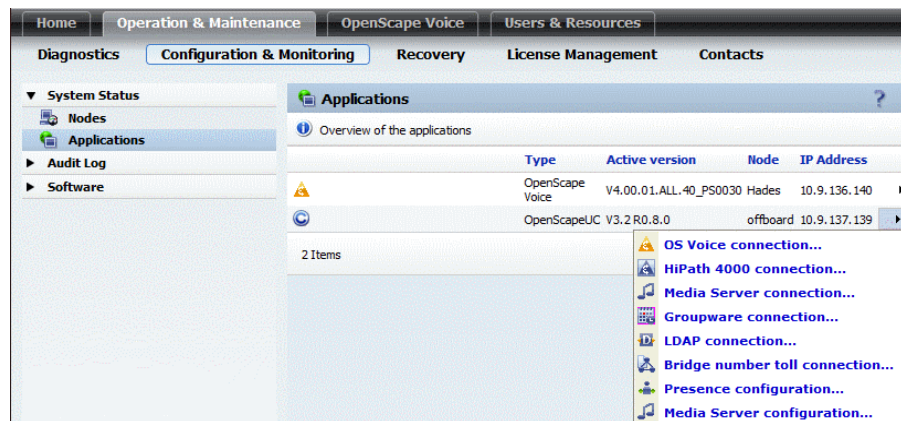
10. Confirm the specifications with **OK**.

NOTE: The IP APL configuration must be identical on the OpenScape tab.

Configuring the address binding as of version OpenScape UC Application V6

NOTE: The address binding configuration of the previous OpenScape UC Application versions deviates from version V6. Information on this is provided in [Section E.1.2.2, “Configuring the address binding for OpenScape UC Application V6 precursors”](#), on page 541.

1. Open the OpenScape CMP.
2. Select in the navigation bar **Operation & Maintenance>Configuration & Monitoring**.
3. Select in the navigation tree **System Status>Applications**.
4. Click on the triangle to the right of **OpenScape UC**.
5. Select **Media Server configuration...** from the menu.



Another dialog, node list, opens.

6. Click on the triangle to the right of **offboard**.
7. Select **Edit** from the menu.
8. Open the **Address Bindings** tab.
9. Click on the **Add...** button.

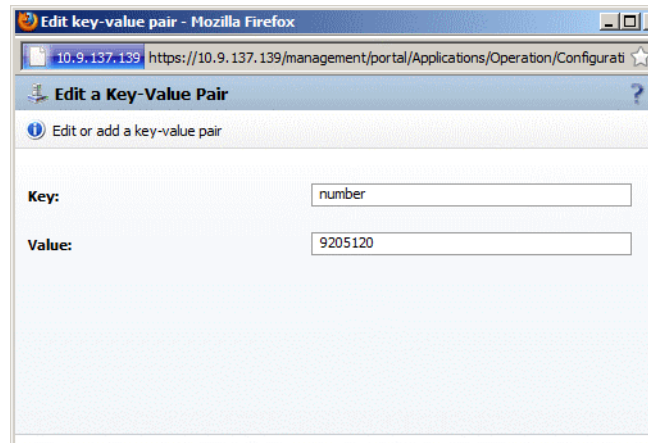
The **Address binding administration** dialog opens.

10. Click on the **Add...** button.

The following dialog opens:

Connecting OpenScape UC Application

Connecting OpenScape-Xpressions via Trusted Transfer Mode



11. Specify the key and the value. Save the pair of keys and repeat the process for the following keys:

- **xprNumber**
- **voicePortalNumber**
- **xprTrustedTransferDomain**
- **xprTrustedTransferParam**

12. Save the specifications and close the dialogs.

13. Reboot OpenScape.

NOTE: In case a second XPR (B) is integrated in the system, a second entity must be created on the voice portal.

Configuring the address binding for OpenScape UC Application V6 precursors

1. Open the **voicemail.xml**.
2. Adjust the following parameters in the **voiceportal.xml** file:
 - **xprNumber:** Specify the IP APL number. In this case, number 9 is dismissed by the PBX.
 - **xprTrustedTransferDomain:** The settings are identical with those of the XPR.
 - **xprTrustedTransferParam:** The settings are identical with those of the XPR except for the characters. OpenScape UC Application uses “v” instead of “\$” and “p” instead of “%”.

Connecting OpenScape UC Application

Connecting OpenScape-Xpressions via Trusted Transfer Mode

- **voicePortalNumber**

```
<terminal appletURI="application:/VoicePortal#start" id="voice-portal-start-H4K">
<line address="regexp:sip:492404673405210@.*">
  <property
    key="permissions">PID_Xpressions,PID_NativeVoice,PID_VoicePortalMessaging,PID_VoiceMail,PID_Email,PID_Team,PID_MeetMeConference,PID_Professional,PID_VoicePortalContactAccess,PID_Presence,PID_SelfServiceVoicePortal,PID_ManageCalendarAppointments,PID_AdHocConference,PID_Rules</property>
  <property key="useprofiles">no</property>
  <property key="symLanguage">EN-US</property>
  <property key="symDomain">system</property>
  <property key="operator">0</property>
  <property key="transferTimeout">30</property>
  <property key="thirdPartyVMNumber">4711</property>
  <property key="xprNumber">9205120</property>
  <property key="voicePortalNumber">+492404673405210</property>
  <property key="xprTrustedTransferDomain">49</property>
  <property key="xprTrustedTransferParam">p0v1p1v2p2v1p3v4p4v4p5v2p6v1</property>
  <property key="ttsLanguages">en-US,de-DE,zh-CN</property>
  <property key="guessLanguages">en-US,en-GB,de-DE,zh-CN</property>
</line>
</terminal>
```

3. Save the settings and reboot OpenScape UC Application.

NOTE: In case a second XPR (B) is integrated in the system, a second entity must be created on the voice portal.

E.1.2.3 Configuring OpenScape Users

NOTE: The user resources must be present in the XPR server.

1. Open the OpenScape CMP.
2. Select in the navigation bar **Users & Resources>Users**.
3. Select in the navigation tree **User Administration>Users**.
4. Click on the triangle to the right of the user in the list.
5. Select **Edit**.

The following dialog opens:

Edit User - 250

Modify existing user - grayed-out items are read-only (password options available only when changing the password)

General **Password/PIN** **Contact Information** **Profiles** **Resources**

System Devices

Voicemail

System: [dropdown]
Number: 492404673405902 [Assign...] [Unassign]

Queue

Number: none [Add/Edit...]

User Devices

To quickly add a new resource complete the fields below and select 'Add'. For more advanced options use the 'Advanced' button.

Name: [text] Number: [text] [Add] [Advanced...]

☐	Name	Number	ONS	Comm. System	Assigned
☐	[icon]	49240467340250	✓	OpenScape Voice	✓

1 Item [Edit...] [Assign/Unassign] [Delete]

[Save] [Cancel]

Done

6. Select the **Resources** tab.
7. Specify the subscriber code for the user at the OpenScape Voice.
8. Confirm the specification with **Save**.

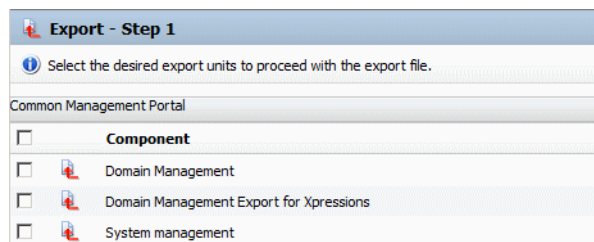
E.1.2.4 Importing OpenScape Users in XPR

The user data is transmitted from the OpenScape to XPR. First, use the export feature in the CMP to store the data in a file that will subsequently be installed in the XPR server.

Exporting users

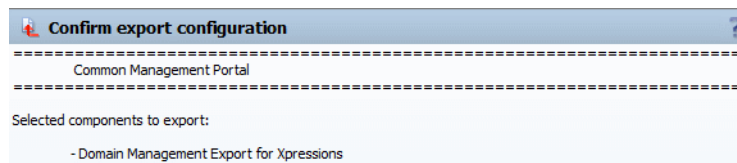
1. Start the CMP.
2. Select in the navigation bar **Operation & Maintenance>Recovery**.
3. Select in the navigation tree **Import & Export>Export**.

The following dialog opens:



4. Activate **Domain Management Export for Xpressions**.
5. Select **Next**.

The following dialog opens:



6. Confirm with **Export**.

The following storage dialog opens:

7. Specify the storage location for **ExportFile.zip** and confirm with **Yes**.

The export starts. When the export is complete, you receive an overview of the process.

8. Open the ExportFile.zip
\${exportWorkingDir}>Package_domainmanagement_domainmanagement_001.zip>\${BackupApplWorkDir} stored in the system.
9. Extract the file **domain_configuration.csv**.

The export is complete.

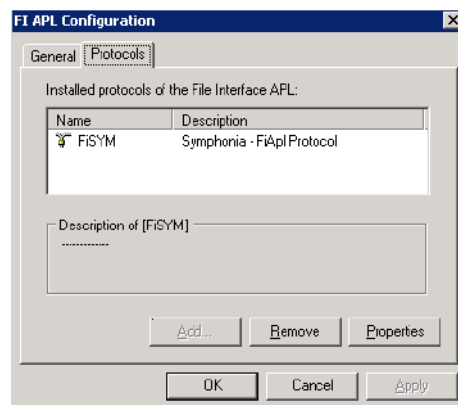
Importing users in XPR

1. Copy the FiSym.e script from the setup medium to the **.../xpr/res/FiApl** folder.

You need to create a folder in the system for the XPR server where the export files are stored and can be read by the XPR server. This file store must be made known to the XPR server since not conventions exist here.

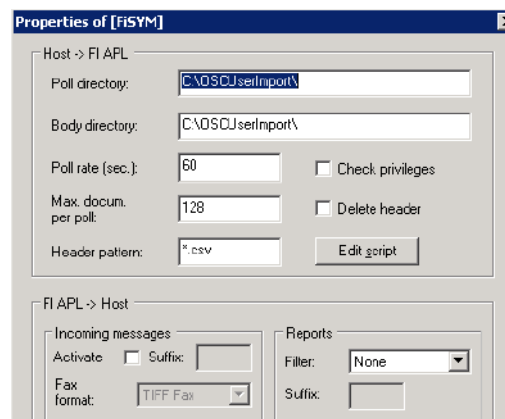
Proceed as follows:

2. Create a folder in the system.
3. Open the XPR monitor.
4. Select the **FiApl>Edit Settings** entry.
5. Open the **Protocols** tab.
6. Add the FiSym.e script to the list via the **Add** button.



The protocol is added to the list.

7. Open the settings of the newly added protocol.
8. Specify the path to the folder previously created in the system.
9. Specify the interval of the import request.



10. Confirm the entries with **OK**.

Connecting OpenScape UC Application

Connecting OpenScape-Xpressions via Trusted Transfer Mode

11. Copy the export file to the previously created folder.

The user specifications are imported in the XPR server. After the import, users can log on via the TUI or WebAssistant.

Importing several users in XPR

If users from the OpenScape UC distribute among several XPR server, the import is controlled by assigning a voicemail number. Only the user data the voicemail entry of which matches the entry in the system is then inserted.

1. Open the registry.
2. Select
`HKLM>Software>Wow6432Node>PP-COM>MRS>FiAPL>FiSYM.`
3. Create a new string value `Voicemail.`
4. Enter the phone number of the Phonemail (IP APL) Direct Access as value.
The value must match the voicemail entry of the OpenScape user.
5. Save the specifications and reboot the FiAPL.

NOTE: The system imports only the users whose voicemail value matches those of the system in the XPR server system.

Index

*.lic 71

A

Access types
 callback access 392
 direct access 392, 414
 fax access 392, 414
 forward access 392, 413
 guest access 392, 414
 Acrobat Reader 154
 Acronym directory 18
 Additional resources 81
 Administrator
 user account 107
 user name 107
 Application Builder
 client 82
 ASR
 client 86
 installation type 86
 ASR applications 86
 Automatic speech recognition 86

B

BGL 496
 BIOS settings 229
 BIRT 98
 Business group line 496
 business intelligence and reporting tool 98

C

Call forwarding 399
 Callback access number 414
 CallerGuide 86
 Cards
 HiPath 4000/CorNet-NQ 244
 CCBS 388
 CCNR 388
 Charge recording 399
 Hicom 300 396
 Class not registered 50
 Client
 Application Builder 82
 Client PC
 minimum equipment 28
 Clients

 SIP authentication 474
 Closed numbering 393, 414
 CMP 496
 Common management portal 496
 Communication hardware 27
 Communications 81
 Communications client 99
 CorNet-N connection
 Hicom 300 388
 HiPath 3000 413
 Crystal Reports XI developer edition 98
 CTI APL 95

D

Data execution prevention 32
 Data protection 20
 Data security 20
 Database connection module 92
 Database folder 101
 DBAPL 92
 Default language 77
 demilitarized zone 162
 DEP 32
 Destination code 500
 Dialing information transmission
 block-by-block 388
 digit-by-digit 388
 Directory synchronization
 LDAP 95, 192
 Distributed system
 domain 198
 kernel computer 199
 SatPrep.exe 201
 user account 194, 198
 DIUN2 module 389
 DIUN4 module 389
 DIUS2 module 389
 DMZ 162
 Document folder 101
 Domain
 distributed system 198

E

Eclipse 98
 Eicon
 DIVA Server Card(s) 244, 348
 Endpoint 496, 498

- Endpoint profile 498
- ERGO 108
- Error
 - Could not open printer 51
- EVO 86
- Exchange 2003 administration 81
- Export formats 98
- Extension range 404
- EXUM APL
 - Exchange 2000 96

F

- Fax code 401, 405
- Fax messaging 401
- Fax-on-demand 94
- Feature profile 467
- FI APL 96

G

- Generating
 - license keys 41
- Grace period 37
- Group fax number 401, 403

H

- Hicom 300
 - charge recording 396
- Hicom PIN 388
- HiPath 8000
 - NMC 474
 - number plan 474
 - SMC 474
- HiPath Fault Management 154
- HiPath license agent
 - installation 61
- HiPath license management
 - installation 57

I

- IIS 30
- IMAP4 clients 121
- Installation
 - from network share 69
 - HiPath license agent 61
 - HiPath license management 57
 - reboot 49
 - summary 100
- Installation sources 69
- Installation type
 - ASR 86
- Installing
 - license service 72
- internet information services 30

- IP APL 95
- IP telephony 95, 192
- IPSec Configuration 503
- ISDN APL 94, 95

J

- Java runtime environment 98
- JDBC driver 98
- JRE 98
- JVM 98

K

- Kernel computer
 - distributed system 199

L

- LAN integration 35
- Language packet 77
- Language settings
 - non-unicode program 29
- Languages
 - available 77
- Layout files 98
- LDAP
 - directory synchronization 95, 192
- Lear 97
- License 71
- License file 37, 71
- License keys
 - generating 41
- License service 71
 - installing 72

M

- MAC address 39
- MAC ID 39, 40
- Manual structure 16
- Manuals 17
- MDF 395
- Message waiting indication 501
- Microsoft SQL Server 2005 Express
 - password 210
 - remote desktop 51
 - terminal server 51
 - use 207
- Minimum equipment
 - client PC 28
- MMC Snap-in 81
- Modem 230
- Monitor
 - share 92
- Monitor event log 92
- Music-on-hold 399

MWI 417, 501

N

Network integration 30

Network segment 198

Network share

installation from 69

New installation

operating system 229

Non-unicode program

language settings 29

Nuance Vocalizer 84

Number list

closed 393

open 393

Numbering plan 35

O

Open numbering 393, 414

Operating system

new installation 229

Optimization options 29

P

Pager 94

Partitioning 29

Password

Microsoft SQL Server 2005 Express 210

PBX connection variants 387

PhoneMail 78

Point-to-point connection 122

POP3 clients 121

POP3/IMAP4 clients 94

Postmaster

user account 106, 108

user name 108

Prefix access code 500

Print APL 96

Privacy user 399

R

RAS service 122

Real-time services manager 433

Reboot 49

installation 49

Recommended settings

Windows 2000 Professional 230

Windows 2000 Server 234

Release notes 79

Remote activation of a call diversion 388

Remote desktop

Microsoft SQL Server 2005 Express 51

settings 51

Rep APL 97

Report APL 98

Report designer component 98

Report Schedule APL 98

Required tools 17

Route 499

RSM 433

S

SAPconnect 96

routing 96

SAPphone 96

Satellite computer 198

Satellite system 191

Send station

SMS 230

Server language 77

Server name

specifying 76, 247, 282, 317, 351

Settings

remote desktop 51

Share

monitor 92

SIP authentication

clients 474

SIP trunk 496

SLMN module (AZA209) 390

SMS 95

send station 230

SMTP APL 94, 121

SMTP messages 121

SMTP service 30

Specifying

server name 76, 247, 282, 317, 351

Speech synthesis 84

STHC module 390

STMD module 390

STMD2 module 390

Subscriber 470

Summary

installation 100

System number 421

System requirements

initial installation 24

T

Target group 16

TCP/IP 92

Terminal server

Microsoft SQL Server 2005 Express 51

Text-to-speech 84

TLS 496

transport layer security 496
Trusted entity 474

U

UDP 496

Use

- Microsoft SQL Server 2005 Express 207

User account

- administrator 107
- distributed system 194, 198
- postmaster 106, 108

User name

- administrator 107
- postmaster 108

Utilities 97

V

V.24 APL 97

Virtual environment 214

VMS 78

VMware ESX server 214

Voice guide 94

Voice messaging 400, 418

Voicemail server 94

VPIM 94

W

Web Assistant 93

Web server 93, 192

Wrapper 48

