



A MITEL
PRODUCT
GUIDE

Unify OpenScape Xpressions V7

Microsoft Exchange Gateway

Microsoft Exchange Gateway

Installation and Administration Manual

05/2025

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	13
1.1 Who should read this Manual?	13
1.2 Manual Structure	13
1.2.1 Conventions	14
1.3 Further XPR Server Documentation	15
1.3.1 Notes for Service Technicians and Support	17
1.4 Data Protection and Data Security	18
1.5 General Considerations	20
1.5.1 Messaging Applications, an Overview	21
1.5.1.1 The Evolutionary Steps of the XPR Server	21
1.6 Features	25
1.7 Hardware, Software and System Requirements	27
1.7.1 Hardware and Software Requirements	27
1.7.2 System Requirements	27
2 Exchange Integration Restrictions	29
3 The <i>Exchange Fail-Safe Wizard</i>	31
3.1 Parameters for the <i>Exchange Fail-Safe Wizard</i>	34
3.1.1 Exchange Server 2007	37
3.1.2 Exchange Server 2010	42
3.2 Interpreting the Test Results	47
4 XPR and Microsoft Exchange Server 2007	49
4.1 General Considerations	49
4.1.1 Changes introduced with Exchange Server 2007	49
4.1.1.1 Administration Modifications	49
4.1.1.2 Exchange Server 2007 Cluster	50
4.1.2 The XPR Connector for Exchange 2007	51
4.1.3 The XPR True Unified Messaging Connector	52
4.1.4 <i>Exchange Servers 2007</i> Administration Novelties	52
4.1.5 XPR Features Modifications	53
4.2 Installation	54
4.2.1 General Considerations	54
4.2.2 Preparations	54
4.2.3 Installation Process Overview	60
4.2.4 Installation of the XPR Components for the Connection to Exchange Server 2007	62
4.2.4.1 Selecting the Components	62
4.2.5 Components Installation Procedure	65
4.2.5.1 Starting the Installation	65
4.2.5.2 General Considerations	65
4.2.5.3 Installing the LDAP APL	66
4.2.5.4 Installing the True Unified Messaging Connector	68
4.2.5.5 XPR Foreign Connector Installation	72
4.2.5.6 Installation of the MMC Snap-in	77
4.2.6 Working on the Exchange Server	80
4.2.6.1 Creating the Transport Directories	80
4.3 Configuration	87
4.3.1 Configuring the LDAP Apl.	87

Contents

4.3.1.1	General Considerations	87
4.3.1.2	Active Directory and XPR	89
4.3.1.3	Installing the LDAP APL	90
4.3.1.4	Editing LDAP Settings	90
4.3.1.5	The “Login” Tab	94
4.3.1.6	The “Search” Tab	97
4.3.1.7	The “Attributes” Tab	102
4.3.1.8	The “Global Settings” Tab	110
4.3.1.9	“My SQL Settings” Tab	111
4.3.2	Monitoring the LDAP APL Activities	112
4.3.3	Uninstalling the LDAP APL	113
4.3.4	User Administration	114
4.3.4.1	The “MRS Settings” Tab	116
4.3.5	Administration of the XPR Foreign Connector	119
4.3.5.1	General Tab	120
4.3.5.2	Exchange Foreign Connector Tab	122
4.3.5.3	CTI Settings Tab	123
4.3.5.4	Formats Tab	124
4.3.5.5	Display Formats Tab	127
4.3.5.6	Version Tab	129
4.4	Multi-Hub Transport Server Support	130
4.4.1	Configuring the Multi-Hub Server Support	131
4.5	Using additional Address Spaces for the Exchange Connectors	134
4.5.1	Overview	134
4.5.1.1	Configuration Overview	135
4.5.2	Configuring additional Address Spaces	135
4.5.2.1	Configuring the Address Space on the Exchange Server	135
4.5.2.2	Creating the “Active Directory Object”	136
4.5.2.3	Copying the DLLs into the corresponding Exchange Directories	136
4.5.2.4	Configuring the e-mail Address Policies	137
4.5.2.5	Adding the required EXADDRESSTYPE registry key	138
4.6	Fax Message Addressing	139
4.6.1	Definition of the “FAX” Address Type	139
4.7	Adding and assigning the MRS E-Mail Address Type retrospectively	140
4.8	Security Settings for Installation and Live Operation of the E2k7 APL and ExUM APL	142
4.8.1	Requirements	143
4.8.2	Privileges for the Exch APL Installation	144
4.8.3	Privileges for the ExUM APL Installation	147
4.8.4	Privileges for the MMC Snap-in Installation	147
4.8.5	Privilege Restrictions for Live Operation	148
4.8.5.1	General Information	148
4.8.5.2	MRS Connector Settings	148
4.8.5.3	Assigning the privilege of operating Exch Apl service to any user	149
4.8.5.4	Privilege Overview	151
4.9	Migration	152
4.10	Integration in Hosted <i>Exchange 2007</i>	153
4.11	Troubleshooting	154
4.11.1	Restrictions for MAPI Sessions with Exchange 2007	154
5	XPR and Microsoft Exchange Server 2010	155
5.1	General Considerations	155
5.1.1	Changes with <i>Exchange Server 2010</i>	155

5.1.2	The XPR Foreign Connector for <i>Exchange Server 2010</i>	156
5.1.3	The XPR True Unified Messaging Connector	157
5.1.4	Administering the <i>Exchange Servers 2010</i>	158
5.1.5	Connection to <i>Exchange Server 2010 DAG</i> and/or <i>Exchange Server 2010 CAS Array</i>	159
5.1.5.1	Connection to an Exchange <i>Database Availability Group</i>	160
5.1.5.2	Connection to an Exchange <i>Client Access Server Array</i>	160
5.2	Installation	161
5.2.1	General Considerations	161
5.2.2	<i>Exchange Server 2010</i>	161
5.2.3	Preparations	161
5.2.4	Installation Process Overview	171
5.2.5	Installation of the XPR Components for the Connection to <i>Exchange Server 2010</i>	173
5.2.5.1	Selecting the Components	173
5.2.6	Components Installation Procedure	176
5.2.6.1	Starting the Installation	176
5.2.6.2	General Considerations	176
5.2.6.3	Installing the LDAP APL	177
5.2.6.4	Installing the XPR True Unified Messaging Connector	179
5.2.6.5	XPR Foreign Connector Installation	185
5.2.6.6	Installation of the MMC Snap-in	193
5.2.6.7	Error Analysis during the Installation	196
5.2.7	Working on the Exchange Server	198
5.2.7.1	Creating the Transport Directories	198
5.3	Configuration	205
5.3.1	Configuring the LDAP Apl	205
5.3.1.1	General Considerations	205
5.3.1.2	Active Directory and XPR Server	207
5.3.1.3	Installing the LDAP APL	208
5.3.1.4	Editing LDAP Settings	208
5.3.1.5	The “Login” Tab	212
5.3.1.6	The “Search” Tab	215
5.3.1.7	The “Attributes” Tab	220
5.3.1.8	The “Global Settings” Tab	228
5.3.1.9	“My SQL Settings” Tab	229
5.3.2	Monitoring the LDAP APL Activities	230
5.3.3	Uninstalling the LDAP APL	231
5.3.4	User Administration	232
5.3.4.1	“MRS Settings” Tab	234
5.3.5	Administration of the XPR Foreign Connector	237
5.3.5.1	General Tab	238
5.3.5.2	Exchange Foreign Connector Tab	240
5.3.5.3	CTI Settings Tab	241
5.3.5.4	Formats Tab	242
5.3.5.5	Display Formats Tab	245
5.3.5.6	Version Tab	247
5.4	Multi-Hub Transport Server Support	248
5.4.1	Configuring the Multi-Hub Server Support	249
5.5	Using additional Address Spaces for the Exchange Connectors	252
5.5.1	Overview	252
5.5.1.1	Configuration Overview	253
5.5.2	Configuring additional Address Spaces	253
5.5.2.1	Configuring the Address Space on the Exchange Server	253

Contents

5.5.2.2	Creating the “Active Directory Object”	254
5.5.2.3	Copying the DLLs into the corresponding Exchange Directories	254
5.5.2.4	Configuring the e-mail Address Policies	255
5.5.2.5	Adding the required EXADDRESSTYPE registry key	256
5.6	Fax Message Addressing	257
5.6.1	Definition of the “FAX” Address Type	257
5.7	Adding and assigning the MRS E-Mail Address Type retrospectively	258
5.8	Security Settings for Installation and Live Operation of the E2k7 APL and ExUM APL	260
5.8.1	Requirements	261
5.8.2	Privileges for the Exch APL Installation	262
5.8.3	Privileges for the ExUM APL Installation	265
5.8.4	Privileges for the MMC Snap-in Installation	265
5.8.5	Privilege Restrictions for Live Operation	266
5.8.5.1	General	266
5.8.5.2	MRS Connector Settings	266
5.8.5.3	Assigning the privilege of operating Exch Apl service to any user	267
5.8.5.4	Privilege Overview	270
5.9	Migration	271
5.10	Integration in Hosted <i>Exchange 2010</i>	272
5.11	Troubleshooting	273
5.11.1	Configuration for the CDO in Systems without public Folders	273
6	Connecting Exchange Server 2013 via an Exchange 2007/2010 Domain	275
6.1	Overview	275
6.2	General System Requirements	276
6.3	XPR Service Account Requirements	277
6.4	Creating an XPR Service Account on the Exchange Server 2013	277
6.5	Checking the Exchange 2013 Server Configuration	278
6.6	Assigning Privileges	279
6.6.1	Assigning the required Privileges to the Service Account	279
6.6.2	Exchange Server 2013 Privileges	280
6.6.2.1	Privileges on Organization and Database Level	280
6.6.2.2	Privileges on User Level	280
6.6.2.3	Configuring a Throttling Policy	280
6.6.3	Assigning local Privileges to the XPR Service Account	282
6.6.4	Switching the ExUM Apl to the new XPR Service Account	282
6.7	Adjusting the LDAP Configuration	283
6.7.1	Extending the User Data Mask on the XPR Server	284
6.7.2	Expanding the LDAP Replication	285
6.8	Adjusting Registry Settings	288
6.8.1	Adjusting Registry Settings for the XPR Server	288
6.8.2	Checking and configuring Certificates for the RPC Proxy Server	290
6.8.3	Registry Settings for the ExUM Apl	291
6.8.3.1	Determining the Registry Values via the EMS	291
6.8.3.2	Configuring the Registry Keys for the ExUM Apl	291
6.9	Log File	293
7	XPR and Microsoft Exchange Server 2013	295
7.1	General Considerations	295
7.2	Overview	295
7.3	General System Requirements	295
7.3.1	Preparations	296
7.4	Requirements for a direct Connection	305

7.4.1 XPR Service Account on Exchange Server 2013	305
7.4.2 Users on the Exchange Server 2013	306
7.5 Creating an XPR Service Account on the Exchange Server 2013	306
7.6 Checking the Exchange 2013 Server Configuration	306
7.7 Assigning Privileges	307
7.7.1 Assigning the required Privileges to the Service Account	307
7.7.2 Exchange Server 2013 Privileges	308
7.7.2.1 Privileges on Organization and Database Level	308
7.7.2.2 Privileges on User Level	308
7.7.2.3 Configuring a Throttling Policy	309
7.7.3 Configuration of Exchange Server 2013 without public Folders	310
7.7.4 Assigning local Privileges to the XPR Service Account	311
7.8 Adjusting the LDAP Configuration	311
7.8.1 Extending the User Data Mask on the XPR Server	312
7.8.2 Expanding and updating the LDAP Replication	313
7.8.3 Switching the ExUM Apl to the new XPR Service Account	315
7.9 Adjusting Registry Settings	316
7.9.1 Adjusting Registry Settings for the XPR Server	316
7.9.2 Checking and configuring Certificates for the RPC Proxy Server	318
7.10 Installing the Connectors	320
7.10.1 General Considerations	320
7.10.2 Installation of the XPR Components for the Connection to <i>Exchange Server 2013</i>	320
7.10.2.1 Selecting the Components	320
7.10.3 Components Installation Procedure	323
7.10.3.1 Starting the Installation	323
7.10.3.2 General Considerations	323
7.10.3.3 Installing the LDAP APL (for a fresh OpenScale Xpressions V7 Server Setup)	324
7.10.4 Installing the OpenScale Xpressions V7 True Unified Messaging Connector (ExUm Apl)	325
7.10.4.1 Log Files for installing the ExUM Apl	330
7.10.4.2 Registry Settings of the ExUM Apl	330
7.10.4.3 Determining the Registry Values via the EMS	330
7.10.4.4 Configuring the Registry Keys for the ExUM Apl	331
7.10.4.5 Making the ExUM Apl failsafe on the Exchange Server 2013	333
7.10.5 Installing the OpenScale Xpressions V7 Foreign Connector	334
7.10.5.1 Log Files for installing the E2k7 Apl	340
7.10.6 Installation of the MMC Snap-in	342
7.10.6.1 Error Analysis during the Installation	345
7.10.7 Working on the Exchange Server	346
7.10.7.1 Creating the Transport Directories	346
7.11 Configuration	353
7.11.1 Configuring the LDAP Apl	353
7.11.1.1 General Considerations	353
7.11.1.2 Active Directory and XPR Server	355
7.11.1.3 Installing the LDAP APL	356
7.11.1.4 Editing LDAP Settings	356
7.11.1.5 The “Login” Tab	360
7.11.1.6 The “Search” Tab	363
7.11.1.7 The “Attributes” Tab	368
7.11.1.8 The “Global Settings” Tab	376
7.11.1.9 “My SQL Settings” Tab	377
7.11.2 Monitoring the LDAP APL Activities	378
7.11.3 Uninstalling the LDAP APL	379

Contents

7.11.4	User Administration	380
7.11.4.1	“MRS Settings” Tab	382
7.11.5	Administration of the XPR Foreign Connector	385
7.11.5.1	General Tab	386
7.11.5.2	Exchange Foreign Connector Tab	388
7.11.5.3	CTI Settings Tab	389
7.11.5.4	Formats Tab	390
7.11.5.5	Display Formats Tab	393
7.11.5.6	Version Tab	395
7.12	Multi-Hub Transport Server Support	396
7.12.1	Configuring the Multi-Hub Server Support	397
7.13	Using additional Address Spaces for the Exchange Connectors	400
7.13.1	Overview	400
7.13.1.1	Configuration Overview	401
7.13.2	Configuring additional Address Spaces	401
7.13.2.1	Configuring the Address Space on the Exchange Server	401
7.13.2.2	Creating the “Active Directory Object”	402
7.13.2.3	Copying the DLLs into the corresponding Exchange Directories	402
7.13.2.4	Configuring the e-mail Address Policies	403
7.13.2.5	Adding the required EXADDRESSTYPE registry key	404
7.14	Fax Message Addressing	405
7.14.1	Definition of the “FAX” Address Type	405
7.15	Adding and assigning the MRS E-Mail Address Type retrospectively	406
7.16	Security Settings for Installation and Live Operation of the E2k7 APL and ExUM APL	408
7.16.1	Requirements	409
7.16.2	Privileges for the Exch APL Installation	410
7.16.3	Privileges for the ExUM APL Installation	413
7.16.4	Privileges for the MMC Snap-in Installation	413
7.16.5	Privilege Restrictions for Live Operation	414
7.16.5.1	General	414
7.16.5.2	MRS Connector Settings	414
7.16.5.3	Assigning the privilege of operating Exch Apl service to any user	415
7.16.5.4	Privilege Overview	418
7.17	Migration	419
7.18	Integration in Hosted <i>Exchange 2013</i>	420
7.19	Troubleshooting	421
7.19.1	Configuration for the CDO in Systems without public Folders	421
7.20	Log File	421
8	Multiline Configuration	423
8.1	Multiline Configuration for independent Exchange Servers	425
8.1.1	General Considerations	425
8.1.2	Configuration Requirements	428
8.1.3	Defining Service Accounts	429
8.1.4	Multiline Configuration	430
8.1.4.1	Editing Registry Keys	431
8.1.4.2	Adding Routing Rules	431
8.1.4.3	Adding/editing a Policy	432
8.1.4.4	Adding XPR User Database Fields	432
8.1.4.5	Supplementing LDAP Attributes	433
8.1.4.6	Assigning Privileges	433
8.1.4.7	Configuring the Cross-Forest Administration	434

8.1.4.8 Creating Linked Role Groups	435
8.1.4.9 Further Configuration Steps	436
8.1.5 Standard Multiline Configuration for a distributed Installation with Exchange Server	437
8.1.6 Multiline Configuration for associated Message Delivery with Exchange Server	438
8.1.7 True Unified Messaging (TUM) in Multiline Environments	439
9 Microsoft Exchange Server 2016/2019/Office 365 (EWS)	443
9.1 General Considerations	443
9.2 Overall Architecture	443
9.2.1 Exchange 2016 / 2019	443
9.2.2 Office 365	444
9.3 Installation and Configuration	446
9.3.1 Preparation/Configuration	446
9.3.2 Message Flow Overview	446
9.3.3 Installing the .Net Framework 3.5	448
9.3.3.1 Windows 2008 R2	448
9.3.3.2 Windows 2012/ Windows 2012 R2/ Windows 2016/2019	449
9.3.4 Required Version/ hotfixes on XPR system	449
9.3.5 TLS 1.2	450
9.3.6 EWSApl installation for Exchange 2016/2019/On-Premises	451
9.3.7 EWSApl installation for Exchange Online (Office 365)	452
9.3.8 EWSApl: OAuth authentication	454
9.3.8.1 Microsoft Entra configuration	454
9.3.8.2 Powershell Configuration	460
9.3.8.3 Client Secret Configuration	461
9.3.8.4 EWSApl Hotfix installation	463
9.3.9 EWSApl "Service User" configuration	465
9.3.10 "Windows Service" Configuration	467
9.3.11 Configuring SmtmApl	468
9.3.12 Configuring MTA Routing Rules	469
9.3.13 User Mask Configuration	469
9.3.14 Configuring Users	472
9.3.14.1 Users synchronization between Xpressions and Active Directory (via LDAP)	472
9.3.14.2 Importing Exchange Users from Active Directory	476
9.3.14.3 Importing users using Powershell scripts	476
9.3.14.4 Importing users with FiApl	481
9.3.15 Registry Settings (Additional setting of EwsApl)	482
9.4 Distributed EWSApls	486
10 Sending Faxes from Exchange to Xpressions	489
10.1 Exchange 2016/2019	489
10.2 Exchange Online (Office 365)	494
10.2.1 SmtmApl accessible via Internet	494
10.2.2 Using Exchange on-premises as relay on a hybrid deployment	500
10.2.2.1 Example of creating a connector on the Exchange Online side	501
10.2.2.2 Example of creating a connector on the Exchange on-premises side	508
10.2.3 SmtmApl configuration	510
11 Troubleshooting	513
11.1 ExchAplConfigurator	513
11.2 EWSApl service	513
11.3 EWSApl - Persistent delay in message synchronization and MWI	513
11.4 EWSApl - OAuth authentication	513

Contents

11.5	Message submission rate for this client has exceeded the configured limit" issue on SmtplApl	515
11.6	Microsoft Tools	515
11.6.1	Exchange Web Services Editor	515
11.6.2	Remote Connectivity Analyzer	518
12	Outlook/Exchange Extensions	521
12.1	Outlook Extensions Features	521
12.2	XPR Icon and Message Forms	523
12.2.1	Icon Forms	523
12.2.2	Message Forms	525
12.2.3	General Information about Installing the Forms	527
12.2.3.1	General Information about Installing the Forms in Outlook 2007	527
12.2.3.2	General Information about Installing the Forms in Outlook 2010 and further versions	527
12.2.4	Installation of the Server Components	529
12.2.4.1	Requirements for Installing the Icon and Message Forms	529
12.2.5	Requirements for Installing the Icon and Message Forms	531
12.2.5.1	Creating the Forms Directory in Exchange Server 2007/2010	531
12.2.5.2	Starting the Installation Routine for the Server Component	533
12.2.5.3	Subsequent Message and Icon Forms Registration	535
12.2.5.4	Uninstalling Message and Icon Forms	537
12.2.6	Security Settings for the ActiveX Control Elements	538
12.2.6.1	Local Configuration on a Workstation	538
12.2.6.2	Configuration for Microsoft Server 2008	539
12.3	Installation of Client Components	542
12.3.1	Configuration Overview	542
12.3.1.1	Windows Client Operating Systems	542
12.3.2	User-defined Installation of the Message Forms on the Clients	543
12.3.2.1	Tables: "Property" for Outlook Forms for Outlook 2007	543
12.3.2.2	Tables: "Registry" for Outlook Forms for Outlook 2007	544
12.3.3	Installation of the Xpressions Outlook Forms for Outlook 2010 and further versions (VSTO Forms)	548
12.3.4	Outlook Forms in Metaframe or Terminal Server Environments	548
12.3.5	Uninstalling the Local Outlook 2007 Forms Components	551
12.3.6	Uninstalling the Server Based Forms for Outlook 2007	551
12.3.7	Uninstalling the Outlook Forms for Outlook 2010 and further versions	552
A	Appendix	553
A.1	Service Provider (MSP)	553
A.2	Connector Installation on Microsoft Small Business Server	554
A.2.1	Activating the Exchange MTA Stacks in SBS 2003	554
A.2.1.1	Removing Registry Keys	554
A.2.1.2	Modifying the Start Type of Microsoft Exchange MTA Stacks	555
A.2.1.3	Restarting Services	555
A.2.1.4	Installing the XPR Exchange Connector	555
A.3	"Xpressions" Folder with <i>PhoneMail</i> in Case of Inbox Replication	556
A.4	Automatic Client Software Distribution	557
A.4.1	Client Log-in via Windows User Account	557
A.5	Registry Entry Directory	558
A.5.1	General Considerations	558
A.5.2	Registry Entries for <i>Exchange Server 2007</i>	559
A.5.2.1	HKLM\SOFTWARE\Wow6432Node\PP-COM\MRS\ExchApl	559
A.5.2.2	HKLM\SOFTWARE\Wow6432Node\PP-COM\MRS\ExUMApl	578
A.5.3	Registry Entries for <i>Exchange Server 2010</i>	586
A.5.3.1	HKLM\SOFTWARE\Wow6432Node\PP-COM\MRS\ExchApl	586

A.5.3.2 HKLM\SOFTWARE\Wow6432Node\PP-COM\MRS\ExUMapl	606
A.5.4 Registry Entries for <i>Exchange Server 2013</i>	614
A.5.4.1 HKLM\SOFTWARE\Wow6432Node\PP-COM\MRS\ExchApl	614
A.5.4.2 HKLM\SOFTWARE\Wow6432Node\PP-COM\MRS\ExUMapl	634
A.5.4.3 HKCU\Software\Microsoft\WindowsNT\CurrentVersion\Windows Messaging Subsystem.	645
A.5.5 Registry Entries for Exchange Server 2016	647
A.5.5.1 HKLM\SOFTWARE\Wow6432Node\PP-COM\MRS\EwsApl	647
A.5.6 HKLM\SOFTWARE\Wow6432Node\PP-COM\MRS\LdapApl	648
A.5.7 HKLM\SOFTWARE\Wow6432Node\Cycos AG \ExchForms Server	649
A.5.8 HKLM\SOFTWARE\Wow6432Node\Cycos AG \ExchForms Client	650
A.5.9 HKLM\SOFTWARE\ or HKCU....	656
A.5.10 HKCU\Software\Cycos AG\COM\....	657
A.5.11 HKLM\SYSTEM\....	661
Acronyms	665
Index	666

1 Introduction

1.1 Who should read this Manual?

This manual addresses the system administrator of an XPR Exchange environment as guiding line for integrating the XPR server in a *Microsoft Exchange* environment. It describes the installation and configuration steps required for the integration of an XPR server in a *Microsoft Exchange* environment. Based on this description, each administrator should be able to perform the required installations and configurations for connecting Exchange.

1.2 Manual Structure

The manual's sections cover the following:

- This introduction in which you find general notes on the Exchange connection and on this manual's content.
- Description of the Exchange *Fail-Save Wizard*, an auxiliary program to check the system requirements for setting up the Exchange connectors.
- Connecting an XPR server to a pure *Exchange Server 2007* environment. See [Chapter 4, "XPR and Microsoft Exchange Server 2007"](#).
- Connecting an XPR server to a pure *Exchange Server 2010* environment. See [Chapter 5, "XPR and Microsoft Exchange Server 2010"](#).
- Connecting an XPR server to a pure *Exchange Server 2013* environment via an Exchange Server 2007 or 2010 domain. See [Chapter 6, "Connecting Exchange Server 2013 via an Exchange 2007/2010 Domain"](#).
- Connecting an XPR server to a pure *Exchange Server 2013* environment directly. See [Chapter 7, "XPR and Microsoft Exchange Server 2013"](#).
- Integrating the XPR*Outlook* Extensions. See [Chapter 12, "Outlook/Exchange Extensions"](#).

1.2.1 Conventions

To differentiate the types of information provided, the following conventions are used in this manual:

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

NOTE: Under this label you find information worth knowing and facilitating your operations.

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

Special fonts have the following meaning:

- Names of configuration parameters, dialog titles, dialog texts, and operating elements (buttons, check boxes, tabs) are in bold lettering, for example: Login Options.
- File and directory names as well as program code lines (listings) appear in font `Courier`.
- Variables are *italicized*.

NOTE: Please note that the dialogs depicted in this manual may vary from those you see as this depends on the desktop design settings.

1.3 Further XPR Server Documentation

This section informs about further technical XPR server documentation.

In principle, a printed version of the manual can only be ordered on special request; all other documents are on the product data carrier as PDF version with full text search. Additionally, online help is available for most of the components (win help or HTML help) that can be started directly from the respective programs.

All input windows necessary for installation and operation are shown in these documents; these masks may differ slightly depending on the operating system, screen resolution and PC configuration. The following XPR server documents are available:

Manual	Topic
Unify OpenScape Xpressions V7Server Installation	Server installation instruction
Unify OpenScape Xpressions V7Server Administration	Configuration and structure of the XPR server
Unify OpenScape Xpressions V7 <i>Microsoft Outlook</i> Extensions	User manual on the functions made available in addition by the XPR integration in <i>MS Outlook</i>
<i>Unify OpenScape Xpressions V7 optiClient 130</i>	Administration and user manual to configure and operate the <i>Unify OpenScape Xpressions V7 optiClient 130</i> features
Unify OpenScape Xpressions V7Web Assistant	Admin manual for administering the XPR server via a Web browser
Unify OpenScape Xpressions V7Communications	PC client of the XPR server

Server Installation

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

Server Administration

This manual provides information about the structure of the entire system. Here you find a description of the XPR kernel functions and of the available APLs. This manual is for XPR server administrators and describes in detail the product in its maximum configuration level. Here a detailed XPR system configuration description is given.

Outlook extensions

User manual for operating the additional *MS Outlook* features:

- Simplified addressing with fax transmission and polling, combined with a convenient editing function to furnish incoming messages with additional text or graphic elements before they are forwarded.
- Simplified SMS message transmission.
- Incoming messages, no matter by which service (fax, e-mail or voicemails), can be furnished with a text and/or voice annotation before forwarding them to one or several addresses. They can also be sent back to the originator as reply or to all original recipients (if the message came in as carbon copy (CC)). The voice annotation can be recorded via telephone or via a microphone connected to the sound card.
- Transmission of new voicemails.
- Incoming fax and voicemails can be read or listened to in the preview window (editing fax and voicemails via the preview window is not possible with Outlook XP). When you open such messages with a double-click, a convenient fax editing function is available so that you can add text or graphic elements to incoming fax messages before they are forwarded. Voicemails can be played back either via sound card or the individual telephone and extended with a voice annotation before they are forwarded.
- Using the XPR server CTI features from Outlook. Precondition is, of course, that the corresponding CTI feature is installed on the XPR server.

This enables calling message originators simply by mouseclick. Subscribers can be called via the local Outlook directories or address books available on the Exchange server just as easily.

Furthermore, you can invoke the CTI client *Unify OpenScape Xpressions V7 optiClient 130* directly from Outlook. Via this client you can make full use of the XPR server CTI features.

Unify OpenScape Xpressions V7 optiClient 130

Administration and user manual for *Unify OpenScape Xpressions V7 optiClient 130*. It describes how to configure and operate the CTI client *Unify OpenScape Xpressions V7 optiClient 130*.

Web Assistant

User manual for administering and using the XPR server via Web browser.

Communications

The Communications manual describes the operating functions for handling communication jobs and the administrative functions to maintain the XPR server by means of a PC client.

1.3.1 Notes for Service Technicians and Support

Besides the user documentation and the administrator manual also heed the XPR server release info found on the product data carrier. This information contains current product notes that may not have been considered for the documentation. You find the file on the product data carrier under `releaseNotes.rtf`. Further current information is also found in the `Read.me` files included in the directories on the product data carrier that contain the corresponding program component.

1.4 Data Protection and Data Security

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

In Germany, the processing and use of such personal data are 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.

Members of the Unify Software and Solutions GmbH & Co. KG are required to observe business and data secrecy as a result 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 data media such as backup disks or printed reports. 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.

1.5 General Considerations

The XPR server unifies the services voicemail, fax, e-mail and Short Message Service (SMS) on one Windows platform to one Unified Messaging system with connection to different PBXs for using the CTI functions. Information flow, flexibility and speed have become decisive factors for the success of modern companies.

Thanks to its modular, scalable client/server architecture, XPR can be optimally configured to meet the users' individual communication needs. Open standards, integration in existing IT and telecommunications environments, and secure PBX access via ISDN, LAN, and the Internet guarantee the protection of your investment in the future. The customer can define the services, number of users and an integration in existing messaging environments according to his/her requirements. In this way, a tailored solution for every requirement from the small entry-level variant right up to networked communication solutions can be created.

One option to integrate the XPR server in an existing messaging environment is, besides *Lotus Notes* and *SAP, Microsoft Exchange*. This integration enables the user to access messages in the journal of the Microsoft Exchange client Outlook that were exclusively received via the XPR server (fax, voicemail and SMS). In addition, CTI functions can be used subject to the PBX connected. The XPR server administers these functions PBX-specifically and provides them in the Microsoft Exchange client. Another integration feature is address book synchronization. Address book data are replicated no matter on which server users are administered.

Connecting the XPR server to Microsoft Exchange makes sure that

- the services e-mail, fax, voicemail, SMS and the CTI functions are integrated on the Microsoft Exchange client and
- address books are synchronized.

Depending on the desired messaging application (for example Integrated Messaging or True Unified Messaging, see also [Section 1.5.1, "Messaging Applications, an Overview", on page 21](#)), the integration is performed by installing some additional components:

- For connecting *Microsoft Exchange Server 2007* respectively *Microsoft Exchange Server 2010*
 - Installation of the XPR Exchange connector (Exch APL, 32-bit service)
 - For using True Unified Messaging in addition to the True Unified Messaging connector (ExUM APL, 32-bit service)
 - Installation of the LDAP APL to administer addresses with Active Directory

1.5.1 Messaging Applications, an Overview

1.5.1.1 The Evolutionary Steps of the XPR Server

First we want to give a short description of what Unified Messaging actually is and in which evolutionary steps the XPR server provides different functions here, so that you basically understand the various configuration options.

Unified Messaging (UM)

Unified Messaging means that you can access all messages via a uniform journal, no matter which service delivers them. For example, you can view or play fax documents, voicemails or e-mails using *Microsoft Outlook*. *Unified Messaging* is possible with the XPR client *Communications* or via telephone by means of modern Interactive Voice Response (IVR) applications, such as the voice prompt controlled PhoneMail or Ergo. Unified Messaging is also possible with *Microsoft Exchange*, *Lotus Notes* or *SAP R/3* connections on the respective foreign systems.

Advanced Unified Messaging

Unified Messaging supplemented with CTI functions is called *Advanced Unified Messaging*. Here CTI journal information is generated that logs user calls and their current state (for example missed calls or failed calling attempts). In addition, operating the individual telephone via the client is enabled.

Integrated Messaging and True Unified Messaging

The next step is deduced via the following example:

A field worker retrieves his/her messages from the XPR server via telephone. Without any further provisions he/she would only be able to access messages (fax, voicemail and SMS) directly received via the XPR server. E-mails e.g. written by colleagues under *Microsoft Exchange* could not be retrieved via telephone. In order to make these also accessible via telephone, two methods can be employed:

Introduction

General Considerations

- **Integrated Messaging (IM)**

This method enables a replication of all messages of this employee to the XPR server so that twice the data amount is generated for this field worker but all e-mails can then immediately be retrieved by telephone. *Integrated Messaging* is available for *Lotus Notes* and *Microsoft Exchange*.

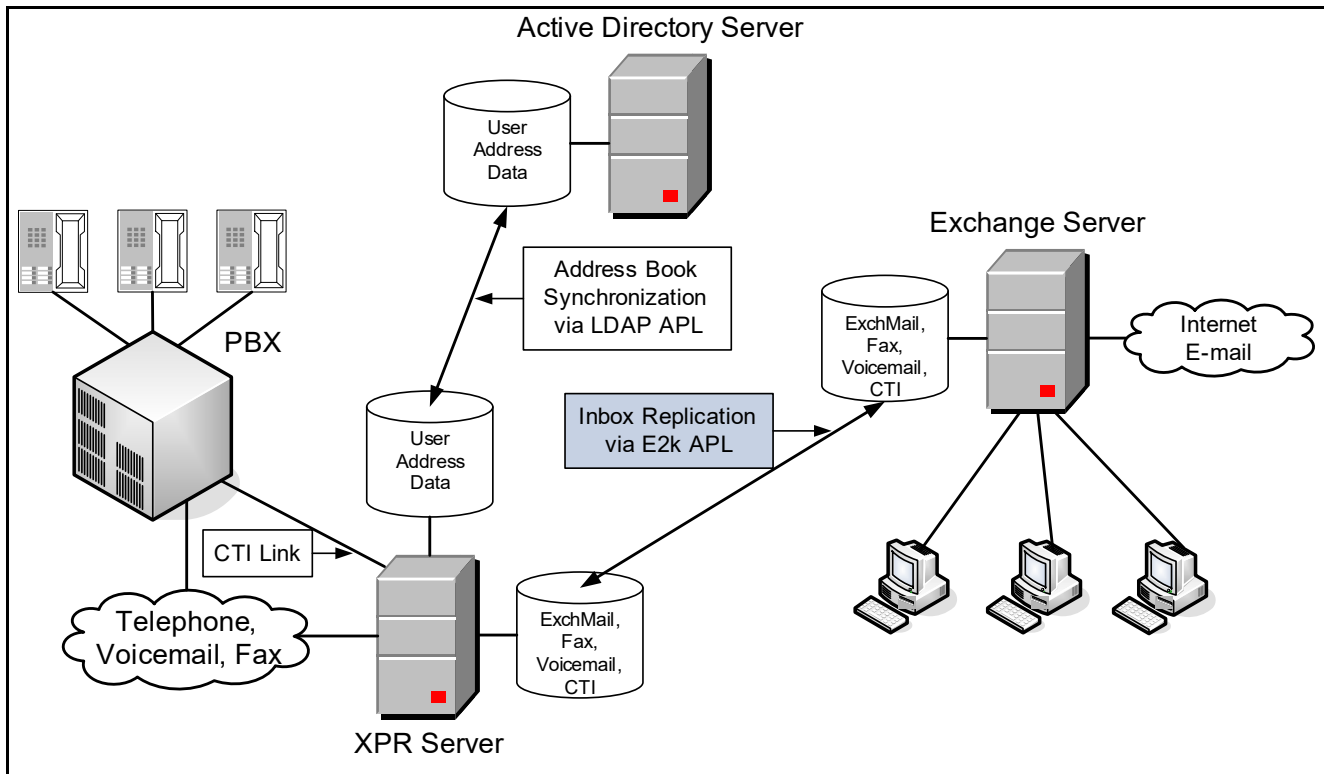


Figure 1

System Structure in Case of Integrated Messaging

- **True Unified Messaging (TUM)**

We can also directly access the data storage of the foreign system, so that messages are only available when they are retrieved by telephone. Here we depend on the foreign system transmitting the message almost in real time so that only very short waiting periods occur at the telephone. This is in most cases guaranteed by the modern servers of nowadays. This type of access without permanent message replication is called *True Unified Messaging*. *True Unified Messaging* is available for *Lotus Notes* and *Microsoft Exchange*. Using *True Unified Messaging* requires the additional installation of the Exchange True Unified Messaging APL.

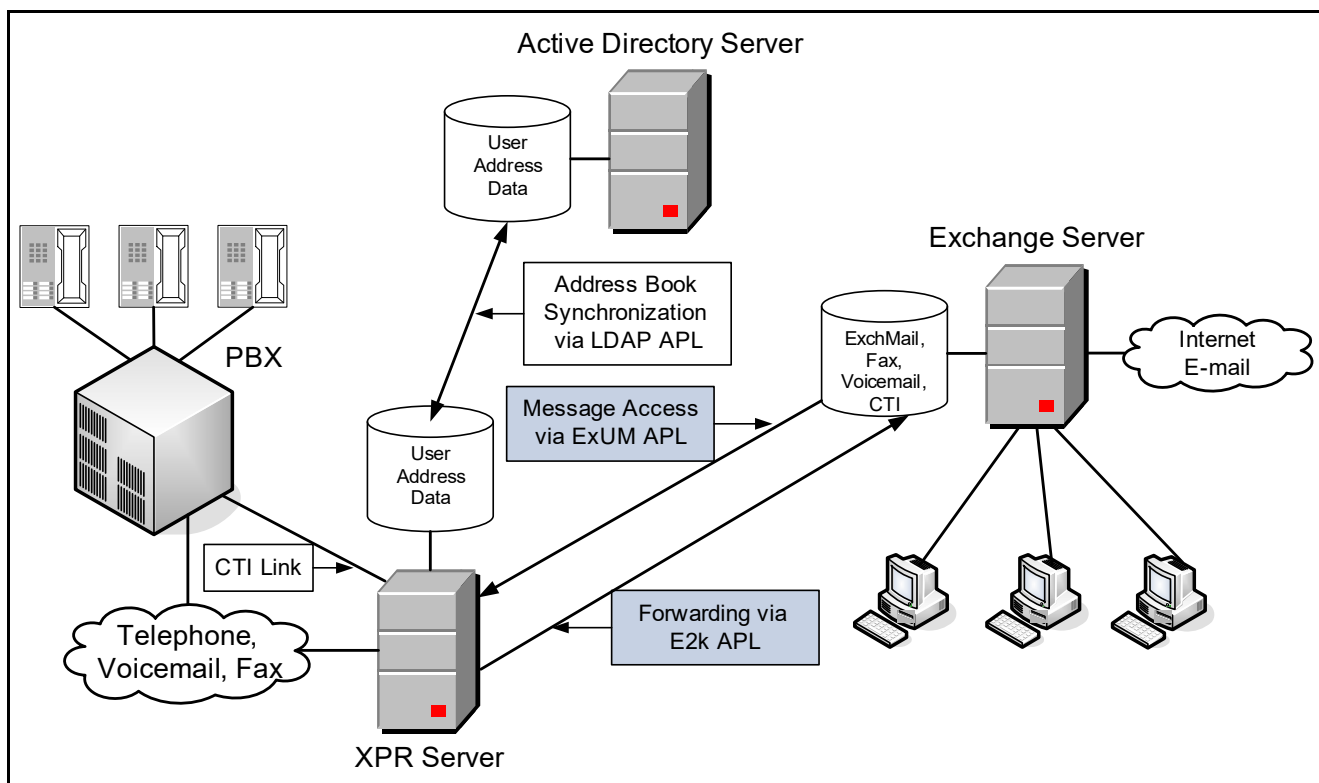


Figure 2 System structure with True Unified Messaging

Integrated Messaging and *True Unified Messaging* can also be operated parallel. For example, *Integrated Messaging* (characteristic: data replication to the XPR server) can then be employed with slow servers for users that permanently need to access messages by means of the XPR server. For all other users that only occasionally retrieve messages and who are willing to wait a few seconds, *True Unified Messaging* (characteristic: direct access to the foreign system's data store) can be used.

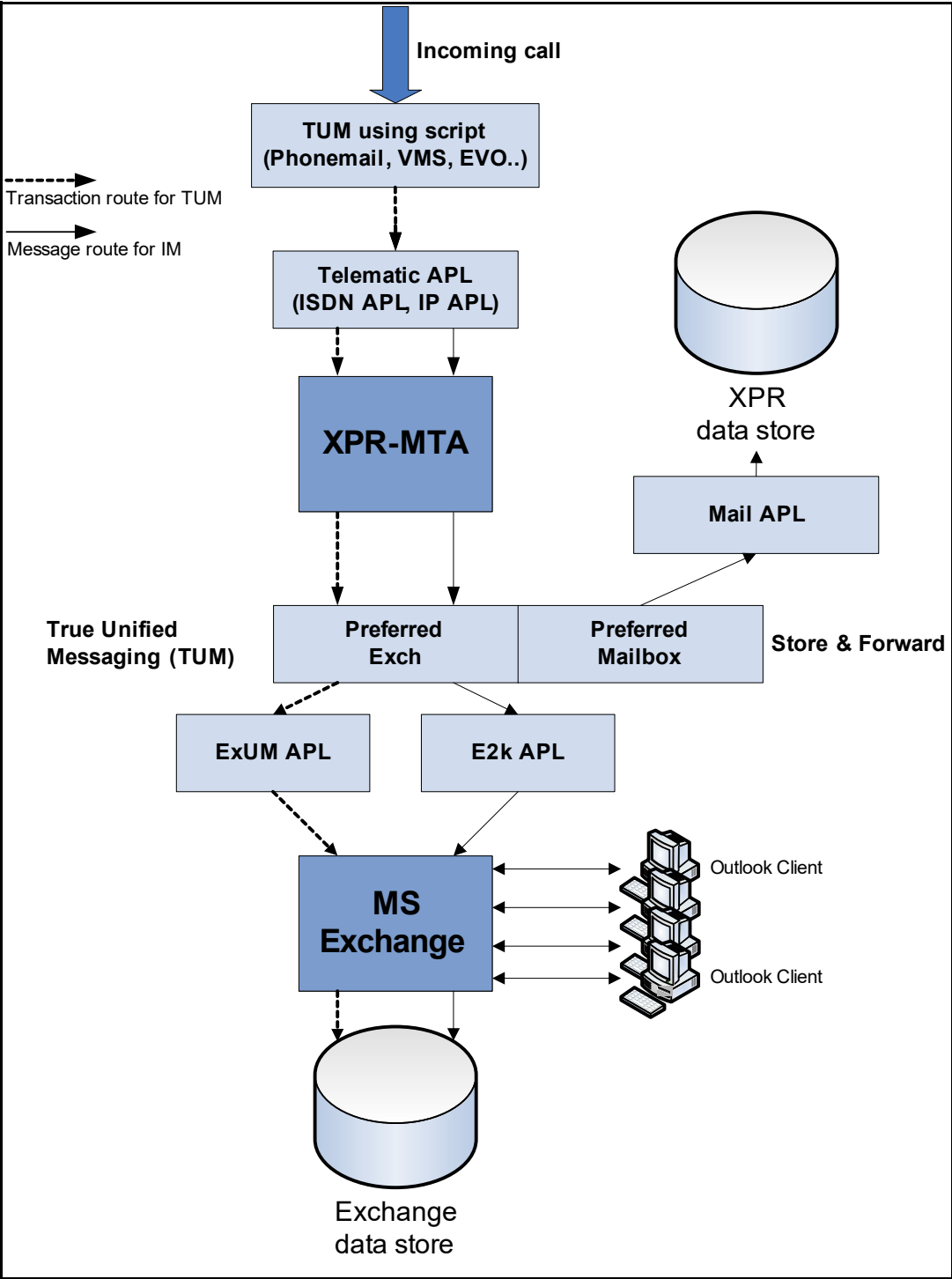


Figure 3 Transaction and Message Paths for True Unified Messaging and Integrated Messaging

1.6 Features

The following table provides an overview of the additionally available services and functions after integrating the XPR server in a *Microsoft Exchange* environment:

Feature	Description
Fax and voicemail receiving	Access to fax and voice messages, received by the XPR server via the <i>MS Outlook</i> client. Convenient editing functions for fax messages and playback features for voicemails in <i>MS Outlook</i> .
Fax transmission	Individual form function in <i>MS Outlook</i> for sending fax messages.
Fax-on-Demand	Individual form function in <i>MS Outlook</i> for polling fax messages provided via special calling numbers.
SMS transmission	Individual form function in <i>MS Outlook</i> for sending SMS messages.
Voicemail transmission	Individual form function in <i>MS Outlook</i> for sending voice messages. Voicemail works similarly to an answering machine – but much more intelligently and with multifarious functions such as forwarding, answering or connecting to the message originator. Messages can be put out via telephone or a computer sound card with attached loudspeakers.
Voice annotation for message transmission	Supplementation to the voicemail form function for attaching voice comments before sending a message or forwarding it.
Message Icons	Automatic use of additional icons in the message journal of <i>MS Outlook</i> : • To indicate incoming fax and voice messages in the inbox journal. • To indicate call states in the telephone journal: successful, unsuccessful, separated according to in or outbound calls.

Table 1 Available Services and Functions after integrating the XPR Server

Feature	Description
CTI features via Unify OpenScape Xpressions V7 optiClient 130	<i>Unify OpenScape Xpressions V7 optiClient 130</i> is a high-performance CTI client with which you can control your desk telephone from your computer. As computer-oriented user you are enabled to – initiate telephone calls, – accept telephone calls and – utilize more complex telephony functions – such as switching telephone conferences – simply from your preferred working environment. <i>Unify OpenScape Xpressions V7 optiClient 130</i> also supports you by – conveniently managing private contacts in the contact list – setting up phone connections the easy way via the team bar – connecting external address books – for example via LDAP – integrating this component in Outlook or Lotus Notes clients <i>Unify OpenScape Xpressions V7 optiClient 130</i> is used as client on an XPR server. You can thus take advantage of further special features provided to the client by the XPR server. Among these are: – <i>Unify OpenScape Xpressions V7 optiClient 130</i>-independent logging of your successful and unsuccessful calls – the XPR-server-based presence function, which informs you about the availability of other users Furthermore, the modular <i>Unify OpenScape Xpressions V7 optiClient 130</i> structure enables you to customize the features and representation of the application.
Representation of additional information in journal columns of <i>MS Outlook</i> (in the Subject line and From journal column)	If required or desired, further information can be displayed in the <i>MS Outlook</i> journal columns Subject and/or From .
Multi-tenant solution for several Exchange organizations	Shared use of an XPR server by several independent tenants.

Table 1 Available Services and Functions after integrating the XPR Server

1.7 Hardware, Software and System Requirements

1.7.1 Hardware and Software Requirements

You find information about the server hardware requirements and the operating systems released for the server installation as well as about the hardware and software requirements on the usable Microsoft Outlook clients in the Release Notice manual.

NOTE: If there have been changes to hardware and software requirements not considered in this manual, you find information about these in the *Release Notes* (`ReleaseNotes.rtf`) of the XPR product data carrier.

1.7.2 System Requirements

- The Exchange connector can only be installed and configured after Microsoft Exchange Server has been installed and is active in the network. The installation may occur in combination with the XPR server setup or later on an XPR server already installed.
- So that telephony functions can be used, a PBX, certified by Unify Software and Solutions GmbH & Co. KG, with the corresponding CTI transaction provider (CTI APL) to the XPR server must be available.
- The Service Provider (MSP) must be installed on the local workstation. This is done automatically with the Outlook extensions installation.

Introduction

Hardware, Software and System Requirements

2 Exchange Integration Restrictions

- Mailbox replication (mirroring of all Exchange messages that arrive for a user in a corresponding XPR mailbox) is limited to a maximum of 500 (Exchange) users. This is not a general, technical limit, but for the time being no pragmatical values are available on larger configurations. Note that in case of more than 200 subscribers with mailbox replication incoming messages or status reports are not immediately replicated but in cycles (cycle time five minutes or longer). We generally recommend to set a cyclic mailbox replication.

NOTE: Mailbox replication is an old-fashioned way of accessing messages directly via user inbox. It has been replaced with the TUM access. Only Exchange Server 2003 still supports it but it should no longer be used regardless.

- Microsoft supports a maximum of 5000 simultaneous MAPI accesses. Therefore, the number of users who can use True Unified Messaging (TUM) is restricted to 5000 per ExUM APL. To push the supported number of users beyond 5000, you can use the Multiline Configuration features. This feature must be configured project-specifically.

NOTE: To improve the load distribution and for special environments (multi tenancy), a *distributed XPR system* can be installed. In this system, additional Exchange gateways are used. See [Section , “Multiline Configuration”, on page 423](#).

- Installing several Exchange gateways on one PC system is not allowed.
- OU descriptions must be in line with the Microsoft name conventions. Therefore, OU names containing special characters, for example \ and /, must be adapted before an installation.
- To communicate with Exchange, XPR uses the MAPI subsystem via the Exchange Apl. This means: As regards the TCP/IP connection to Exchange, the same requirements must be met as for Outlook. You can obtain information on this direct from Microsoft under

<http://support.microsoft.com/default.aspx?scid=kb;en-us;280132>

<http://support.microsoft.com/default.aspx?scid=kb;en-us;270836>

<http://support.microsoft.com/default.aspx?scid=kb;en-us;278339>

<http://support.microsoft.com/default.aspx?scid=kb;en-us;291615>

Using a firewall between Exchange and XPR is only possible with the considerable exceptions described in the above sections.

3 The *Exchange Fail-Safe Wizard*

The *Exchange Fail-Save Wizard* (`ExchFailSafe.exe`) is an auxiliary program for checking the system requirements to be met for setting up the Exchange connector and for checking some system parameters for operating the Exchange connectors after the installation.

You can use it to check whether the Exchange connector installation requirements have been met before the setup. Beyond that it serves the purpose of error diagnosis after a failed installation.

The *Exchange Fail-Save Wizard* provides the following options for you to determine for which Exchange connection the test shall be performed:

Exchange Server 2007,

Exchange Server 2010 or

Check Exchange version automatically.

You find this auxiliary program on the product data carrier in the `Prerequisites` directory.

After the XPR server setup you find the auxiliary program in the directory `... \xpr \SDKTools` and you can start it from there.

The *Exchange Fail-Safe Wizard* checks the following setup requirements:

- Under “Dll Version Check” it checks for all Exchange versions whether the DLLs (CDO and MAPI) used comply with the minimum requirements and have the same release level on the XPR and Exchange server.
- Under “Rights Exch. Organization and Active Directory” it checks whether the required privileges are available under Exchange as well as for the Active Directory. A detailed check is performed as to whether the service account (`<domain \XPR_service account>`) has the following privileges for the connector services:
 - **For all Exchange versions**
 - “Send As”,
 - “Receive As”
 - Administer Information Store,
 - Full Control AD properties
 - Domain Administrator privileges
 - Local Administrator privileges

- Read & Write for the Active Directory object:
'CN=Default Policy, CN=Recipient Policies, CN=First Organization, CN=Microsoft Exchange, CN=Services, CN=Configuration, DC=Fishing, DC=lan'.
- Read & Write for the Active Directory object:
'CN=user-Display, CN=401, CN=DisplaySpecifiers, CN=Configuration, DC=Fishing, DC=lan'.
- Create & Delete for “This object and all child objects” for the Active Directory object:
'CN=Connections, CN=Exchange Routing Group (DWBGZMFD01QNBJR), CN=Routing Groups, CN=Exchange Administrative Group (FYDIBOHF23SPDLT), CN=Administrative Groups, CN=First Organization, CN=Microsoft Exchange, CN=Services, CN=Configuration, DC=Fishing, DC=lan'.
- Full Control of the below LDAP object:
'LDAP://CN=Connections, CN=Exchange Routing Group (DWBGZMFD01QNBJR), CN=Routing Groups, CN=Exchange Administrative Group (FYDIBOHF23SPDLT), CN=Administrative Groups, CN=First Organization, CN=Microsoft Exchange, CN=Services, CN=Configuration, DC=Fishing, DC=lan'.

NOTE: This warning refers to the hotfix “MS06-019 or MS06-029”. If this hotfix has not been installed, you can ignore this warning.

- **Additionally for Exchange Server 2007**
 - Exchange View-Only Administrators group
 - Exchange Organization Administrators group
- **Additionally for Exchange Server 2010**
 - View-Only Organization Management group
 - Organization Management group
- Under “Local Permissions Check” it checks whether the privileges required on the local system are given. In detail, the following privileges are checked for the service account:
 - “Logon on as a service” **
 - “Act as part of operation system”
 - “Adjust memory quotas for a process”
 - “Backup files and directories”
 - “Restore files and directories”

- “Logon as a batch job”
- Under “Verification of the Exchange server share” the write privilege on the addresses of the Exchange shares is tested.

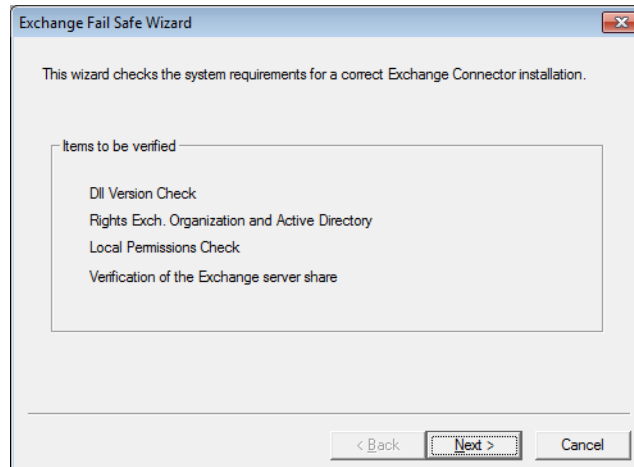
The Exchange Fail-Safe Wizard

Parameters for the Exchange Fail-Safe Wizard

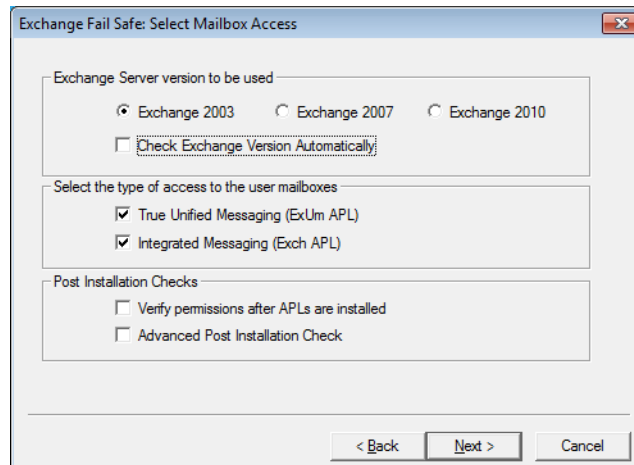
3.1 Parameters for the *Exchange Fail-Safe Wizard*

After you have started the *Exchange Fail-Safe Wizard*, some dialogs will prompt you to enter test parameters. Such parameters serve for identifying the desired Exchange server in the network.

The wizard's start is followed by a welcome dialog that lists the test items to be performed.



Click the **Next** button. The following dialog for configuring the test run opens:



Selecting the Exchange Server version

In the **Exchange Server version to be used** section, select the Exchange server environment for which the test shall be performed:

- for [Exchange Server 2007](#) or
- for [Exchange Server 2010](#)

This selection specifies the configuration dialogs to be used for the selected connection. Click on the corresponding Exchange server environment.

If you wish to have the Exchange version being determined automatically, select the **Check Exchange Version Automatically** option.

Choosing this option disables the selection switches for the various Exchange connections and the auxiliary program attempts automatically to determine the version of the specified Exchange server.

In the course of the configuration settings a message will inform you whether or not the Exchange server was found. This occurs after a click on **Next** in the dialog in which you have selected the Exchange server to be connected by the Exchange connector.

NOTE: If a message informs you that the Exchange server could not be automatically detected at this point, try to start the *Exchange Fail-Safe Wizard* by setting the Exchange server version manually.

Selecting the mailbox access

In the **Select the type of access to the user mailboxes** section specify whether the test shall only be performed for the Exchange True Unified Messaging Connector (ExUM APL) or Exchange Connector (Exch APL), or for both.

Post Installation Checks

This option enables the following tests when the installation is finished:

- Testing the privileges required for operating the Exchange connectors.

Setting up the Exchange connectors requires more advanced privileges than operating them. You can perform this test to find out whether the privileges required for operating the Exchange connectors are sufficient. This is useful e. g. in the event that the privileges are to be withdrawn after the Exchange connectors' setup.

You can perform this test after setting up the Exchange connectors by starting the *Exchange Fail-Safe Wizard* and selecting the **Verify permissions after APLs are installed** option in the **Post Installation Checks** section. As a result you will be informed about whether or not the assigned privileges are sufficient for granting the APLs' operation.
- Advanced test that checks the privileges required for operating the Exchange connectors

plus the following:
 - Whether the required Exchange services operate on the Exchange server.

NOTE: The Exchange services differ depending on the Microsoft Exchange Server version.

The Exchange Fail-Safe Wizard

Parameters for the Exchange Fail-Safe Wizard

- The consistency of the registry keys for the Exchange-Connector (Exch APL) and the Exchange True Unified Messaging Connector (ExUM APL) depending on the selected Exchange Server environment.
- Whether the XPR service account has a valid mailbox if Exchange Server 2010 has been selected as Exchange server to be used.
- Whether the registry keys respectively required for setting up the Database Availability Group (DAG) or Client Access Server Array (CAS Array) connectors have been configured correctly.

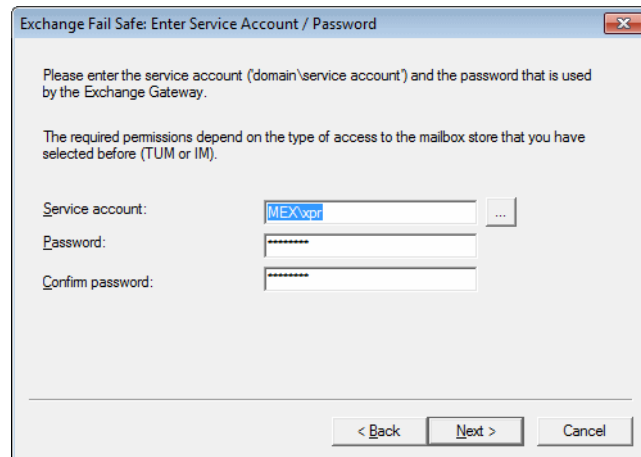
Finally, tips and hints that concern the integration of the XPR server in an Exchange environment are summarized in a result dialog.

After you have configured the test run click on **Next**. Then proceed as described in the following chapters to configure the *Exchange Fail-Safe Wizard* for the single server versions.

3.1.1 Exchange Server 2007

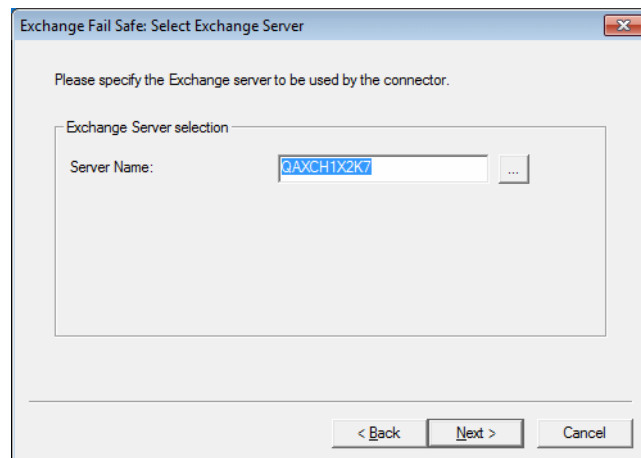
After selecting the Exchange server version, perform the following *Exchange Fail-Safe Wizard* settings for connecting the XPR server to an *Exchange Server 2007* environment:

1. In the next dialog specify under **Service account** the domain account (format: *domain\service account*) under which the connector services run. Alternatively, you can use the browse button next to the input line for selecting the service account. Enter the associated password in the **Password** and **Confirm password** fields.

A screenshot of the 'Exchange Fail Safe: Enter Service Account / Password' dialog box. The title bar is blue with a close button. The main area has a light gray background. It contains instructional text: 'Please enter the service account (domain\service account) and the password that is used by the Exchange Gateway.' and 'The required permissions depend on the type of access to the mailbox store that you have selected before (TUM or IM)'. Below this are three input fields: 'Service account:' with the text 'MEXvpr' and a browse button (...), 'Password:' with masked characters (*****), and 'Confirm password:' with masked characters (*****). At the bottom are three buttons: '< Back', 'Next >', and 'Cancel'.

Click on **Next**.

2. In the following dialog select the Exchange server to be connected by the Exchange connectors.

A screenshot of the 'Exchange Fail Safe: Select Exchange Server' dialog box. The title bar is blue with a close button. The main area has a light gray background. It contains instructional text: 'Please specify the Exchange server to be used by the connector.' Below this is a section titled 'Exchange Server selection' which contains a 'Server Name:' input field with the text 'QAXCH1X2K7' and a browse button (...). At the bottom are three buttons: '< Back', 'Next >', and 'Cancel'.

Click on **Next**.

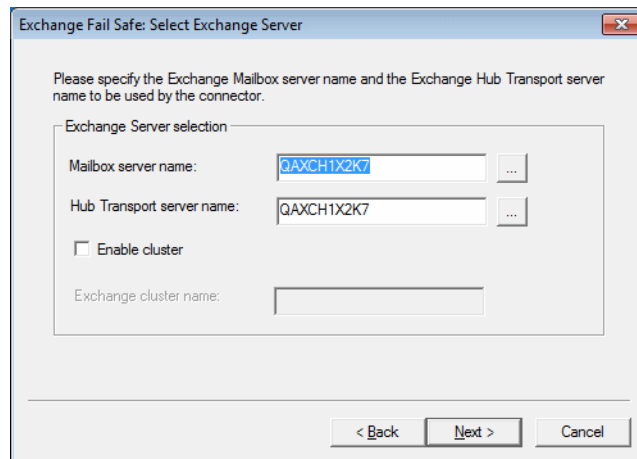
If you have selected the **Check Exchange Version Automatically** option in the **Select Mailbox Access** dialog, a message informs you about whether or not the specified Exchange server could be reached. Close the message with a click on **OK**.

The Exchange Fail-Safe Wizard

Parameters for the Exchange Fail-Safe Wizard

If the Exchange server could not be reached, try to start the *Exchange Fail-Safe Wizard* by setting the Exchange server version manually. To do this, click on **Back** until you reach the **Select Mailbox Access** dialog.

3. If the Exchange server could not be reached, specify in the following dialog the Exchange server(s) that the Exchange connectors are to connect.

The image shows a Windows-style dialog box titled "Exchange Fail Safe: Select Exchange Server". Inside the dialog, there is a text prompt: "Please specify the Exchange Mailbox server name and the Exchange Hub Transport server name to be used by the connector." Below this, there is a section titled "Exchange Server selection" which contains two text input fields. The first field is labeled "Mailbox server name:" and contains the text "QAXCH1X2K7". The second field is labeled "Hub Transport server name:" and also contains "QAXCH1X2K7". To the right of each input field is a small button with three dots "...". Below these fields is a checkbox labeled "Enable cluster" which is currently unchecked. Underneath the checkbox is a text input field labeled "Exchange cluster name:". At the bottom of the dialog, there are three buttons: "< Back", "Next >", and "Cancel".

In case of a modular *Exchange Server 2007* environment structure the XPR Foreign Connector must establish a connection from the XPR server to the Mailbox Server Role **and** to the Hub Transport Server Role.

- **Mailbox server name**
Specify here the name of the server that hosts the Exchange Mailbox Server Role. The connection to this server is used to open a MAPI connection for address resolution.
- **Hub Transport server name**
Specify here the name of the server that hosts the Exchange Hub Transport Server Role. The connection to this server is for transporting messages from/to the XPR server.

NOTE: If the *Exchange server 2007* has a monolithic structure, specify the name of the *Exchange server 2007* in both entry lines.

In case of connecting a clustered Exchange server

Select the **Enable cluster** option. The **Exchange cluster name** input line is released. In addition, the feature in the **Mailbox server name** input line changes to **Windows cluster name**.

- **Windows cluster name**
Specify here the name of the Windows cluster in the clustered Exchange environment.

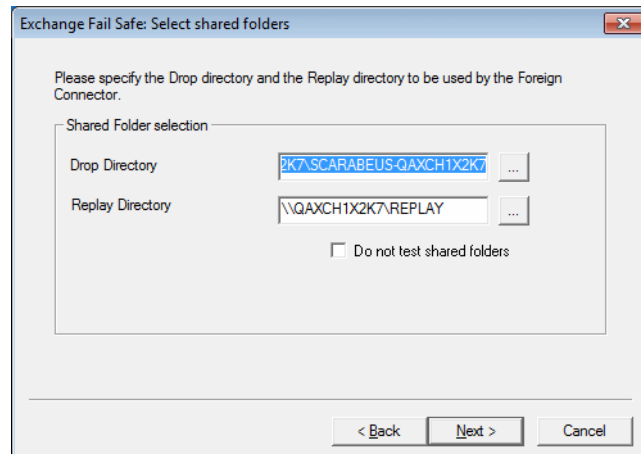
– **Exchange cluster name**

Specify here the name of the Exchange cluster in the clustered Exchange environment.

NOTE: You can select the servers by directly entering the server name. You can also use the  button to look for the corresponding server in the network. In the latter case a window opens for selecting the corresponding servers.

Click on **Next** after you have performed the corresponding settings. The dialog for specifying the path to the **Drop Directory** and **Replay Directory** opens.

4. In the **Shared Folder selection** dialog, the **Drop directory** and **Replay directory** entry lines are used for specifying the path to the shares (drop and replay directory) deployed for the message transport.



In the **Drop directory** and **Replay directory** specify the path to the shared transport directories according to the following pattern:

– **For the Drop directory**

`\\<Ip address or name of the Exchange server on which the Hub Transport Server operates>\<XPR server name>-<name of the Exchange Server 2007 Mailbox Server Role>`

– **For the Replay directory**

`\\<Ip address or name of the Exchange server on which the Hub Transport Server operates>\Replay`

NOTE: You can select the shares by making direct entries according to the above pattern. You can also use the  button to look for the corresponding shares in the network. In the latter case a window opens for selecting the corresponding shares.

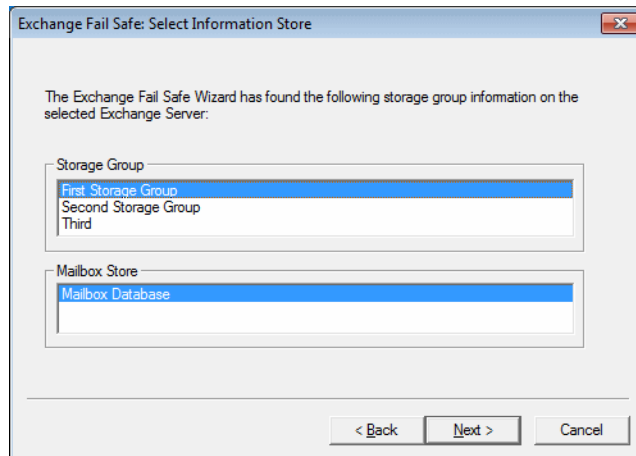
The Exchange Fail-Safe Wizard

Parameters for the Exchange Fail-Safe Wizard

Using the **Do not test shared folders** option you can skip specifying the transport directories. Select this option if the connectors have not been installed yet. In this case specifying the transport directories is not required.

Click on **Next** after you have performed all settings.

5. The next dialog displays the Storage Group information of the selected Exchange server.



Click on **Next**.

6. In the following dialog the installing user needs to authenticate at the system. Enter the domain account of the installing user (format: *domain\service account*) under **User account**. Enter the associated password in the **Password** and **Confirm password** fields. The parameter entries for the *Exchange Fail-Safe Wizard* are thus complete.

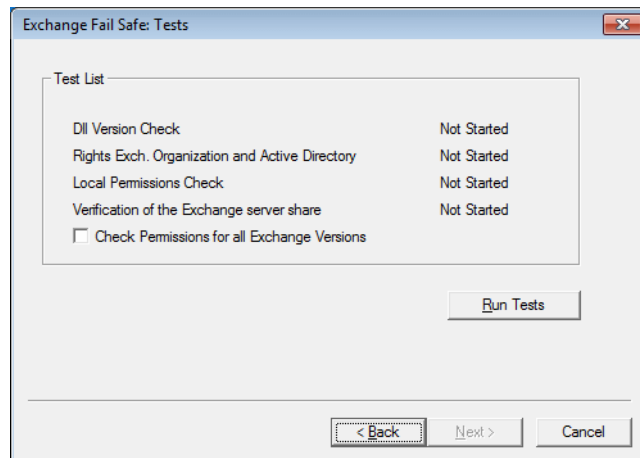


Click on **Next**. The dialog for starting the checking process opens.

7. Click on **Run Tests**.

The Exchange Fail-Safe Wizard

Parameters for the Exchange Fail-Safe Wizard



NOTE: If you select the **Check Permissions for all Exchange Versions** option, the privileges for all Exchange server versions are checked. If an error occurs during this check, it is displayed in the error list in combination with the relevant Exchange version.

In [Section 3.2, “Interpreting the Test Results”](#), on page 47 you find information about interpreting the test results.

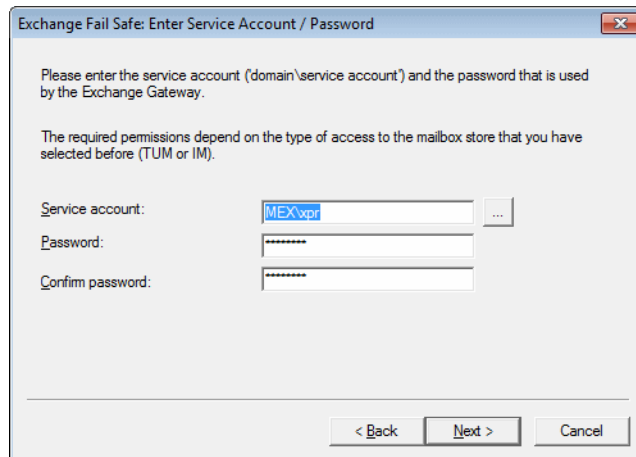
The Exchange Fail-Safe Wizard

Parameters for the Exchange Fail-Safe Wizard

3.1.2 Exchange Server 2010

After selecting the Exchange server version and the mailbox access, perform the following *Exchange Fail-Safe Wizard* settings for connecting the XPR server to an *Exchange Server 2010* environment:

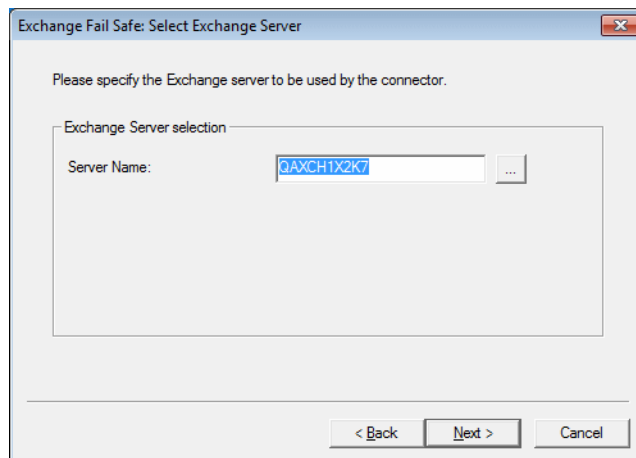
1. In the next dialog specify under **Service account** the domain account (format: *domain\service account*) under which the connector services run. Alternatively, you can use the browse button next to the input line for selecting the service account. Enter the associated password in the **Password** and **Confirm password** fields.



The dialog box is titled "Exchange Fail Safe: Enter Service Account / Password". It contains the following text: "Please enter the service account (domain\service account) and the password that is used by the Exchange Gateway." and "The required permissions depend on the type of access to the mailbox store that you have selected before (TUM or IM).". There are three input fields: "Service account:" with the value "MEXvpr" and a browse button "...", "Password:" with a masked password "*****", and "Confirm password:" with a masked password "*****". At the bottom are buttons "< Back", "Next >", and "Cancel".

Click on **Next**.

2. In the following dialog select the Exchange server to be connected by the Exchange connectors.



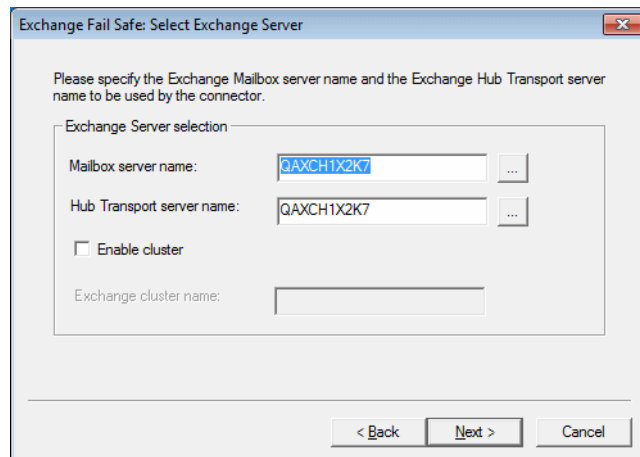
The dialog box is titled "Exchange Fail Safe: Select Exchange Server". It contains the text: "Please specify the Exchange server to be used by the connector." and "Exchange Server selection:". There is one input field: "Server Name:" with the value "QAXCH1X2K7" and a browse button "...". At the bottom are buttons "< Back", "Next >", and "Cancel".

Click on **Next**.

If you have selected the **Check Exchange Version Automatically** option in the **Select Mailbox Access** dialog, a message informs you about whether or not the specified Exchange server could be reached. Close the message with a click on **OK**.

If the Exchange server could not be reached, try to start the *Exchange Fail-Safe Wizard* by setting the Exchange server version manually. To do this, click on **Back** until you reach the **Select Mailbox Access** dialog.

3. If the Exchange server could not be reached, specify in the following dialog the Exchange server(s) that the Exchange connectors are to connect.



In case of a modular *Exchange Server 2010* environment structure the XPR Foreign Connector must establish a connection from the XPR server to the Mailbox Server Role **and** to the Hub Transport Server Role.

- **Mailbox server name**
Specify here the name of the server that hosts the Exchange Mailbox Server Role. The connection to this server is used to open a MAPI connection for address resolution.
- **Hub Transport server name**
Specify here the name of the server that hosts the Exchange Hub Transport Server Role. The connection to this server is for transporting messages from/to the XPR server.

NOTE: If the *Exchange server 2010* has a monolithic structure, specify the name of the *Exchange server 2010* in both entry lines.

In case of connecting a clustered Exchange server

Select the **Enable cluster** option. The **Exchange cluster name** input line is released. In addition, the feature in the **Mailbox server name** input line changes to **Windows cluster name**.

- **Windows cluster name**
Specify here the name of the Windows cluster in the clustered Exchange environment.

The Exchange Fail-Safe Wizard

Parameters for the Exchange Fail-Safe Wizard

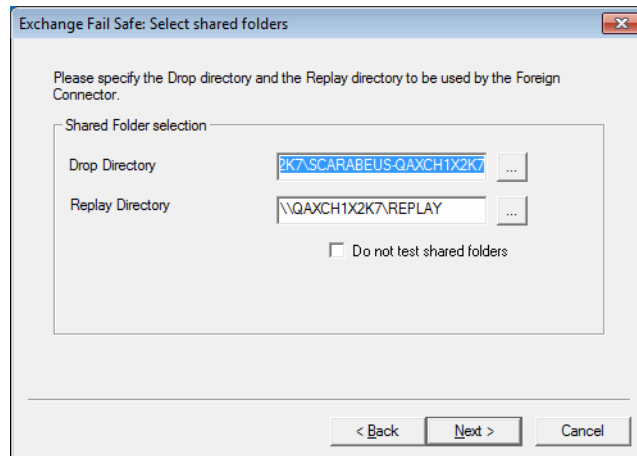
- **Exchange cluster name**

Specify here the name of the Exchange cluster in the clustered Exchange environment.

NOTE: You can select the servers by directly entering the server name. You can also use the  button to look for the corresponding server in the network. In the latter case a window opens for selecting the corresponding servers.

Click on **Next** after you have performed the corresponding settings. The dialog for specifying the path to the **Drop Directory** and **Replay Directory** opens.

4. In the **Shared Folder selection** dialog, the **Drop directory** and **Replay directory** entry lines are used for specifying the path to the shares (drop and replay directory) deployed for the message transport.



In the **Drop directory** and **Replay directory** specify the path to the shared transport directories according to the following pattern:

- **For the Drop directory**

`\\<Ip address or name of the Exchange server on which the Hub Transport Server operates>\<XPR server name>-<name of the Exchange Server 2010 Mailbox Server Role>`

- **For the Replay directory**

`\\<Ip address or name of the Exchange server on which the Hub Transport Server operates>\Replay`

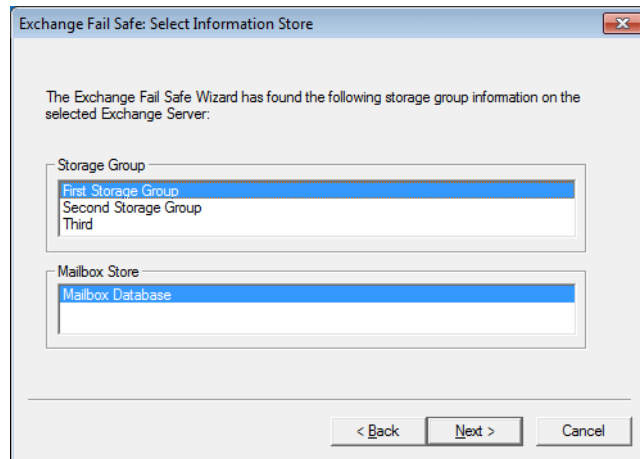
NOTE: You can select the shares by making direct entries according to the above pattern. You can also use the  button to look for the corresponding shares in the network. In the latter case a window opens for selecting the corresponding shares.

Using the **Do not test shared folders** option you can skip specifying the transport directories. Select this option if the connectors have not been installed yet. In this case specifying the transport directories is not required.

Click on **Next** after you have performed all settings.

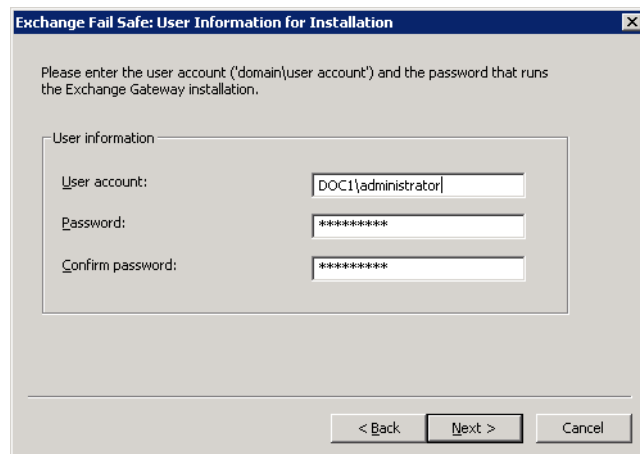
Click on **Next** after you have performed all settings.

5. The next dialog displays the Storage Group information of the selected Exchange server.



Click on **Next**.

6. In the following dialog the installing user needs to authenticate at the system. Enter the domain account of the installing user (format: *domain\service account*) under **User account**. Enter the associated password in the **Password** and **Confirm password** fields. The parameter entries for the *Exchange Fail-Safe Wizard* are thus complete.

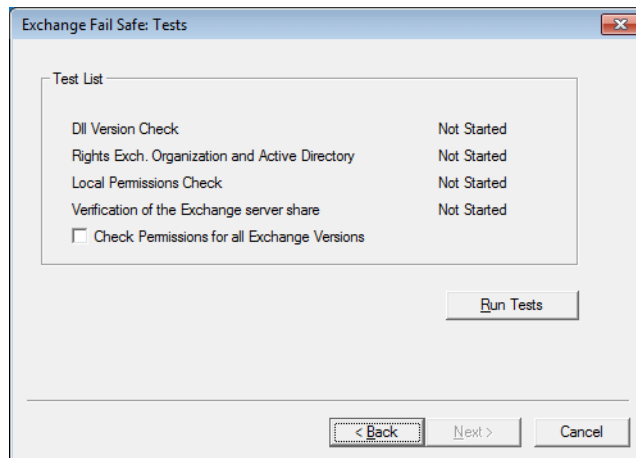


Click on **Next**. The dialog for starting the checking process opens.

7. Click on **Run Tests**.

The Exchange Fail-Safe Wizard

Parameters for the Exchange Fail-Safe Wizard

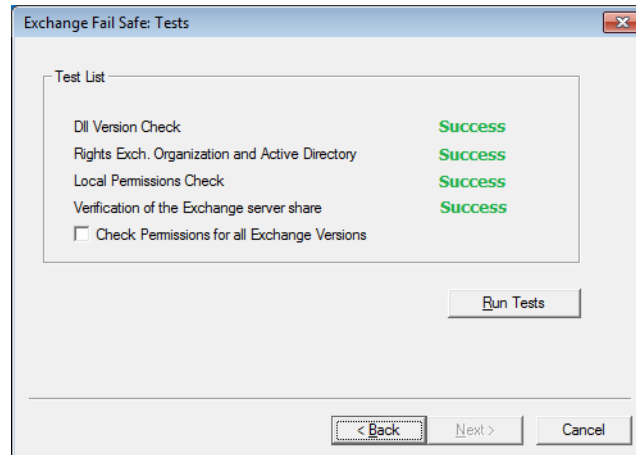


NOTE: If you select the **Check Permissions for all Exchange Versions** option, the privileges for all Exchange server versions are checked. If an error occurs during this check, it is displayed in the error list in combination with the relevant Exchange version.

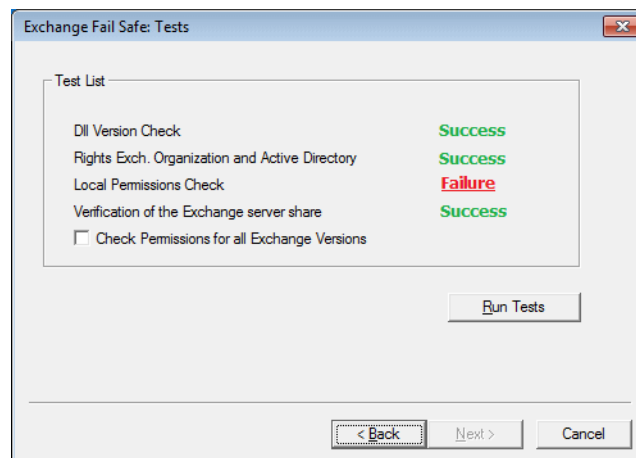
In [Section 3.2, “Interpreting the Test Results”](#), on page 47 you find information about interpreting the test results.

3.2 Interpreting the Test Results

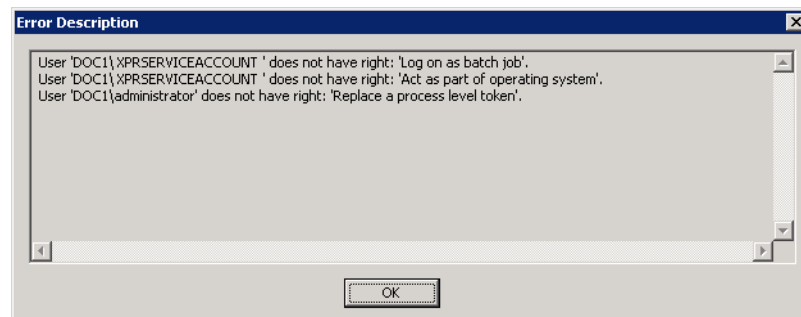
When all test items are indicated as **Successful**, the requirements for a successful Exchange connector installation are complied with.



If one or several test items appear as **Failure**, you need to fix the corresponding error(s) before the Exchange connector installation.



Click the **Failure** link for a detailed error analysis. An information dialog opens in which you find an error description on the detected problems.



The Exchange Fail-Safe Wizard

Interpreting the Test Results

Fix the displayed error and restart checking via **Run Tests** until no errors are detected anymore.

NOTE: You need not restart the *Exchange Fail-Safe Wizard* each time and re-enter the service account parameters and the connection to the Exchange server. In case of an error keep the auxiliary program running and correct the error. Then, click on the **Run Tests** button again. Repeat the error analysis until all errors have been removed.

4 XPR and Microsoft Exchange Server 2007

4.1 General Considerations

4.1.1 Changes introduced with Exchange Server 2007

With *Exchange Server 2007*, Microsoft has introduced some essential modifications and further developments compared to the previous version *Exchange Server 2003*. The most important differences are:

- Upgrade of a 32-bit system to a 64-bit system. In other words, Microsoft allows live operation of *Exchange Server 2007* only as 64-bit system on a *Windows Server 2003* (64-bit).
- The combination of Exchange features to modules, the so-called Roles, which enables a distributed setup of the *Exchange Server 2007* on different servers. This results in an improved scalability of the Exchange components. The individual roles are called: Mailbox Server Role, Hub Transport Server Role, UM Server Role, Client Access Server Role and Edge Transport Server Role.
- Replacement of the SDK-connector concept with the foreign-connector concept. This required an XPR connector redevelopment.

4.1.1.1 Administration Modifications

- **Exchange management console**

Exchange Server 2007 provides the new *Exchange management console* for administering the *Exchange Server 2007*. Different from the *Exchange system manager*, the sites and administrative groups known so far and also the routing groups inclusive the routing group connectors have ceased to exist in the *Exchange management console*, for example. The information for that is in case of *Exchange Server 2007* administered via the Active Directory (sites and services).

- **Exchange management shell**

The basic connector configurations are on the Exchange side performed via the *Exchange management shell*.

4.1.1.2 Exchange Server 2007 Cluster

As of version XPR 5.0 R4 FixRelease 6, the **ExchApl** and **ExUMApl** can be installed in a clustered Exchange environment.

The following solutions are implemented:

- Elimination of problems that occur with the installation of the ExchApl on clustered Exchange servers 2007.
- Configuration of several Exchange 2007 Hub Transport servers.

4.1.2 The XPR Connector for Exchange 2007

The XPR connector is a so-called *Exchange 2007 Foreign Connector*. Its executable file is the `E2k7Apl.exe`. You find this file in the `\bin` directory of the XPR server. The name of the connector in the XPR monitor still reads **ExchApl**.

The Foreign Connector is required for “store-and-forward” operation. It delivers the messages received via the XPR server to the Exchange users and transmits the Exchange server messages to be sent via the XPR server.

To this, a logical connection is established between the XPR server and the Exchange modules “Mailbox Server Role” and “Hub Transport Server Role” via the Foreign Connector.

The connection to the Exchange Mailbox Server Role is required for opening a MAPI connection to resolve addresses. The connection to the Exchange Hub Transport Server Role serves for transporting messages from/to the XPR server.

NOTE: In case of a monolithic *Exchange Server 2007* environment structure no differentiation needs to be made between Mailbox Server Role and Hub Transport Server Role. In this case the Foreign Connector is connected to the computer that hosts the Exchange server 2007.

Message transport

Messages to be sent by Exchange users via the XPR server are stored in the **Drop Directory**.

The messages to be sent from the XPR server to users on the Exchange server are stored in the **<Replay Directory>**.

In both cases such messages are SMTP messages with the file extension `.eml`, and they are buffered in the above directories until their final delivery.

The transport directories are created on the server that has the Hub Transport Server role.

NOTE: In case of an *Exchange Server 2007* with a role distribution among several servers, the Replay Directory must be reachable via a UNC path in the network. Only then this directory can be accessed from all Hub Transport servers.

You find a detailed description of the transport directory configuration in [Section 4.2.6.1, “Creating the Transport Directories”, on page 80](#).

4.1.3 The XPR True Unified Messaging Connector

Messages are exclusively retrieved via direct access to the Exchange mailboxes by means of the **ExUMApi**. Mailbox replication is not supported. **Integrated Messaging (IM)** as XPR server operation mode is thus not possible anymore.

NOTE: Exchange users hidden from global and other Exchange address books via the **Hide from Exchange address lists** cannot access their mailboxes via the ExUMAPL because of the then incomplete user information. The ExUMAPL indicates this via an error message.

The XPR True Unified Messaging Connector must establish a connection from the XPR server to the Client Access Server Role or Client Access RoleArray Server Role.

NOTE: In case of a monolithic *Exchange Server 2010* environment structure no differentiation needs to be made between Mailbox Server Role and Hub Transport Server Role. In this case the XPR True Unified Messaging Connector is connected to the computer that hosts the *Exchange server 2010*.

4.1.4 *Exchange Servers 2007* Administration Novelties

Owing to the changed *Exchange Server 2007* administration, the administrative access options differ from those you know from *Exchange Server 2003*.

- The XPR Foreign Connector is now exclusively configured via the **ExchApi** settings dialog in the XPR monitor.
- Users are still administered via the MMC Snap-in extension for Active Directory Users and Computers, which was already used for *Exchange Server 2003*. The Snap-in is installed on the system from which users are configured. How to proceed is described in [Section 4.2.5.6, "Installation of the MMC Snap-in", on page 77](#).

4.1.5 XPR Features Modifications

In the Exchange connection context, the following XPR server features are modified as a result from the new XPR Foreign Connector:

- Integrated Messaging (mailbox replication) is not supported anymore.
- The connector is exclusively configured via the **ExchApl** settings dialog in the XPR monitor.

4.2 Installation

4.2.1 General Considerations

NOTE: You cannot install two XPR Foreign Connectors, e.g. from two different XPR servers, for one Exchange organization.

The XPR Foreign Connector is installed basically in the same way as the SDK Connector for *Exchange Server 2003*.

During the XPR Foreign Connector installation all required properties are set and the APL service is configured. In addition, the `Proxy.dll` is installed, the MRS address type defined and various address templates for fax, voicemail etc. are provided for selection during the setup process.

4.2.2 Preparations

The following preparatory steps must be executed to set up the XPR Foreign Connector:

- **For migration scenarios only**
Users who deployed Integrated Messaging (mailbox replication) so far must be switched to True Unified Messaging beforehand. The users with Integrated Messaging will otherwise only be able to work as voice-only users, since they can only deploy the mailbox on the XPR server.
- **MAPI and CDO**
Because the *Exchange System Manager* cannot be used in *Exchange Server 2007* any more, the *Microsoft Collaboration Data Object* (CDO) must be installed on the XPR server manually.

Installing the **ExchApl** and **ExUMapl** requires the `ExchangeMapiCdo.EXE` file.

This file complies with all requirements as regards MAPI and CDO for the **ExchApl** and **ExUMapl**.

You find information about the installation and the setup file `ExchangeMapiCdo.EXE` provided by Microsoft for this purpose on the following web page:

<http://www.microsoft.com/downloads/details.aspx?FamilyID=e17e7f31-079a-43a9-bff2-0a110307611e&DisplayLang=en>

- **Configuring a service account**
Configure a user account (service account) in the context of which the connectors are to operate. Under this service account the **ExchApl** and

ExUM APL service operates on the kernel computer. The privileges assigned to this account enable the operation of the Exchange connector in the system. Using the service account you can easily administer the privileges for operating the connectors.

- **Assigning privileges**

Assigning the privileges for the installation and operation of the connectors has slightly changed with the XPR Foreign Connector. Which privileges are required and how to set them is described further down the text under **"Requirements and privileges for installing the connectors"**.

- **Transport directories**

Message transport between the two systems requires two transport directories (`\<drop directory>` and `\<playback directory>`) on the *Exchange server 2007*. The drop directory serves for transporting messages from Exchange to the XPR server; the playback directory is in charge of transporting in the reverse direction. You find information about the configuration and activation of these transport directories in [Section 4.2.6.1, "Creating the Transport Directories"](#), on page 80.

- **Requirements and privileges for installing the connectors**

Installation Requirements	
☐	The server components Mailbox Server Role and Hub Transport Server Role are installed and active.
☐	The network function as well as the name resolution in the network work correctly. You can use DCDiag and NetDiag (Windows support tools) to check this.
☐	You are logged in at the domain as installing user with domain admin privileges and Exchange admin privileges. This gives you unrestricted access to the service database. This is important with respect to installing and configuring the service.

Table 2

Check List: Installation Requirements for the Exchange 2007 Connectors

Installation Requirements	
☐	A service account for operating the Exch and ExUM Apl has been created. The Exch and ExUM APL service runs under this user account on the kernel computer. The privileges assigned to this account enable the operation of the Exchange connector in the system. This also enables the simple administration of the privileges for this service account. Operating the gateway via a service account always requires the following privileges: • Exchange View-Only Administrator Role. This privilege is required for starting and stopping the services. This privilege is required on the Mailbox Server Role as well as on the Hub Transport Server Role. The privilege is assigned via the <i>Exchange management console</i> as follows: – Start the <i>Exchange management console</i>. – Open the “Organization Configuration” context menu. – Invoke here the Add Exchange Administrator feature. The Add Exchange Administrator dialog opens. – Select here the XPR service account. – Set in the same dialog the Exchange View-Only Administrator role option. – Click Add. – Click Finish. • Local administrator on the Mailbox Server Role as well as on the Hub Transport Server Role. You find details about the setup and operating privileges in Section 4.8, “Security Settings for Installation and Live Operation of the E2k7 APL and ExUM APL”, on page 142. The service account requires locally the following privileges on the XPR system: Notes: • Privilege assignment occurs via the Security Policies. You reach the corresponding setting dialog via Start > Administrative Tools > Local Security Policy under Local Policies > User Rights Assignment. Under the local security policies you find the locally set and “effective” policies. • Separate policies can be entered for domains and domain controllers. These policies overwrite, as the case may be, the locally defaulted ones. After a policy modification on domain level, a restart of the corresponding computers (domain controllers and Exch APL computers) may be required. • If you plan a system allowing more than 5000 MAPI accesses, use the Multiline Configuration feature. See Section , “Multiline Configuration”, on page 423. ☒ Log on as service – is set upon the connector installation. (Log on as service) ☒ Act as part of the operating system – is set upon the connector installation. (Act as part of the operating system) ☒ Back up files and directories – is set upon the connector installation. (Back up files and directories)

Table 2

Check List: Installation Requirements for the Exchange 2007 Connectors

Installation Requirements	
☒	Restore files and directories – is set upon the connector installation. (Restore files and directories)
☒	Log on as batch job – is set upon the connector installation. (Log on as batch job)
☒	Adjust memory quotas for a process – is set upon the connector installation. (Adjust memory quotas for a process)
On the organization level of the Exchange server (Active Directory level), the following privileges are required for the service account:	
☐	The installing user must be Exchange Organization Administrator in the Exchange 2007 organization. This provides full access to the Exchange-specific part of the Active Directory for installing and uninstalling various objects (for example: connector, address type, templates, etc.).
☐	User “service account” must belong to the group of “domain administrators”
☐	User “service account” must belong to the group of “domain users”

Table 2

Check List: Installation Requirements for the Exchange 2007 Connectors

Table 2 *Check List: Installation Requirements for the Exchange 2007 Connectors*

Installation Requirements

Note: As of Exchange Server 2007 SP1 you can perform this privilege assignment via the *Exchange management console* also. Proceed as follows:

- Start the *Exchange management console*.
- In the console structure expand the recipient configuration.
- Select the **Mailbox** branch.
- In the middle section of the window invoke the context menu for the mailbox that you want to grant the “Full Access” privilege.
- Select here the **Manage "Full Access" Permissions** feature. The wizard for managing the "Full Access" privilege opens.
- In the **Manage "Full Access" Permissions** dialog click on the **Add** button.
- Select in User or Group the user whom you want to grant the “Full Access” privilege and click on OK.
- Click on **OK**. You return to the **Manage "Full Access" Permissions** dialog.
- Enable here the **Manage** button. The **Completion** dialog opens. In the **Completion** dialog you can see a summary that indicates the successful accomplishment of the “Full Access” privilege assignment.
- Complete the process with a click on the **Finish** button.

Table 2

Check List: Installation Requirements for the Exchange 2007 Connectors

To conclude the privilege assignment, restart the **Microsoft Exchange Information Store** service for the new privileges to take effect.

4.2.3 Installation Process Overview

Installation process on the XPR server

After the component selection the following components are installed on the XPR server in succession:

- The LDAP APL
It makes sure that address data relevant to XPR and centrally maintained via the Active Directory can be replicated in both directions.
- The Exchange True Unified Messaging Connector (ExUM Apl)
The Exchange mailbox store can be immediately accessed via the ExUM APL. In this way Exchange messages can be directly forwarded to a telephone interface via XPR. This connector is also required for the notification function.
- The Exchange connector (Exch APL)
It forms the *store & forward* connection between the XPR server and *Exchange Server 2007*. Messages received or to be sent via the XPR server are transmitted via this connector. With the **ExchAPL** installation a new Foreign Connector is created. This connector establishes a connection to the Exchange Mailbox Server Role and to the Exchange Hub Transport Server Role on the Exchange Hub Transport server.
- The MMC Snap-in (if selected for installation on the XPR server).
The MMC Snap-in displays the XPR-specific administration dialog **MRS Settings** for the XPR users (under Active Directory Users and Computers).

NOTE: Managing users with help of the Active Directory Users and Computers program is normally not performed via the XPR server. Therefore, the MMC Snap-in must be manually installed on the server from which the user administration occurs.

During the component installation, all parameters required for successfully connecting the XPR server to the previously installed *Exchange Server 2007* are queried, and the necessary program files copied.

Working on the Exchange server

After the installation of the XPR components the transport directories need to be created on the Exchange server that has the Hub Transport Server Role. See [Section 4.2.6.1, “Creating the Transport Directories”, on page 80](#).

Configuring the Exchange Foreign Connector

After you have completed the setup, you can perform further configurations via the settings dialogs in the XPR monitor. The Foreign Connector configuration is described in [Section 4.3, “Configuration”, on page 87](#).

Connection to an Exchange Server 2007 cluster

If you want to realize a connection to a clustered Exchange 2007 server via the ExUMApi you need to consider the following factors:

- The ExUMApi must be installed for the server that has the Mailbox Server Role. Also in case of a clustered mailbox server the ExUMApi must be connected to the server that has the Mailbox Server Role.
- This server must be visible in the network and accessible by DNS.
- The name of the server that has the Mailbox Server Role must be specified in the ExUMApi setup dialog for this purpose. The ExUMApi then connects to the right server. In this process it does not matter which cluster node is currently active.
- If the name of the clustered mailbox server deviates from the name of the Windows cluster, the name of the computer via which the cluster can be reached in the network must be specified. The ExUMApi always checks whether the server is available in the network. This is done by checking the domain and executing some AD queries. In addition, you should verify that an Exchange server 2007 is actually addressed.

Installation to a clustered Exchange Server 2007 environment is supported as of version XPR 5.0 R4 FixRelease 6.

4.2.4 Installation of the XPR Components for the Connection to Exchange Server 2007

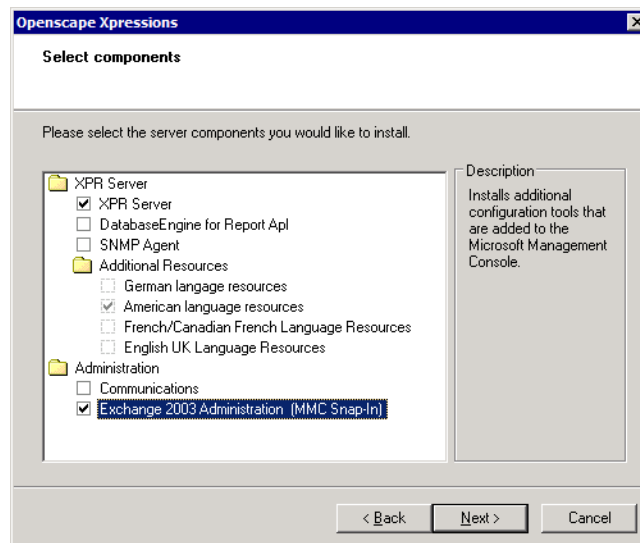
4.2.4.1 Selecting the Components

In the XPR server setup, after the license service installation, the language selection as well as reading the release notes you reach the setup dialogs for the Exchange connection.

After you have confirmed to have taken notice of the release notes you perform a first selection of components for the XPR server in the following dialog. Here you can select the MMC Snap-in for installation on the XPR server. This, however, is only required if the XPR user administration is to occur from the XPR server.

NOTE: Managing users with help of the service program Active Directory Users and Computers is normally not performed via the XPR server. Therefore, the MMC Snap-in must be manually installed on the server from which the user administration occurs. You find the setup file on the product data carrier in the directory `<X>:\...\AddOn\Client\Exchange\MMCSnapIns`. X corresponds to the current letter of the device that holds your product data carrier.

If you want to install the Snap-in on the XPR server, select the **Exchange 2003 Administration (MMC Snap-In)** option. The installation is then automatically started at the end of the server installation.



NOTE: If you do not see the MMC Snap-in component in this dialog, a license is likely to be missing. In this case please check the licenses and restart the setup program.

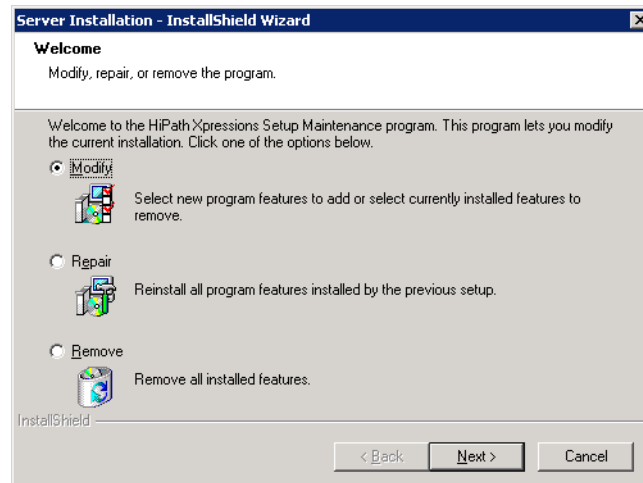
Exchange 2003 administration (MMC Snap-in extension)

XPR users are still administered via the MMC Snap-in extension for *Active Directory Users and Computers*.

The MMC Snap-in displays the XPR-specific administration dialog **MRS Settings** for the XPR users (see [Section 4.3.4, “User Administration”, on page 114](#)).

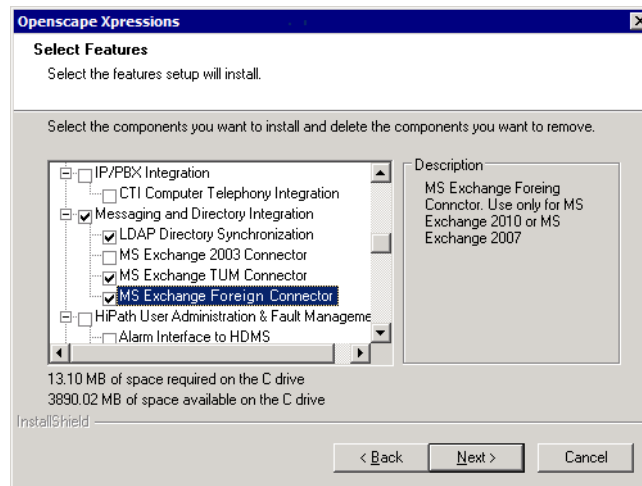
NOTE: A 64-bit operating system supports the available 32-bit XPR MMC Snap-in without restriction. This requires starting the XPR MMC Snap-in in 32-bit mode (`mmc /32`).

After the setup dialogs for the client components, external software, documentation and ASR components, you reach the selection of the desired installation scenario. Select **Modify** to install the Exchange components of the XPR server.



In the next dialog, select the following additional components from the **Messaging and Directory Integration** branch:

- LDAP Directory Synchronization
- MS Exchange TUM Connector
- MS Exchange Foreign Connector



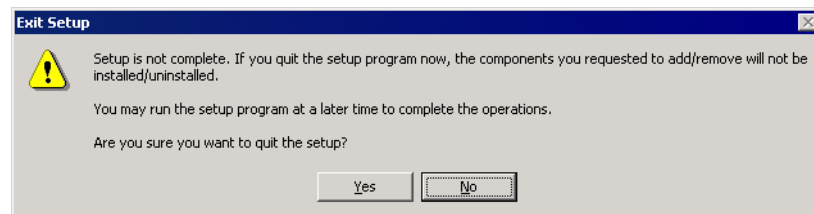
4.2.5 Components Installation Procedure

4.2.5.1 Starting the Installation

Installing the Exchange components in the running XPR setup starts with dialogs invoked for the preparative LDAP APL configuration. The steps lying between the setup start and this stage serve to install other XPR server components. The respective settings are comprehensively described in the *Server Installation* manual.

4.2.5.2 General Considerations

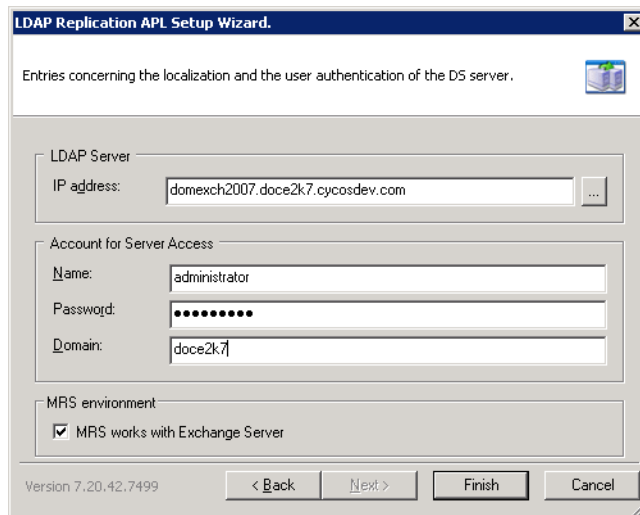
Pushing the **Cancel** button in the installation dialogs delivers the information that Setup has not been duly accomplished yet. If you select **Yes** here, only the installation of the current component is terminated – the XPR setup will then be continued with the next component. With **No** you return to the currently running setup.



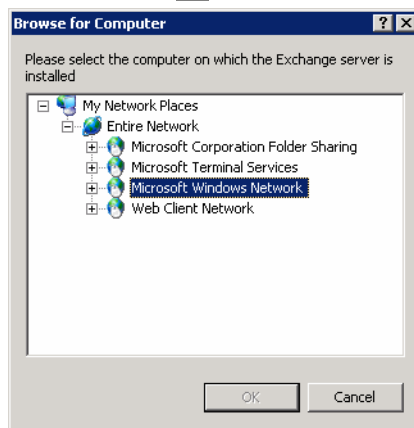
4.2.5.3 Installing the LDAP APL

At the stage where in the XPR server setup the installation of the LDAP directory synchronization (LDAP APL) starts, the LDAP setup wizard first appears in its welcome window.

With a click on Next the dialog opens in which you find the **IP Address** entry field (**LDAP Server** section) to specify the name of the computer that the LDAP APL is to access for data replication. This is in most cases the Primary Domain Controller computer (PDC), which contains the Global Catalog of the Active Directory.



This can either be done by directly entering the server name in this entry line or via the **Browse for Computer** dialog. This dialog opens when you enable the selection icon (...) next to the entry line.



Now create the **Account for Server Access**. In doing so, select a user account that has read as well as write privileges for the Active Directory. This is usually the domain administrator. You can also use the service account if it has the corresponding privileges.

In the **MRS environment** section, via the **MRS works with Exchange Server** checkbox, you integrate the configuration file required for *Exchange Server 2007*. This configuration file is identical with the one used for connecting *Exchange Server 2003*. It is called `ExRepl.lcf`. To access other directory services via LDAP, leave the checkbox inactive. The `AdRepl.lcf` configuration file is then selected by default. It enables LDAP access to the Active Directory if no *Exchange server* has been installed.

Finish completes the entries and the LDAP setup.

Via **Back** you return to the LDAP APL setup welcome window again.

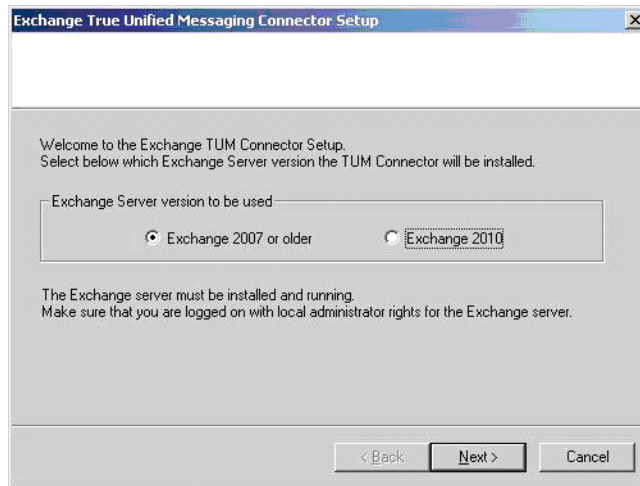
Cancel terminates the LDAP APL setup and initiates the installation of the next XPR server component.

How to configure the LDAP APL is described in [Section 4.3.1, "Configuring the LDAP Apl", on page 87](#).

4.2.5.4 Installing the True Unified Messaging Connector

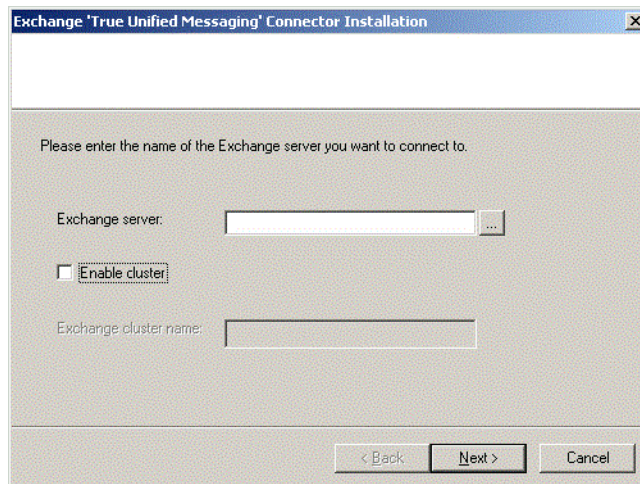
After completion of the LDAP APL installation, the ExUM APL for True Unified Messaging Setup follows automatically, provided this connector has been previously selected as component.

In the first setup step you select the version of the Exchange server to which the TUM connection is to be established. Select here *Exchange Server 2007*.



Click on **Next**.

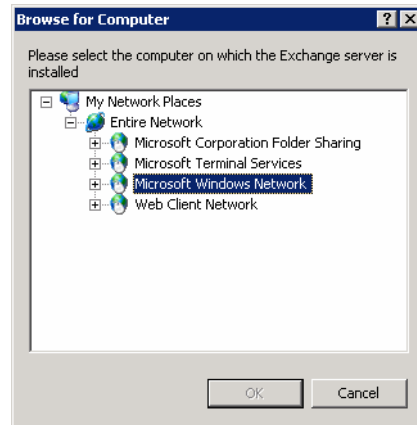
Connection to an Exchange server



In the first dialog define the Exchange server the ExUM APL is to establish a connection to. In a modular *Exchange Server 2007* environment structure this is the Mailbox Server Role.

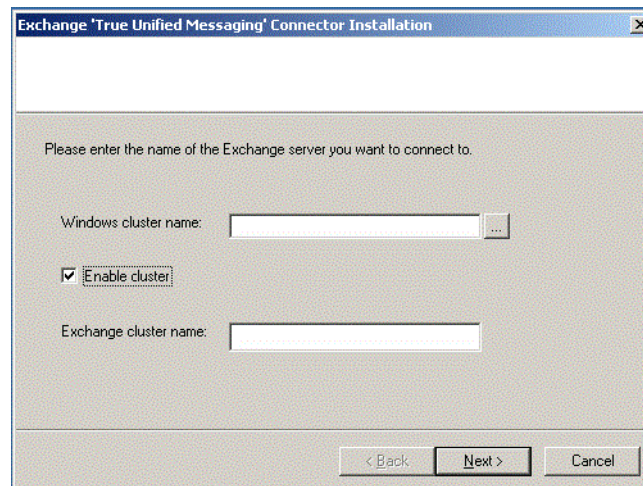
NOTE: In case of an *Exchange server 2007* with monolithic structure the connection is set up to the server on which the *Exchange server 2007* is installed.

You can do this by directly entering the server name. You can also use the  button to look for the corresponding server in the network. In the latter case a window opens for selecting the Exchange server.



Connection to a clustered Exchange server

Select the **Enable cluster** option. The **Exchange cluster name** input line is released. In addition, the feature in the **Exchange server** input line changes to **Windows cluster name**.

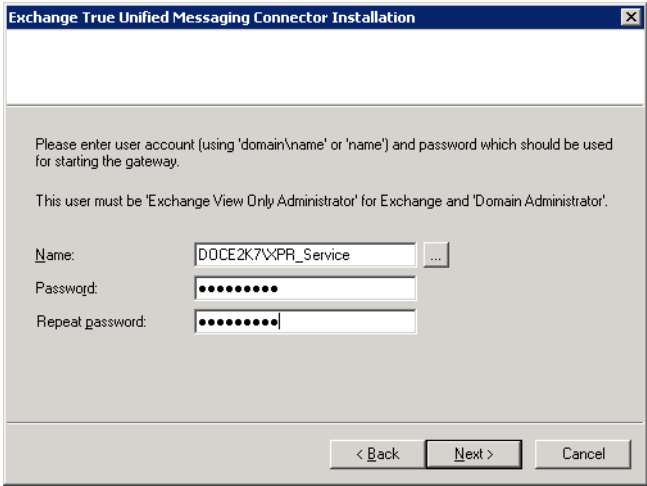


- **Windows cluster name**
Specify here the name of the Windows cluster in the clustered Exchange environment.
- **Exchange cluster name**
Specify here the name of the Exchange cluster in the clustered Exchange environment.

NOTE: Using the *Windows Cluster Administrator* you can verify the *Windows* and *Exchange cluster name*.

After you have completed this process, click on Next to reach the dialog for specifying the user account under which the ExUM APL is to run.

When this process is complete, you can click on **Next** to reach the selection of the user account under which the ExUM APL is to operate.



Exchange True Unified Messaging Connector Installation

Please enter user account (using 'domain\name' or 'name') and password which should be used for starting the gateway.

This user must be 'Exchange View Only Administrator' for Exchange and 'Domain Administrator'.

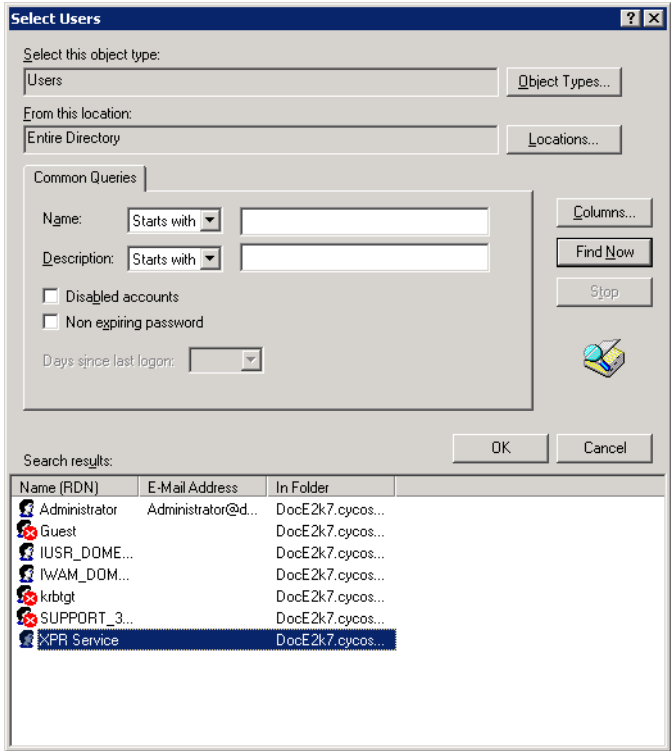
Name: DOCE2K7\XPR_Service

Password: [masked]

Repeat password: [masked]

< Back Next > Cancel

Here you can directly enter the name of the service account in the format <domain\name>. You can also use the ... button to select the service account.



Select Users

Select this object type: Users

From this location: Entire Directory

Common Queries

Name: Starts with

Description: Starts with

☐ Disabled accounts

☐ Non expiring password

Days since last login:

Search results:

Name (RDN)	E-Mail Address	In Folder
Administrator	Administrator@d...	DocE2k7.cycos...
Guest		DocE2k7.cycos...
IUSR_DOME...		DocE2k7.cycos...
IWAM_DOM...		DocE2k7.cycos...
krbtgt		DocE2k7.cycos...
SUPPORT_3...		DocE2k7.cycos...
XPR Service		DocE2k7.cycos...

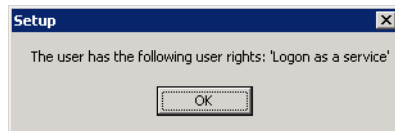
OK Cancel

You can proceed as follows to transmit the service account to the ExUM APL configuration page via the user selection dialog:

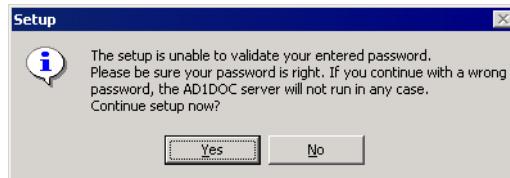
- By means of a double-click on the selected user name.

- Via direct entry of the name in the lower portion of the dialog. Then verify the name by pressing the **Check Names** button.
- Through selection of the name in the list. Then click the **Add** button.

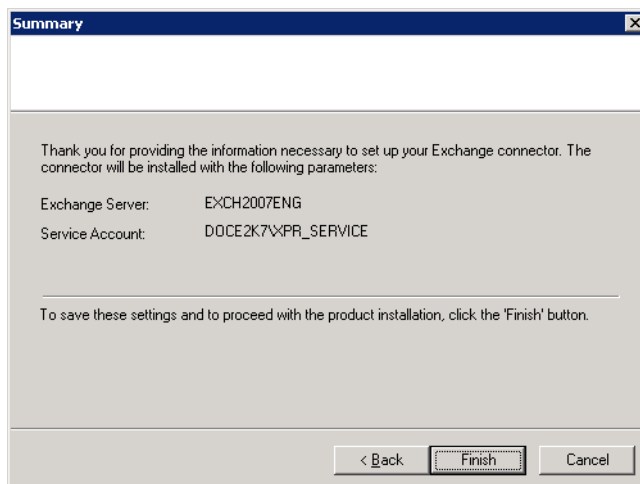
Click **OK** to complete this process. Then enter the password to legitimate this service account. If the specified service account is valid, the user privileges assigned by Setup are displayed in a message.



Confirm this message with **OK**. You are then informed that the entered password cannot be checked for validity. If you are not sure at this point, enable **No** to return to the password entry for making an alteration if necessary.



When you continue the ExUM APL setup with **Yes**, the **Summary** window displays the entered parameters once again.



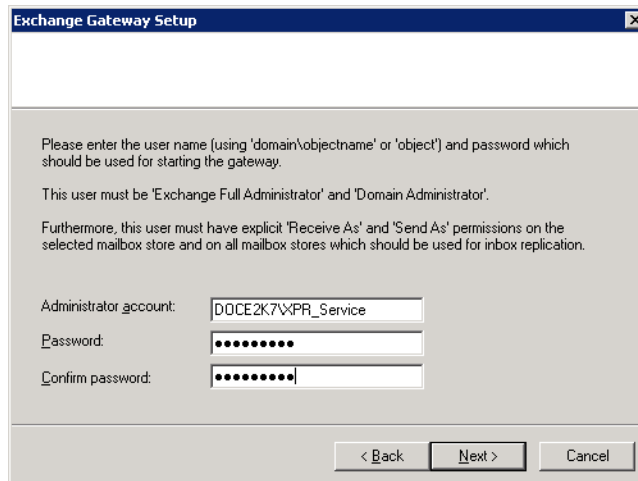
Click **Finish** to save your entries. The ExUM APL installation is thus accomplished.

4.2.5.5 XPR Foreign Connector Installation

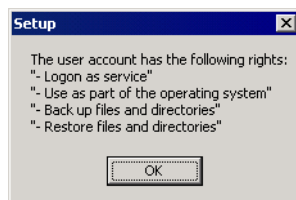
The ExUM APL installation is automatically followed by the XPR foreign connector setup if this component was previously selected.

The welcome dialog of the Exch APL installation once again points to the requirements that must be met for a successful installation.

After you have clicked on **Next** in the welcome dialog, you reach the dialog in which you enter the service account under which the Exch APL is to operate. You specify the service account under Name in the format `<domain\name>`. Then enter the service account password twice.

The image shows a Windows-style dialog box titled "Exchange Gateway Setup". It contains instructional text: "Please enter the user name (using 'domain\objectname' or 'object') and password which should be used for starting the gateway. This user must be 'Exchange Full Administrator' and 'Domain Administrator'. Furthermore, this user must have explicit 'Receive As' and 'Send As' permissions on the selected mailbox store and on all mailbox stores which should be used for inbox replication." Below the text are three input fields: "Administrator account:" with the text "DOCE2K7\XPR_Service", "Password:" with masked characters, and "Confirm password:" with masked characters. At the bottom are three buttons: "< Back", "Next >", and "Cancel".

Since the Exchange gateway cannot link up with *Exchange Server 2007* when a wrong password has been specified, the entry must occur twice to rule out typing errors as source of error. A correct entry and a click on **Next** opens an information dialog that displays a list of the user privileges assigned to the user account by Setup.

The image shows a small Windows-style dialog box titled "Setup". It contains a list of rights: "The user account has the following rights: '- Logon as service', '- Use as part of the operating system', '- Back up files and directories', '- Restore files and directories'. There is an "OK" button at the bottom.

Confirm the user privilege information display with **OK**.

Setup is then continued with entering the computer name for the connection to *Exchange Server 2007*.

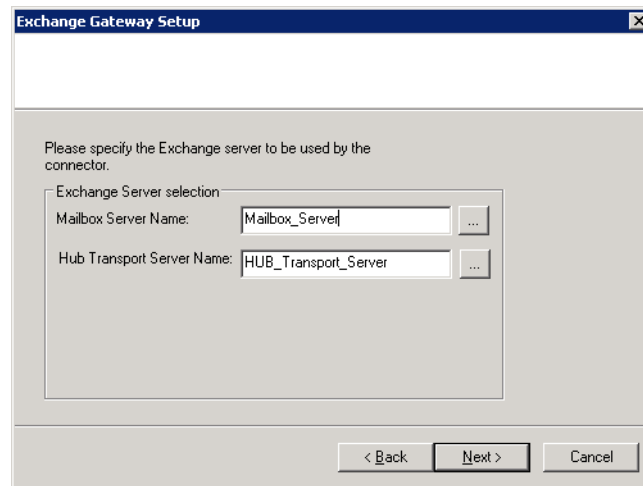
In case of a modular *Exchange Server 2007* environment structure the XPR Foreign Connector must establish a connection from the XPR server to the Mailbox Server Role **and** to the Hub Transport Server Role.

The connection to the Exchange Mailbox Server Role is required for opening a

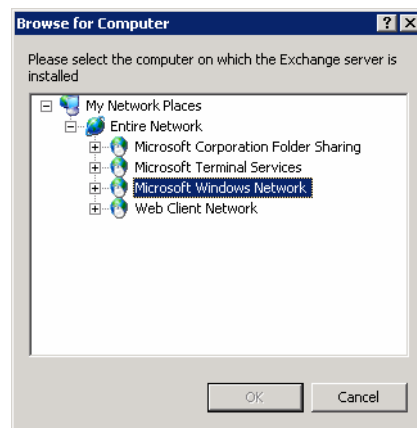
MAPI connection to resolve addresses.

The connection to the Exchange Hub Transport Server Role serves for transporting messages from/to the XPR server.

NOTE: If the *Exchange server 2007* has a monolithic structure, specify the name of the *Exchange server 2007* in both entry lines.

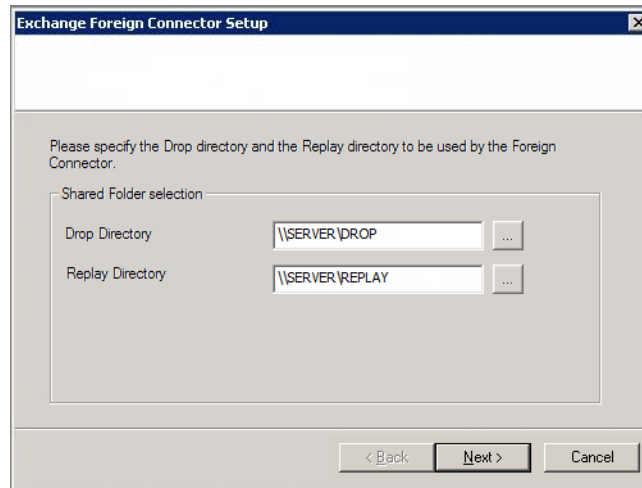


Here you can either directly enter the server name or use the ... button to look for the relevant servers in the network.



Click on the **Next** button after you have selected the corresponding server roles of the *Exchange server 2007* in the network.

You reach the dialog in which you have selected the transport directories.



In the **Drop directory** and **Replay directory** specify the path to the shared transport directories according to the following pattern:

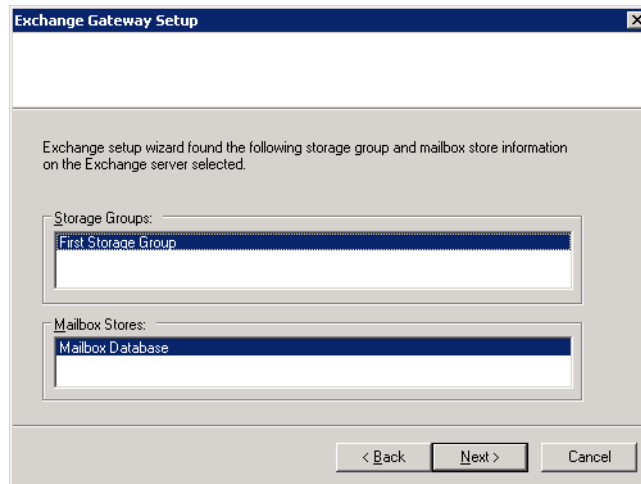
- For the **Drop directory**
`\\<Ip address or name of the Exchange server on which the Hub Transport Server operates>\<XPR server name>-<name of the Exchange Server 2007 Mailbox Server Role>`
- For the **Replay directory**
`\\<Ip address or name of the Exchange server on which the Hub Transport Server operates>\Replay`

You can also use the browse button  to look for the corresponding shares in the network. In the latter case a window opens for selecting the corresponding shares.

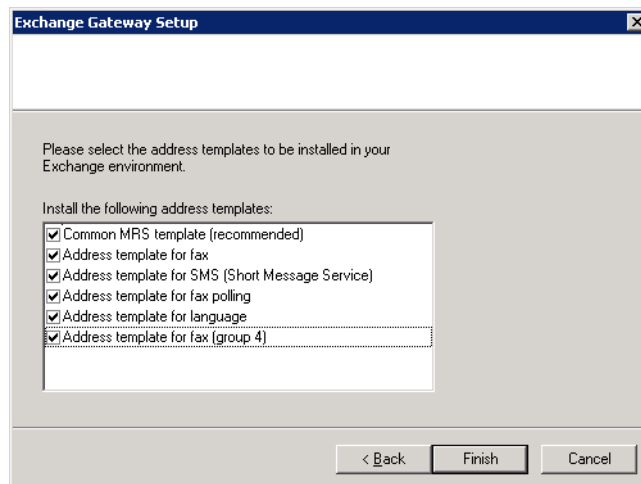
NOTE: The settings performed here during the installation for the paths of the transport directories can later be changed via the **ExchApl** configuration dialogs in the XPR monitor (**Exchange Foreign Connector** tab).

After you have selected the drop directory and the playback directory, click on **Next**.

The next dialog confirms the successful localization of the two specified servers by displaying the **Storage Groups** and the **Mailbox Stores**.



Click on **Next**. The installation continues with the **address template** configuration.



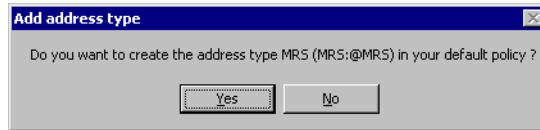
Here you can have **address templates** installed in your Exchange environment for various services offered by the XPR server.

In this way you can later generate e.g. a new address for the address book in the client, so that you only need to enter the corresponding number and select the desired service in there instead of working with the somewhat cryptic default Exchange addressing.

After you have clicked on **Finish**, the dialog for creating the MRS address type (MRS:@MRS) opens. This address type is globally created in the Default Policy.

NOTE: As of Exchange Server 2007 the distribution groups support the **sAMAaccountName**. As a result, all Exchange users with this attribute are replicated as full XPR users to the XPR server. This causes problems when assigning

the MRS address type and the number of replicated users exceeds the number of available user licenses. Therefore, the number of user groups to be replicated may have to be restricted beforehand via the LDAP configuration.



Yes starts the address assignment and immediately defines an MRS address for each Exchange user.

NOTE: In large system environments, address assignment may take a while.

If not all Exchange users are to be assigned the MRS address, click the **No** button in this dialog.

This will directly resume the setup process with the installation of the next XPR component. The MRS address type will not be specified then and there is no assignment of the MRS address to the Exchange users either. The MRS address type must then be manually defined afterwards. See [Section 4.7, “Adding and assigning the MRS E-Mail Address Type retrospectively”](#), on page 140.

A subsequent manual definition of the MRS address type is useful if only specific users are to use this address type. After that, the MRS address can be assigned to users via the definition of filter rules in the Default Policy (or in a newly created policy).

The installation of the XPR components for connecting Exchange Server 2007 is now complete.

NOTE: If the ExchAPL does not start when the XPR server is booted, a privilege problem is in most cases responsible for this. You may then see an error message on the XPR monitor like:

Exchange Server seems not to be running <0x80004005>

In this case check whether the service account was assigned the required privileges or whether the service account was added on all system components to the local administrators.

4.2.5.6 Installation of the MMC Snap-in

Administering the XPR user data requires the MMC Snap-in. It displays the **MRS Settings** tab in the properties dialog for the AD users. To this the MMC Snap-in that was already deployed with *Exchange Server 2003* is used.

NOTE: The MMC Snap-in can be installed on a 32-bit as well as on a 64-bit system. When using a 64-bit system, start this application in 32-bit mode (execution command in the command line: `mmc /32`).

You find further information in the Microsoft KB article

[http://msdn.microsoft.com/en-us/library/ms692753\(VS.85\).aspx](http://msdn.microsoft.com/en-us/library/ms692753(VS.85).aspx)

The MMC Snap-in can be integrated in a new installation of the XPR server if the XPR users are to be administered from the XPR server. In the first installation dialog, after invoking the server setup, select the component **Exchange 2003 Administration (MMC SnapIn)**. See also [Section 4.2.4.1, "Selecting the Components"](#), on page 62.

If the MMC Snap-in is required on another system, the installation must occur manually and belatedly from the XPR product data carrier. You find the setup file on this carrier in the directory: `X:\AddOn\Client\Exchange\MMCSnapIns` (X corresponds to the current letter of the device that holds your product data carrier).

How to manually install the MMC Snap-in:

1. Start the setup by executing the `setup.exe` from the above directory.
A welcome dialog opens. It points out that all running applications should be terminated before Setup is started. So, if any applications are still open, close them after selecting **Cancel**. Setup is left then and active programs can be shut down. Subsequently, it must be started again.
2. Click the **Next** button in the welcome dialog.
The dialog for defining the target directory opens.

During the installation, the following files are created in the `%ProgramFiles%\MMC Exchange SnapIns` directory by default:

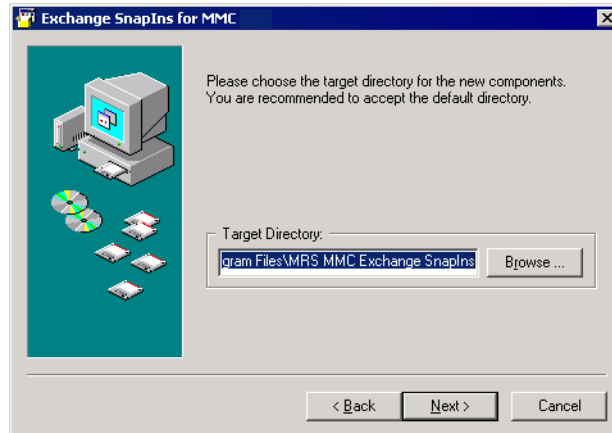
`ExtInst.MMCExchSnapIns.ini`

`setup.MMCExchSnapIns.ini`

`Uninstall.MMCExchSnapins.exe`

`Uninstall.MMCExchSnapins.exe`

In addition, the `ExtInst.log` log file that logs the setup process is created in the `X:\Documents and Settings\<installing user>\Local Settings\Temp` directory.

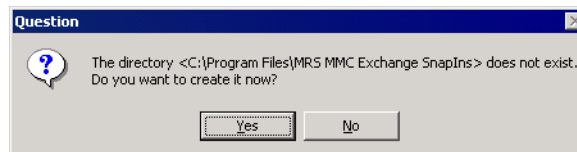


You can also push **Browse...** to specify or newly define a directory to which the program files are then copied. A file selection dialog opens after you have pushed this button. However, we recommend to copy the preset directory since the program components are then easier to find when the necessity arises.

NOTE: The **Back** button takes you back to the welcome dialog and via **Cancel** you can terminate the setup after a security prompt.

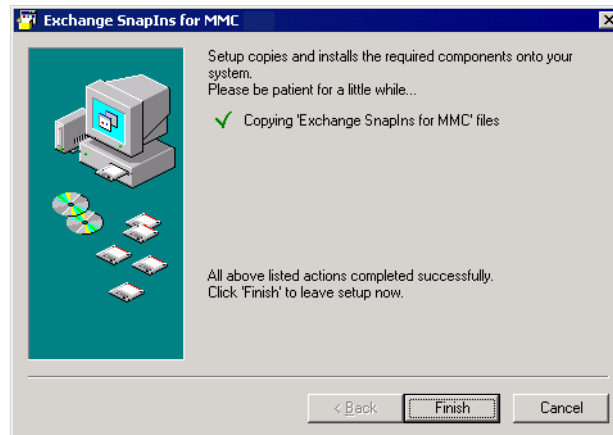
3. Click on the **Next** button after you have made your selection for the target directory.

If this directory does not exist yet, you are asked as to whether or not you want to have the directory defined. Confirm this query with **Yes** if you want to perform the installation.



The program files are being copied to the specified directory.

You can follow the progress of the copying and installation process in the next window by the icon next to **Copying 'Exchange SnapIns for MMC' files**. While the activities continue, a black cross precedes the “Copying 'Exchange SnapIns for MMC' files:” line. After completion of the data transmission, a green tick replaces the black cross.



4. Click **Finish** to complete the installation.

The MMC Snap-in installation is now complete.

4.2.6 Working on the Exchange Server

4.2.6.1 Creating the Transport Directories

The transport of messages from the XPR server to Exchange and vice versa requires two directories, the drop and replay directory. These two directories serve to buffer the messages in a waiting loop until they are processed, meaning, sent to the respective target server. Storing the messages in these directories depends on the transmission direction.

Both directories are created on the server on which the Hub Transport Server Role operates.

NOTE: If the Exchange environment has a monolithic structure, the directories are created on the server on which the *Exchange server 2007* is installed.

Activating the transport directories requires configurations on the server with the Hub Transport Server Role (in case of a monolithic structure on the *Exchange server 2007*) as well as for the settings of the **ExchApl** on the XPR server.

- The drop directory
This directory serves for delivering messages sent from the Exchange server to the XPR server. The messages are retrieved and further processed by the XPR server.
During the **ExchApl** installation this object is created as “DropDirectory” object. It contains by default the name:

<XPR server name>-<name of the Exchange Server 2007 Mailbox Server Role>

NOTE: Due to the system, the object name for the Foreign Connector is created using the Mailbox Server Name instead of the Hub Transport Server Name.

You can have the drop directory name put out by entering the following command in the *Exchange management shell*:

```
get-foreignconnector|fl
```

The listing entry you look for has the format:

```
DropDirectory      :  <XPR server name>-<name of the Exchange
                        Server 2007 Mailbox Server Role>
```

NOTE: In case of a modular Exchange Server 2007 installation distributed among several servers, the drop directory must be reachable via a UNC path in the network. Only then this directory can be accessed from the Hub Transport server (or from all further Hub Transport servers, if available). This is not required if the system has a monolithic structure.

- The replay directory
This directory buffers the messages sent by message servers different from Exchange to the Exchange organization. Exchange retrieves the messages from there and delivers them to the mailbox of the Exchange user.

NOTE: You can rename both directories and store them anywhere in the system. If this is desired, adjust the new directory names and the directory paths in the system upon the creation, activation or configuration.

How to create and activate these directories:

Creating and activating the drop directory

1. Using the Hub Transport Server Role create a directory with the following properties on the server:

Path:

`%ProgramFiles%\Microsoft\Exchange Server`

Directory name:

<XPR server name>-<name of the Exchange Server 2007 Mailbox Server Role>

The path is defaulted as the drop directory is expected at this point. If several servers with the Hub Transport Role are available, select the one for which the XPR Foreign Connector is installed.

Example:

`%ProgramFiles%\Microsoft\Exchange Server
\<XPR server name>-<name of the Exchange Server 2007
Mailbox Server Role>`

NOTE: In case of an *Exchange server 2007* with monolithic structure the **drop directory** is created in the following path of the server on which the Exchange server 2007 is installed:

%ProgramFiles%\Microsoft\Exchange Server

NOTE: Please note that the drop directory may only be configured on one Hub Transport server and that there is only one path to the drop directory.

2. Set the following access privileges:
 - Grant the XPR service account under which the Exchange APLs operate **Full Control** of this directory share. Proceed as follows:
 - Invoke the context menu for the drop directory.
 - Change to the **Sharing** tab in the configuration dialog.
 - Enable here the **Permissions** button.
 - Add the XPR service account as user via the **Add** button.
 - Assign the **Full Control** privilege to the XPR service account.
 - Grant the XPR service account **Full Control** of the drop directory for the NTFS authentication. Proceed as follows:
 - Invoke the context menu for the drop directory.
 - Change to the **Security** tab in the properties dialog.
 - Add the XPR service account as user via the **Add** button.
 - Assign the **Full Control** privilege to the XPR service account.
 - Grant the NETWORKSERVICE on the server with the Hub Transport Server Role **Full Control** of the drop directory. Proceed as follows:
 - Invoke the context menu for the drop directory.
 - Change to the **Security** tab in the properties dialog.
 - Add the NETWORKSERVICE as user via the **Add** button.
 - Assign the **Full Control** privilege to the NETWORKSERVICE.

- Grant the Hub Transport server **Full Control** of this directory share.

NOTE: If several Hub Transport servers have been installed, this must occur for every single Hub Transport server.

Proceed as follows:

- Invoke the context menu for the drop directory.
 - Change to the **Security** tab in the properties dialog.
 - Use the **Add** button to add the Hub Transport server(s) as computer.
 - Assign the **Full Control** privilege to the Hub Transport server(s).
3. In case of several Hub Transport servers set the UNC path to the drop directory.

Use the Exchange management shell command:

```
Set-ForeignConnector -Identity "MrsConnector (<XPR server
name>:<name of the Exchange Server 2007 Mailbox Server
Role>)" -DropDirectory "\\<Hub Transport server
name>\<XPR server name>-<name of the Exchange Server 2007
Mailbox Server Role>" for this purpose
```

The creation of the drop directory is now complete.

NOTE: If you do not use the default path for the drop directory you need to reconfigure your individual path in the system. When you configure the path the drop directory is simultaneously activated. To modify the directory path start the *Exchange management shell*.

Enter the following command in the *Exchange management shell*:

```
Set-TransportServer <hub transport server>
-RootDropDirectoryPath "<drive>:\<path>"
```

The first line of this command is separated from the second line by a blank (...port server> -RootDropDir...).

In the *Exchange management shell* you can check whether the activation has been successful with the following command:

```
Get-TransportServer <Hub Transport Server>|fl
```

In the subsequently displayed list the previously empty `RootDropDirectoryPath`: entry must now feature the entered path specification.

Creating or activating the replay directory

In the list put out by the

```
Get-TransportServer <your Hub Transport Server>|fl
```

command you find the defaulted path to the replay directory. It reads:

```
ReplayDirectoryPath    : %ProgramFiles%\Microsoft\  
                        Exchange Server\TransportRoles\Replay
```

NOTE: You can create the replay directory anywhere on the server that has the Hub Transport Server Role. In doing so you need to adjust the path, though. You do this via the command:

```
Set-TransportServer <hub transport server>  
-ReplayDirectoryPath "<path>"
```

The first line of this command is separated from the second line by a blank (`...port server> -ReplayDir...`).

1. Set the following privileges for accessing the “Replay” replay directory:

- Grant the XPR service account under which the Exchange APLs operate full control of this directory share. Proceed as follows:
 - Invoke the context menu for this directory.
 - Change to the **Sharing** tab in the configuration dialog.
 - Enable here the **Permissions** button.
 - Add the XPR service account as user via the **Add** button.
 - Assign the **Full Control** privilege to the XPR service account.
- Grant the XPR service account **Full Control** of the drop directory for the NTFS authentication. Proceed as follows:
 - Invoke the context menu for the replay directory.
 - Change to the **Security** tab in the properties dialog.
 - Add the XPR service account as user via the **Add** button.
 - Assign the **Full Control** privilege to the XPR service account.

- Grant the NETWORKSERVICE on the server with the Hub Transport Server Role **Full Control** of the replay directory. Proceed as follows:
 - Invoke the context menu for the replay directory.
 - Change to the **Security** tab in the properties dialog.
 - Add the NETWORKSERVICE as user via the **Add** button.
 - Assign the **Full Control** privilege to the NETWORKSERVICE.

Creating the replay directory is now complete.

Configuration of the ExchApl for access to the transport directories

The transport directories on the XPR side must now be configured.

1. In the XPR monitor open the configuration dialog of the **ExchApl**.
2. Switch to the **Exchange Foreign Connector** tab.
The entry lines for **Drop directory** and **Replay directory** display the XPR server name as default.
3. In the **Drop directory** and **Replay directory** specify the path to the shared transport directories according to the following pattern:

For the **Drop directory**

\\<Ip address or name of the Exchange server on which the Hub Transport Server operates>\<XPR server name>-<Exchange2007 mailbox server name>

For the **Replay directory**

\\<Ip address or name of the Exchange server on which the Hub Transport Server operates>\Replay

4. Click on **Apply** and **OK** to save the modifications.

The entered values are stored in the XPR server registry:

Registry path:

HKLM\SOFTWARE\Wow6432Node\Wow6432Node\PP-COM\MRS\ExchApl

Key:

DropDirectory and ReplayDirectory).

The configuration of the XPR foreign connector on the XPR side is thus complete.

The **ExchApl** must be rebooted for the configuration settings to take effect.

NOTE: If the default logging window of the XPR monitor displays an error message after you have saved the modifications, the system is unable to locate the two directories via the specified path. Open the ExchAPL settings dialog again and correct your path specifications.

4.3 Configuration

4.3.1 Configuring the LDAP Api

4.3.1.1 General Considerations

With Windows 2000, Microsoft have introduced the Active Directory Concept which allows a much more flexible administration of any kind of user data. Browsing the Active Directory requires a protocol, specially developed for this purpose. This protocol is called Lightweight Directory Access Protocol, LDAP for short. It is a further development of the access protocol Directory Access Protocol (DAP), based on the X.500 Directory Service, since the DAP could not meet the demands in terms of speed and overhead any more.

Active directory

The Active Directory Service¹ (DS) is understood as a scalable directory service structured similarly to a folder directory in a file system. However, here we do not deal with a file hierarchy (e.g. nested directories as with the complete path: `c:\Company\Site\Department\Group...`) but with an object hierarchy. An object is in this context a unit described by a unique, named set of attributes. With folder directories, the Explorer would principally be the counterpart to the LDAP protocol, used for Active Directory display and editing.

During log-in to the network and the search for released resources, Active Directory clients must be able to communicate with computers on which Active Directory is executed. This means that extraneous access to the domain control and global catalogs has to be performed using LDAP (Lightweight Directory Access Protocol).

LDAP (Lightweight Directory Access Protocol)

LDAP² is a communication protocol developed for TCP/IP networks. The LDAP protocol defines in which way directory clients access directory servers, carry out directory actions and make use of shared directory data. LDAP standards are established by IETF (Internet Engineering Task Force) working parties. In Active Directory the LDAP specifications for attributes and the IETF standards for the LDAP versions 2 and 3 are implemented.

-
1. See also the five-volume reference by Microsoft:
Active Directory Developer's Reference Library, David Iseminger,
Microsoft Press 2000, ISBN 0-7356-0993-6
 2. Further literature to deepen the LDAP subject:
Implementing LDAP, Mark Wilcox, Wrox Press Ltd.-1999, ISBN 1-861002-21-1

As the name already suggests, LDAP is an efficient method to access directory services without the complexity of other directory protocols. Since the LDAP protocol defines which processes are permitted in querying and modifying directory information and how to perform safe access, you can list directory objects, execute queries or administer Active Directory with LDAP.

LDAP and interoperability

LDAP is an open Internet standard. The use of LDAP enables cooperation of Active Directory with the directory services of other suppliers. As component of Active Directory Interfaces (DSI), the Active Directory support of LDAP comprises an LDAP supplier object. The Active Directory interfaces support the LDAP application programming interfaces for C defined in the internet standard RFC 1823. You can easily adjust other applications for directory services to access Active Directory information via DSI and LDAP.

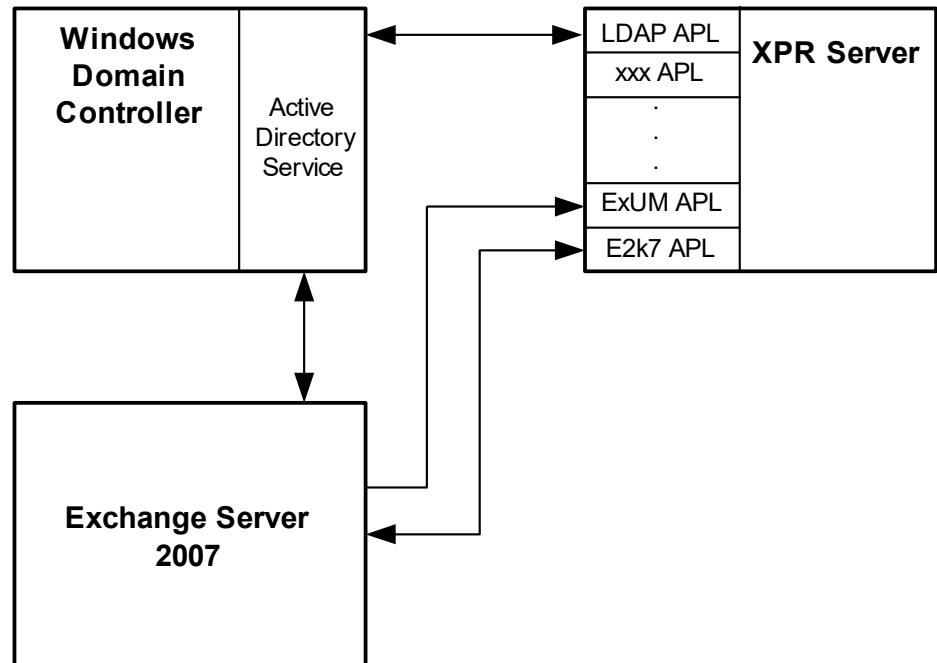
Active Directory and Exchange Server

In the course of standardization and a stronger integration of Exchange in the operating system Windows 2000, Exchange Server (from version Exchange 2000 Server) has been completely adapted to cooperation with the directory service Active Directory introduced in Windows 2000. This means that now all Exchange directory information is stored in Active Directory, too. Thus the individual Exchange directory used in previous versions to centrally store objects of an organization (e.g. addresses, mail boxes, distribution lists and public folders...) has been replaced. Among other things it was necessary to install a special directory service to administer data replication between individual Exchange servers. Connecting Exchange to the Active Directory Service of Windows has the following advantages:

- Enabling a centralized object administration.
This means that the directory objects can be administered from one place with only one management tool as of operating system version Windows 2000 Server.
- Security management simplification.
Since Exchange 2003/2007 uses the same security features as Windows, modifications to the security policies (user or group accounts) apply likewise for data stored in Exchange and in Windows.
- Efficient creation of distribution lists.
The security groups specified in Windows are automatically used by Exchange 2003/2007 as distribution lists.
- Simplified access to directory information.
By creating an LDAP interface you can display and edit the Active Directory data via the native LDAP protocol.

4.3.1.2 Active Directory and XPR

In order to meet future requirements and to ensure the interplay with the Exchange 2003/2007 server, the Active Directory (DS) directory service was integrated in the XPR system with the help of the LDAP APL.



For this purpose a separate connection to the Active Directory via the LDAP APL is required. The function of this is to enable a mapping between the attributes of the Active Directory and the data relevant for XPR, in other words to establish correct assignment. Since manual adaption of the database fields is relatively laborious, the effort is minimized by performing the basic configuration via the import of a standard configuration file (`xxx.lcf`).

Miscellaneous

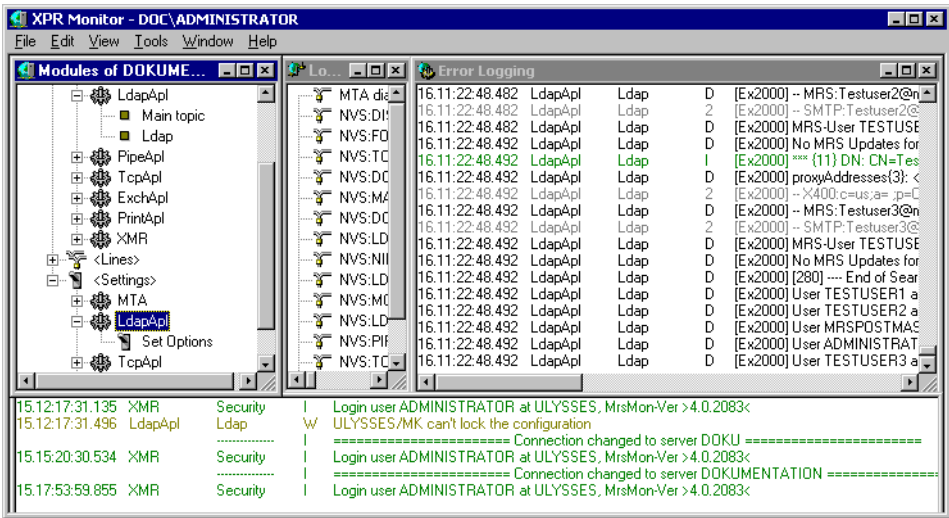
1. The LDAP APL only serves to replicate user data - the DS pattern is not extended or modified.
2. The LDAP port used is configured on 389 by default.
3. The LDAP APL is so conceived that it can additionally access other systems supporting the LDAP protocol.

4.3.1.3 Installing the LDAP APL

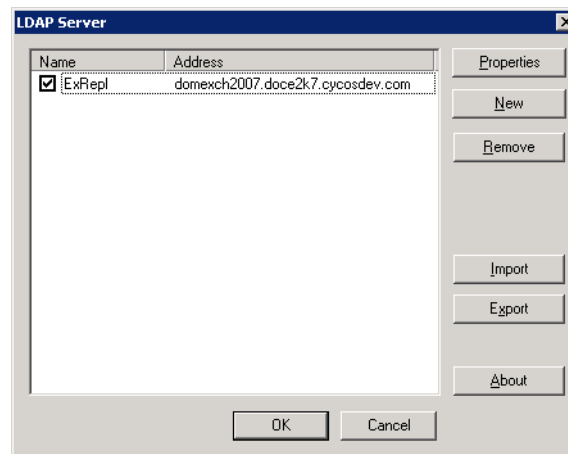
Installation via the XPR setup

Installation of the LDAP APL is embedded in the XPR server setup. If a new XPR server is to be set up for Exchange Server 2007, the LDAP APL must be integrated in the installation for selecting the Exch APL. The LDAP APL installation procedure in the XPR setup is described in [Section 4.2.5.3, “Installing the LDAP APL”](#), on page 66.

4.3.1.4 Editing LDAP Settings



All LDAP settings are performed from within the XPR monitor. You reach the setting options via the **Modules of <XPR server name>** window. Expand the branch next to **<Settings>**. Then open the subtree **LdapApl**. Subsequently, double-click **Set Options** to open the LDAP APL settings dialog.



This first dialog **LDAP Servers** serves general administration purposes. The names and IP addresses of already existing LDAP configurations are listed here. From here you can define further LDAP configurations (LDAP links) and edit already existing ones. In use is the server that features a check mark before the name entry.

The buttons in this dialog have the following significance:

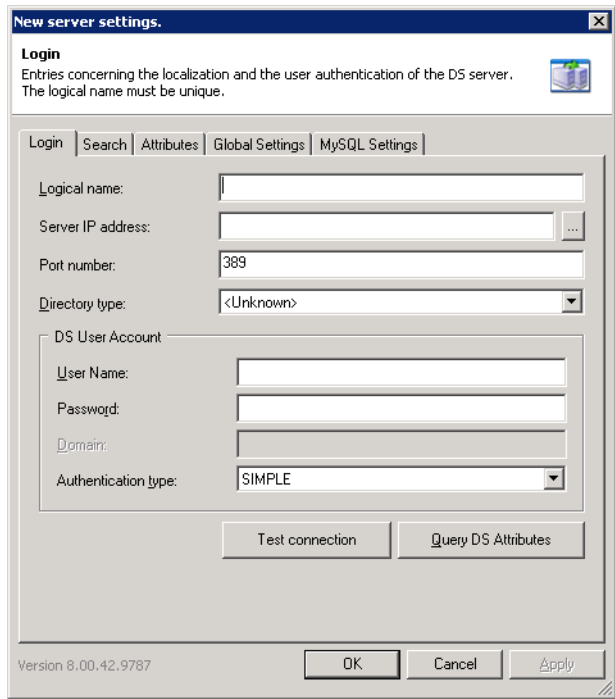
Properties

When you select an arbitrary configuration entry, the **Properties** button takes you to the configuration dialog **Edit server settings**. In there you find four setting tabs used for changing the LDAP configuration.

New

Via the **New** button you can add further LDAP configurations. When you enable it you are taken to the **New server settings** configuration dialog. To define a new LDAP configuration here, fill in the four tabs **Login**, **Search**, **Attributes** and **Global Settings**.

The significance of the individual entry lines can be gathered from the **Properties** button description further below.

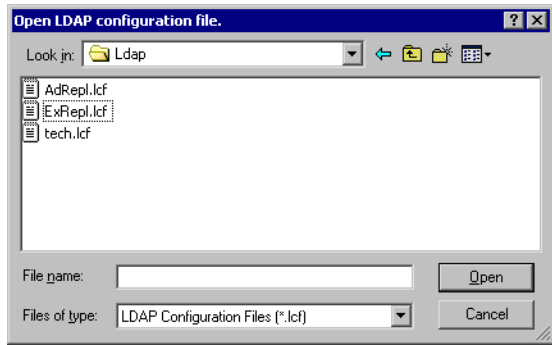


Remove

Deletes a selected LDAP configuration file.

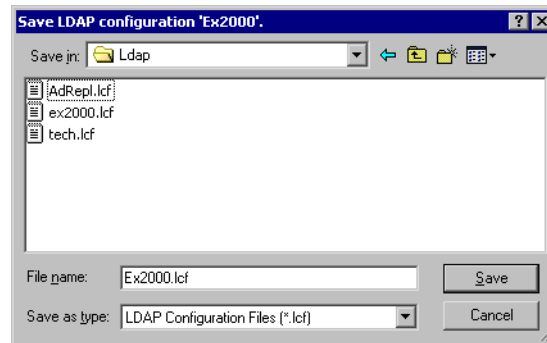
Import

Branches to the file selection window **Open LDAP configuration file**. Here you can enter an existing configuration file (format: xxx.lcf). In this way it is possible to implement different configuration files. Completing this step takes you to the **Login** tab in the **Edit server settings** window where you can perform modifications.



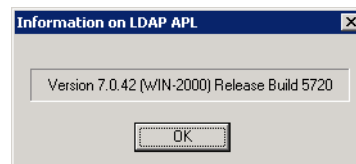
Export

If stored as `xxx.lcf` file, a configuration file can be created, which includes all current settings of the selected server.



Info

The About button opens an information dialog that displays the currently active LDAP APL version. With a click on **OK** you leave this dialog again.



OK

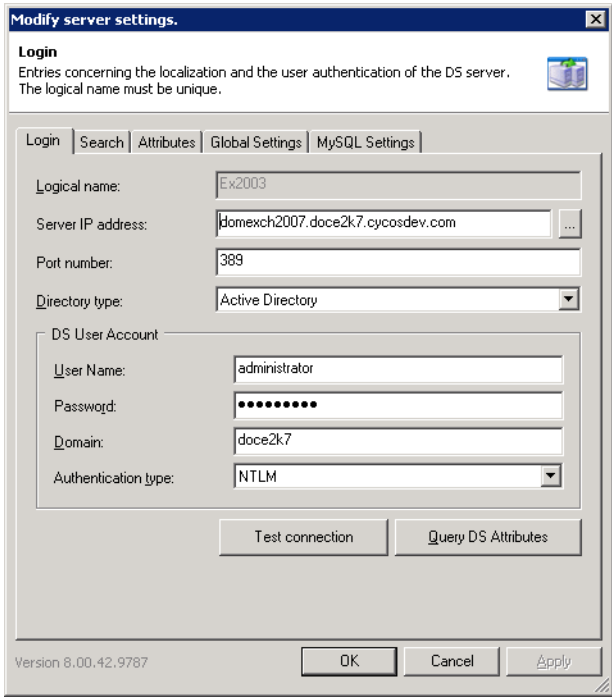
Copies the entries made in the **Edit server settings** tab and closes the LDAP APL setting dialog.

Cancel

Terminates the LDAP APL configuration without copying modifications previously made.

4.3.1.5 The “Login” Tab

Here all information on this DS server is displayed. In the upper section you find the assigned LDAP configuration name and the entry lines for the IP address, the port number and the directory type of the LDAP server. Thereunder, entry lines for user identification data are available. With the exception of the short name (name of the LDAP connection) assigned upon the reconfiguration you can now edit settings for DS server localization and the access privileges.



NOTE: The LDAP configuration name (**Logical name**) is only possible via a redefinition of the configuration settings.

The functions of the input fields on the **Login** tab are as follows:

Dialog Entry	Description
Logical name:	Here you can assign an arbitrary name to a new LDAP configuration. This name must be unique since it is used for registry entry replication. If you open an already existing DS server configuration via the Properties button, the previously assigned name is displayed. It can, however, not be changed in this form.

Table 3 Entry Fields in the LDAP Settings Tab “Login”

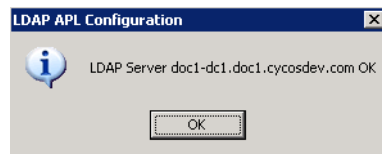
Dialog Entry	Description
Server IP address:	In this entry line you can specify the valid DS server IP address (either the qualified host name or the numeric address), or the IP address of the selected entry is displayed. If you have opened an existing configuration, the IP address of the selected configuration is displayed. To simplify things you can use the  button (to the right of the entry line) to search the entire network for the desired DS server.
Port number	Entry field for displaying the currently set port or to modify the port number. Note: Ports 3268 cannot be used for searching the Active Directory. Via port 3268 the global catalog (thus the entire forest) is searched for a specific attribute, with only reading access being possible. In addition, the global catalog only holds a subset of the AD attributes. The extensionData attribute does not belong to this subset. Consequently, the extensionData attribute cannot be read out or written via this port. The following warning is issued via the LDAP APL in this case: <i>LdapApl Ldap W [Ex2003] ldap_modify [1 attributes]: Unwilling To Perform</i>
Directory type:	This menu allows selection of either Active Directory, <unknown> or DirX. For our purposes set Active Directory here. The other options refer to LDAP connections to other systems.
In the DS User Account section	
User name	Here, the name of the user account is entered/displayed that is furnished with the corresponding privileges for the AD access. The AD access is possible if this user account belongs to the group of domain administrators or to the group of Builtin account administrators.
Password	This entry field is for definition of the password associated with the above user account.
Domain	Field for entry (or display) of the domain name associated to the above user account.
Authentication type	The definition of the authentication type must be set to NTLM (NT Lan Manager) for connecting the Active Directory Service. The alternatives SIMPLE and Negotiate are intended for other directory systems. Annotation: When you log in with the authentication type SIMPLE , the user name must be entered in the LDAP format, i.e. as "Distinguished Name" (DN). Example: uid=admin,ou=administrators,ou=TopologyManagement,o=NetscapeRoot

Table 3 Entry Fields in the LDAP Settings Tab "Login"

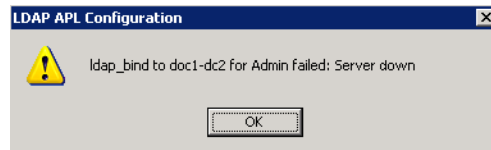
The data relevant for the DS server selection are now entered.

Testing the connection

Via the **Test connection** button you can verify the entered connection data. You are informed about the status of the connection to the DS server by a message shown in the below illustration.



In case of an error (the connection cannot be established), the same dialog appears with a special text message that, if possible, contains details on the problem occurred.



Polling DS attributes

Via this button you can manually trigger the initial transmission of the DS attributes. Otherwise, the selected DS server reads out the DS attributes by way of a periodically occurring query and lists them in the **Attributes** tab (see **Polling interval** and **Schedule** in the **Search** tab). You can watch this process on the XPR monitor as well. See also [Section 4.3.2, "Monitoring the LDAP APL Activities"](#), on page 112.

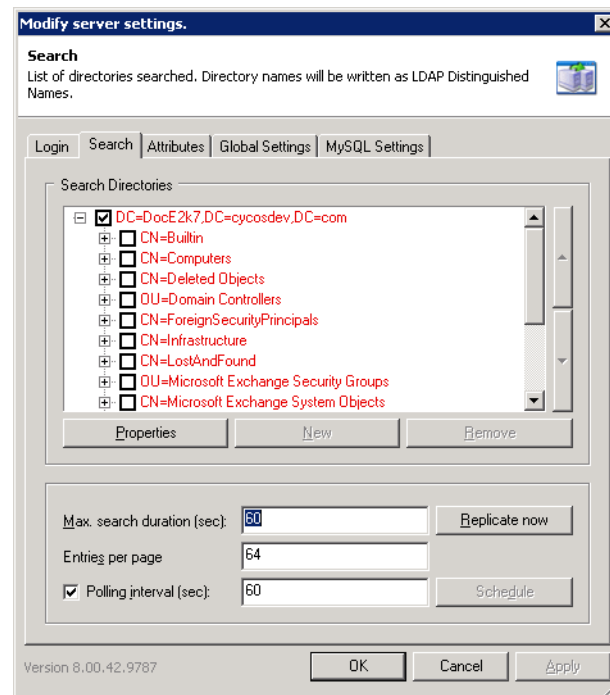
4.3.1.6 The “Search” Tab

General information

The **Search** tab is used to define directories or user entries that are to be integrated in the replication process. Here you must explicitly select the containers that include users whose attributes are to be replicated.

NOTE: Make sure to only select containers that include real users. Otherwise unwanted entries (for example the Exchange system mailbox) may be integrated in the replication process. A new user “system mailbox” would then be generated on the XPR server with each replication process.

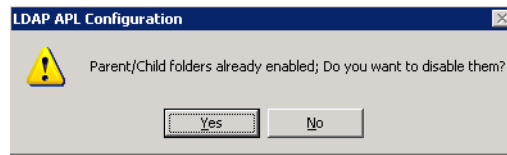
The containers or user entries in the search directory are color highlighted according to the search depth.



The **Search Directories** section displays the directories of the entire DS tree. You can expand the tree (click the [+] icons) to display the single user entries. To select a directory, place a check mark in the corresponding box next to the branching nodes of the tree.

- **Black entry:** Only the attributes of the users defined in the respective container object are replicated.
- **Blue entry:** Only the user attributes of the first level below the selected container will be replicated.
- **Red entry:** The entire subtree will be included in the replication.

An implemented logic prevents a redundant replication. An error message is issued when a new selection includes an already existing one.



If you confirm this message with **Yes**, the new setting becomes active and the old one is automatically adapted. **No** restores the state before the modification.

NOTE: Annotation on selecting users whose attributes are to be replicated: If in a larger organization all users have been defined in one container and attribute replication is only required for a subset of these users, the selection process may become relatively protracted when all users have to be selected individually. In this case filter rule definition can be applied to specify the selection. Another option is to define the users intended of replication in a special container.

The two arrow icons on the right margin of this window display serve to modify the directory sequence in the list represented. Select the container or container object to be moved with a click and move it up or down according to the new position desired. In this way you can customize the replication priority since otherwise, with several selected directories, the processing sequence is from top to bottom.

Replication settings

The buttons and entry fields in the bottom section of the dialog define the temporal replication process.

- **Polling interval**

IMPORTANT: Default after the installation is 0 seconds. Thus replication is at first deactivated so that it does not occur uncontrolled.

Each entered number value *x* starts the replication after *x* seconds (for example: with an entry of 12 the next replication starts after 12 seconds). Instead of via a polling interval, replication can also be performed via a schedule definition. Deactivate the checkbox next to the **Polling interval** entry to automatically activate the **Schedule** button. Schedule definition is described further below. If you want regular replication via a polling interval and no valid time value has been entered yet, an error message informs you accordingly.

- **Max. search duration** (Default 60 seconds)

This value determines the maximum duration of a replication. Any numeric value x ($x > 0$) entered there terminates the replication when this value has been reached after x seconds.

- **Entries per page**

Since timeout problems may occur when extremely large amounts of data have to be replicated, you can determine the number of data records to be transferred per transmission unit via the **Entries per page** field. 0 means that all data records are to be transmitted in one go; any other value restricts the number of data records. For example, 128 data records are sent per transmission unit with the entry 128.

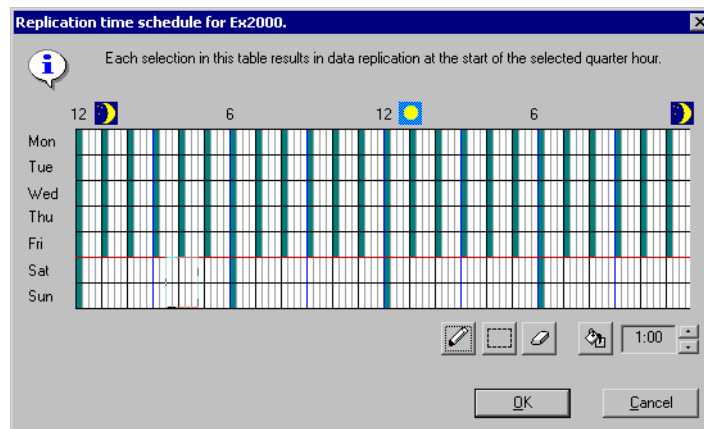
- **Replicate now**

Via the **Replicate now** button you can start this process manually.

- **Schedule**

With a click on the **Schedule** button you can create a replication week profile. Replication can be set in 15-minute steps for each weekday.

NOTE: Replication does not occur if it is to be performed via a schedule but no settings have been made there. No error message is issued on this.



After opening the schedule you can edit the replication times. The following tools are available:

Tool	Description
	Serves to arbitrarily enter replication times in the schedule.
	Selection tool for marking sections in the week profile.

Table 4 Tools to create a Replication Schedule

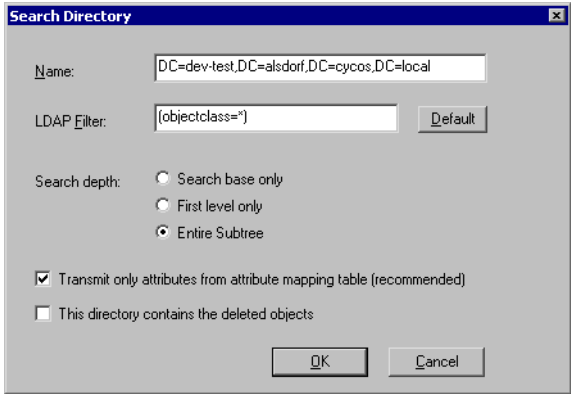
Tool	Description
	With the eraser function you can remove single replication times from the week profile. If and entire area has previously been selected with the selection tool, the replication marks within the marked area are maintained in case of replication mark deletion.
	Is used to define a replication time for a whole week if replication is to occur each day at the same time in the same interval. The intervals can be specified in the entry field next to this icon.

Table 4 Tools to create a Replication Schedule

The Properties, New, and Remove buttons

The **New** and **Remove** buttons are intended for manual configuration (directory type “unknown”). In the *Exchange Server 2007* connection context (directory type “Active Directory”) they are meaningless the therefore inactive.

After clicking on **Properties** you can view and modify the search directory settings.



The **Name** specifies the **search base** or the starting point of the search run within the directory hierarchy. Under **Name** the search base is displayed as node of the DS branch.

The **LDAP Filter** field specifies the **search filter** that determines the conditions for searching the data records (objects). This filtering also enables looking for special criteria of the user data replication. In the **LDAP Filter** field the search filter can be restricted to specific attributes. The default filter `objectclass=*` replicates all entries. Any complex logical filter¹ is conceivable.

NOTE: As of Exchange Server 2007 the distribution groups support the **sAMAaccountName**. As a result, all Exchange users with this attribute are replicated as full XPR users to the XPR server. This causes problems when assigning the MRS address type and the number of replicated users exceeds the number of available user licenses. Applying suitable filtering here, for example via `(&(objectclass=*)(!objectClass=group))`, you may restrict the users to

1. For more information see: Implementing LDAP, Mark Wilcox, Wrox Press Ltd. 1999, ISBN 1-861002-21-1

be replicated. In the above filtering example this would concern users who do not have an `ObjectClass=Group`. In the single case the filter to be defined depends on the structure in which the users are implemented in the Active Directory.

After changing the filter you can click on the **Default** button to switch to the `objectclass=*` filter again.

The **search area** indicates which part of the directory starting from the search base is to be searched. The search area can be set for the selected object via the **Search depth** option:

- **Search base only**
Only the attributes of the users defined in this container object are replicated.
- **First level only.**
Only the user attributes of the first level below the selected container will be replicated.
- **Entire Subtree**
The entire subtree is included in the replication.

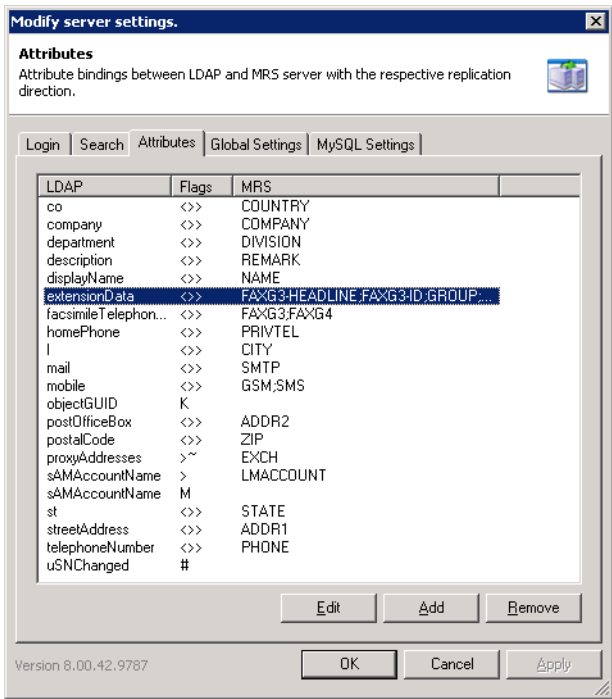
By means of the checkbox **Transmit only attributes from attribute mapping table (recommended)** you can define that only the entries listed on the **Attributes** tab are transmitted. This setting is recommended since it optimizes IP transmission (only attributes needed most are transmitted).

When the checkbox **This directory contains the deleted objects** is active, the elements of the folder entered in the **Name** field are interpreted as “deleted”. The expression “deleted” is somewhat inaccurate here since objects thus defined are not removed but only hidden.

The settings become valid with **OK**; **Cancel** terminates the previously described process without performing any modifications. Simultaneously you are taken back to the **Search** tab.

4.3.1.7 The “Attributes” Tab

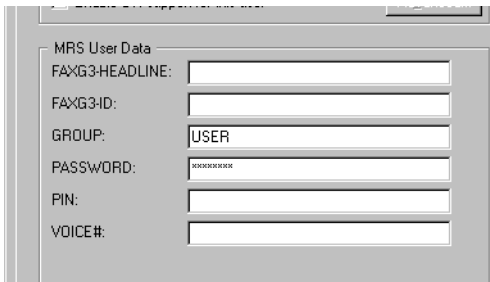
The central window of the **Attributes** tab lists the DS attributes, the corresponding XPR data fields and the set flags. They are already defaulted by the basic setting respectively by importing the configuration file for the *Exchange Server 2007* connection (*ExRepl.lcf*).



Of the listed attributes the **extensionData** attribute is especially significant. The XPR data fields assigned to this DS attribute are exactly those you find in the Exchange users' properties dialog on the **MRS Settings** tab, where they are configured.

The configuration of the **extensionData** LDAP attribute is stored in the “MRS Setting Object” in the Active Directory. The MRS Setting Object for the LDAP configuration is available only once for the entire Exchange environment.

Via editing this attribute you can add further fields on the **MRS Settings** tab. See [Section 4.3.1.7, “Extending XPR attributes”, on page 106](#).



When you click on the **Edit** button, settings for selected attributes can be changed and via **Add** further attributes are selected, assigned and various attribute parameters set.

The following illustration shows the empty form to select a new attribute and the required mapping as well as settings of the individual parameters (usage of attributes, replications etc.).

The attribute to which the following settings relate is selected and displayed in a combo box in the **Directory Service Attribute** section. Next to this name field, the data type is specified in the field with the gray background under **LDAP Type**. Thus you are informed whether the type is a string variable (**str**), an integer variable (**int**) etc. Thereunder, another field is placed to display the **Subtype**: if there is another differentiation in subtypes as e.g. with an Octets type.

The checkboxes included in this portion have the following functions:

Checkbox	Description
Create new MRS user Sets Flag: M	Use this attribute if a new XPR user is to be defined. The value of this LDAP attribute is used as user ID on the definition of new XPR users. If the Use attributes to link DS users to XPR users option is not active, this value also serves to directly link an LDAP data record to the data of an XPR user of this name.

Table 5 Settings for the LDAP Directory Service Attribute

Checkbox	Description
Cache key Sets Flag: K	Integrates an attribute in the cache (for faster access). Once an XPR user has been found, he/she is then directly found via the cache key in each following search and his/her data are available faster.
Update Sequence Number (USN) Sets Flag: #	The USN is an update ID incremented from XPR attributes to DS attributes with every search request. When this checkbox is active, only records that have a larger USN-ID than the one generated with the last search run are replicated.
Mandatory for MRS user	Defines that this attribute is mandatory for an XPR user. If this option is set, a user is only defined if the attribute is filled in. In other words, if the attribute entry is deleted, all users that do not have this attribute entry will be deleted with the next replication.

Table 5 Settings for the LDAP Directory Service Attribute

Thereunder you find the **XPR Attributes** selection field to assign the above selected DS attribute to the corresponding XPR database field. All XPR database fields are listed here so that each DS attribute can be mapped on each XPR field (and vice versa).

The associated checkbox allows using this attribute when a new **DS user** is to be created (sets flag: **D**). This option is presently not available but will be implemented for future applications.

The checkboxes coming next determine the replication direction. You can alternatively replicate to the XPR server (**Replicate to XPR**, sets flag: **>**), to the domain server (**Replicate to DS**, sets flag: **<**) or to both simultaneously (both flags are set: **< >**). If a reciprocative replication is desired, you need to define one of the two servers as the superordinate one. This is done via activation of the **DS is master** or **XPR is master** switches.

Through activating the checkbox **Use attributes to link DS users to XPR users** (sets flag **~**) you can directly relate a DS user to an XPR user via attributes. Indirect linkages can thus be defined. For example, with DS attribute *proxyAddresses*, XPR attribute *EXCH* and activated option, all DS data of a user are assigned via the value of the DS attribute *proxyAddresses* to the XPR user who has the same contents in the *EXCH* database field.

The switches in the **Filter for Attribute Values** section can be set to manipulate attributes in various manners (for example, to quickly determine a user etc.). Depending on the complexity of the manipulation, this can either be done by a regular expression or by an e-Script. E-Scripts are programs for establishing e.g. complex filters.

The following setting options are available:

Filter setting	Description
None	The filter function is deactivated.
Regular expression:	Entry fields for regular expressions.
E-Script	Entry field for the name of the e-Script to be applied to the DS attribute.

Table 6 Filter Settings for the LDAP Attribute Values

Definition example of an attribute's replication properties with usage of the **Regular expression** filter function.

The entries in the above dialog have the following significance:

- All entries of the directory attribute *proxyAddresses* are filtered.
- When an entry matches the regular expression *XPR:%t*, it is replaced with the expression on the right and copied; all other are rejected. *%t* serves as wild card for an arbitrary, not empty chain of characters without blanks entered in the right field for *%1*. You can generally enter several sub-patterns in the regular expression field on the left-hand side; on the right-hand side you can then indicate the *n*th sub-pattern with *%n*. You find more information on regular expressions in the **E Programming Language** and **XPR Server Administration** manual, chapter "LDAP APL".

The settings performed are copied with **OK**. You are simultaneously taken back to the **Attributes** tab. Newly selected and edited attributes are added at the bottom of the list.

Extending XPR attributes

An additional example explains how to add new fields to user data (in **Active Directory Users and Computers**) on the **MRS Settings** configuration tab.

IMPORTANT: If additional XPR attributes are defined here for the DS server, data replication to the XPR server may lead to the deletion of XPR-significant data fields. If an XPR data field is replicated when empty, then a completed data field may be deleted (overwritten by the empty data field). Data fields must consequently not be left empty with defining a user.

1. In the XPR monitor under LDAP APL select the **Set Options** function.
2. Next, mark the desired server in the list of possible LDAP servers and enable the **Properties** button.
3. In the **Edit server settings** dialog then open switch to the **Attributes** tab.
4. Select the **extensionData** entry from the attribute list.
5. Click **Edit**.

The **XPR Attributes** combination field displays all entries of the **extensionData** directory attribute.

6. You can now select additional data fields via the associated checkboxes in the **XPR Attributes** selection dialog. These fields are then additionally integrated after a click on **OK** in the user settings with **Active Directory Users and Computers**.

Cancel terminates the process and modifications already performed are disregarded. A click on either button simultaneously takes you back to the **Attributes** tab.

If the attributes are defined by the configuration file, they are listed on the **Attributes** tab with the already existing assignment to the XPR system. This means that with the represented attribute the corresponding XPR data field on which this attribute has been mapped is displayed. There are various flag symbols between the attribute name and the XPR data fields which already provide information about how certain attribute or replication parameters are set. The following flags or combinations of them can be set:

Flag Symbol	Significance for the selected attribute
M	The attribute is used when a new XPR user is to be defined.
D	The attribute is used when a new DS user is to be defined (this option is presently not available).
K	Integrating the attribute in the cache (for faster access).
#	This flag indicates that the search run is only performed from the last replicated records.

Table 7 List of possible Attribute Flags

Flag Symbol	Significance for the selected attribute
<	Replicates this attribute to the DS server (with XPR as master). This setting can be used if e.g. a new Exchange Server 2007 is to be coupled to an existing XPR server to replicate all XPR data to the AD.
>	Replicates this attribute to the XPR server (AD is master).
<>	Replication in both directions.
<>>	Replication in both directions with AD as master.
<<>	Replication in both directions with XPR as master.
~	This flag shows that the directory service user is linked directly with an XPR user by means of the attribute.

Table 7 *List of possible Attribute Flags*

The **Edit** button enables the modification of the attribute parameters of a selected entry at a later date. When you click it, the **LDAP/XPR Attributes** dialog opens with the entries made for the selected attribute. You can adapt entries and save them as described above.

Replication of XPR multivalued fields

The XPR server database can be so extended that for some entries so-called multivalued entries can be generated. In this way it is possible to define several phone numbers for one database entry. The field **VOICE** or **PHONE** can be intended for this purpose, if several phones or voiceboxes are needed for one user. The fields are stored in the database consecutively numbered: **PHONE** (primary field), **PHONE.01** (the first non-primary field) etc.

However, since the AD does not provide any number of attributes for phone numbers, these fields cannot be directly replicated to the AD in this format. The phone number entries in the AD are so organized that only the first phone number (primary) can be replicated via the *telephoneNumber* attribute, all other phone numbers (non-primary) are replicated via the *otherTelephone* attribute.

So that these fields can be integrated in replication to the AD server, an additional field is offered (for example **PHONE.***). This field serves exclusively for replicating non-primary fields, thus for example the database fields **PHONE.01**, **PHONE.02** etc. It is possible to replicate the multivalued fields in different ways:

- LDAP single value to XPR multivalued field.

Example: *telephoneNumber* to *PHONE*

Only the primary entry is replicated to XPR.

- LDAP multivalued to XPR multivalued field.

Example: *otherTelephone* to *PHONE*

All multivalued entries are replicated to XPR 1:1.

- LDAP multivalued to XPR multivalued fields without the primary field

Example: *otherTelephone* to *PHONE.**

All multivalued entries, except for the primary field, are replicated to XPR.

Attribute settings for additional LDAP servers (e.g. subdomains)

As attributes for additional LDAP servers, e.g. additional subordinate domains, are not automatically preset, these must be set as follows:

1. Select the first server in the **LDAP Servers** window and export its settings to a file by means of the Export button. The changes for the new server must now be made in this file.
2. Open this file with the editor, change the entries for the Domain Controller **DC** and for the Container **CN** and, where applicable, **OU** to be replicated and save your changes in a file.

```
dirType:ActiveDir
Script:EXRep1
AttMap:21
co:COUNTRY:0, str:toM, toD:none
company:COMPANY:0, str:toM, toD:none
department:DIVISION:0, str:toM, toD:none
description:REMARK:0, str:toM, toD:none
displayName:NAME:0, str:toM, toD:none
extensionData:FAXG3-HEADLINE;FAXG3-ID;GROUP;PASSWORD;PIN;VOICE#:2, octets:toM, toD:none
facsimileTelephoneNumber:FAXG3#;FAXG4#:0, str:toM, toD:none
homePhone:PRIVTEL#:0, str:toM, toD:none
l:CITY:0, str:toM, toD:none
mail:SMTP:0, str:toM, toD:none
mobile:GSM#;SMS#:0, str:toM, toD:none
objectGUID::1, octets:key:none
postOfficeBox:ADDR2:0, str:toM, toD:none
postalCode:ZIP:0, str:toM, toD:none
proxyAddresses:EXCH:0, str:toM, cor:rule:"MRS:%t":%l
sAMAccountName:LMACCOUNT:0, str:toM, script
sAMAccountName::0, str:newM:none
st:STATE:0, str:toM, toD:none
streetAddress:ADDR1:0, str:toM, toD:none
telephoneNumber:PHONE#:0, str:toM, toD:none
uSNCchanged::0, int64:usn:none
Folders:3
DC=doc-test, DC=aisdorf, DC=cycos, DC=local:(objectclass=):2:a:2
OU=Test_UO:(objectclass=):0:3:0
CN=Users:(objectclass=):0:3:0
```

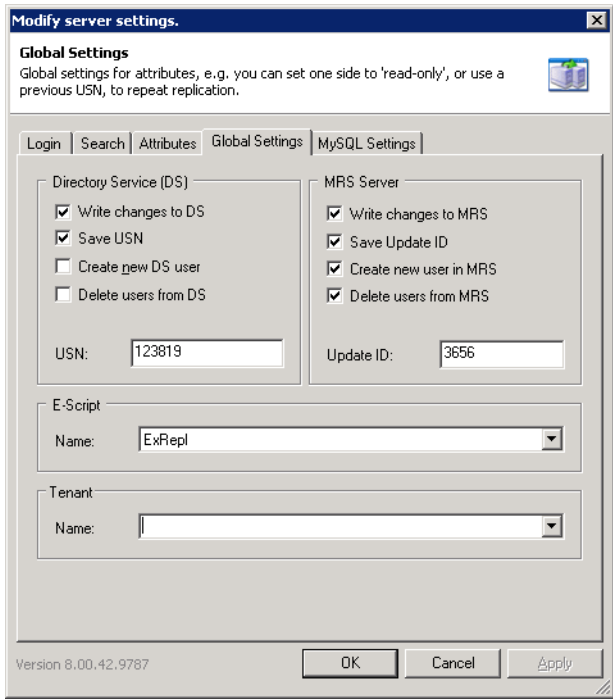
3. This file is now imported into the LDAP Servers window.
In the following the same specifications are demanded for the new server as already described in section 2.4.3.1, "The "Login" Tab", on page 281. The **Search** and **Global Settings** tabs must now be filled out. Enter the same settings here as for the first server.

4.3.1.8 The “Global Settings” Tab

You can perform further detailed settings on the **Global Settings** tab.

The **Global Settings** tab consists of four sections.

- Settings that refer to the Directory Service (DS),
- Settings that concern XPR (**MRS Server**) and
- a selection dialog to pick an e-script and



Settings in the **Directory Service** and **XPR Server** section are performed analog for the Active Directory and XPR side. You can perform the following settings:

Dialog Function	Description
Write changes to DS and Write changes to MRS	Modifications can either be saved in the Active Directory, on the XPR system or in both.
Save USN and Save Update ID	With the modifications copied upon LDAP APL shutdown, the USN (Update Sequence Number) and/or the UID (Update ID) is incremented. Here you can determine whether this is desired for one of the two or for both. The corresponding values are stored in the registry. Both IDs make sure that replication processes performed at a later date can start from a certain flag rather than all over again.

Table 8 Global Directory Service Settings for the LDAP APL

Dialog Function	Description
Create new user in MRS	Depending on the preset replication directions, creation of a user entry can be suppressed for testing purposes by deactivating the checkbox .
Delete users from MRS	Via this checkbox deletion of user entries can be suppressed for testing purposes (resetting the checkbox).
Entry fields: USN and Update ID	By means of these entry fields, a replication can be started from a certain USN (Update ID). In doing so it should always be clear what has been replicated with the entered USD. In this context it is useful to keep a log on the replication processes.

Table 8 Global Directory Service Settings for the LDAP APL

E-Script

You can select an e-script in the corresponding section used for automatic attribute editing. The defaulted e-script **ExRepl** active for the Exchange connection sets the predefined values for the standard replication.

An e-script can act as complex filter allowing e.g. telephone number normalization or special actions upon creating a new XPR user. Selection of e-scripts is performed via the pull-down list. Existing e-scripts are generally contained in the . . . \XPR\res\Ldap directory.

Tenant (with Exchange Server 2003 only)

NOTE: Here you can select one of the defaulted tenants for a multi-tenant scenario with several Exchange organizations.

4.3.1.9 “My SQL Settings” Tab

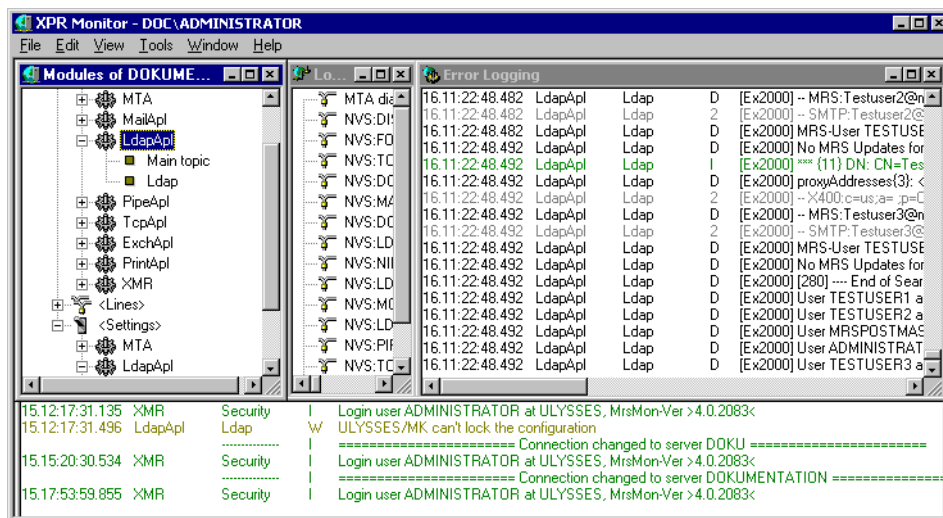
No settings need to be performed here for connecting the Active Directory to the XPR server in an Exchange scenario. The **MySQL Settings** tab serves for configuring another deployment scenario for the LDAP Apl.

4.3.2 Monitoring the LDAP APL Activities

Via the XPR monitor you can precisely observe which actions are currently carried out by the LDAP APL. The following short instruction shows you the path to this display:

1. In the XPR monitor access the **Modules of <XPR server name>** window and drag the gear wheel icon  LdapApl named "LdapApl" from the <Topics>  branch to the **Error Logging** window per Drag&Drop.
2. Adapt the parameters for the data to be displayed in the **Logging Monitor Properties** window.
3. Verify your settings with the **Copy** button.
4. Confirm your selection with **OK**.

The selected LDAP APL activities are now logged in the **LdapApl-All Topics** window (see next figure).



The **XPR Monitor** chapter of the **XPR Server Administration** manual informs you about further monitoring and logging options.

4.3.3 Uninstalling the LDAP APL

Analog to the uninstallation of other XPR components, you can uninstall these from the command line with the following command:

```
LdapApl remove.
```

The running component must previously be closed down via the *Service Control Manager*. You do this by selecting the component in the services list and a click on **Stop**.

You can also close the LDAP service via the DOS console. Enter the following command in the command line:

```
LdapApl stop
```

4.3.4 User Administration

The XPR MMC Snap-in installation extends the **Properties of <user>** in **Active Directory Users and Computers** with the **MRS Settings** tab.

NOTE: Users who do not have an Exchange mailbox cannot see the **MRS Settings** tab.

If the XPR MMC Snap-in is installed on a 32-bit operating system you reach this settings page as follows:

1. Start the administration program **Active Directory Users and Computers** via **Start > Programs > Administrative Tools**.
2. Select the corresponding user directory there.
3. Open the associated properties dialog with a doubleclick on the desired user entry.

NOTE: You can also reach the **Properties** dialog through opening the context menu.

4. Switch to the **MRS Settings** tab.
On this tab, XPR-relevant settings are performed individually for each user.

If the XPR MMC Snap-in is installed on a 64-bit operating system, you need to start it in 32-bit mode (`mmc /32`).

NOTE: You find further information in the Microsoft KB article [http://msdn.microsoft.com/en-us/library/ms692753\(VS.85\).aspx](http://msdn.microsoft.com/en-us/library/ms692753(VS.85).aspx)

Proceed as follows:

1. Open the application start-up panel via **Start > Run**.
2. Enter the following command:

```
dsa.msc /32
```

The managing program **Active Directory Users and Computers** opens.

3. Select the corresponding user directory there.
4. Open the associated properties dialog with a doubleclick on the desired user entry.

NOTE: You can also reach the **Properties** dialog through opening the context menu.

5. Switch to the **MRS Settings** tab.
On this tab, XPR-relevant settings are performed individually for each user.

4.3.4.1 The “MRS Settings” Tab

The screenshot shows the 'Test User 1 Properties' dialog box with the 'MRS Settings' tab active. The 'Unified Messaging and telephony features' checkbox is checked. Under 'CTI settings', the 'Activate CTI' checkbox is also checked, and an 'Advanced...' button is visible. The 'MRS User data' section contains several text input fields: 'FAXG3-HEADLINE', 'FAXG3-ID', 'GROUP' (containing 'USER'), 'PASSWORD' (masked with asterisks), 'PIN', and 'VOICE' (containing '101'). At the bottom of the dialog, it indicates 'Data last modified: 05.12.2007 17:08:41' and provides 'OK', 'Cancel', 'Apply', and 'Help' buttons.

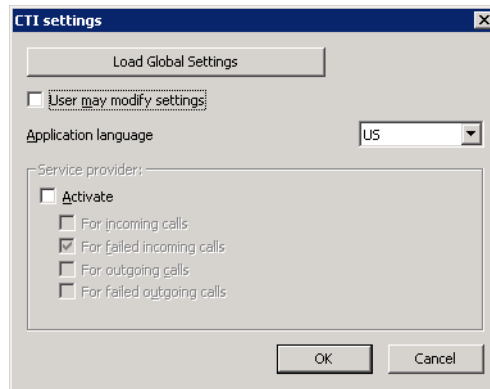
With the **Unified Messaging and telephony features** option it is possible to exclude this user from the features provided on the XPR system. Remove the checkmark to delete the user from the XPR database.

CTI settings

Via the **Activate CTI** checkbox, telephony functions (for the CTI client) can be released for the respective user provided they are implemented and configured. This generates and activates the **CTIJOURNAL** database field for this user on the XPR server.

Advanced CTI settings

Via the **Advanced...** button you reach the **CTI settings** dialog in which you can set a user's CTI functions different from the global settings. The global settings are defaulted via the connector configuration. See [Section 4.3.5.3, “CTI Settings Tab”, on page 123](#).



Via the **Load Global Settings** button you copy the global settings (those defaulted with the connector settings) for this user.

User may modify settings

Setting this option allows the user to change his/her settings for the CTI client.

Application language

Here you can select the language to be used in the CTI client dialogs for this user.

Service provider

The CTI client does not log calls if the program has not been started. Enabling the **Activate** checkbox you can set for all calls that the associated XPR-CTI journal entries are sorted into the corresponding CTI client directories via the service provider.

The behavior can be individually configured for the following call states:

- For incoming calls
- For failed incoming calls
- For outgoing calls
- For failed outgoing calls

XPR user data

These are the database fields that were defined in the LDAP APL via the default setting or after extending the **extensionData** field. You find further information about database fields and how to expand them in the description of the LDAP APL configuration in [Section 4.3.1.7, “The “Attributes” Tab”, on page 102.](#)

NOTE: If the **PIN** field remains empty, the default PIN will be used. This PIN is specified via the general voicemail settings in the respectively installed telematics APL. If a PIN is entered in the Exchange user definition that deviates from the default PIN, the relevant user will not be automatically forced anymore to change the PIN assigned here when he/she logs on to his/her voice box for the first time.

Which database fields are available by default and the purposes they serve is described in detail in the Server Administration manual, chapter **User Data Administration**, section **Database Fields Significance**.

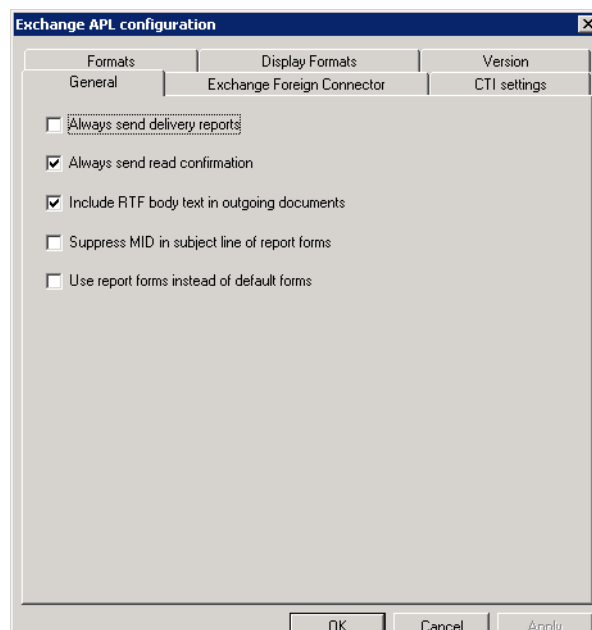
4.3.5 Administration of the XPR Foreign Connector

All connector properties that need to be configured for the XPR server are configured with the new XPR foreign connector via the settings dialog of the **ExchAPL** in the XPR monitor. The following connector properties can be set:

- The connections to the transport directories found on the server that has the Mailbox Server Role.
- The global CTI settings.
- The message formats

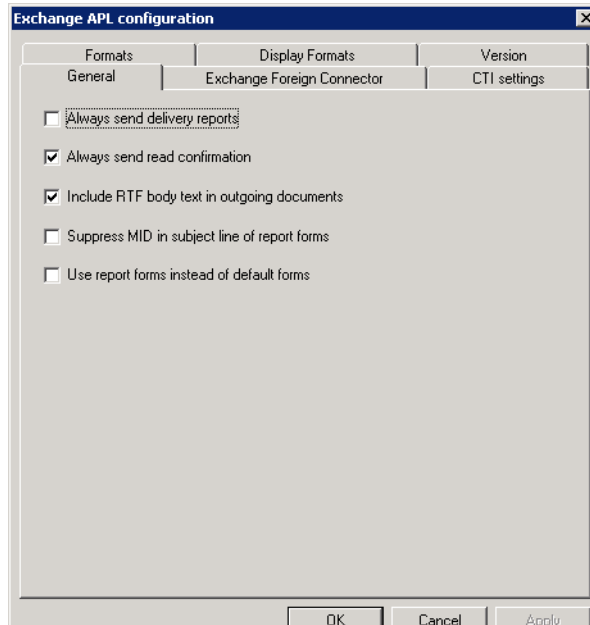
How to edit the settings of the XPR foreign connector:

1. Start the XPR monitor.
2. In the **Modules of <XPR server name>** window expand the branch **<XPR server name>**, then the branch **<Settings>** and finally the branch **ExchApl**.
3. Open the **ExchApl** settings dialog with a doubleclick on **Set Options**.
The configuration dialog of the XPR foreign connector opens.



4.3.5.1 General Tab

On the **General** tab you perform settings for creating and sending delivery reports.



The **Always send delivery reports** option generates a delivery report for messages that originate from Exchange, even when not explicitly asked for. The **Always send read confirmation** option returns a read report to the MRS originator as soon as messages are read on the Exchange server. The originator on XPR side receives a read report as soon as the Exchange user opens the document.

If you activate the **Include RTF body text in outgoing documents** option, a document in Rich Text Format (RTF) is sent as attachment in addition to the normal text representation. RTF is the official data exchange format used by Microsoft for text files. Text files exchanged in this format retain their formatting e.g. font weight, etc. when being transferred between users.

When the **Suppress MID info in subject line of report forms** option is activated, the message IDs in square brackets are omitted from the subject line. The ID display is of no significance to the normal user, but it helps tracking a routing process. Furthermore, IDs are used to assign a report to a message.

NOTE: In case of default reports it is not possible to suppress the message ID display.

Via **Use report forms instead of default forms** XPR confirmation forms are used instead of the normal Exchange default forms. For a more detailed description of the function and installation of XPR reports refer to the *Unify OpenScape Xpressions V7 Server Administration* manual from the **Automatic Report Transmission per Mail** section.

4.3.5.2 Exchange Foreign Connector Tab

The screenshot shows the 'Exchange APL configuration' dialog box with the 'Exchange Foreign Connector' tab selected. The 'Drop directory' field contains '\\<Hub Transport Server>\<Drop Directory>' and the 'Replay directory' field contains '\\<Hub Transport Server>\Replay'. There is a checkbox for 'Multiple Hub Transport Servers' which is currently unchecked. Below it are fields for 'Replay directory (Server 2)', 'Replay directory (Server 3)', 'Replay directory (Server 4)', 'Replay directory (Server 5)', and 'Replay directory (Server 6)', all of which are empty. At the bottom, there is a note: 'Before saving these values the Apl checks for their validity and logs errors otherwise. Changes take effect after Apl restart.' and buttons for 'OK', 'Cancel', and 'Apply'.

On the **Exchange Foreign Connector** tab, in the **Drop directory** and **Replay directory** entry lines, you specify the path to the shares (drop and replay directory) used for the message transport.

NOTE: If this path is not defined yet, the XPR server name is displayed here as default.

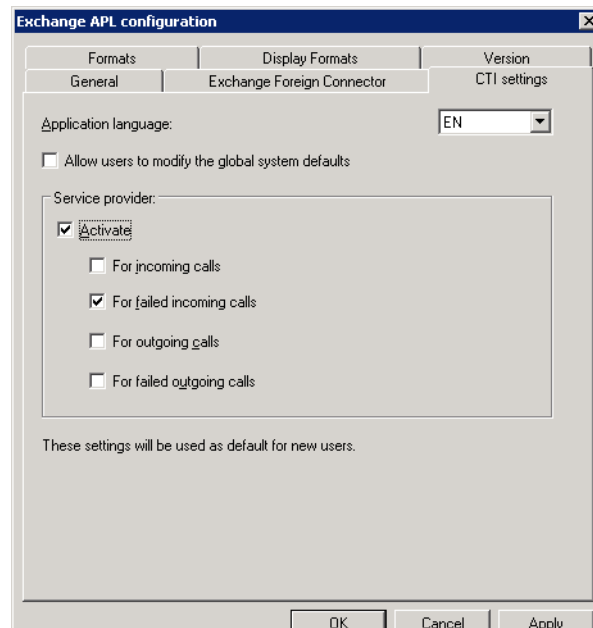
In the **Drop directory** and **Replay directory** specify the path to the shared transport directories according to the following pattern:

- For the **Drop directory**
`\\<Ip address or name of the Exchange server on which the Hub Transport Server operates>\<XPR server name>-<name of the Exchange Server 2007 Mailbox Server Role>`
- For the **Replay directory**
`\\<Ip address or name of the Exchange server on which the Hub Transport Server operates>\Replay`

After you have specified the path click on **Apply** and **OK** to save the modifications.

NOTE: The configuration respectively a modification of the configuration settings does not take effect until the **ExchApl** is rebooted.

4.3.5.3 CTI Settings Tab



On the **CTI settings** tab you find the **global** CTI settings valid for all users. These global defaults may later be customized in the course of the user definition.

Application language

Sets the language to be used in the CTI client dialogs.

Allow users to modify the global system defaults

This option enables all users to change the settings globally defaulted here.

NOTE: The permission to modify global defaults can be individually and belatedly granted as part of the CTI settings on user level. See [Section 4.3.4.1, “CTI settings”](#), on page 116.

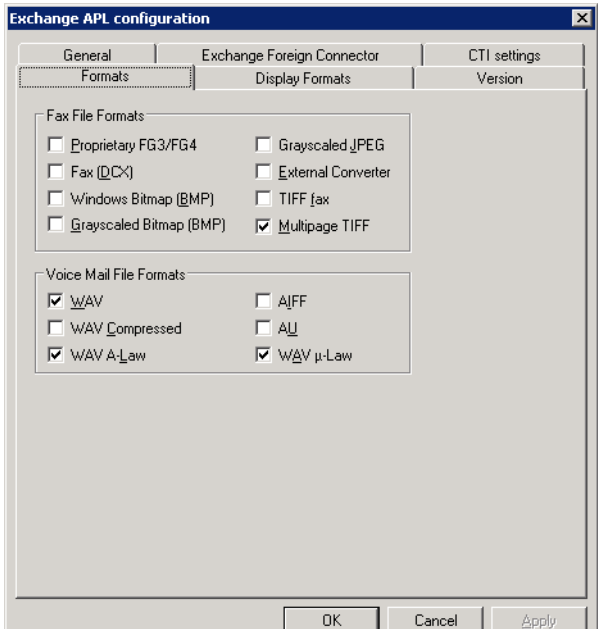
Service provider

The CTI client does not log calls if the program has not been started. Enabling the **Activate** checkbox you can set for all calls that the associated XPR-CTI journal entries are sorted into the corresponding directory via the service provider after the CTI client start.

The behavior can be individually configured for the following call states:

- For incoming calls
- For failed incoming calls
- For outgoing calls
- For failed outgoing calls

4.3.5.4 Formats Tab



On the **Formats** tab you can set the file formats accepted by the XPR foreign connector.

The Exchange client should be able to display these formats of course. Documents received by the XPR server that are not in one of the formats selected in this dialog would be converted into one of these formats prior to being sent to the Exchange gateway.

NOTE: A maximum of one conversion is performed, even if several possible target formats are specified. Here, an internal evaluation comes to bear that performs the “cheapest” conversion from the converter’s point of view.

When using the XPR Outlook extensions, the WAV format must be selected for the voicemail feature.

The following **Fax Formats** are available:

File formats for fax messages	Description
Proprietary FG3/FG4	Proprietary fax format (XPR Viewer).
Fax (DCX)	Multi-page PCX graphic format. Used by Microsoft fax.
Windows Bitmap (BMP)	Individual fax pages are converted in a Windows Bitmap.
Grayscale Bitmap (BMP)	Individual fax pages are converted in a Windows Bitmap, where a trilinear grayscale interpolation is performed.

Table 9 File formats for fax messages

File formats for fax messages	Description
Grayscale JPEG	Fax data are converted in a nine-grayscale JPEG format. This format is suitable for viewing with HTML mail clients.
External Converter	When you select this format, a configurable program is called, which executes a conversion from TIFF in an arbitrary format instead (see info box under this table). When you activate this external conversion, further fax formats must not have been selected beforehand.
TIFF Fax	Single-paged, compressed TIFF fax format.
TIFF multipage	Fax data according to TIFF stand (multi-page).

Table 9 File formats for fax messages

External Converter Support

Selecting this option activates an external converter. You find the preferred Fax2PDF converter in the `AddOn` directory on the product data carrier. For this feature you need to perform the following registry entries under the key:

```
[HKLM\SOFTWARE\PPCOM\mrs\Mrs-Globals\Converter\]
```

TiffToExternalConverter REG_SZ *<Program name with parameters>*

TiffToExternalExtension REG_SZ *<Extension>*

Example of *<Program name with parameters>*:

```
D:\XPR\res\convert\Fax2PDF\Fax2Pdf %1 %2
```

Example of *<extension>*:

```
pdf
```

You find further information about the functions of the external converter in the *Server Administration* manual in Appendix A under the caption: *Document Formats*.

The following **voicemail file formats** are available for selection:

Voicemail File Formats	Description
WAV	Windows Audio Format
WAV Compressed	Compressed Windows Audio Format. This format enables direct compression of voicemails that are routed via the Exchange gateway. Further settings, such as the Audio-Codec used for compression, are performed via the maintenance options in the MTA configuration. The appropriate codec to play-back compressed files is also required on the client computer. Note: Besides the subsequent compression for memory-saving storage on the XPR server, the Codecs setting is also responsible for direct compression. Direct compression is available for Integrated as well as for Unified Messaging and applies with the arrival of a message. It is used for all voicemails transmitted by the XPR MTA, i.e. all voicemails recorded by Forward and Guest Access. Direct compression is not used with messages directly created in Microsoft Exchange by True Unified Messaging. These are all messages recorded in Direct Access.
WAV A-Law	European ISDN-voicemail format.
AIFF	Audio format used predominantly on Apple computers.
AU	Unix audio format.
WAV μ-Law	US ISDN-voicemail format.

Table 10

Voicemail File Formats

4.3.5.5 Display Formats Tab

Via definitions in the **Display Formats** tab you can replace formats for message information defaulted by the XPR system with customer-specific defaults in the Outlook journal **Subject** and **From** column. This setting applies system-wide for all Exchange users receiving XPR voice and fax messages.

From	Subject

To replace the XPR default formats, you need to fill the opposite fields with new format texts, with the generic defaults in the **From** and **Subject** being replaceable with specific defaults.

NOTE: If no configuration is performed here, the standard entries for the **From** and **Subject** columns generated by the XPR server are passed on to Exchange 1:1.

You can set:

- In which of the two Outlook journal columns (**From** and **Subject**) the additional information is to appear.
- For which message types (fax, voicemails or both) the information is to be displayed.
- Which message parameters are to be shown and whether the parameters are to be embedded in an explanatory text.

The top three entry lines are intended for entries in the **From** column in the Outlook journal. The three bottom columns are allocated for the **Subject** column.

If you want to display information for both message types (fax and voicemails), enter the corresponding parameters in the **From:** and **Subject:** entry lines, possibly supplemented with text.

You can display the information separately in the Outlook journal according to fax and voicemails via the **From (Fax)** and **From (Voice)** or **Subject (Fax)** and **Subject (Voice)** entry lines.

NOTE: Please note that entries in these fields will overwrite possible entries in the **From:** and **Subject:** fields, which then become effectless.

Possible parameters include:

Parameter	Description
<i>{originator}</i>	When a message comes in, this parameter is replaced with the XPR originator. Example: <i>FAXG3/01234567</i>
<i>{callername}</i>	When a message comes in, this parameter is replaced with the display name of the originator, provided it has been found in the XPR database. Example: <i>Joe User</i> .
<i>{callernumber}</i>	When a message comes in, this parameter is replaced with the formatted calling number of the caller. Example: <i>447711</i>
<i>{size}</i>	When a message comes in, this parameter is replaced with the number of fax pages or the voicemail message length. Example of fax messages: 2 (number of pages). Example of voicemails: 23 (message length in seconds).
<i>{orgnumber}</i>	When a message comes in, this parameter is replaced with the original calling number of the caller. Example: <i>49123987654</i>
<i>{service}</i>	When a message comes in, this parameter is replaced with the service used for transmitting the document. Example: <i>FAXG3</i>

Table 11 *Parameters for additional XPR Information Display in the Outlook Journal*

Examples:

The entry

{service} mail from "{caller name}" <{caller number}> {size} page(s)

either in the **From:** or **From (Fax):** entry line would generate the following text in the **From** journal column with an incoming fax message:

FAXg3 mail from "Joe User" <0240412345678> 2 page(s)

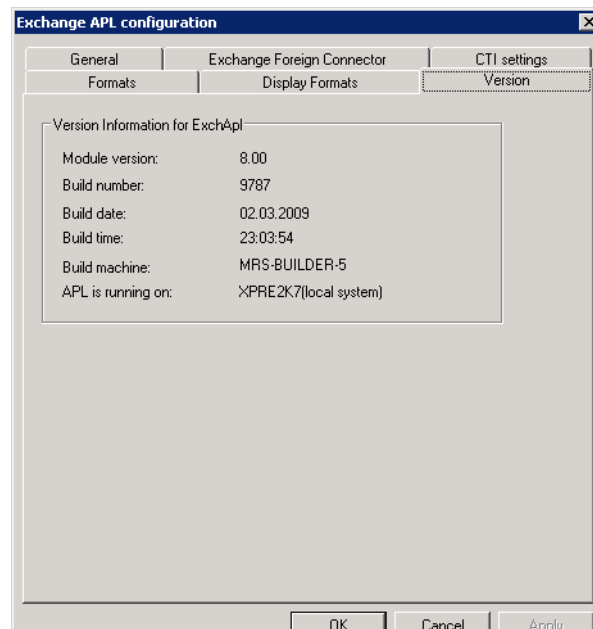
The entry

Voice message from: {caller name} ({caller number}) {size} seconds

either in the **Subject:** or **Subject (Voice):** entry line would generate the following text in the **Subject** journal column in case of an incoming voicemail:

Voice message from: Joe User (0240412345678) 23 seconds

4.3.5.6 Version Tab



The version number of the Exchange APL installed is shown on the **Version** tab. This number should always be entered when reporting errors.

4.4 Multi-Hub Transport Server Support

You can use several hub transport servers to configure a load distribution and to grant high availability. You can connect a maximum of five additional hub transport servers to the system. These servers must have been configured in the network and contain a shared replay directory called **Replay** in the path %ProgramFiles%\Microsoft\Exchange Server\TransportRoles in each case.

IMPORTANT: All hub transport servers additionally connected for this purpose also require access to the drop directory. These additional hub transport servers must therefore be granted the privileges for accessing the drop directory share.

NOTE: You can rename both directories and store them anywhere in the system. If this is desired, adjust the new directory names and the directory paths in the system upon the creation, activation or configuration.

NOTE: You cannot install two XPR Foreign Connectors, e.g. from two different XPR servers, for one Exchange organization.

If you use the multi-hub transport server version, the Exchange server and the XPR server require a commonly used and shared resource for the drop directory. Since only one XPR Foreign Connector can be installed on the XPR server, the drop directory must be on the server that all hub transport and mail servers as well as the XPR server can access.

Depending on the Exchange environment, the drop directory needs to be configured on the following servers:

- If only one mail server is available for several multi-hub transport servers, the drop directory is created on a commonly used and shared resource of the mail server.
- If the mail server is a clustered server with an SAN drive, the drop directory is created on a commonly used and shared resource of the cluster.
- If the mail server is a clustered server without SAN drive, the drop directory is created on a commonly used and shared resource of the XPR server.

You find more detailed information about adjusting the path and sharing the **drop** and **replay directory** in [Section 4.2.6.1, "Creating the Transport Directories"](#), on [page 80](#).

4.4.1 Configuring the Multi-Hub Server Support

How to configure the multi-hub transport support:

1. Install the Exchange connection pretending that only one Exchange Hub Transport server is available. See [Section 4.2.5.5, "XPR Foreign Connector Installation", on page 72.](#)

Besides the mailbox server, select an arbitrary, already existing hub transport server in the Exchange servers' setup dialog. The name of this server is automatically entered as value in the registry key HUBTRANSPORTSERVER.

NOTE: You cannot configure a multi-hub transport support during the setup. This is only possible after the Exchange connection has already been installed. Only then the required **ExchApi** registry branch and the configuration dialog for the **ExchApi** can be accessed on the XPR server.

2. Register all additionally deployed hub transport servers that send messages from the XPR server to the Exchange 2007 system via the Exchange Foreign Connector. The server names of all hub transport servers used are entered in the Exchange system in the **SourceTransportServers** parameter.

Proceed as follows:

- Start the Exchange Server 2007 management shell.
- Enter the following command in the console:

```
Set-ForeignConnector -Identity
<ForeignConnectorIdParameter>
-SourceTransportServers "<DEFAULT hub transport server
name>",
"<name hub transport server 1>", "<name hub transport server 2>",
... "<name hub transport server 5>"
```

You find further information about the console command `Set-ForeignConnector` in the *Microsoft TechNet*:

<http://technet.microsoft.com/en-us/library/bb123789.aspx>

NOTE: The first line of this command is separated from the second line by a blank

```
(...IdParameter> -SourceTransp...).
```

3. Define where you wish to install the drop directory.

- Follow the instructions given in [Section 4.2.6.1, “Creating the Transport Directories”](#), on page 80 to configure this commonly used and shared resource.
- Set the “RootDropDirectoryPath” path of the hub transport server to zero:

```
Set-TransportServer -identity <hub transport server>  
  
-RootDropDirectoryPath ""
```

NOTE: The first line of this command is separated from the second line by a blank

(...port server> -RootDropDi...).

- Repeat this process for the other available hub transport servers.
- Set the complete UNC path of the commonly used and shared drop directory for the Foreign Connector:

```
Set-ForeignConnector -Identity "MrsConnector (<XPR server  
name>  
:<name of the Exchange Server 2007 Mailbox Server role>)"  
-DropDirectory "\\<UNC path to the commonly used and  
shared drop directory>\<XPR server name>-<name of the  
Exchange Server 2007 Mailbox Server role>" or <name of the  
commonly used and shared drop directory>
```

NOTE: The second line of this command is separated from the third line by a blank

(...Server role>)" -DropDirectory "...).

4. Test the previously performed configuration steps. Use Outlook to check whether messages to be sent via the XPR server are delivered to the new drop directory.
5. Start the XPR server.
6. Expand the registry in the HKLM\Software\Wow6432Node\PP-COM\MRS\ExchApl branch and create manually the corresponding key (HUBTRANSPORTSERVER<1...5>) for each additionally used hub transport server (maximum 5). Enter the server name associated to the respective hub transport server as value.
7. Enter the UNC path names of the replay directories additionally used in the **ExchApl** settings dialog.
8. Open the **ExchApl** settings dialog in the XPR monitor via **ExchApl -> Set Options**.

9. Switch to the **Exchange Foreign Connector** tab.
10. Enable the **Multi Hub Transport Server** option. This activates the entry fields for specifying the UNC names of the replay directories additionally used.
11. In the entry fields, specify the UNC path names of the drop directory used.
12. Enter the UNC path names of the replay directories additionally used in the corresponding fields.

The screenshot shows the 'Exchange APL configuration' dialog box with the 'Exchange Foreign Connector' tab selected. The 'General' sub-tab is active. The 'Drop directory' field contains '\\<Hub Transport Server>\<Drop Directory>'. The 'Replay directory' field contains '\\<Hub Transport Server>\<Replay>'. The 'Multiple Hub Transport Servers' checkbox is checked. Below it, there are six 'Replay directory' fields for Server 2 through Server 6, each containing '\\<Hub Transport Server 2>\<Replay>' through '\\<Hub Transport Server 6>\<Replay>'. At the bottom, there is a note: 'Before saving these values the Apl checks for their validity and logs errors otherwise. Changes take effect after Apl restart.' and three buttons: 'OK', 'Cancel', and 'Apply'.

13. Click on **Apply** to save the data.
14. Click on **OK** to close the settings dialog.
15. Reboot the **ExchApl**.

NOTE: By monitoring the drop directory, you can now check whether the XPR server retrieves the messages delivered here, thus whether they are removed from the drop directory.

4.5 Using additional Address Spaces for the Exchange Connectors

4.5.1 Overview

In Exchange organizations where you find two or more XPR kernels that provide a connection to this Exchange environment, you need to assign message transmission to a fixed XPR connector that delivers messages to a specific Exchange server. This avoids addressing the wrong Exchange server, which leads to an increased server load and thus to additional message transport efforts.

Because the XPR Foreign Connector designed for *Exchange Server 2007* is no longer capable of configuring message transport restrictions with the help of user lists, the path must lead here via different address space types.

If several Xpressions servers are to connect a single Exchange organization via connectors, a unique MRS proxy ID, thus an individual address space type, is required for each connector.

The default address space type for each Exchange connector is **MRS**. However, you can assign a different address space type to each Exchange connector per configuration. This restricts the message transmission to the connector for which it is configured.

Example:

Address space definition via EXADDRESSTYPE	Assigned users
MRS1	User 11, user 12, ..., user 1n
MRS2	User 21, user 22, ..., user 2n
...	...
MRSn	User n1, user n2, ..., user nn

Defining the address space type for the single Exchange connectors with assignment to the desired Exchange servers then determines the connector to handle the message transport.

4.5.1.1 Configuration Overview

Required configuration steps:

1. Configuring the address space on the Exchange server
2. Creating the required "Active Directory object" using the `CreateProxyAddr.bat` batch file.
3. Copying the DLLs into the corresponding Exchange directories for creating the proxy addresses.
4. Configuring the e-mail address policies.
5. Adding the required **EXADDRESSTYPE** registry key. You need to configure this registry key for the XPR Foreign Connector (Exch APL) as well as for the Unified Messaging Connector (ExUM APL). The additional address spaces are assigned to the respective connectors via this key.

4.5.2 Configuring additional Address Spaces

4.5.2.1 Configuring the Address Space on the Exchange Server

On the Exchange side you need to set the "AddressSpaces" of the XPR Foreign Connectors in such a way that they correspond to those on the "ExAddressType" Xpressions side.

You need to configure the address space type in Exchange manually via the *Exchange Management Shell* (EMS). In this process you need change the default address space type (**MRS:*;1**) on all *Exchange servers 2007* for the second and all further connectors.

The following address space types are assigned to the additional connectors on the Exchange servers:

XPR Server	MRS Address Space Type	Exchange Address Space Value
For the first server	MRS1	MRS1:*;1
For the second server	MRS2	MRS2:*;1
...	...	...
For the n-th server	MRSn	MRSn:*;1

Use the *Exchange Management Shell* command prompt to execute the following command on the Exchange servers for configuring the assignment:

```
Set-Foreignconnector -Identity "MrsConnector (XPRESSIONS:EXCHANGE)" -AddressSpaces "MRSx:*;1"
```

MRS_x with _x= 1, 2, 3,... continually for each additional XPR connector for labeling the connectors uniquely

NOTE: You find additional information about this topic under:
<http://technet.microsoft.com/en-us/library/bb123789.aspx>

4.5.2.2 Creating the “Active Directory Object”

To define a new address space type, a batch file that creates this address space type must be started once for each additional connector.

How to create a new address space type for another connector in the Active Directory:

1. Log on to the Xpressions server with the account under which the Exch APL runs.

NOTE: For this action, the service account must be a domain account that has administrator privileges on the Exchange server.

2. Start the batch file `CreateProxyAddr.bat`
After installing the XPR connectors you find this batch file in the setup directory of the Xpressions server under:

... \xpr\bin

Example:

```
CreateProxyAddr "DC=<MYDOMAIN,DC=COM>" Temp.txt MRS1
```

Replace `<MYDOMAIN,DC=COM>` with the given domain information of the relevant customer environment.

The `MRS1` parameter must match the address space type created in the previous step.

NOTE: You can enter any file name under `Temp.txt`. Merely the `.txt` file extension must be kept. This is a temporary file created by the batch file as auxiliary file. You therefore need not create this file manually.

4.5.2.3 Copying the DLLs into the corresponding Exchange Directories

Creating the proxy addresses must now be harmonized with the new address space type.

This requires copying the DLL that generates the proxy addresses into a new directory. To do this, copy the content of the directory

```
...\Program Files\Microsoft\ExchangeServer\Mailbox\address\MRS
```

into another directory to be newly created:

```
...\Program Files\Microsoft\Exchange Server\Mailbox\address\MRSx
```

NOTE: MRSx with x= 1, 2, 3,... continually for each additional XPR connector for labeling the connectors uniquely. For example, MRS1 for the first XPR connector, MRS2 for the second etc.

Example:

```
...\Program Files\Microsoft\Exchange Server\Mailbox\address\MRS1
```

```
...\Program Files\Microsoft\Exchange Server\Mailbox\address\MRS2
```

```
...
```

```
...\Program Files\Microsoft\Exchange Server\Mailbox\address\MRSn
```

4.5.2.4 Configuring the e-mail Address Policies

The connector e-mail address policy concerned must be adjusted for each new address space type.

Proceed as follows:

1. Start the *Exchange Management Console (EMC)*.
2. Open the configuration dialog for the e-mail address policies

NOTE: You reach this dialog via: **Microsoft Exchange > Organization Configuration > Hub Transport > E-mail Address Policies.**

3. Enter a new address space type according to the sample of the available default address space type **MRS**.

Example:

E-mail address: **@MRS**

E-mail (address)type: **MRS1**

NOTE: If desired, you can remove the default e-mail address policy after adding a new custom address space type (for example **MRS1**). This will not affect this feature's function.

4.5.2.5 Adding the required EXADDRESSTYPE registry key.

The address space types that associate the XPR connectors must be activated on every XPR server. A registry key added to the corresponding registry path is used for this purpose.

For the XPR Foreign Connector (Exch APL):

HKLM\SOFTWARE\Wow6432Node\PP-COM\MRS\ExchAp1

For the XPR True Unified Connector (ExUM APL):

HKLM\SOFTWARE\Wow6432Node\PP-COM\MRS\ExUMAp1

For the Exch APL

EXADDRESSTYPE [REG_SZ]

Default:	-
Possible values:	<address space <i>name</i> >
Example:	MRSn, with n = 1, 2, 3, ...

If several XPR servers and consequently several Exchange connectors are connected to an Exchange environment, this registry key is required for differentiating the Exchange foreign connectors. Assigning special address space names then optimizes message transmission. The foreign connectors are labeled by consecutive numbering.

For the ExUm APL

EXADDRESSTYPE [REG_SZ]

Default:	-
Possible values:	<address space <i>name</i> >
Example:	MRSn, with n = 1, 2, 3, ...

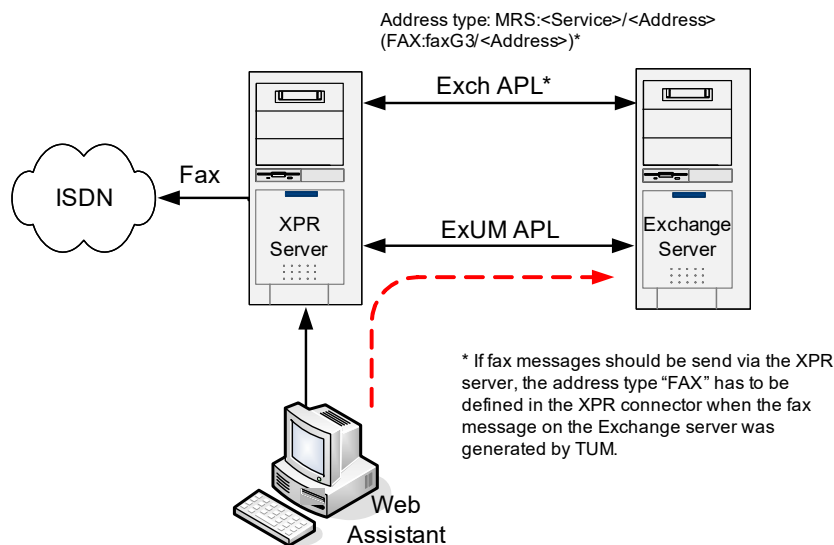
If several XPR servers and consequently several Exchange TUM connectors are connected to an Exchange environment, this registry key is required for differentiating the Exchange TUM connectors. Assigning special address space names then optimizes message transmission. The TUM connectors are labeled by consecutive numbering.

NOTE: Registry entry modifications require a reboot of the concerned Exchange Apl to take effect.

4.6 Fax Message Addressing

When addressing fax messages, the address space in the Exchange foreign connector may have to be extended by the “FAX” address type.

This is always required if fax messages were directly generated on the Exchange server and are to be transmitted via the XPR server. Fax messages are directly stored on the Exchange server e.g. if they are generated by a client that transmits the message by TUM transaction via the ExUM APL to the Exchange server (for example *Web Assistant*).



4.6.1 Definition of the “FAX” Address Type

How to configure the “FAX” address type:

1. Start the *Exchange management shell*.
2. Enter the following command in the command prompt:

```
Set-ForeignConnector "MrsConnector (<XPR-server name>:<name of the Exchange Server 2007 Mailbox Server Role>)"
-AddressSpaces "MRS:*;1","FAX:*;1"
```

The “FAX” address type is now defined for fax transmission via the XPR server.

4.7 Adding and assigning the MRS E-Mail Address Type retrospectively

NOTE: As of Exchange Server 2007 the distribution groups support the **sAMAaccountName**. As a result, all Exchange users with this attribute are replicated as full XPR users to the XPR server. This causes problems when assigning the MRS address type and the number of replicated users exceeds the number of available user licenses. Therefore, the number of user groups to be replicated may have to be restricted beforehand via the LDAP configuration.

If no default policy has been created for the MRS address type upon the installation or further address types are required, this must be done in a retrospective procedure. The MRS address type is required for assigning messages arriving via the XPR server to Exchange users.

How to retrospectively add and assign the MRS address type:

1. Start the Exchange management console.
2. In the left section of the management console expand the object group **Organization Configuration**.
3. From the list of organization objects select **Hub Transport**.
The middle section of the management console now displays the Hub Transport objects.
4. In the middle section of the management console switch to the **E-mail Address Policy** tab.
5. Select the **Default Policy** entry. The right section of the management console now displays the default policy editing features.

NOTE: You can also use the **New E-mail Address Policy** feature to specify a new policy for creating and assigning the MRS address type via this policy.

6. Select **Edit** via the actions section to add the MRS address type to this policy. The wizard for editing the policy will then open with the first dialog **Introduction**.
7. Since no settings need to be made here, push the **Next >** button in this dialog. The **Conditions** dialog opens.
8. Since no settings need to be made here, push the **Next >** button in this dialog. The **E-Mail Addresses** dialog opens.
9. Use here the selection button (next to the **Add** button) to select **Custom Address** for the MRS address.
The Custom Address entry mask opens.

10. In the **E-mail address** field specify the address description (e. g. **@MRS** or, if additional address descriptions are required, **@MRS1** etc.).
11. In the **E-mail type** field specify the address type **MRS**.
12. Complete your entries with **OK**.
You return to the **E-Mail Addresses** dialog. The new address type is displayed here under **Address**.
13. In the **E-Mail Addresses** dialog click on **Next >**.
The **Schedule** dialog opens.
14. In the **Schedule** dialog set the time when the newly defined address type is to be adopted by the system. Then click **Next >**. The **E-mail Address Policy** dialog opens.
15. In the **E-mail Address Policy** dialog click the **Edit** button to continue the address type definition.
The **Completion** dialog opens.
16. In this dialog you can trace the address policy update. When the process is complete, click the **Finish** button.

The definition and assignment of the MRS E-Mail address type is now complete.

4.8 Security Settings for Installation and Live Operation of the E2k7 APL and ExUM APL

To ensure maximum security, various security settings can be reduced **after** the installation for real operation. This section describes which privileges are required for the installation and which privileges can be restricted for real operation.

IMPORTANT: To accomplish its tasks the XPR Exchange connector uses MAPI access. Since Microsoft have not revealed the MAPI access privilege hierarchy, the connector function can only be granted under an account with Exchange full-admin privileges. The privilege restrictions described in the following have been tested on a system with the default policy by Microsoft. After modifying the default security policy by service packs or corporate security adaptations, the below privilege restrictions may lose their validity.

The test environment is composed of the following elements:

- Windows Server 2003 Enterprise SP2.
- Exchange Server 2007 Enterprise Edition x64.
- Exchange Mailbox Server Role and Exchange Hub Transport Server Role are installed on two physically separated servers.
- The installation is performed with the default security policy

With the installation description for each single XPR component the required privileges are named as well.

4.8.1 Requirements

The following tools are required for displaying and configuring the privileges:

- **ADSI Edit** (contained in the Microsoft Support Tools on the product data carrier for the Windows installation).
- **Exchange management console** and/or **Exchange management shell** on the product data carrier for the Exchange installation.
- The administration program **Active Directory Users and computer**.
- The administration program **Local Security Settings** (from the Windows Admin Pack, if you administer remotely from a workstation).

Definitions

<i><organization></i>	Wildcard for the name of your Exchange organization.
<i><Domain></i>	Wildcard for the name of your domain.
<i>APLSRV</i>	Name of the server on which the ExchApl runs as service.
<i>MBSRV</i>	Name of the Exchange server on which the Mailbox Server Role is installed.
<i>HTSRV</i>	Name of the Exchange server on which the Hub Transport Server Role is installed.

4.8.2 Privileges for the Exch APL Installation

Creating the XPR service account

Generate a user entry in your domain. This user account is required as service account for the Exch APL. In the following we will call this account USER. This USER needs to have a mailbox.

Microsoft demands this USER to be member of the group of domain administrators for the required MAPI access. Therefore, add this USER to the domain administrator group.

Local administrator

Promote the USER on the XPR server, on the *MBSESV* and on the *HTSRV* to local administrator.

NOTE: You must be domain administrator for installing the Exch APL. Only then you are entitled to check whether the USER is a member of the domain. If you do not have the corresponding privilege, the installation will fail.

The USER must be assigned further special privileges on the XPR server. This is required for the services to work correctly. Via **Start > Programs > Administrative Tools > Local Security Policy** open the **Local Security Settings** dialog. Select **Local Policy > User Rights Assignment** and assign the corresponding privileges to the USER. The following privileges are to be assigned:

- “Logon on as a service” **1
- “Act as part of operation system” ¹
- “Backup files and directories” ¹
- “Restore files and directories” ¹
- “Logon as a batch job” ¹
- “Adjust memory quotas for a process” ¹

Exchange administrator

Promote the USER to “Exchange administrator with Read Privilege Role”. This privilege is required on the Mailbox Server Role as well as on the Hub Transport Server Role.

This setting is required for reading the Exchange objects properties.

1. Such privileges are set with the connector installation. They are also required for the ExUM APL.

MRSProxy64.dll (optional for manual creation)

If you want to use the **MRS Proxy address generation** function, the USER requires “full access” to the Exchange directory \\MBSRV\address. Share this folder with the USER for this purpose (sharing permissions).

Address templates

For the address templates (407 German or 409 English) the USER must have the privilege to “create address template objects” and to “delete address template objects”. To assign these privileges start ADSI Edit and switch to the directory:

```
CN=407|CN=409, CN=Address-Templates, CN=Addressing,  
CN=<Organization>, CN=Microsoft Exchange, CN=Services,  
CN=Configuration, DC=<Domain>.
```

Open the properties dialog here and switch to the **Security Settings** tab. Add the USER via **Add** to the list displayed. Click on the **Advanced** button to change the privilege and assign the “Create address template objects” and “Delete address template objects” privileges to the USER. In the entry line select **Apply onto** “This object only”.

Address types (optional for manual creation)

Creating address types requires the privileges “Create addr type objects” and “Delete addr type objects”. To assign these privileges start ADSI Edit and switch to the directory:

```
CN=Address-Types, CN=Addressing, CN=<Organization>, CN=Microsoft  
Exchange, CN=Services, CN=Configuration, DC=<Domain>.
```

Open the properties dialog here and switch to the **Security Settings** tab. Add the USER via **Add** to the list displayed. Click on the **Advanced** button to change the privilege and assign the “Create addr type objects” and “Delete addr type objects” privileges to the USER. In the entry line select **Apply onto** “This object only”.

Default policy (optional for manual creation)

Adding address types to the default policy requires the read and write privilege. To assign these privileges start ADSI Edit and switch to the directory:

```
CN=Default Policy, CN=Recipient Policies, CN=<Organization>,  
CN=Microsoft Exchange, CN=Services, CN=Configuration,  
DC=<Domain>.
```

Open the properties dialog here and switch to the **Security Settings** tab. Assign the USER read and write privileges here.

MRS container object (1)

To create the MRS container object the USER requires the “Create container objects” privilege. To assign this privilege start ADSI Edit and switch to the directory:

```
CN=<Organization>, CN=Microsoft Exchange, CN=Services,  
CN=Configuration, DC=<Domain>.
```

Open the properties dialog here and switch to the **Security Settings** tab. Add the USER via **Add** to the list displayed. Click the **Advanced** button to change the privilege and assign the USER the “Create container objects” privilege. In the entry line select **Apply onto** “This object only”.

NOTE: As option, you can simultaneously grant the privilege to “Delete container objects” at this point.

MRS container object (2)

Creating the MRS container object additionally requires the privileges “Create directory synchronization objects” and “Delete directory synchronization objects”. To assign these privileges start ADSI Edit and switch to the directory:

CN=<Organization>,CN=Microsoft Exchange, CN=Services,
CN=Configuration, DC=<Domain>.

Open the properties dialog here and switch to the **Security Settings** tab. Add the USER via **Add** to the list displayed. Click on the **Advanced** button to change the privilege and assign the USER the “Create directory synchronization objects” and “Delete directory synchronization objects” privilege. In the entry line select **Apply onto** “Child objects only”.

MRS connector object

Creating the MRS connector object requires the “Create all child objects ” and “Delete all child objects” privileges. To assign these privileges start ADSI Edit and switch to the directory:

CN=Connections, CN=<RG>, CN=Routing Groups, CN=<AG>,
CN=Administrative Groups, CN=<Organization>, CN=Microsoft
Exchange, CN=Services, CN=Configuration, DC=<Domain>.

Open the properties dialog here and switch to the **Security Settings** tab. Add the USER via **Add** to the list displayed. Click on the **Advanced** button to change the privilege and assign the “Create all child objects” and “Delete all child objects” privileges to the USER. In the entry line **Apply onto** select “This and all child objects”.

MRS settings object

The MRS settings object serves as storage location for the connector settings and other XPR settings for the connector. First, it must be defined. The USER of this MRS settings object must then be assigned additional privileges for accessing this object. Start the ADSI Edit and switch to the directory:

CN=Microsoft Exchange, CN=Services, CN=Configuration, DC=<Domain>

Generate a new object “MRS” (object class = container) here.

Open the properties dialog here and switch to the **Security Settings** tab. Add the USER via **Add** to the list displayed. Push the **Advanced** button and assign the USER the following privileges:

- “List Contents”, “Read all properties” and “Write all properties”
- “Delete”, “Read permissions” and “Modify permissions”
- “Create all child objects” and “Delete all child objects”

In the entry line **Apply onto** select “This and all child objects”.

With these privileges the XPR component “Exch APL” can be installed via the XPR setup.

4.8.3 Privileges for the ExUM APL Installation

To set up the ExUM APL the USER must be promoted from domain user to domain administrator.

Subsequently, the ExUM APL can be installed by the XPR setup.

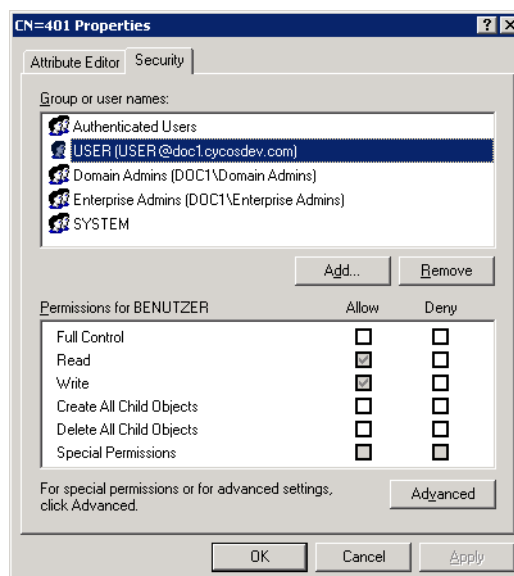
4.8.4 Privileges for the MMC Snap-in Installation

The installing user requires the privileges for modifying the AdminPropertyPages. Otherwise the installation will fail. To check this, start ADSI Edit and change to any directory under DisplaySpecifiers. For example:

CN= <401>, CN=DisplaySpecifiers, CN=Configuration, DC=<Domain>

Open the properties dialog here and switch to the **Security Settings** tab. Check whether the installing user has this right. If not, make the corresponding modifications.

read [inherited] & write [explicit]



Modify the privileges for all speech containers on the `DisplaySpecifiers` level. When you assign the privilege, select “This object and all child objects” under **Apply to**. The rights will be inherited by setting the option “Apply this permission to objects and/or containers within this container only”.

4.8.5 Privilege Restrictions for Live Operation

4.8.5.1 General Information

The USER can be relegated to the domain user privilege for operating the ExUM APL.

IMPORTANT: If you want to install an update, turn the restricted privileges into the state in which they were “before the installation”. After the update you can restrict the privileges again.

4.8.5.2 MRS Connector Settings

MRS connector settings (1)

The following setting is only required if you want to restrict the privilege assignment for the **MRS Settings Object** (see [Section 4.8.2, “MRS settings object”, on page 146](#)). Start the ADSI Edit and switch to the directory:

```
CN=APLSRV:MBSRV, CN=MRS,CN=Microsoft Exchange, CN=Services,  
CN=Configuration, DC=<Domain>
```

Open the properties dialog here and switch to the **Security Settings** tab. Assign the USER the following privileges:

read [inherited] & write [explicit]

MRS connector settings (2)

This privilege is only required to save administrative settings group-wide. Start the ADSI Edit and switch to the directory:

```
CN=Admin Group (Exchange Administrative Group (FYDIBOHF23SPDLT)),  
CN=MRS, CN=Microsoft Exchange, CN=Services, CN=Configuration,  
DC=<Domain>
```

Open the properties dialog here and switch to the **Security Settings** tab. Assign the USER the following privileges:

read [inherited] & write [explicit]

MRS connector object

The following privilege is required to save connector-specific settings. Start the ADSI Edit and switch to the directory:

CN=MrsConnector (APLSRV:MBSRV), CN=Connections, CN=Exchange Routing Group< (DWBGZMFD01QNBJR), CN=Routing Groups, CN=Exchange Administrative Group (FYDIBOHF23SPDLT), CN=Administrative Groups, CN=<Organization>, CN=Microsoft Exchange, CN=Services, CN=Configuration, DC=<Domain>

Open the properties dialog here and switch to the **Security Settings** tab. Assign the USER the following privileges:

Full control [explicit]

Privilege settings can be withdrawn after the installation for the following objects:

• MRS Proxy.dll	• MRS container (1)
• Address template	• MRS container (2)
• Address types	• MRS connector
• Default policy	• MMC Snap-in

All other privileges are required for operating the Exch APL.

4.8.5.3 Assigning the privilege of operating Exch Apl service to any user

In environments where operating the Exch Apl service with “Local Administrator” privileges via the service account is not desired, this privilege can be assigned to another user after the installation. This is necessary, because the Apl does not start anymore after the withdrawal of the “Local Administrator” privilege.

How to assign privileges necessary for starting the Exch Apl service to a user who does not have administrative privileges:

1. Download the **SubInACL** (SubInACL.msi) via the following link:
<http://www.microsoft.com/en-us/download/details.aspx?id=23510>
2. Start SubInACL.msi on the system on which you wish to assign the privileges.
3. Start the command line by entering the **cmd** command in the **Start > <Search programs and files>** input line and pushing the enter key.
4. Switch in the command line to the directory
C:\Program Files (x86)\Windows Resource Kits\Tools>

XPR and Microsoft Exchange Server 2007

Security Settings for Installation and Live Operation of the E2k7 APL and ExUM APL

5. Edit the Exchange components
Microsoft Exchange Transport (MSEExchangeTransport)
Microsoft Exchange System Attendant (MSEExchangeSA)
Microsoft Exchange Information Store (MSEExchangeIS)
according to the following pattern:

```
subinacl.exe /service MSEExchangeSA/grant=<domain>\<service account>=SEL  
subinacl.exe /service MSEExchangeIS/grant=<domain>\<service account>=SEL  
subinacl.exe /service MSEExchangeTransport /grant=<domain>\<service account>=SEL
```

You find further details on using `SubInACL.exe` under the following link:

<http://support.microsoft.com/kb/325349>

4.8.5.4 Privilege Overview

Topic	Privilege	Restrictable after the installation	Required for	
			TUM	Exch APL
Configuring a user pool		No	•	•
Local administrator	Inclusive the local security policies	Yes	• *	•
MrsProxy.dll	Sharing the ... \Exchsrvr \ADDRESS folder	Yes		•
Mailbox stores	send as & receive as	No	•	•
Address templates (407 409)	Template generation	Yes		•
Address types	Address type generation	Yes		•
Default policy	Read & write	Yes		•
MRS container (1)	Container object generation	Yes		•
MRS container (2)	Generating & deleting the Directory Synchronization Object	Yes		•
MRS connector	Generating & deleting all child objects	Yes		•
MRS settings object	Creating the XPR object	No		•
MRS connector settings (1)	Read & write	No		•
MRS connector settings (2)	Read & write	No		•
MRS connector settings (3)	Full access	No		•
*) requires special settings. See the explanations.				

Table 12 Privilege Overview

4.9 Migration

NOTE: Users who deployed Integrated Messaging (mailbox replication) so far must be switched to True Unified Messaging users. The users with Integrated Messaging will otherwise only be able to work as voice-only users, since they can only deploy the mailbox on the XPR server.

How to migrate an XPR server from an existing connection to *Exchange Server 2003* to a connection to *Exchange Server 2007*:

1. Uninstall the existing connector (E2kApl) and, if installed, the ExUM Apl. To do this, use the **Modify** option from the XPR server setup.

NOTE: If the ExUM Apl is also installed on the system, it must be uninstalled, since the TUM connection must be established to the new *Exchange Server 2007*. It will later be installed again in the E2k7 Apl setup.

IMPORTANT: In case of this system modification the E2k7 Apl must not be simultaneously selected for installation. The E2k7 Apl setup must be performed later in a separate step.

2. Uninstall the *Exchange system manager* that supplied the required CDO for the *Exchange Server 2003* connection.
3. Install the **MAPICDO**. Because the *Exchange System Manager* cannot be used in *Exchange Server 2007* any more, the *Microsoft Collaboration Data Object* (CDO) must be installed on the XPR server manually.

The following file is required to install the connectors for the *Exchange Server 2007* connection:

ExchangeMapiCdo.EXE

This file complies with all requirements as regards MAPI and CDO for the **ExchApl** and **ExUMApl**.

The ExchangeMapiCdo.EXE setup file provided by Microsoft for this purpose can be downloaded from the following website:

<http://www.microsoft.com/downloads/details.aspx?FamilyID=e17e7f31-079a-43a9-bff2-0a110307611e&DisplayLang=en>

4. Install the new XPR Foreign Connector (E2k7Apl) **and** the ExUM Apl. To do this, use the **Modify** option from the XPR server setup.

4.10 Integration in Hosted *Exchange* 2007

IMPORTANT: When planning the *XPR* setup we urgently recommend to discuss the following requirements with the provider to ensure that the provider is willing and able to meet such requirements.

The following requirements must be met for integrating an *XPR* server in Hosted Exchange Server 2007:

- The *XPR* server is installed at the customer's and not on the provider side. Thus, it does not share its location with Exchange.
- An *XPR* satellite, on which the connectors run **within the Exchange domain** on the provider side, must be installed.

NOTE: This does not require a physical server. A virtual server is sufficient.

- This satellite must have been connected to the *XPR* kernel computer in the customer domain. This connection requires:
 - A VPN connection or a similar network connection between the satellite and the *XPR* kernel computer.
 - Data traffic on this connection must be allowed in both directions to the destination ports 137, 138, 139, 445 and 13010.
- The services on the satellite and on the *XPR* kernel computer must be able to access the respectively other computer. In other words, either the domains must trust each other or workgroup authentication must be reverted to.

If you use workgroup authentication, execute the following sub-steps:

1. Create a local user on the *XPR* kernel computer with the same user name and password that is specified for the domain user account. This user name and password is used for the services of the Exchange satellite.
2. Add this user account to the group of local administrators.
3. Execute the sub-steps 1. and 2. for the reverse direction. That means, create a local user on the satellite with the same user name and password that is specified for the domain user account of the services on the *XPR* kernel computer. Add this user account to the group of local administrators.
4. Open **Start > Control Panel > Administrative Tools > Local Security Policy > Security Settings > Local Policies > Security Options** and verify that the entry **Network access: Sharing and security model for local accounts** has value **Classic - local users authenticate as themselves**.

4.11 Troubleshooting

4.11.1 Restrictions for MAPI Sessions with Exchange 2007

With *Microsoft Exchange Server 2007* problems may occur because of increased restrictions for MAPI sessions, as the number of different object types per MAPI session has been restricted. For example, the maximum number of objects of the type "objtStream" possible in a MAPI session has been restricted to 250. If the maximum value of one of the object types used is reached, the Exchange server does not reply to further requests. I.e. no messages can be opened, sent or processed in any other way. Therefore we urgently recommend to increase the respective registry values.

For further information on occurring problems and how to implement a solution please refer to the *Microsoft Exchange Server 2007* information pages under:

[http://technet.microsoft.com/en-us/library/bb676486\(EXCHG.80\).aspx](http://technet.microsoft.com/en-us/library/bb676486(EXCHG.80).aspx)

5 XPR and *Microsoft Exchange Server 2010*

5.1 General Considerations

5.1.1 Changes with *Exchange Server 2010*

Exchange Server 2010 is based on version *Exchange Server 2007*. Compared to its precursor, *Exchange Server 2010* was further extended and improved.

Please note the following general system-property novelties:

- *Exchange Server 2010* is shipped exclusively as 64-bit version. The 32-bit evaluation version is no longer available.
- *Exchange Server 2010* runs only on the operating system *Windows Server 2008* or *Windows Server 2008 R2*: Standard as well as Enterprise can be used as version.
The domain structure in which the *Exchange Server 2010* shall be integrated need not be *Windows Server 2008*-based, though.
- There is a new privilege model in *Microsoft Exchange Server 2010*. This privilege model is called *Role Based Access Control* (RBAC). A new method to assign privileges to users of an organization in this new privilege model is to group users in so-called *Management Role Groups*.

5.1.2 The XPR Foreign Connector for *Exchange Server 2010*

The XPR Foreign Connector for *Exchange Server 2010* was developed from a modification of the XPR *Foreign Connector for Exchange Server 2007*. Its executable file is therefore also called `E2k7Ap1.exe`. You find this file in the `\bin` directory of the XPR server. The name of the new Foreign Connector in the XPR monitor still reads **ExchAp1**.

The XPR Foreign Connector is required for “store-and-forward” operation. It delivers the messages received via the XPR server to the Exchange users and transmits the Exchange server messages to be sent via the XPR server.

To this, a logical connection is established between the XPR server and the Exchange modules “Mailbox Server Role or Database Availability Group and “Hub Transport Server Role” via the XPR Foreign Connector.

The connection to the Exchange Mailbox Server Role is required for opening a MAPI connection to resolve addresses.

The connection to the Exchange Hub Transport Server Role serves for transporting messages from/to the XPR server.

NOTE: In case of a monolithic *Exchange Server 2010* environment structure no differentiation needs to be made between Mailbox Server Role and Hub Transport Server Role. In this case the Foreign Connector is connected to the computer that hosts the *Exchange server 2010*.

Message transport

Messages to be sent by Exchange users via the XPR server are stored in the **Drop Directory**.

The messages to be sent from the XPR server to users on the Exchange server are stored in the **<Replay Directory>**.

In both cases such messages are SMTP messages with the file extension `.eml`, and they are buffered in the above directories until their final delivery.

The transport directories are created on the server that has the Hub Transport Server role.

NOTE: In case of an *Exchange Server 2010* with a role distribution among several servers, the Replay Directory must be reachable via a UNC path in the network. Only then this directory can be accessed from all Hub Transport servers.

You find a detailed description of the transport directory configuration in [Section 5.2.7.1, “Creating the Transport Directories”, on page 198](#).

5.1.3 The XPR True Unified Messaging Connector

Messages are exclusively retrieved via direct access to the Exchange mailboxes by means of the **ExUMApi**. Mailbox replication is not supported. **Integrated Messaging (IM)** as XPR server operation mode is thus not possible anymore.

NOTE: Exchange users hidden from global and other Exchange address books via the **Hide from Exchange address lists** cannot access their mailboxes via the ExUMAPL because of the then incomplete user information. The ExUMAPL indicates this via an error message.

The XPR True Unified Messaging Connector must establish a connection from the XPR server to the Client Access Server Role or Client Access RoleArray Server Role.

NOTE: In case of a monolithic *Exchange Server 2010* environment structure no differentiation needs to be made between Mailbox Server Role and Hub Transport Server Role. In this case the XPR True Unified Messaging Connector is connected to the computer that hosts the *Exchange server 2010*.

5.1.4 Administering the *Exchange Servers 2010*

You perform the management works for *Exchange Server 2010* using the following tools:

- The XPR Foreign Connector is now exclusively configured via the **ExchApl** settings dialog in the XPR monitor.
- Users are still administered via the MMC Snap-in extension for Active Directory Users and Computers, which was already used for *Exchange Server 2003*. The Snap-in is installed on the system from which users are configured. How to proceed is described in [Section 5.2.6.6, “Installation of the MMC Snap-in”](#), on page 193.

5.1.5 Connection to Exchange Server 2010 DAG and/or Exchange Server 2010 CAS Array

Up to now, only the connection of the XPR connectors (ExUM Apl and Exch Apl) to a monolithically installed *Exchange Server 2010* (all server roles on one server) as well as connecting a server on which the *Exchange Client Access Server Role* (CAS Server Role) is installed separately is supported. Now, you can use the XPR connectors in the following application environments also:

- *Database Availability Group (DAG)*. In the application environment provided by *Exchange Server 2010* several mailbox servers are combined to a cluster. This improves the mailbox availability in case of disorders significantly. The XPR Foreign Connector supports this application scenario.
- *Client Access Server Array (CAS Array)*. Using this *Exchange Server 2010* feature you can configure load balancing. You can enable this load balancing in hardware or software *Windows Load Balancing (WNLB)*. The XPR True Unified Messaging Connector supports this application scenario. You find notes on *WNLB* on the *Microsoft* web site:

<http://technet.microsoft.com/en-us/library/ff625247.aspx>

The following application environments and their combinations are supported:

- *Exchange Server 2010 DAG*
- *Exchange Server 2010 DAG with Exchange Server 2010 CAS*
- *Exchange Server 2010 CAS array*
- *Exchange Server 2010 DAG with Exchange Server 2010 CAS Array*

IMPORTANT: Please note the deviations from the default setup routine if a connection to one of these application environments shall be used.

5.1.5.1 Connection to an Exchange *Database Availability Group*

The XPR Foreign Connector (Exch APL) supports connecting an *Exchange Server 2010* with *Database Availability Group (DAG)*.

The steps required for installing the XPR Foreign Connector at an *Exchange Server 2010* with *Database Availability Group (DAG)* are detailed in [Section 5.2.6.5, “XPR Foreign Connector Installation”, on page 185](#).

5.1.5.2 Connection to an Exchange *Client Access Server Array*

The XPR True Unified Messaging Connector (ExUM APL) supports connecting an *Exchange Server 2010* with *Client Access Server Array (CAS Array)*.

NOTE: Depending on the installed product version, the XPR hotfix EXUMAPL-803FR2-14001 or later must be installed first. If you use an XPR version as of XPR V6 R2 FR3 you need not install the hotfix.

The steps required for installing the XPR True Unified Messaging Connector at an *Exchange Server 2010* with *Client Access Server Array (CAS Array)* are detailed in [Section 5.2.6.4, “Installing the XPR True Unified Messaging Connector”, on page 179](#).

5.2 Installation

5.2.1 General Considerations

This XPR version allows using the `E2K7Ap1.exe` and the `ExUmAp1.exe` in adjusted version for *Exchange Server 2007* as well as for *Exchange Server 2010*. During the connector installation, the installing user activates a radio button to decide for which Exchange server version the setup is to occur.

During the XPR Foreign Connector installation all required properties are set and the APL service is configured. In addition, the `Proxy.dll` is installed, the MRS address type defined and various address templates for fax, voicemail etc. are provided for selection during the setup process.

5.2.2 Exchange Server 2010

You need to set up the XPR Exchange Foreign Connector on an *Exchange Server 2010* with the Update Rollup 1 (KB976573). You can download the update file `Exchange2010-KB976573-x64-en.msp` provided by Microsoft for this purpose from the following web page:

<http://www.microsoft.com/downloads/details.aspx?FamilyID=371add31-d7a0-4c8b-8325-a6fced2d05e6&displaylang=en>

5.2.3 Preparations

The following preparatory steps must be executed to set up the XPR Foreign Connector:

- **For migration scenarios only**
Users who deployed Integrated Messaging (mailbox replication) so far must be switched to True Unified Messaging beforehand. The users with Integrated Messaging will otherwise only be able to work as voice-only users, since they can only deploy the mailbox on the XPR server.
- **MAPI and CDO**
Because the *Exchange System Manager* cannot be used in *Exchange Server 2010* any more, the *Microsoft Collaboration Data Object* (CDO) must be installed on the XPR server manually.

Installing the **ExchApl** and **ExUMApl** requires the `ExchangeMapiCdo.EXE` file in version 6.5.8153 or later.

This file complies with all requirements as regards MAPI and CDO for the **ExchApl** and **ExUMApl**.

You find information about the installation and the setup file `ExchangeMapiCdo.EXE` provided by Microsoft for this purpose on the following web page:

<http://www.microsoft.com/downloads/details.aspx?FamilyID=e17e7f31-079a-43a9-bff2-0a110307611e&DisplayLang=en>

- **Configuring a service account**

Configure a user account (service account) in the context of which the connectors are to operate. This service account must have an Exchange mailbox. Under this service account the Exch Apl and ExUM APL service operates on the kernel computer. The privileges assigned to this account enable the operation of the Exchange connector in the system. Using the service account you can easily administer the privileges for operating the connectors.

- **Assigning privileges**

Assigning the privileges for the installation and operation of the connectors has slightly changed with the XPR Foreign Connector. Which privileges are required and how to set them is described further down the text under **"Requirements and privileges for installing the connectors"**.

- **Transport directories**

Message transport between the two systems requires two transport directories (`\<drop directory>` and `\<replay directory>`) on the *Exchange server 2010*. The drop directory serves for transporting messages from Exchange to the XPR server, the replay directory is in charge of transporting in the reverse direction. You find information about the configuration and activation of these transport directories in [Section 5.2.7.1, "Creating the Transport Directories"](#), on page 198.

- **Requirements and privileges for installing the connectors**

Management role groups

The new privilege model in *Microsoft Exchange Server 2010* is called *Role Based Access Control* (RBAC). A method to assign privileges to users of an organization in this new privilege model is to group users in so-called *Management Role Groups*.

Management Role Groups facilitate assigning management roles to a user group considerably, because the same roles are assigned to all members of a role group at the same time.

Administrator and specialist roles are grouped in role groups, for example. This enables combining users for important management tasks such as organization management, recipient management and more in *Exchange Server 2010*.

You find further information about this topic under:

<http://technet.microsoft.com/en-us/library/dd298183.aspx>

Installation Requirements	
☐	The server components Mailbox Server Role and Hub Transport Server Role are installed and active.
☐	The network function as well as the name resolution in the network work correctly. You can use DCDiag and NetDiag (Windows support tools) to check this.
☐	You are logged in at the domain as installing user with domain admin privileges and Exchange admin privileges. This gives you unrestricted access to the service database. This is important with respect to installing and configuring the service.
The service account requires locally the following privileges on the XPR system: Notes: • Privilege assignment occurs via the Security Policies. You reach the corresponding setting dialog via Start > Administrative Tools > Local Security Policy under Local Policies > User Rights Assignment. Under the local security policies you find the locally set and “effective” policies. • Separate policies can be entered for domains and domain controllers. These policies overwrite, as the case may be, the locally defaulted ones. After a policy modification on domain level, a restart of the corresponding computers (domain controllers and Exch APL computers) may be required. • If you plan a system allowing more than 5000 MAPI accesses, use the Multiline Configuration feature. See Section , “Multiline Configuration”, on page 423. ☒ Log on as service – is set upon the connector installation. (Log on as service)	

Table 13

Check List: Installation Requirements for the Exchange -2010 Connectors

Installation Requirements
☒ Act as part of the operating system – is set upon the connector installation. (Act as part of the operating system) ☒ Back up files and directories – is set upon the connector installation. (Back up files and directories) ☒ Restore files and directories – is set upon the connector installation. (Restore files and directories) ☒ Log on as batch job – is set upon the connector installation. (Log on as batch job) ☒ Adjust memory quotas for a process – is set upon the connector installation. (Adjust memory quotas for a process) On the organization level of the Exchange server (Active Directory level), the following privileges are required for the service account: ☐ The installing user must have the “Organization Management” privilege in the Exchange 2010. This provides full access to the Exchange-specific part of the Active Directory for installing and uninstalling various objects (for example: connector, address type, templates, etc.). ☐ User “service account” must belong to the group of “domain administrators” ☐ User “service account” must belong to the group of “domain users”

Table 13

Check List: Installation Requirements for the Exchange -2010 Connectors

Installation Requirements
☐ The XPR service account requires configuring a Client Throttling Policy. Proceed as follows: – Start the Exchange Management Shell (EMS). – Enter the following commands in the command prompt in succession: <pre>New-ThrottlingPolicy -Name "XPR Throttling Policy" -RCAMaxConcurrency \$null -RCAPercentTimeInAD \$null -RCAPercentTimeInCAS \$null -RCAPercentTimeInMailboxRPC \$null;</pre> <pre>Set-Mailbox-Identity <XPR service account> -ThrottlingPolicy "XPR Throttling Policy"</pre> – Restart the RPC Client Access service on all Exchange servers. – Restart the ExUM Apl. The new policy is thus configured. Logging of the throttling events in the RPC Client Access service is disabled by default. The RPC Client Access log does therefore not display any throttling information. How to activate the throttling event logging: – Start any text editor, for example Notepad. – Open the file: <pre>Microsoft.Exchange.RpcClientAccess.Service.exe.config</pre> You find this file in path: <pre>C:\Program Files\Microsoft\Exchange Server\V14\Bin</pre> – Find the following line in the opened file: <pre><add key="LoggingTag" value="ConnectDisconnect, Logon, Failures, ApplicationData, Warnings" /></pre> – Add "Throttling" to the comma-separated list of events to be displayed in the log. – The relevant line of the above example will then read: <pre><add key="LoggingTag" value="ConnectDisconnect, Logon, Failures, ApplicationData, Warnings, Throttling" /></pre> – Save the file in the text editor. – Close the file: – Restart the RPC Client Access service. Logging the throttling events is now active. You find more detailed information about the "Throttling" subject under: <pre>http://technet.microsoft.com/en-us/library/ dd297964(v=exchg.141).aspx</pre>

Table 13

Check List: Installation Requirements for the Exchange -2010 Connectors

Installation Requirements	
☐	A service account with Exchange mailbox for operating the Exch and ExUM Apl has been created. The Exch and ExUM APL service runs under this user account on the kernel computer. The privileges assigned to this account enable the operation of the Exchange connector in the system. This also enables the simple administration of the privileges for this service account. Operating the gateway via a service account always requires the following privileges: • View-Only Organization Management role group In the pool that forms the <i>Role Based Access Control (RBAC)</i> privilege model in <i>Microsoft Exchange Server 2010</i>, the <i>View-Only Organization Management role group</i> is one of the <i>Management Role Groups</i> available by default. Administrators or users who belong to this role group can have the properties of every Exchange organization object displayed. The <i>View-Only Organization Management role group</i> in <i>Exchange Server 2010</i> is comparable with the <i>Exchange View-Only Administrators role</i> in <i>Microsoft Exchange Server 2007</i>. You find more information about this topic under: http://technet.microsoft.com/en-us/library/dd351130.aspx Add the user to the "View-Only Organization Management" via Active Directory Users & Computers. Alternatively you can do this only by deploying the Exchange Management Shell, EMS). Execute the following steps for assignments to this <i>Management Role Group</i>: – Start the <i>Exchange management shell</i>. – Enter the following command in the command prompt: <code>Add-RoleGroupMember "View-Only Organization Management" -Member "<XPR service account>"</code> Note: You can check whether the assignment for the XPR service account was successful, thus the XPR service account now belongs to the <i>View-Only Organization Management role group</i>, via the following command: <pre>Get-RoleGroupMember "View-Only Organization Management"</pre> You find more information about this topic under: http://technet.microsoft.com/en-us/library/dd638143.aspx
☐	• Local administrator on the Mailbox Server Role as well as on the Hub Transport Server Role.

Table 13 Check List: Installation Requirements for the Exchange -2010 Connectors

Installation Requirements	
☐	• Organization Management role group (required for the setup only) With <i>Exchange Server 2010</i> the <i>Exchange Organization Administrators</i> role has changed to <i>Organization Management</i> role group. The <i>Organization Management</i> role group is comparable to the <i>Exchange Organization Administrators</i> role in <i>Exchange Server 2007</i>. The installing user must belong to the <i>Management Role Group "Organization Management role group"</i> in the <i>Exchange Server 2010</i> organization. This gives the user full access to the Exchange-specific part of the Active Directory for installing/uninstalling different objects such as the connector, the address types and templates etc. Add the user to the "Organization Management" via Active Directory Users & Computers. Alternatively you can do this only by deploying the Exchange Management Shell, EMS). Execute the following steps for assignments to this <i>Management Role Group</i>: – Start the <i>Exchange management shell</i>. – Enter the following command in the command prompt: <pre>Add-RoleGroupMember "Organization Management" -Member "<XPR service account>"</pre> Note: You can check whether the assignment for the XPR service account was successful, thus the XPR service account now belongs to the <i>Organization Management</i> role group, via the following command: <pre>Get-RoleGroupMember "Organization Management"</pre>
☐	• Privileges "Send As", "Receive As" and "Administer Information Store" on organization level How to assign the XPR service account the privileges <i>Send As</i>, <i>Receive As</i> and <i>Administer Information Store</i> on organization level: – Start the <i>Exchange management shell</i>. – Enter the following command in the command prompt: <pre>Get-OrganizationConfig Add-ADpermission -User "<XPR service account>" -ExtendedRights "ms-Exch-Store-Admin", "Send As", "Receive As"</pre> Note: You can check whether the assignment for the XPR service account was successful, thus the XPR service account now has the privileges <i>ms-Exch-Store-Admin</i>, <i>Send As</i> and <i>Receive As</i> on organization level, via the following command: <pre>Get-OrganizationConfig Get-AdPermission -User "<XPR service account>" Select -Property User,ExtendedRights, Deny, IsValid</pre>

Table 13

Check List: Installation Requirements for the Exchange -2010 Connectors

Installation Requirements	
☐	• Explicit privileges “Send As”, “Receive As” and “Administer Information Store” on mailbox database level How to assign the XPR service account the explicit privileges <i>Send As</i>, <i>Receive As</i> and <i>Administer Information Store</i> on mailbox database level: – Start the <i>Exchange management shell</i>. – Enter the following command in the command prompt: Get-MailboxDatabase Add-ADPermission -User "<XPR service account>" -ExtendedRights "send as", "receive as", "ms-Exch-Store-Admin" Note: You can check whether the assignment for the XPR service account was successful, thus the XPR service account now has the explicit privileges <i>ms-Exch-Store-Admin</i>, <i>Send As</i> and <i>Receive As</i> on mailbox database level, via the following command: Get-MailboxDatabase Get-AdPermission -User "<XPR service account>" Select -Property User,ExtendedRights, Deny, IsValid

Table 13

Check List: Installation Requirements for the Exchange -2010 Connectors

Installation Requirements☐ • **Explicit privilege “Send As” on user mailbox level**

How to assign the explicit privilege *Send As* to the MRS user account on user mailbox level:

- Start the *Exchange management shell*.
- Enter the following command in the command prompt:

For a specific user:

```
Get-Mailbox -Identity
"<Exchange user>" | Add-ADpermission -user
"<XPR service account>" -ExtendedRights "Send As"
```

For all users of a specific organization unit:

```
$XPRUSERS=Get-User -OrganizationalUnit
"<XPR organization unit>";

FOREACH ($USER in $XPRUSERS)
{ Add-MailboxPermission -User "<XPR service account>"
-Identity $USER.NAME -ExtendedRights "Send As" }
```

Note: You can check whether the assignment for the XPR service account was successful, thus the XPR service account has the explicit privilege *Send As* on the user mailbox level, via the following command:

```
Get-Mailbox -Identity
"Exchange User" | Get-AdPermission -User
"<XPR service account>" | Select -Property
User,ExtendedRights
```

You find further information about this topic under:

<http://technet.microsoft.com/en-us/library/bb676368.aspx>

Table 13

Check List: Installation Requirements for the Exchange -2010 Connectors

Installation Requirements	
☐	• Explicit privilege “FullAccess” on user mailbox level How to assign the explicit privilege <i>FullAccess</i> to the XPR service account: – Start the <i>Exchange management shell</i>. – Enter the following command in the command prompt: For a specific user: <pre>Add-MailboxPermission -User "<XPR service account>" -Identity "<Exchange user>" -AccessRights FullAccess</pre> For all users of a specific organization unit: <pre>\$XPRUSERS= Get-User -OrganizationalUnit "<XPR organization unit>" FOREACH (\$USER in \$XPRUSERS) { Add-MailboxPermission -User "<XPR service account>" -Identity \$USERS.NAME -AccessRights FullAccess}</pre> Note: You can check whether the assignment for the XPR service account was successful, thus the XPR service account now has the explicit privilege <i>FullAccess</i> on the user mailbox level, via the following command: <pre>Get-MailboxPermission -Identity "<Exchange user>" -User "MRS Service Account"</pre> You find further information about this topic under: http://technet.microsoft.com/en-us/library/aa996343.aspx for additional details)

Table 13 Check List: Installation Requirements for the Exchange -2010 Connectors

Finally, reboot the service *Microsoft Exchange Information Store* for the privilege assignments to take immediate effect.

5.2.4 Installation Process Overview

Installation process on the XPR server

After the component selection the following components are installed on the XPR server in succession:

- The LDAP APL
It makes sure that address data relevant to XPR and centrally maintained via the Active Directory can be replicated in both directions.
- The Exchange True Unified Messaging Connector (ExUM Apl)
The Exchange mailbox store can be immediately accessed via the ExUM APL. In this way Exchange messages can be directly forwarded to a telephone interface via the XPR server. This connector is also required for the notification function.
- The Exchange connector (Exch APL)
It forms the *store & forward* connection between the XPR server and *Exchange Server 2010*. Messages received or to be sent via the XPR server are transmitted via this connector. With the **ExchAPL** installation a new Foreign Connector is created. This connector establishes a connection to the Exchange Mailbox Server Role and to the Exchange Hub Transport Server Role on the Exchange Hub Transport server.
- The MMC Snap-in (if selected for installation on the XPR server).
The MMC Snap-in displays the XPR-specific administration dialog **MRS Settings** for the XPR users (under Active Directory Users and Computers).

NOTE: Managing users with help of the Active Directory Users and Computers program is normally not performed via the XPR server. Therefore, the MMC Snap-in must be manually installed on the server from which the user administration occurs.

During the component installation, all parameters required for successfully connecting the XPR server to the previously installed *Exchange Server 2010* are queried, and the necessary program files copied.

Working on the Exchange Server

After the installation of the XPR components the transport directories need to be created on the Exchange server that has the Hub Transport Server Role. See [Section 5.2.7.1, “Creating the Transport Directories”, on page 198](#).

Configuration of the Exchange Foreign Connector for *Exchange Server 2010*

After you have completed the setup, you can perform further configurations via the settings dialogs in the XPR monitor. The Foreign Connector configuration is described in [Section 5.3, “Configuration”, on page 205](#).

Connecting an *Exchange Server 2010 cluster environment*

If you want to realize a connection to a clustered Exchange 2010 server via the ExUMApI you need to consider the following factors:

- The ExUMApI must be installed for the server that has the Client Access Server Role. Also in case of a clustered Client Access Server(CAS Array) the ExUMApI must be connected to the CAS Array.
- This server must be visible in the network and accessible by DNS.
- The name of the server that has the Client Server Role must be specified in the ExUMApI setup dialog for this purpose. The ExUMApI then connects to the right server. In this process it does not matter which cluster node is currently active.

Installation to a clustered *Exchange Server 2010* environment is supported as of version XPR 5.0 R4 FixRelease 6.

5.2.5 Installation of the XPR Components for the Connection to *Exchange Server 2010*

5.2.5.1 Selecting the Components

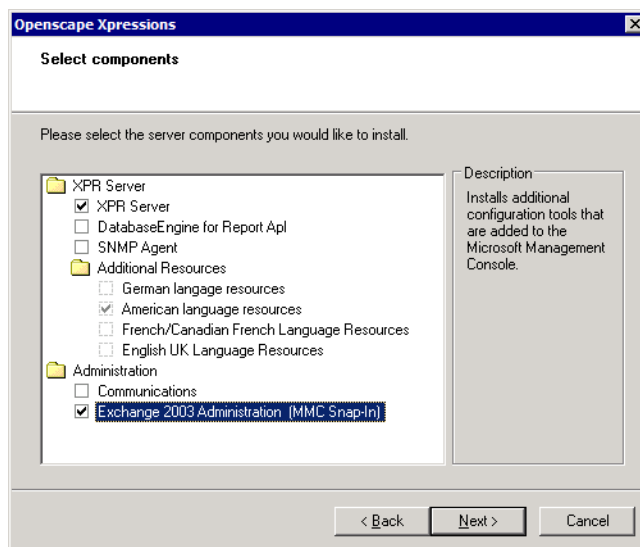
In the XPR server setup, after the license service installation, the language selection as well as reading the release notes you reach the setup dialogs for the Exchange connection.

After you have confirmed to have taken notice of the release notes you perform a first selection of components for the XPR server in the following dialog. Here you can select the MMC Snap-in for installation on the XPR server. This, however, is only required if the XPR user administration is to occur from the XPR server.

NOTE: Managing users with help of the Active Directory Users and Computers program is normally not performed via the XPR server. Therefore, the MMC Snap-in must be manually installed on the server from which the user administration occurs. You find the setup file on the product data carrier in the directory <X>:\...\AddOn\Client\Exchange\MMCSnapIns.

X corresponds to the current letter of the device that holds your product data carrier.

If you want to install the Snap-in on the XPR server, select the **Exchange 2003 Administration (MMC Snap-In)** option. The installation is then automatically started at the end of the server installation.



NOTE: If you do not see the MMC Snap-in component in this dialog, a license is likely to be missing. In this case please check the licenses and restart the setup program.

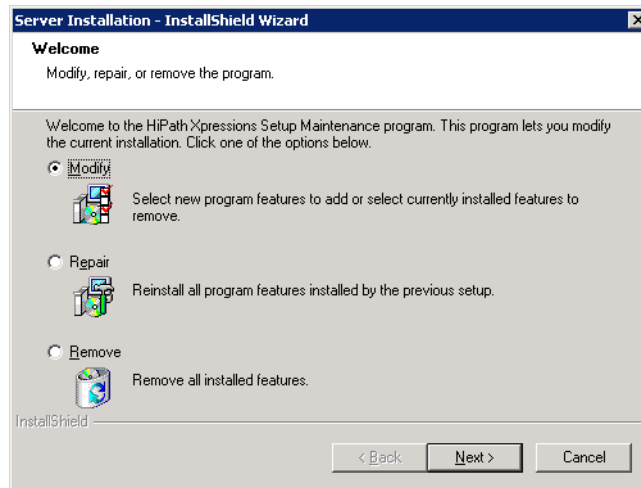
Exchange 2003 administration (MMC Snap-in extension)

users are still administered via the MMC Snap-in extension for Active Directory Users and Computers.

The MMC Snap-in displays the XPR-specific administration dialog **MRS Settings** for the XPR users (see [Section 4.3.4, “User Administration”, on page 114](#)).

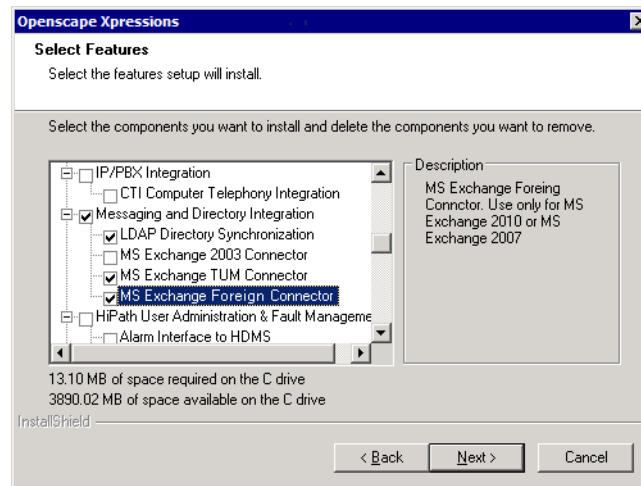
NOTE: A 64-bit operating system supports the available 32-bit XPR MMC Snap-in without restriction. This requires starting the XPR MMC Snap-in in 32-bit mode (`mmc /32`).

After the setup dialogs for the client components, external software, documentation and ASR components, you reach the selection of the desired installation scenario. Select **Modify** to install the Exchange components of the XPR server.



In the next dialog, select the following additional components from the **Messaging and Directory Integration** branch:

- LDAP Directory Synchronization
- MS Exchange TUM Connector
- MS Exchange Foreign Connector



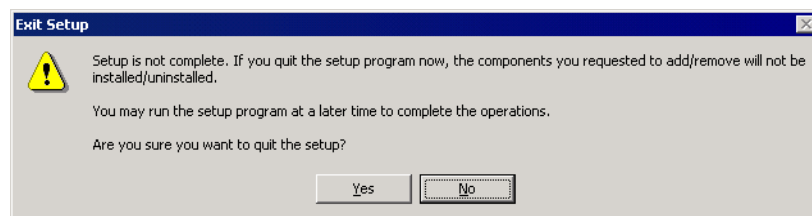
5.2.6 Components Installation Procedure

5.2.6.1 Starting the Installation

Installing the Exchange components in the running XPR setup starts with dialogs invoked for the preparative LDAP APL configuration. The steps lying between the setup start and this stage serve to install other XPR server components. The respective settings are comprehensively described in the *Server Installation* manual.

5.2.6.2 General Considerations

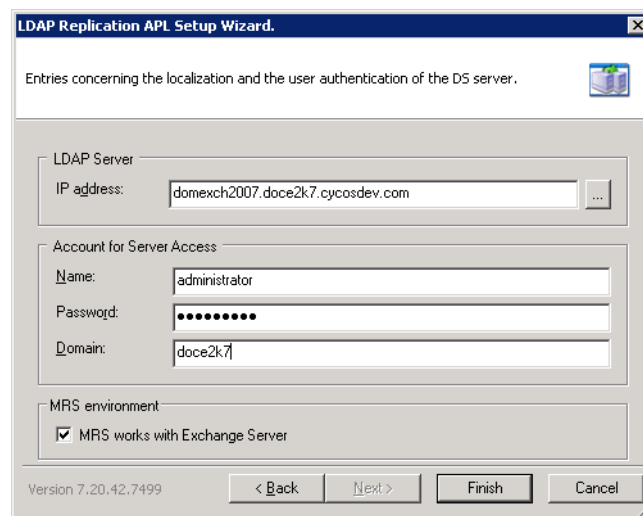
Pushing the Cancel button in the installation dialogs delivers the information that Setup has not been duly accomplished yet. If you select **Yes** here, only the installation of the current component is terminated – the XPR setup will then be continued with the next component. With **No** you return to the currently running setup.



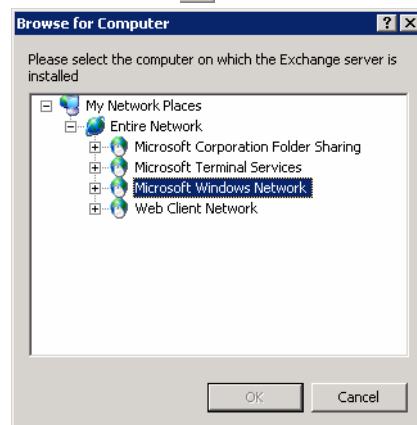
5.2.6.3 Installing the LDAP APL

At the stage where in the XPR server setup the installation of the LDAP directory synchronization (LDAP APL) starts, the LDAP setup wizard first appears in its welcome window.

With a click on Next the dialog opens in which you find the **IP Address** entry field (**LDAP Server** section) to specify the name of the computer that the LDAP APL is to access for data replication. This is in most cases the Primary Domain Controller computer (PDC), which contains the Global Catalog of the Active Directory.



This can either be done by directly entering the server name in this entry line or via the **Browse for Computer** dialog. This dialog opens when you enable the selection icon ... next to the entry line.



Now create the **Account for Server Access**. In doing so, select a user account that has read as well as write privileges for the Active Directory. This is usually the domain administrator. You can also use the service account if it has the corresponding privileges.

In the **MRS environment** section, via the **MRS works with Exchange Server** checkbox, you integrate the configuration file required for *Exchange Server 2010*. It is called `ExRepl.lcf`.

The **Active Directory** option is intended for accessing other Active Directory directory services via LDAP. The `AdRepl.lcf` configuration file is then integrated by default. It enables LDAP access to the Active Directory if no *Exchange server* has been installed.

Finish completes the entries and the LDAP setup.

Via **Back** you return to the LDAP APL setup welcome window again.

Cancel terminates the LDAP APL setup and initiates the installation of the next server component.

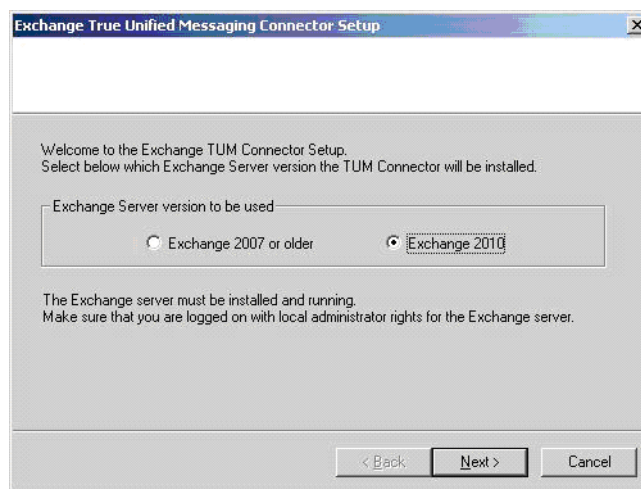
How to configure the LDAP APL is described in [Section 5.3.1, "Configuring the LDAP Apl", on page 205](#).

5.2.6.4 Installing the XPR True Unified Messaging Connector

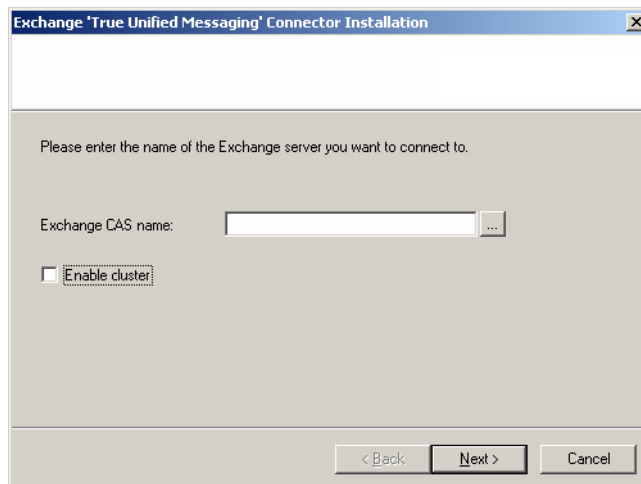
NOTE: Please note the modified setup routine when installing the XPR True Unified Messaging Connector to an *Exchange CAS Array*.

After completion of the LDAP APL installation, the XPR True Unified Messaging Connector setup follows automatically, provided the ExUM APL has been previously selected as component for using True Unified Messaging.

In the first setup step you select the version of the Exchange server to which the TUM connection is to be established. Select *Exchange Server 2010* here.



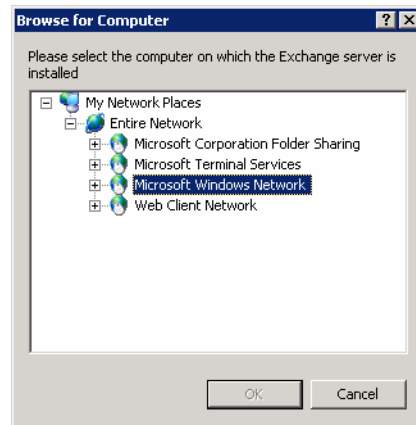
Click on **Next**.



In the first dialog define the Exchange Client Server Role the ExUM APL is to establish a connection to. In a modular *Exchange Server 2010* environment structure this is the server that has the *Client Access Server (CAS)* role.

NOTE: In case of an *Exchange server 2010* with monolithic structure the connection is set up to the server on which the *Exchange server 2010* is installed.

You can do this by directly entering the server name. You can also use the  button to look for the corresponding server in the network. A click on this button opens a dialog for selecting the *Exchange Server 2010*.

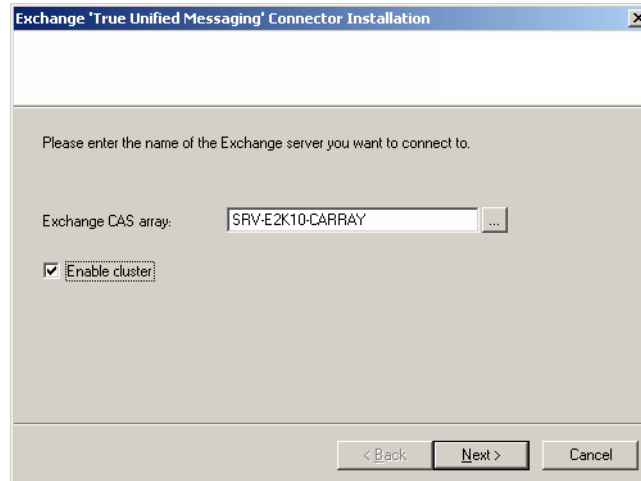


In the first setup dialog, select the **Enable cluster** option if you wish to connect an *Exchange Client Access Server Array*.

Installing the Exchange True Unified Messaging Connectors at an Exchange Client Access Server Array

In the running setup you need to execute the following worksteps for the XPR True Unified Messaging Connector at this point:

1. Select the **Enable cluster** option for choosing the CAS server in the setup dialog.
This option enables installing the XPR True Unified Messaging Connector at an *Exchange Client Access Server Array (CAS Array)*.



2. Enter the name of the *Exchange Client Access Server Array* in the **Exchange CAS array** input line.
3. In the next setup dialog, select the service account under which the Exch APL is to run.
You specify the service account under Name in the format *<domain\name>*. Then enter the service account password twice.
4. The next setup dialog shows a summary of the entered parameters.
5. Activation and configuration of the XPR True Unified Messaging Connector for the *Client Access Server Array*.
After you have installed the Exchange XPR True Unified Messaging Connector for the *Client Access Server Array* you need to activate and also further configure this feature via two registry keys.

To do this you must add the following registry keys under **HKLM\SOFTWARE\...\Wow6432Node\PP-COM\ExUmApl** manually:

CASARRAY [REG_DWORD]

Default:	-
Possible values:	0 and 1
Remark:	Setting this value to 1 activates the connection to a Client Access Server Array.

CASARRAYNAME [REG_MULTI_SZ]

Default:	-
Possible values:	CASARRAY01-DNS CASARRAY02-DNS CASARRAYn-DNS <DNS-names of the respective Exchange Server CAS Arrays>
Remark:	Name of the <i>Exchange Server 2010 CAS Arrays</i> . You need to use the DNS name of the respective CAS array as value for CASARRAYNAME.

You find additional information about the concept and management of a *Client Access Server Arrays (CAS Array)* on the following web pages:

Understanding Load Balancing in Exchange Server 2010

<http://technet.microsoft.com/en-us/library/ff625247.aspx>

New-ClientAccessArray

[http://technet.microsoft.com/en-us/library/ee332317\(v=exchg.141\).aspx](http://technet.microsoft.com/en-us/library/ee332317(v=exchg.141).aspx)

If you have configured a connection to an *Exchange Client Access Server* or *Exchange Client Access Server Array*, a click on **Next** takes you to the dialog for defining the user account under which the ExUM APL is to run.

Exchange True Unified Messaging Connector Installation

Please enter user account (using 'domain\name' or 'name') and password which should be used for starting the gateway.

This user must be 'Exchange View Only Administrator' for Exchange and 'Domain Administrator'.

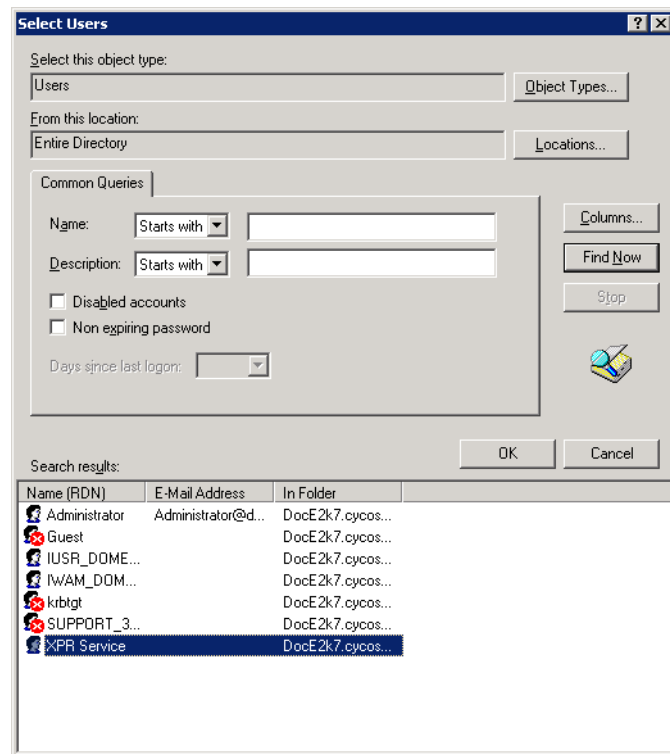
Name: DOCE2K7\XPR_Service ...

Password:

Repeat password:

< Back Next > Cancel

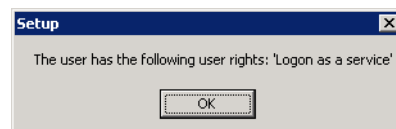
Here you can directly enter the name of the service account in the format <domain\name>. You can also use the ... button to select the service account.



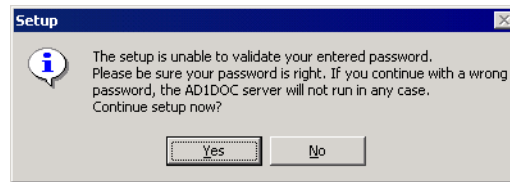
You can proceed as follows to transmit the service account to the ExUM APL configuration page via the user selection dialog:

- By means of a double-click on the selected user name.
- Via direct entry of the name in the lower portion of the dialog. Then verify the name by pressing the **Check Names** button.
- Through selection of the name in the list. Then click the **Add** button.

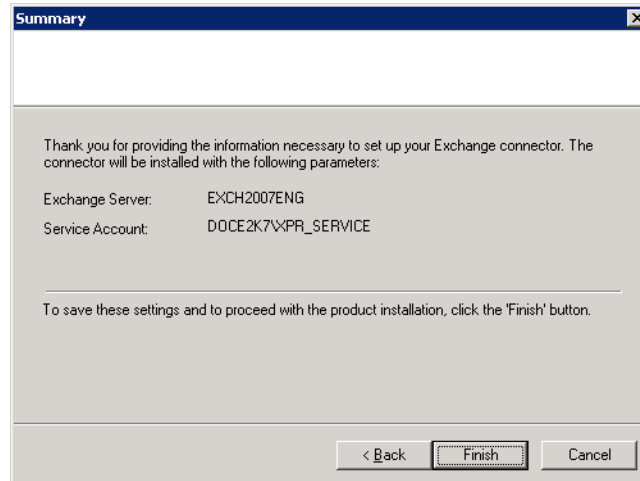
Click **OK** to complete this process. Then enter the password to legitimate this service account. If the specified service account is valid, the user privileges assigned by Setup are displayed in a message.



Confirm this message with **OK**. You are then informed that the entered password cannot be checked for validity. If you are not sure at this point, enable **No** to return to the password entry for making an alteration if necessary.



When you continue the ExUM APL setup with **Yes**, the concluding dialog displays the entered parameters once again.



Click **Finish** to save your entries. The ExUM APL installation is thus accomplished.

5.2.6.5 XPR Foreign Connector Installation

NOTE: If you install the XPR Foreign Connector for an *Exchange Database Availability Group* please heed the modified setup routine.

The ExUM APL installation is automatically followed by the XPR Foreign Connector setup if this component was previously selected.

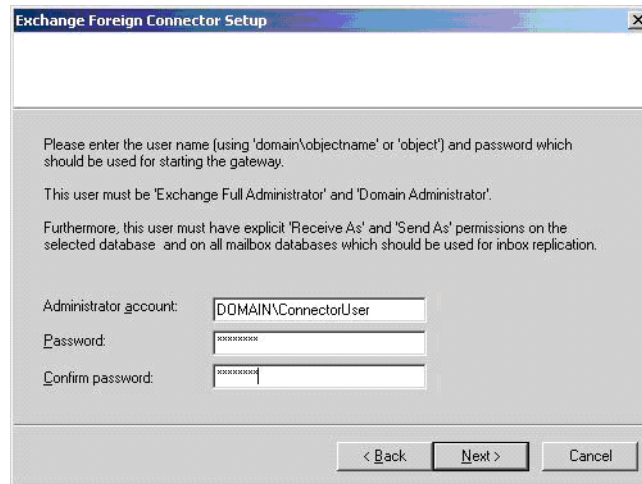
The welcome dialog of the Exch APL installation once again points to the requirements that must be met for a successful installation.

After you have clicked on **Next** in the welcome dialog, you reach the dialog for selecting the Exchange server. Here you determine the Exchange server version that the XPR Foreign Connector is to connect. Select Exchange Server 2010 here.

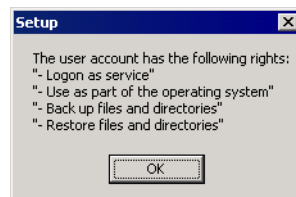


Then click on the **Next** button.

In the next dialog you need to enter the service account under which the Exch APL is to operate. You specify the service account under Name in the format `<domain\name>`. Then enter the service account password twice.



Since the Exchange gateway cannot link up with *Exchange Server 2010* when a wrong password has been specified, the entry must occur twice to rule out typing errors as source of error. A correct entry opens an information dialog as confirmation and to display a list of the user privileges assigned to the user account by Setup.



Confirm the user privilege information display with **OK**.

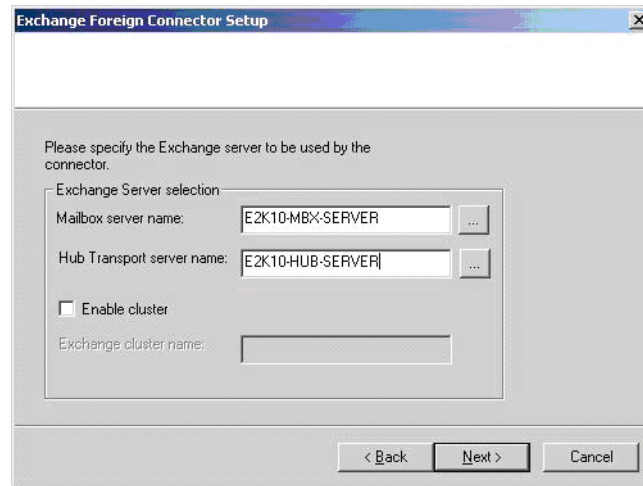
Setup is then continued with entering the computer name for the connection to *Exchange Server 2010*.

In case of a modular *Exchange Server 2010* environment structure the XPR Foreign Connector must establish a connection from the XPR server to the Mailbox Server Role **and** to the Hub Transport Server Role.

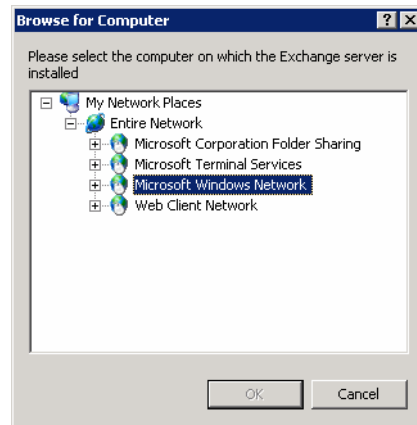
The connection to the Exchange Mailbox Server Role is required for opening a MAPI connection to resolve addresses.

The connection to the Exchange Hub Transport Server Role serves for transporting messages from/to the XPR server.

NOTE: If the *Exchange server 2010* has a monolithic structure, specify the name of the *Exchange server 2010* in both entry lines.



Here you can either directly enter the server name or use the ... button to look for the relevant servers in the network.

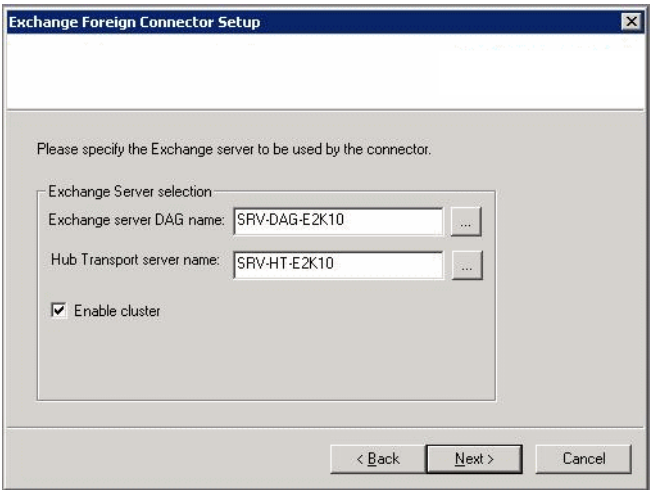


In the first setup dialog, select the **Enable cluster** option if you wish to connect an *Exchange Database Availability Group*.

Installing the XPR Foreign Connector at an *Exchange Server 2010* with DAG

After the setup start you need to execute the following worksteps for the XPR Foreign Connector:

- 1. Select the **Enable cluster** option for choosing the Exchange Server Roles in the setup dialog. Using this option you can install the XPR Foreign Connector at an *Exchange Server 2010 with Database Availability Group (DAG)*.



- 2. Enter the required Exchange server DAG name in the **Exchange server DAG name** input field.
- 3. Enter the name of the Hub Transport server in the **Hub Transport server name** input field.
- 4. Select the desired address templates after the found database and mailbox data list have been displayed.
- 5. Configuration of the XPR Foreign Connector for the *Database Availability Group*.

Setting up the XPR Foreign Connector creates the **DAGONES** key in the **HKLM\SOFTWARE\Wow6432Node\PP-COM\MRS\ExchApI** registry path. Enter the names of the servers that form the *Database Availability Group*.

DAGNODES [REG_MULTI_SZ]

Default:	-
Possible values:	NODE1, NODE2,...NODEn
Remark:	NODE1..NODEn are the names of the servers that form the Database Availability Group.

You find additional information about the concept and management of a *Database Availability Group (DAG)* on the following web pages:

Understanding Database Availability Groups

[http://technet.microsoft.com/en-us/library/dd979799\(EXCHG.140\).aspx](http://technet.microsoft.com/en-us/library/dd979799(EXCHG.140).aspx)

Managing High Availability and Site Resilience

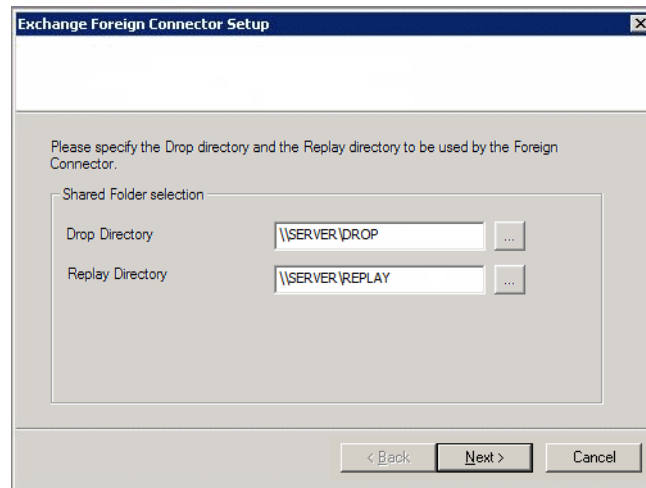
<http://technet.microsoft.com/en-us/library/dd638215.aspx>

Managing Database Availability Groups

<http://technet.microsoft.com/en-us/library/dd351172.aspx>

After you have entered the mailbox server of the Exchange server via the mailbox server name or the DAG name or selected the mailbox server in the network, click on **Next**.

You reach the dialog in which you have selected the transport directories.



In the **Drop directory** and **Replay directory** specify the path to the shared transport directories according to the following pattern:

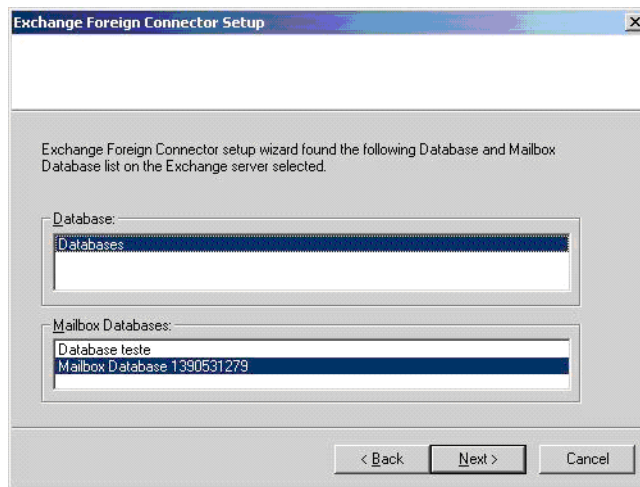
- For the **Drop directory**
`\\<Ip address or name of the Exchange server on which the Hub Transport Server operates>\<XPR server name>-<name of the Exchange Server 2010 Mailbox Server Role>`
- For the **Replay directory**
`\\<Ip address or name of the Exchange server on which the Hub Transport Server operates>\Replay`

You can also use the browse button  to look for the corresponding shares in the network. In the latter case a window opens for selecting the corresponding shares.

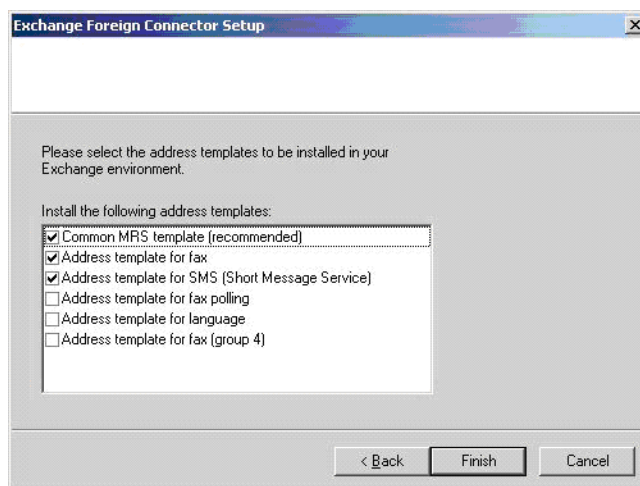
NOTE: The settings performed here during the installation for the paths of the transport directories can later be changed via the **ExchApl** configuration dialogs in the XPR monitor (**Exchange Foreign Connector** tab).

After you have selected the drop directory and the replay directory, click on **Next**.

The next dialog confirms the successful localization of the two specified servers by displaying the **Database** and the **Mailbox Database**.



Click on **Next**. The installation continues with the **address template** configuration.

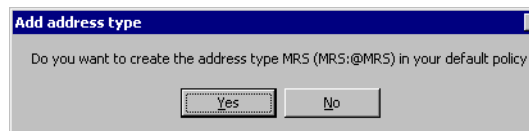


Here you can have **address templates** installed in your Exchange environment for various services offered by the XPR server.

In this way you can later generate e.g. a new address for the address book in the client, so that you only need to enter the corresponding number and select the desired service in there instead of working with the somewhat cryptic default Exchange addressing.

After you have clicked on **Finish**, the dialog for creating the MRS address type (MRS:@MRS) opens. This address type is globally created in the Default Policy.

NOTE: As of Exchange Server 2007 the distribution groups support the **sAMAaccountName**. As a result, all Exchange users with this attribute are replicated as full XPR users to the XPR server. This causes problems when assigning the MRS address type and the number of replicated users exceeds the number of available user licenses. Therefore, the number of user groups to be replicated may have to be restricted beforehand via the LDAP configuration.



Yes starts the address assignment and immediately defines an MRS address for each Exchange user.

NOTE: In large system environments, address assignment may take a while.

If not all Exchange users are to be assigned the MRS address, click the **No** button in this dialog.

This will directly resume the setup process with the installation of the next XPR component. The MRS address type will not be specified then and there is no assignment of the MRS address to the Exchange users either. The MRS address type must then be manually defined afterwards. See [Section 5.7, “Adding and assigning the MRS E-Mail Address Type retrospectively”](#), on page 258.

A subsequent manual definition of the MRS address type is useful if only specific users are to use this address type. After that, the MRS address can be assigned to users via the definition of filter rules in the Default Policy (or in a newly created policy).

The installation of the XPR components for connecting *Exchange Server 2010* is now complete.

NOTE: If the ExchAPL does not start when the XPR server is booted, a privilege problem is in most cases responsible for this. You may then see an error message on the XPR monitor like:

Exchange Server seems not to be running <0x80004005>

In this case check whether the service account was assigned the required privileges or whether the service account was added on all system components to the local administrators.

5.2.6.6 Installation of the MMC Snap-in

Administering the XPR user data requires the MMC Snap-in. It displays the **MRS Settings** tab in the properties dialog for the AD users. To this the MMC Snap-in that was already deployed with *Exchange Server 2003* is used.

NOTE: The MMC Snap-in can be installed on a 32-bit as well as on a 64-bit system. When using a 64-bit system, start this application in 32-bit mode (`mmc / 32`).

You find further information in the Microsoft KB article

[http://msdn.microsoft.com/en-us/library/ms692753\(VS.85\).aspx](http://msdn.microsoft.com/en-us/library/ms692753(VS.85).aspx)

The MMC Snap-in can be integrated in a new installation of the XPR server if the XPR users are to be administered from the XPR server. In the first installation dialog, after invoking the server setup, select the **Exchange 2003 Administration (MMC SnapIn)** component. See also [Section 5.2.5.1, "Selecting the Components"](#), on page 173.

If the MMC Snap-in is required on another system, the installation must occur manually and belatedly from the XPR product data carrier. You find the setup file on this carrier in the directory: `X:\AddOn\Client\Exchange\MMCSnapIns` (X corresponds to the current letter of the device that holds your product data carrier).

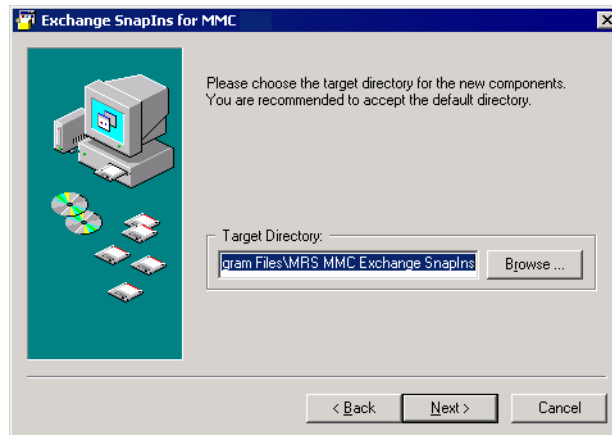
How to manually install the MMC Snap-in:

1. Start the setup by executing the `setup.exe` from the above directory.
A welcome dialog opens. It points out that all running applications should be terminated before Setup is started. **So, if any applications are still open, close them after selecting Cancel.** Setup is left then and active programs can be shut down. Subsequently, it must be started again.
2. Click the **Next** button in the welcome dialog.
The dialog for defining the target directory opens.

During the installation, the following files are created in the `%ProgramFiles%\MMC Exchange SnapIns` directory by default:

```
ExtInst.MMCEXchSnapIns.ini
setup.MMCEXchSnapIns.ini
Uninstall.MMCEXchSnapins.exe
Uninstall.MMCEXchSnapins.exe
```

In addition, the `ExtInst.log` log file that logs the setup process is created in the `X:\Documents and Settings\<installing user>\Local Settings\Temp` directory.

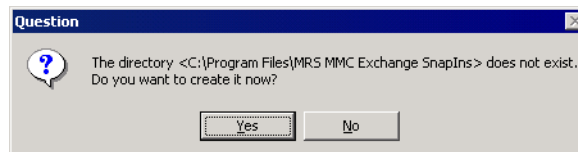


You can also push **Browse...** to specify or newly define a directory to which the program files are then copied. A file selection dialog opens after you have pushed this button. However, we recommend to copy the preset directory since the program components are then easier to find when the necessity arises.

NOTE: The **Back** button takes you back to the welcome dialog and via **Cancel** you can terminate the setup after a security prompt.

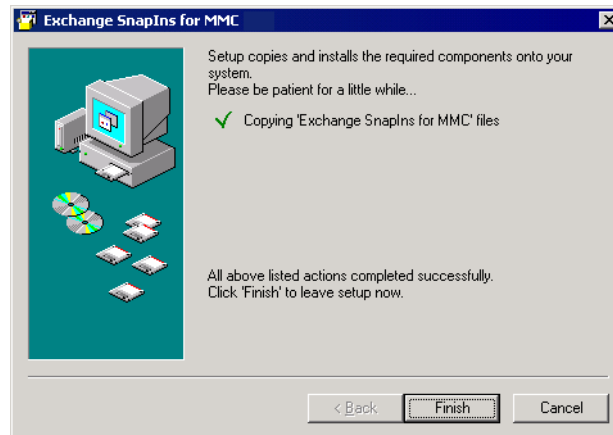
3. Click on the **Next** button after you have made your selection for the target directory.

If this directory does not exist yet, you are asked as to whether or not you want to have the directory defined. Confirm this query with **Yes** if you want to perform the installation.



The program files are being copied to the specified directory.

You can follow the progress of the copying and installation process in the next window by the icon next to **Copying 'Exchange SnapIns for MMC' files**. While the activities continue, a black cross precedes the “Copying 'Exchange SnapIns for MMC' files:” line. After completion of the data transmission, a green tick replaces the black cross.



4. Click **Finish** to complete the installation.

The MMC Snap-in installation is now complete.

5.2.6.7 Error Analysis during the Installation

In the event that an error has occurred during the installation, the cause of a termination can be detected in the log file automatically created with the installation.

Depending on the suggested setup directory, the log file is stored in the following directories:

- If the installation is performed in the directory suggested by Setup, you find the log file in the directory:

```
...\xpr\logs
```

- If the installation is performed in a directory that you determine, you find the log file in the temporary directory of the installing user.

In the log file (`MrsEXCH.log`) all setup steps are itemized and classified with a status description.

Example:

```
...
ExchangeUpdate HrInstallAddressTemplates successful
EnterpriseGDI successfully read
Successfully remove Exchange 2000 Gateway object.
Successfully got MRS-Container-Object (LDAP://AD1DOC/
CN=XPR,CN=Microsoft Exchange,CN=Services,CN=Configuration,
DC=doc-test,DC=alsdorf,DC=cycos,DC=local) Settings Object
(C) successfully removed.
MrsExchSetup HrInstallService successful
Active Directory Object successfully installed.
Successfully got MRS-Container-Object (LDAP://AD1DOC/
CN=XPR,CN=Microsoft Exchange Gateway,CN=Services,
CN=Configuration,Settings Object (<XPR server name>)
<CN=<XPR server name>:AD1DOC> successfully installed
ExchangeUpdate HrInstallGateway successful
Registering Extensions Successfully registered Admin
Extension
Successfully registered User Extension
ExchangeUpdate completed and successful
MaintProxy finished ...
```

If an error has occurred, the corresponding installation step is followed by “failed” instead of “successful”.

Example:

```
MrsExchSetup HrInstallService failed
```


When solving setup problems, the Event Viewer under Windows, which you can use for diagnosis, comes in handy (**Start** > rightclick on **Computer** > select **Manage** from the context menu > expand **Computer Management** > **System Tools** > open the **Event Viewer**).

In there all running processes are logged. When you select the desired protocol or service, the events that happened therein are displayed.

5.2.7 Working on the Exchange Server

5.2.7.1 Creating the Transport Directories

The transport of messages from the XPR server to Exchange and vice versa requires two directories, the drop and replay directory. These two directories serve to buffer the messages in a waiting loop until they are processed, meaning, sent to the respective target server. Storing the messages in these directories depends on the transmission direction.

Both directories are created on the server on which the Hub Transport Server Role operates.

NOTE: If the Exchange environment has a monolithic structure, the directories are created on the server on which the *Exchange server 2010* is installed.

Activating the transport directories requires configurations on the server with the Hub Transport Server Role (in case of a monolithic structure on the *Exchange server 2010*) as well as for the settings of the **ExchApl** on the XPR server.

- The drop directory
This directory serves for delivering messages sent from the Exchange server to the XPR server. The messages are retrieved and further processed by the XPR server.
During the **ExchApl** installation this object is created as “DropDirectory” object. It contains by default the name:

<XPR server name>-<name of the Exchange Server 2010 Mailbox Server Role>

NOTE: Due to the system, the object name for the Foreign Connector is created using the Mailbox Server Name instead of the Hub Transport Server Name.

You can have the drop directory name put out by entering the following command in the *Exchange management shell*:

```
get-foreignconnector|fl
```

The listing entry you look for has the format:

```
DropDirectory      : <XPR server name>-<name of the Exchange  
Server 2010 Mailbox Server Role>
```

NOTE: In case of a modular *Exchange Server 2010* installation distributed among several servers, the drop directory must be reachable via a UNC path in the network. Only then this directory can be accessed from the Hub Transport server (or from all further Hub Transport servers, if available). This is not required if the system has a monolithic structure.

- The replay directory
This directory buffers the messages sent by message servers different from Exchange to the Exchange organization. Exchange retrieves the messages from there and delivers them to the mailbox of the Exchange user.

NOTE: You can rename both directories and store them anywhere in the system. If this is desired, adjust the new directory names and the directory paths in the system upon the creation, activation or configuration.

How to create and activate these directories:

Creating and activating the drop directory

1. Using the Hub Transport Server Role create a directory with the following properties on the server:

Path:

`%ProgramFiles%\Microsoft\Exchange Server\V14`

Directory name:

`<XPR server name>-<name of the Exchange Server 2010 Mailbox Server Role>`

The path is defaulted as the drop directory is expected at this point. If several servers with the Hub Transport Role are available, select the one for which the XPR Foreign Connector is installed.

Example:

```
%ProgramFiles%\Microsoft\Exchange Server\V14
\<XPR server name>-<name of the Exchange Server 2010
Mailbox Server Role>
```

NOTE: In case of an *Exchange server 2010* with monolithic structure, the **drop directory** is created in the following path of the server on which the *Exchange server 2010* is installed:

%ProgramFiles%\Microsoft\Exchange Server\V14

NOTE: Please note that the drop directory may only be configured on one Hub Transport server and that there is only one path to the drop directory.

2. Set the following access privileges:
 - Grant the XPR service account under which the Exchange APLs operate **Full Control** of this directory share. Proceed as follows:
 - Invoke the context menu for the drop directory.
 - Change to the **Sharing** tab in the configuration dialog.
 - Enable here the **Permissions** button.
 - Add the XPR service account as user via the **Add** button.
 - Assign the **Full Control** privilege to the XPR service account.
 - Grant the XPR service account **Full Control** of the drop directory for the NTFS authentication. Proceed as follows:
 - Invoke the context menu for the drop directory.
 - Change to the **Security** tab in the properties dialog.
 - Add the XPR service account as user via the **Add** button.
 - Assign the **Full Control** privilege to the XPR service account.
 - Grant the NETWORKSERVICE on the server with the Hub Transport Server Role **Full Control** of the drop directory. Proceed as follows:
 - Invoke the context menu for the drop directory.
 - Change to the **Security** tab in the properties dialog.
 - Add the NETWORKSERVICE as user via the **Add** button.
 - Assign the **Full Control** privilege to the NETWORKSERVICE.

- Grant the Hub Transport server **Full Control** of this directory share.

NOTE: If several Hub Transport servers have been installed, this must occur for every single Hub Transport server.

Proceed as follows:

- Invoke the context menu for the drop directory.
 - Change to the **Security** tab in the properties dialog.
 - Use the **Add** button to add the Hub Transport server(s) as computer.
 - Assign the **Full Control** privilege to the Hub Transport server(s).
3. In case of several Hub Transport servers set the UNC path to the drop directory.

Use the Exchange management shell command:

```
Set-ForeignConnector -Identity "MrsConnector (<XPR server
name>:<name of the Exchange Server 2010
Mailbox Server Role>)" -DropDirectory "\\<Hub Transport
server name>\<XPR server name>-<name of the Exchange Server
2010 Mailbox Server Role>" for this purpose
```

The creation of the drop directory is now complete.

NOTE: If you do not use the default path for the drop directory you need to reconfigure your individual path in the system. When you configure the path the drop directory is simultaneously activated. To modify the directory path start the *Exchange management shell*.

Enter the following command in the *Exchange management shell*:

```
Set-TransportServer <hub transport server>
-RootDropDirectoryPath "<drive>:\<path>"
```

The first line of this command is separated from the second line by a blank (...port server> -RootDropDir...).

In the *Exchange management shell* you can check whether the activation has been successful with the following command:

```
Get-TransportServer <Hub Transport Server>|fl
```

In the subsequently displayed list the previously empty `RootDropDirectoryPath`: entry must now feature the entered path specification.

Creating or activating the replay directory

In the list put out by the

```
Get-TransportServer <your Hub Transport Server>|fl
```

command you find the defaulted path to the replay directory. It reads:

```
ReplayDirectoryPath    :    %ProgramFiles%\Microsoft\  
                        Exchange Server\TransportRoles\Replay
```

NOTE: You can create the replay directory anywhere on the server that has the Hub Transport Server Role. In doing so you need to adjust the path, though. You do this via the command:

```
Set-TransportServer <hub transport server>  
-ReplayDirectoryPath "<path>"
```

The first line of this command is separated from the second line by a blank (`...port server> -ReplayDir...`).

1. Set the following privileges for accessing the “Replay” replay directory:

- Grant the XPR service account under which the Exchange APLs operate full access to this directory share. Proceed as follows:
 - Invoke the context menu for this directory.
 - Change to the **Sharing** tab in the configuration dialog.
 - Enable here the **Permissions** button.
 - Add the XPR service account as user via the **Add** button.
 - Assign the **Full Control** privilege to the XPR service account.
- Grant the XPR service account **Full Control** of the drop directory for the NTFS authentication. Proceed as follows:
 - Invoke the context menu for the replay directory.
 - Change to the **Security** tab in the properties dialog.
 - Add the XPR service account as user via the **Add** button.
 - Assign the **Full Control** privilege to the XPR service account.

- Grant the NETWORKSERVICE on the server with the Hub Transport Server Role **Full Control** of the replay directory. Proceed as follows:
 - Invoke the context menu for the replay directory.
 - Change to the **Security** tab in the properties dialog.
 - Add the NETWORKSERVICE as user via the **Add** button.
 - Assign the **Full Control** privilege to the NETWORKSERVICE.

Creating the replay directory is now complete.

Configuration of the ExchApl for access to the transport directories

The transport directories on the XPR side must now be configured.

1. In the XPR monitor open the configuration dialog of the **ExchApl**.
2. Switch to the **Exchange Foreign Connector** tab.
The entry lines for **Drop directory** and **Replay directory** display the XPR server name as default.
3. In the **Drop directory** and **Replay directory** specify the path to the shared transport directories according to the following pattern:

For the **Drop directory**

\\<Ip address or name of the Exchange server on which the Hub Transport Server operates>\<XPR server name>-<Exchange2010 mailbox server name>

For the **Replay directory**

\\<Ip address or name of the Exchange server on which the Hub Transport Server operates>\Replay

4. Click on **Apply** and **OK** to save the modifications.

The entered values are stored in the XPR server registry:

Registry path:

HKLM\SOFTWARE\Wow6432Node\PP-COM\MRS\ExchApl

Key:

DropDirectory and ReplayDirectory).

The configuration of the XPR Foreign Connector on the side is thus complete.

The **ExchApl** must be rebooted for the configuration settings to take effect.

NOTE: If the default logging window of the monitor displays an error message after you have saved the modifications, the system is unable to locate the two directories via the specified path. Open the ExchAPL settings dialog again and correct your path specifications.

5.3 Configuration

5.3.1 Configuring the LDAP Api

5.3.1.1 General Considerations

With Windows 2000, Microsoft have introduced the Active Directory Concept which allows a much more flexible administration of any kind of user data. Browsing the Active Directory requires a protocol, specially developed for this purpose. This protocol is called Lightweight Directory Access Protocol, LDAP for short. It is a further development of the access protocol Directory Access Protocol (DAP), based on the X.500 Directory Service, since the DAP could not meet the demands in terms of speed and overhead any more.

Active directory

The Active Directory Service¹ (DS) is understood as a scalable directory service structured similarly to a folder directory in a file system. However, here we do not deal with a file hierarchy (e.g. nested directories as with the complete path: `c:\Company\Site\Department\Group...`) but with an object hierarchy. An object is in this context a unit described by a unique, named set of attributes. With folder directories, the Explorer would principally be the counterpart to the LDAP protocol, used for Active Directory display and editing.

During log-in to the network and the search for released resources, Active Directory clients must be able to communicate with computers on which Active Directory is executed. This means that extraneous access to the domain control and global catalogs has to be performed using LDAP (Lightweight Directory Access Protocol).

LDAP (Lightweight Directory Access Protocol)

LDAP² is a communication protocol developed for TCP/IP networks. The LDAP protocol defines in which way directory clients access directory servers, carry out directory actions and make use of shared directory data. LDAP standards are established by IETF (Internet Engineering Task Force) working parties. In Active Directory the LDAP specifications for attributes and the IETF standards for the LDAP versions 2 and 3 are implemented.

-
1. See also the five-volume reference by Microsoft:
Active Directory Developer's Reference Library, David Iseminger,
Microsoft Press 2000, ISBN 0-7356-0993-6
 2. Further literature to deepen the LDAP subject:
Implementing LDAP, Mark Wilcox, Wrox Press Ltd.-1999, ISBN 1-861002-21-1

As the name already suggests, LDAP is an efficient method to access directory services without the complexity of other directory protocols. Since the LDAP protocol defines which processes are permitted in querying and modifying directory information and how to perform safe access, you can list directory objects, execute queries or administer Active Directory with LDAP.

LDAP and interoperability

LDAP is an open Internet standard. The use of LDAP enables cooperation of Active Directory with the directory services of other suppliers. As component of Active Directory Interfaces (DSI), the Active Directory support of LDAP comprises an LDAP supplier object. The Active Directory interfaces support the LDAP application programming interfaces for C defined in the internet standard RFC 1823. You can easily adjust other applications for directory services to access Active Directory information via DSI and LDAP.

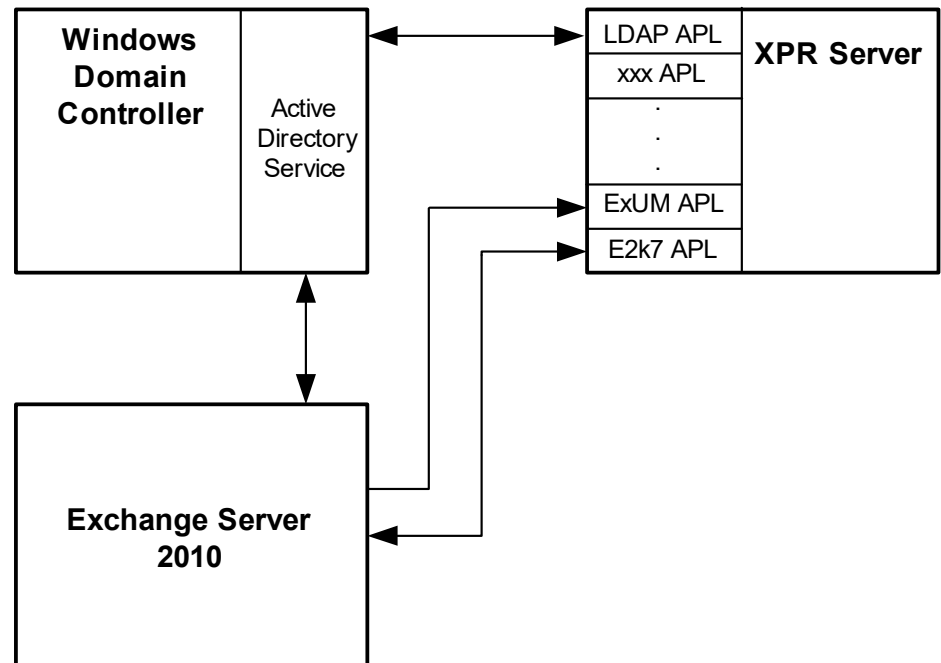
Active Directory and Exchange Server

In the course of standardization and a stronger integration of Exchange in the operating system Windows 2000, Exchange Server (from version Exchange 2000 Server) has been completely adapted to cooperation with the directory service Active Directory introduced in Windows 2000. This means that now all Exchange directory information is stored in Active Directory, too. Thus the individual Exchange directory used in previous versions to centrally store objects of an organization (e.g. addresses, mail boxes, distribution lists and public folders...) has been replaced. Among other things it was necessary to install a special directory service to administer data replication between individual Exchange servers. Connecting Exchange to the Active Directory Service of Windows has the following advantages:

- Enabling a centralized object administration.
This means that the directory objects can be administered from one place with only one management tool as of operating system version Windows 2000 Server.
- Security management simplification.
Because *Exchange Server 2003*, *2007* and *2010* uses the same security functions as Windows, all security regulation modifications (user or group accounts) apply to data stored in Exchange and Windows as well.
- Efficient creation of distribution lists.
The security groups defined in Windows are automatically used as distribution lists by *Exchange Server 2003*, *2007* and *2010*.
- Simplified access to directory information.
By creating an LDAP interface you can display and edit the Active Directory data via the native LDAP protocol.

5.3.1.2 Active Directory and XPR Server

In order to meet future requirements and to ensure the interplay with *Exchange Server 2003*, *Exchange Server 2007* and *Exchange Server 2010*, the Active Directory (DS) directory service was integrated in the XPR system with the help of the LDAP APL.



For this purpose a separate connection to the Active Directory via the LDAP APL is required. The function of this is to enable a mapping between the attributes of the Active Directory and the data relevant for XPR, in other words to establish correct assignment. Since manual adaption of the database fields is relatively laborious, the effort is minimized by performing the basic configuration via the import of a standard configuration file (`xxx.lcf`).

Miscellaneous

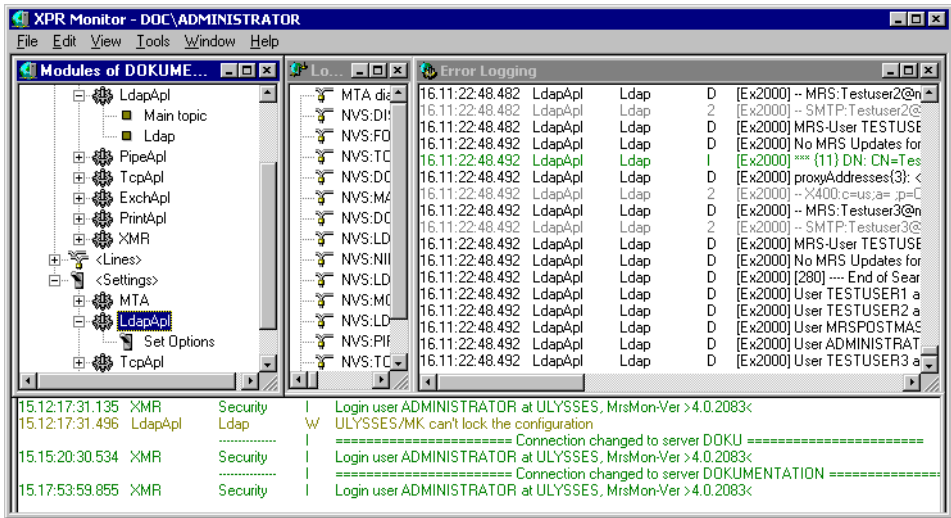
1. The LDAP APL only serves to replicate user data - the DS pattern is not extended or modified.
2. The LDAP port used is configured on 389 by default.
3. The LDAP APL is so conceived that it can additionally access other systems supporting the LDAP protocol.

5.3.1.3 Installing the LDAP APL

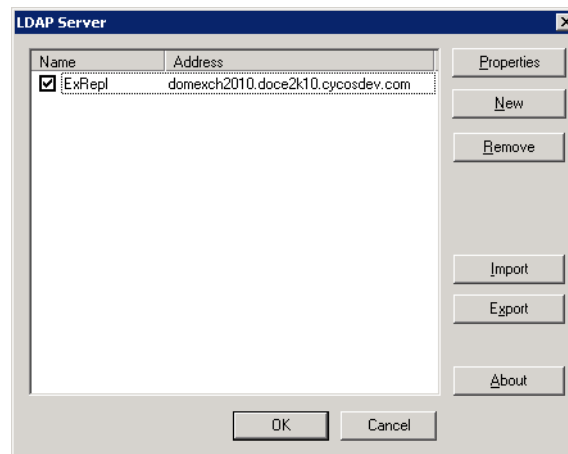
Installation via the XPR setup

Installation of the LDAP APL is embedded in the XPR server setup. If a new XPR server is to be set up for *Exchange Server 2010*, the LDAP APL must be integrated in the installation for selecting the Exch APL. The LDAP APL installation procedure in the XPR setup is described in [Section 5.2.6.3, “Installing the LDAP APL”](#), on page 177.

5.3.1.4 Editing LDAP Settings



All LDAP settings are performed from within the XPR monitor. You reach the setting options via the **Modules of <XPR server name>** window. Expand the branch next to **<Settings>**. Then open the subtree **LdapApl**. Subsequently, double-click **Set Options** to open the LDAP APL settings dialog.



This first dialog **LDAP Servers** serves general administration purposes. The names and IP addresses of already existing LDAP configurations are listed here. From here you can define further LDAP configurations (LDAP links) and edit already existing ones. In use is the server that features a check mark before the name entry.

The buttons in this dialog have the following significance:

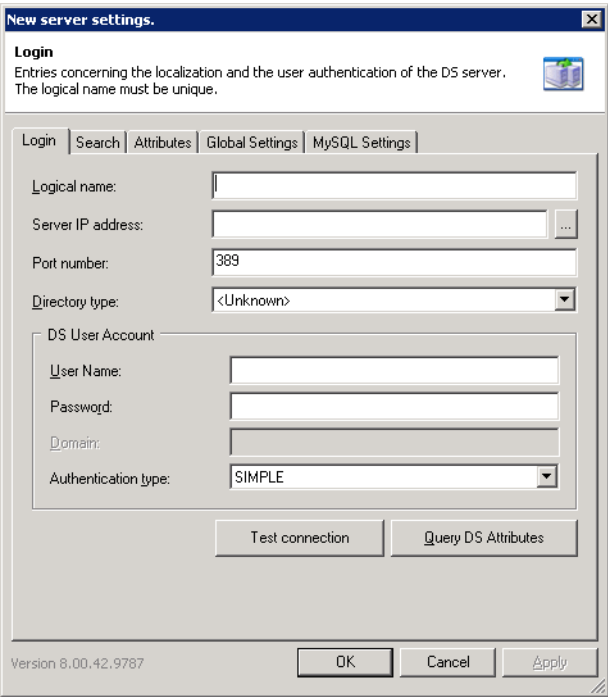
Properties

When you select an arbitrary configuration entry, the **Properties** button takes you to the configuration dialog **Edit server settings**. In there you find four setting tabs used for changing the LDAP configuration.

New

Via the **New** button you can add further LDAP configurations. When you enable it you are taken to the **New server settings** configuration dialog. To define a new LDAP configuration here, fill in the four tabs **Login**, **Search**, **Attributes** and **Global Settings**.

The significance of the individual entry lines can be gathered from the **Properties** button description further below.

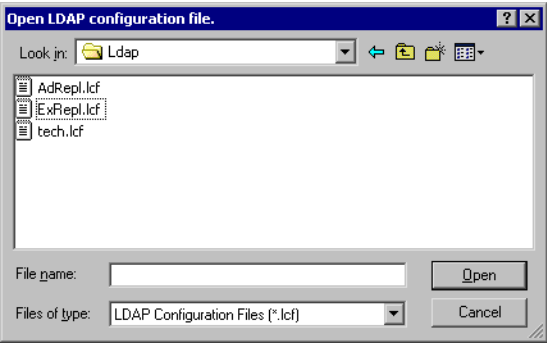


Remove

Deletes a selected LDAP configuration file.

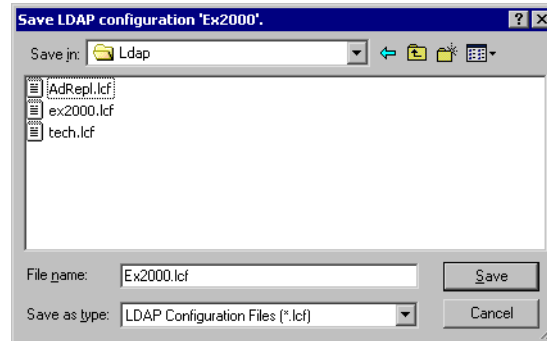
Import

Branches to the file selection window **Open LDAP configuration file**. Here you can enter an existing configuration file (format: xxx.lcf). In this way it is possible to implement different configuration files. Completing this step takes you to the **Login** tab in the **Edit server settings** window where you can perform modifications.



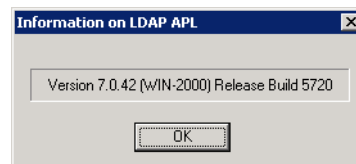
Export

If stored as `xxx.lcf` file, a configuration file can be created, which includes all current settings of the selected server.



Info

The About button opens an information dialog that displays the currently active LDAP APL version. With a click on **OK** you leave this dialog again.



OK

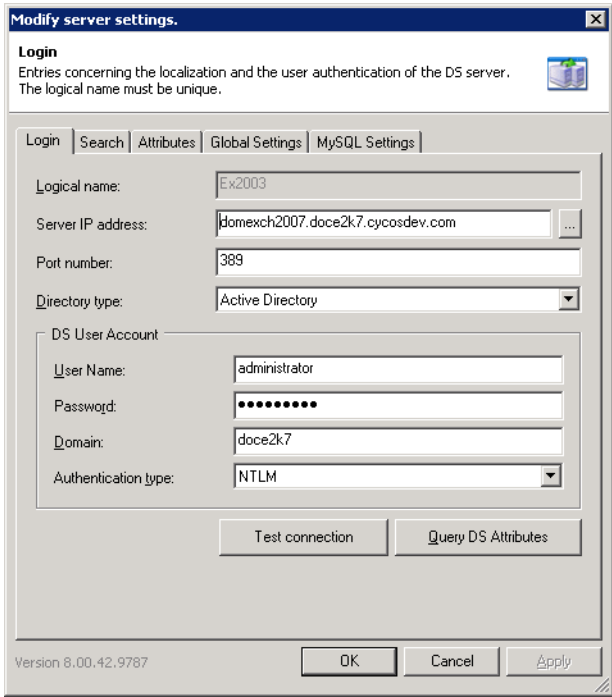
Copies the entries made in the **Edit server settings** tab and closes the LDAP APL setting dialog.

Cancel

Terminates the LDAP APL configuration without copying modifications previously made.

5.3.1.5 The “Login” Tab

Here all information on this DS server is displayed. In the upper section you find the assigned LDAP configuration name and the entry lines for the IP address, the port number and the directory type of the LDAP server. Thereunder, entry lines for user identification data are available. With the exception of the short name (name of the LDAP connection) assigned upon the reconfiguration you can now edit settings for DS server localization and the access privileges.



NOTE: The LDAP configuration name (**Logical name**) is only possible via a redefinition of the configuration settings.

The functions of the input fields on the **Login** tab are as follows:

Dialog Entry	Description
Logical name:	Here you can assign an arbitrary name to a new LDAP configuration. This name must be unique since it is used for registry entry replication. If you open an already existing DS server configuration via the Properties button, the previously assigned name is displayed. It can, however, not be changed in this form.

Table 14 Entry Fields in the LDAP Settings Tab “Login”

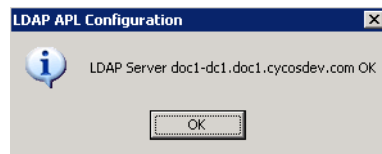
Dialog Entry	Description
Server IP address:	In this entry line you can specify the valid DS server IP address (either the qualified host name or the numeric address), or the IP address of the selected entry is displayed. If you have opened an existing configuration, the IP address of the selected configuration is displayed. To simplify things you can use the  button (to the right of the entry line) to search the entire network for the desired DS server.
Port number	Entry field for displaying the currently set port or to modify the port number. Note: Ports 3268 cannot be used for searching the Active Directory. Via port 3268 the global catalog (thus the entire forest) is searched for a specific attribute, with only reading access being possible. In addition, the global catalog only holds a subset of the AD attributes. The extensionData attribute does not belong to this subset. Consequently, the extensionData attribute cannot be read out or written via this port. The following warning is issued via the LDAP APL in this case: <i>LdapApl Ldap W [Ex2003] ldap_modify [1 attributes]: Unwilling To Perform</i>
Directory type:	This menu allows selection of either Active Directory, <unknown> or DirX. For our purposes set Active Directory here. The other options refer to LDAP connections to other systems.
In the DS User Account section	
User name	Here, the name of the user account is entered/displayed that is furnished with the corresponding privileges for the AD access. The AD access is possible if this user account belongs to the group of domain administrators or to the group of Builtin account administrators.
Password	This entry field is for definition of the password associated with the above user account.
Domain	Field for entry (or display) of the domain name associated to the above user account.
Authentication type	The definition of the authentication type must be set to NTLM (NT Lan Manager) for connecting the Active Directory Service. The alternatives SIMPLE and Negotiate are intended for other directory systems. Annotation: When you log in with the authentication type SIMPLE , the user name must be entered in the LDAP format, i.e. as "Distinguished Name" (DN). Example: uid=admin,ou=administrators,ou=TopologyManagement,o=NetscapeRoot

Table 14 Entry Fields in the LDAP Settings Tab "Login"

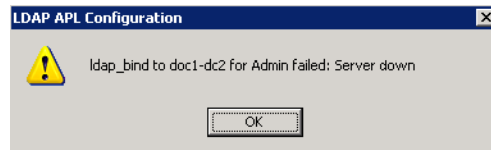
The data relevant for the DS server selection are now entered.

Testing the connection

Via the **Test connection** button you can verify the entered connection data. You are informed about the status of the connection to the DS server by a message shown in the below illustration.



In case of an error (the connection cannot be established), the same dialog appears with a special text message that, if possible, contains details on the problem occurred.



Polling DS attributes

Via this button you can manually trigger the initial transmission of the DS attributes. Otherwise, the selected DS server reads out the DS attributes by way of a periodically occurring query and lists them in the **Attributes** tab (see **Polling interval** and **Schedule** in the **Search** tab). You can watch this process on the XPR monitor as well. See also [Section 5.3.2, "Monitoring the LDAP APL Activities"](#), on page 230.

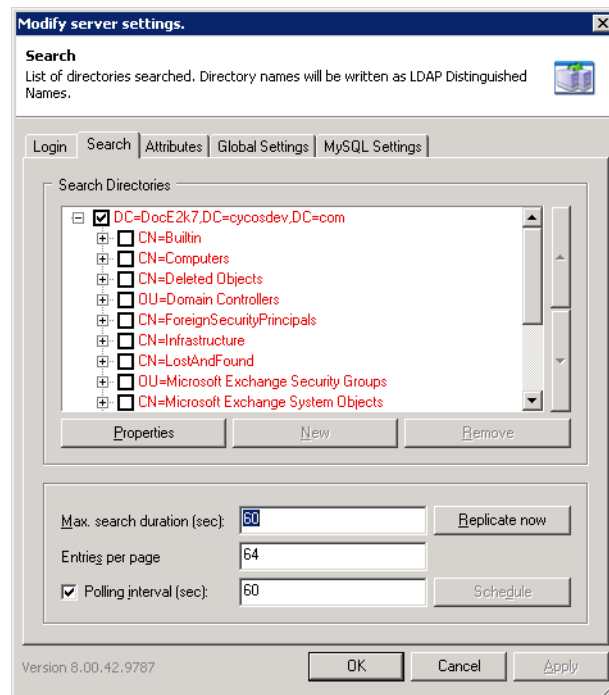
5.3.1.6 The “Search” Tab

General

The **Search** tab is used to define directories or user entries that are to be integrated in the replication process. Here you must explicitly select the containers that include users whose attributes are to be replicated.

NOTE: Make sure to only select containers that include real users. Otherwise unwanted entries (for example the Exchange system mailbox) may be integrated in the replication process. A new user “system mailbox” would then be generated on the XPR server with each replication process.

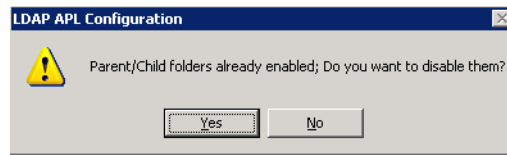
The containers or user entries in the search directory are color highlighted according to the search depth.



The **Search Directories** section displays the directories of the entire DS tree. You can expand the tree (click the [+] icons) to display the single user entries. To select a directory, place a check mark in the corresponding box next to the branching nodes of the tree.

- **Black entry:** Only the attributes of the users defined in the respective container object are replicated.
- **Blue entry:** Only the user attributes of the first level below the selected container will be replicated.
- **Red entry:** The entire subtree will be included in the replication.

An implemented logic prevents a redundant replication. An error message is issued when a new selection includes an already existing one.



If you confirm this message with **Yes**, the new setting becomes active and the old one is automatically adapted. **No** restores the state before the modification.

NOTE: Annotation on selecting users whose attributes are to be replicated: If in a larger organization all users have been defined in one container and attribute replication is only required for a subset of these users, the selection process may become relatively protracted when all users have to be selected individually. In this case filter rule definition can be applied to specify the selection. Another option is to define the users intended of replication in a special container.

The two arrow icons on the right margin of this window display serve to modify the directory sequence in the list represented. Select the container or container object to be moved with a click and move it up or down according to the new position desired. In this way you can customize the replication priority since otherwise, with several selected directories, the processing sequence is from top to bottom.

Replication settings

The buttons and entry fields in the bottom section of the dialog define the temporal replication process.

- **Polling interval**

IMPORTANT: Default after the installation is 0 seconds. Thus replication is at first deactivated so that it does not occur uncontrolled.

Each entered number value *x* starts the replication after *x* seconds (for example: with an entry of 12 the next replication starts after 12 seconds). Instead of via a polling interval, replication can also be performed via a schedule definition. Deactivate the checkbox next to the **Polling interval** entry to automatically activate the **Schedule** button. Schedule definition is described further below. If you want regular replication via a polling interval and no valid time value has been entered yet, an error message informs you accordingly.

- **Max. search duration** (Default 60 seconds)

This value determines the maximum duration of a replication. Any numeric value x ($x > 0$) entered there terminates the replication when this value has been reached after x seconds.

- **Entries per page**

Since timeout problems may occur when extremely large amounts of data have to be replicated, you can determine the number of data records to be transferred per transmission unit via the **Entries per page** field. *0* means that all data records are to be transmitted in one go; any other value restricts the number of data records. For example, 128 data records are sent per transmission unit with the entry *128*.

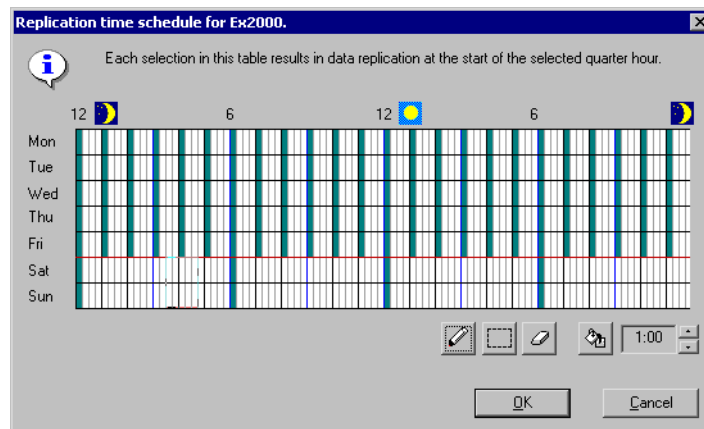
- **Replicate now**

Via the **Replicate now** button you can start this process manually.

- **Schedule**

With a click on the **Schedule** button you can create a replication week profile. Replication can be set in 15-minute steps for each weekday.

NOTE: Replication does not occur if it is to be performed via a schedule but no settings have been made there. No error message is issued on this.



After opening the schedule you can edit the replication times. The following tools are available:

Tool	Description
	Serves to arbitrarily enter replication times in the schedule.
	Selection tool for marking sections in the week profile.

Table 15

Tools to create a Replication Schedule

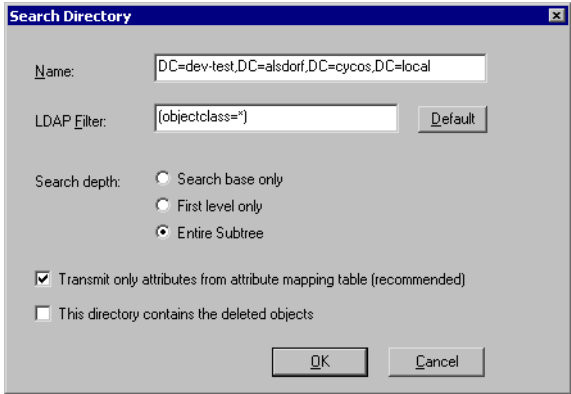
Tool	Description
	With the eraser function you can remove single replication times from the week profile. If and entire area has previously been selected with the selection tool, the replication marks within the marked area are maintained in case of replication mark deletion.
	Is used to define a replication time for a whole week if replication is to occur each day at the same time in the same interval. The intervals can be specified in the entry field next to this icon.

Table 15 Tools to create a Replication Schedule

The Properties, New, and Remove buttons

The **New** and **Remove** buttons are intended for manual configuration (directory type “unknown”). In the *Exchange Server 2010* connection context (directory type “Active Directory”) they are meaningless the therefore inactive.

After clicking on **Properties** you can view and modify the search directory settings.



The **Name** specifies the **search base** or the starting point of the search run within the directory hierarchy. Under **Name** the search base is displayed as node of the DS branch.

The **LDAP Filter** field specifies the **search filter** that determines the conditions for searching the data records (objects). This filtering also enables looking for special criteria of the user data replication. In the **LDAP Filter** field the search filter can be restricted to specific attributes. The default filter `objectclass=*` replicates all entries. Any complex logical filter¹ is conceivable.

NOTE: As of Exchange Server 2007 the distribution groups support the **sAMAaccountName**. As a result, all Exchange users with this attribute are replicated as full XPR users to the XPR server. This causes problems when assigning the MRS address type and the number of replicated users exceeds the number of available user licenses. Applying suitable filtering here, for example via `(&(objectclass=*)(!objectClass=group))`, you may restrict the users to

1. For more information see: Implementing LDAP, Mark Wilcox, Wrox Press Ltd. 1999, ISBN 1-861002-21-1

be replicated. In the above filtering example this would concern users who do not have an `ObjectClass=Group`. In the single case the filter to be defined depends on the structure in which the users are implemented in the Active Directory.

After changing the filter you can click on the **Default** button to switch to the `objectclass=*` filter again.

The **search area** indicates which part of the directory starting from the search base is to be searched. The search area can be set for the selected object via the **Search depth** option:

- **Search base only**
Only the attributes of the users defined in this container object are replicated.
- **First level only**
Only the user attributes of the first level below the selected container will be replicated.
- **Entire Subtree**
The entire subtree is included in the replication.

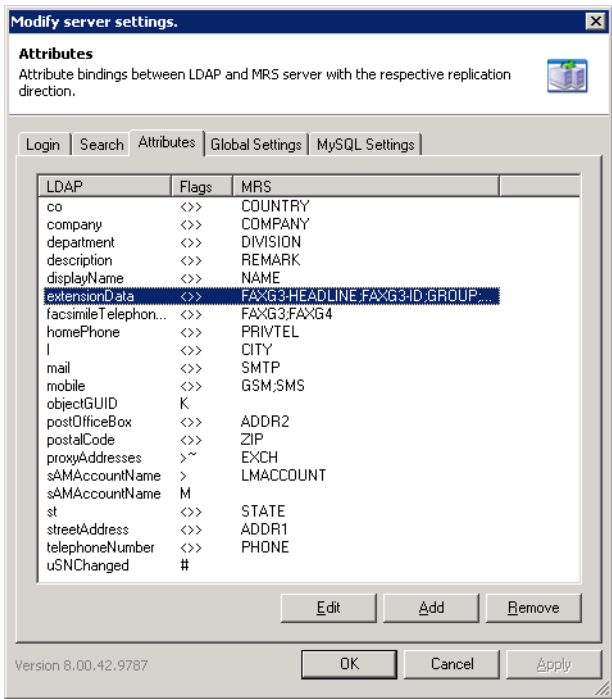
By means of the checkbox **Transmit only attributes from attribute mapping table (recommended)** you can define that only the entries listed on the **Attributes** tab are transmitted. This setting is recommended since it optimizes IP transmission (only attributes needed most are transmitted).

When the checkbox **This directory contains the deleted objects** is active, the elements of the folder entered in the **Name** field are interpreted as “deleted”. The expression “deleted” is somewhat inaccurate here since objects thus defined are not removed but only hidden.

The settings become valid with **OK**; **Cancel** terminates the previously described process without performing any modifications. Simultaneously you are taken back to the **Search** tab.

5.3.1.7 The “Attributes” Tab

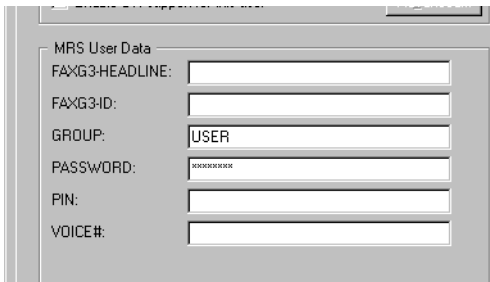
The central window of the **Attributes** tab lists the DS attributes, the corresponding XPR data fields and the set flags. They are already defaulted by the basic setting respectively by importing the configuration file for the *Exchange Server 2010* connection (*ExRepl.lcf*).



Of the listed attributes the **extensionData** attribute is especially significant. The XPR data fields assigned to this DS attribute are exactly those you find in the Exchange users' properties dialog on the **MRS Settings** tab, where they are configured.

The configuration of the **extensionData** LDAP attribute is stored in the “MRS Setting Object” in the Active Directory. The MRS Setting Object for the LDAP configuration is available only once for the entire Exchange environment.

Via editing this attribute you can add further fields on the **MRS Settings** tab. See [Section 5.3.1.7, “Extending XPR attributes”, on page 224.](#)



When you click on the **Edit** button, settings for selected attributes can be changed and via **Add** further attributes are selected, assigned and various attribute parameters set.

The following illustration shows the empty form to select a new attribute and the required mapping as well as settings of the individual parameters (usage of attributes, replications etc.).

The attribute to which the following settings relate is selected and displayed in a combo box in the **Directory Service Attribute** section. Next to this name field, the data type is specified in the field with the gray background under **LDAP Type**. Thus you are informed whether the type is a string variable (**str**), an integer variable (**int**) etc. Thereunder, another field is placed to display the **Subtype**: if there is another differentiation in subtypes as e.g. with an Octets type.

The checkboxes included in this portion have the following functions:

Checkbox	Description
Create new MRS user Sets Flag: M	Use this attribute if a new XPR user is to be defined. The value of this LDAP attribute is used as user ID on the definition of new XPR users. If the Use attributes to link DS users to XPR users option is not active, this value also serves to directly link an LDAP data record to the data of an XPR user of this name.

Table 16 Settings for the LDAP Directory Service Attribute

Checkbox	Description
Cache key Sets Flag: K	Integrates an attribute in the cache (for faster access). Once an XPR user has been found, he/she is then directly found via the cache key in each following search and his/her data are available faster.
Update Sequence Number (USN) Sets Flag: #	The USN is an update ID incremented from XPR attributes to DS attributes with every search request. When this checkbox is active, only records that have a larger USN-ID than the one generated with the last search run are replicated.
Mandatory for MRS user	Defines that this attribute is mandatory for an XPR user. If this option is set, a user is only defined if the attribute is filled in. In other words, if the attribute entry is deleted, all users that do not have this attribute entry will be deleted with the next replication.

Table 16 Settings for the LDAP Directory Service Attribute

Thereunder you find the **XPR Attributes** selection field to assign the above selected DS attribute to the corresponding XPR database field. All XPR database fields are listed here so that each DS attribute can be mapped on each XPR field (and vice versa).

The associated checkbox allows using this attribute when a new **DS user** is to be created (sets flag: **D**). This option is presently not available but will be implemented for future applications.

The checkboxes coming next determine the replication direction. You can alternatively replicate to the XPR server (**Replicate to XPR**, sets flag: **>**), to the domain server (**Replicate to DS**, sets flag: **<**) or to both simultaneously (both flags are set: **< >**). If a reciprocative replication is desired, you need to define one of the two servers as the superordinate one. This is done via activation of the **DS is master** or **XPR is master** switches.

Through activating the checkbox **Use attributes to link DS users to XPR users** (sets flag **~**) you can directly relate a DS user to an XPR user via attributes. Indirect linkages can thus be defined. For example, with DS attribute *proxyAddresses*, XPR attribute *EXCH* and activated option, all DS data of a user are assigned via the value of the DS attribute *proxyAddresses* to the XPR user who has the same contents in the *EXCH* database field.

The switches in the **Filter for Attribute Values** section can be set to manipulate attributes in various manners (for example, to quickly determine a user etc.). Depending on the complexity of the manipulation, this can either be done by a regular expression or by an e-Script. E-Scripts are programs for establishing e.g. complex filters.

The following setting options are available:

Filter setting	Description
None	The filter function is deactivated.
Regular expression:	Entry fields for regular expressions.
E-Script	Entry field for the name of the e-Script to be applied to the DS attribute.

Table 17 Filter Settings for the LDAP Attribute Values

Definition example of an attribute's replication properties with usage of the **Regular expression** filter function.

The entries in the above dialog have the following significance:

- All entries of the directory attribute *proxyAddresses* are filtered.
- When an entry matches the regular expression *XPR:%t*, it is replaced with the expression on the right and copied; all other are rejected. *%t* serves as wild card for an arbitrary, not empty chain of characters without blanks entered in the right field for *%1*. You can generally enter several sub-patterns in the regular expression field on the left-hand side; on the right-hand side you can then indicate the *n*th sub-pattern with *%n*. You find more information on regular expressions in the **E Programming Language** and **XPR Server Administration** manual, chapter "LDAP APL".

The settings performed are copied with **OK**. You are simultaneously taken back to the **Attributes** tab. Newly selected and edited attributes are added at the bottom of the list.

Extending XPR attributes

An additional example explains how to add new fields to user data (in **Active Directory Users and Computers**) on the **MRS Settings** configuration tab.

IMPORTANT: If additional XPR attributes are defined here for the DS server, data replication to the XPR server may lead to the deletion of XPR-significant data fields. If an XPR data field is replicated when empty, then a completed data field may be deleted (overwritten by the empty data field). Data fields must consequently not be left empty with defining a user.

1. In the XPR monitor under LDAP APL select the **Set Options** function.
2. Next, mark the desired server in the list of possible LDAP servers and enable the **Properties** button.
3. In the **Edit server settings** dialog then open switch to the **Attributes** tab.
4. Select the **extensionData** entry from the attribute list.
5. Click **Edit**.

The **XPR Attributes** combination field displays all entries of the **extensionData** directory attribute.

6. You can now select additional data fields via the associated checkboxes in the **XPR Attributes** selection dialog. These fields are then additionally integrated after a click on **OK** in the user settings with **Active Directory Users and Computers**.

Cancel terminates the process and modifications already performed are disregarded. A click on either button simultaneously takes you back to the **Attributes** tab.

If the attributes are defined by the configuration file, they are listed on the **Attributes** tab with the already existing assignment to the XPR system. This means that with the represented attribute the corresponding XPR data field on which this attribute has been mapped is displayed. There are various flag symbols between the attribute name and the XPR data fields which already provide information about how certain attribute or replication parameters are set. The following flags or combinations of them can be set:

Flag Symbol	Significance for the selected attribute
M	The attribute is used when a new XPR user is to be defined.
D	The attribute is used when a new DS user is to be defined (this option is presently not available).
K	Integrating the attribute in the cache (for faster access).
#	This flag indicates that the search run is only performed from the last replicated records.

Table 18 List of possible Attribute Flags

Flag Symbol	Significance for the selected attribute
<	Replicates this attribute to the DS server (with XPR as master). This setting can be used if e.g. a new <i>Exchange Server 2010</i> is to be coupled to an existing XPR server to replicate all XPR data to the AD.
>	Replicates this attribute to the XPR server (AD is master).
<>	Replication in both directions.
<>>	Replication in both directions with AD as master.
<<>	Replication in both directions with XPR as master.
~	This flag shows that the directory service user is linked directly with an XPR user by means of the attribute.

Table 18 List of possible Attribute Flags

The **Edit** button enables the modification of the attribute parameters of a selected entry at a later date. When you click it, the **LDAP/XPR Attributes** dialog opens with the entries made for the selected attribute. You can adapt entries and save them as described above.

Replication of XPR multivalued fields

The XPR server database can be so extended that for some entries so-called multivalued entries can be generated. In this way it is possible to define several phone numbers for one database entry. The field **VOICE** or **PHONE** can be intended for this purpose, if several phones or voiceboxes are needed for one user. The fields are stored in the database consecutively numbered: **PHONE** (primary field), **PHONE.01** (the first non-primary field) etc.

However, since the AD does not provide any number of attributes for phone numbers, these fields cannot be directly replicated to the AD in this format. The phone number entries in the AD are so organized that only the first phone number (primary) can be replicated via the *telephoneNumber* attribute, all other phone numbers (non-primary) are replicated via the *otherTelephone* attribute.

So that these fields can be integrated in replication to the AD server, an additional field is offered (for example **PHONE.***). This field serves exclusively for replicating non-primary fields, thus for example the database fields **PHONE.01**, **PHONE.02** etc. It is possible to replicate the multivalued fields in different ways:

- LDAP single value to XPR multivalued field.

Example: *telephoneNumber* to *PHONE*

Only the primary entry is replicated to the XPR server.

- LDAP multivalued to XPR multivalued field.

Example: *otherTelephone* to *PHONE*

All multivalued entries are replicated to the XPR server 1:1.

- LDAP multivalued to XPR multivalued fields without the primary field

Example: *otherTelephonetoPHONE.**

All multivalued entries, except for the primary field, are replicated to the XPR server.

Attribute settings for additional LDAP servers (e.g. subdomains)

As attributes for additional LDAP servers, e.g. additional subordinate domains, are not automatically preset, these must be set as follows:

1. Select the first server in the **LDAP Servers** window and export its settings to a file by means of the Export button. The changes for the new server must now be made in this file.
2. Open this file with the editor, change the entries for the Domain Controller **DC** and for the Container **CN** and, where applicable, **OU** to be replicated and save your changes in a file.

```
dirType:ActiveDir
Script:EXRep1
AttMap:21
co:COUNTRY:0, str:toM, toD:none
company:COMPANY:0, str:toM, toD:none
department:DIVISION:0, str:toM, toD:none
description:REMARK:0, str:toM, toD:none
displayName:NAME:0, str:toM, toD:none
extensionData:FAXG3-HEADLINE;FAXG3-ID;GROUP;PASSWORD;PIN;VOICE#:2, octets:toM, toD:none
facsimileTelephoneNumber:FAXG3#;FAXG4#:0, str:toM, toD:none
homePhone:PRIVTEL#:0, str:toM, toD:none
l:CITY:0, str:toM, toD:none
mail:SMTP:0, str:toM, toD:none
mobile:GSM#;SMS#:0, str:toM, toD:none
objectGUID::1, octets:key:none
postOfficeBox:ADDR2:0, str:toM, toD:none
postalCode:ZIP:0, str:toM, toD:none
proxyAddresses:EXCH:0, str:toM, cor:rule:"MRS:%t":%l
sAMAccountName:LMACCOUNT:0, str:toM, script
sAMAccountName::0, str:newM:none
st:STATE:0, str:toM, toD:none
streetAddress:ADDR1:0, str:toM, toD:none
telephoneNumber:PHONE#:0, str:toM, toD:none
uSNCchanged::0, int64:usn:none
Folders:3
DC=doc-test, DC=aisdorf, DC=cycos, DC=local: (objectclass=):2:a:2
OU=Test_UO: (objectclass=):0:3:0
CN=Users: (objectclass=):0:3:0
```

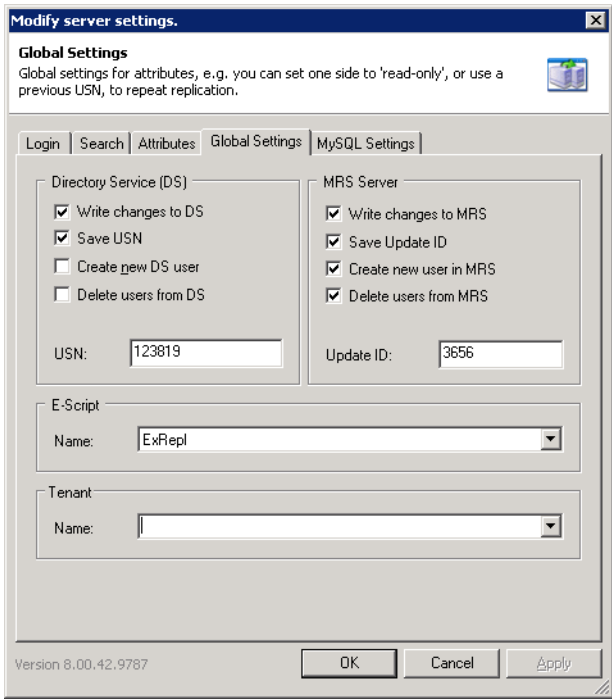
3. This file is now imported into the LDAP Servers window. In the following the same specifications are demanded for the new server as already described in section 2.4.3.1, “The “Login” Tab”, on page 281. The **Search** and **Global Settings** tabs must now be filled out. Enter the same settings here as for the first server.

5.3.1.8 The “Global Settings” Tab

On the **Global Settings** tab you can perform additional, more detailed settings.

The **Global Settings** tab consists of four sections.

- Settings that refer to the Directory Service (DS),
- Settings that concern XPR (**MRS Server**) and
- a selection dialog to pick an e-script and



Settings in the **Directory Service** and **XPR Server** section are performed analog for the Active Directory and XPR side. You can perform the following settings:

Dialog Function	Description
Write changes to DS and Write changes to MRS	Modifications can either be saved in the Active Directory, on the XPR system or in both.
Save USN and Save Update ID	With the modifications copied upon LDAP APL shutdown, the USN (Update Sequence Number) and/or the UID (Update ID) is incremented. Here you can determine whether this is desired for one of the two or for both. The corresponding values are stored in the registry. Both IDs make sure that replication processes performed at a later date can start from a certain flag rather than all over again.

Table 19 Global Directory Service Settings for the LDAP APL

Dialog Function	Description
Create new user in MRS	Depending on the preset replication directions, creation of a user entry can be suppressed for testing purposes by deactivating the checkbox .
Delete users from MRS	Via this checkbox deletion of user entries can be suppressed for testing purposes (resetting the checkbox).
Entry fields: USN and Update ID	By means of these entry fields, a replication can be started from a certain USN (Update ID). In doing so it should always be clear what has been replicated with the entered USD. In this context it is useful to keep a log on the replication processes.

Table 19 Global Directory Service Settings for the LDAP APL

E-Script

You can select an e-script in the corresponding section used for automatic attribute editing. The defaulted e-script **ExRepl** active for the Exchange connection sets the predefined values for the standard replication.

An e-script can act as complex filter allowing e.g. telephone number normalization or special actions upon creating a new XPR user. Selection of e-scripts is performed via the pull-down list. Existing e-scripts are generally contained in the `... \XPR\res\Ldap` directory.

Tenant (with Exchange Server 2003 only)

NOTE: Here you can select one of the defaulted tenants for a multi-tenant scenario with several Exchange organizations.

5.3.1.9 “My SQL Settings” Tab

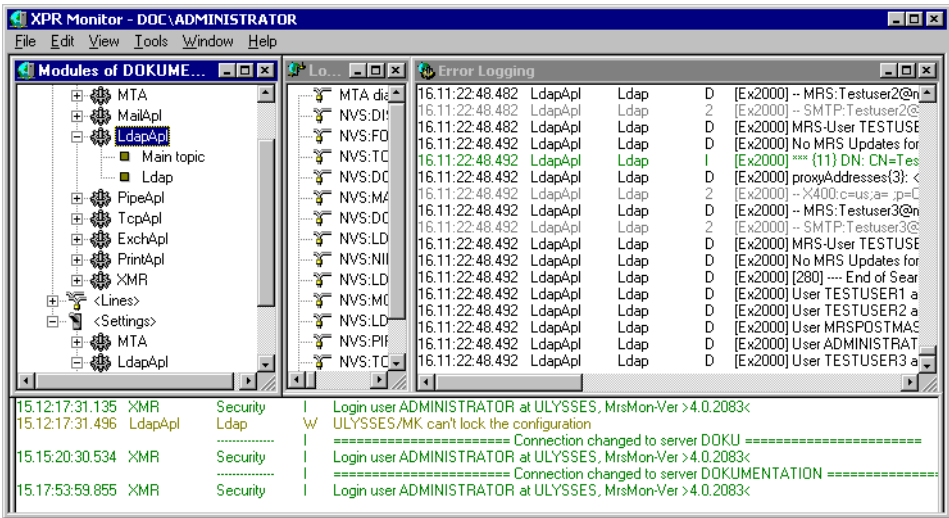
No settings need to be performed here for connecting the Active Directory to the XPR server in an Exchange scenario. The **MySQL Settings** tab serves for configuring another deployment scenario for the LDAP Apl.

5.3.2 Monitoring the LDAP APL Activities

Via the XPR monitor you can precisely observe which actions are currently carried out by the LDAP APL. The following short instruction shows you the path to this display:

1. In the XPR monitor access the **Modules of <XPR server name>** window and drag the gear wheel icon  LdapApl named “LdapApl” from the <Topics>  branch to the **Error Logging** window per Drag&Drop.
2. Adapt the parameters for the data to be displayed in the **Logging Monitor Properties** window.
3. Verify your settings with the **Copy** button.
4. Confirm your selection with **OK**.

The selected LDAP APL activities are now logged in the **LdapApl-All Topics** window (see next figure).



The **XPR Monitor** chapter of the **XPR Server Administration** manual informs you about further monitoring and logging options.

5.3.3 Uninstalling the LDAP APL

Analog to the uninstallation of other XPR components, you can uninstall these from the command line with the following command:

```
LdapApl remove.
```

The running component must previously be closed down via the *Service Control Manager*. You do this by selecting the component in the services list and a click on **Stop**.

You can also close the LDAP service via the DOS console. Enter the following command in the command line:

```
LdapApl stop
```

5.3.4 User Administration

The XPR MMC Snap-in installation extends the **Properties of <user>** register in **Active Directory Users and Computers** with the **MRS Settings** tab.

NOTE: Users who do not have an Exchange mailbox cannot see the **MRS Settings** tab.

If the XPR MMC Snap-in is installed on a 32-bit operating system you reach this settings page as follows:

1. Start the administration program **Active Directory Users and Computers** via **Start > Programs > Administrative Tools**.
2. Select the corresponding user directory there.
3. Open the associated properties dialog with a doubleclick on the desired user entry.

NOTE: You can also reach the **Properties** dialog through opening the context menu.

4. Switch to the **MRS Settings** tab.
On this tab, XPR-relevant settings are performed individually for each user.

If the XPR MMC Snap-in is installed on a 64-bit operating system, you must start the Active Directory Users & Computers Snapin in 32-bit mode (`dsa /32`).

NOTE: You find further information in the Microsoft KB article [http://msdn.microsoft.com/en-us/library/ms692753\(VS.85\).aspx](http://msdn.microsoft.com/en-us/library/ms692753(VS.85).aspx)

Proceed as follows:

1. Open the application start-up panel via **Start > Run**.
2. Enter the following command:

```
dsa.msc /32
```

The managing program **Active Directory Users and Computers** opens in 32-bit mode.

3. Select the corresponding user directory there.
4. Open the associated properties dialog with a doubleclick on the desired user entry.

NOTE: You can also reach the **Properties** dialog through opening the context menu.

5. Switch to the **MRS Settings** tab.
On this tab, XPR-relevant settings are performed individually for each user.

5.3.4.1 “MRS Settings” Tab

The screenshot shows the 'Test User 1 Properties' dialog box with the 'MRS Settings' tab selected. The dialog has a tabbed interface with the following tabs: Member Of, Dial-in, Environment, Sessions, General, Address, Account, Profile, Telephones, Organization, Remote control, Terminal Services Profile, COM+, and MRS Settings. The 'MRS Settings' tab is active, showing a checkbox for 'Unified Messaging and telephony features' which is checked. Below this is a section for 'CTI settings' with a checkbox for 'Activate CTI' which is also checked, and an 'Advanced...' button. The 'MRS User data' section contains several text boxes: 'FAXG3-HEADLINE:', 'FAXG3-ID:', 'GROUP:' (containing 'USER'), 'PASSWORD:' (containing 'XXXXXXXX'), 'PIN:', and 'VOICE:' (containing '101'). At the bottom, it says 'Data last modified: 05.12.2007 17:08:41' and has 'OK', 'Cancel', 'Apply', and 'Help' buttons.

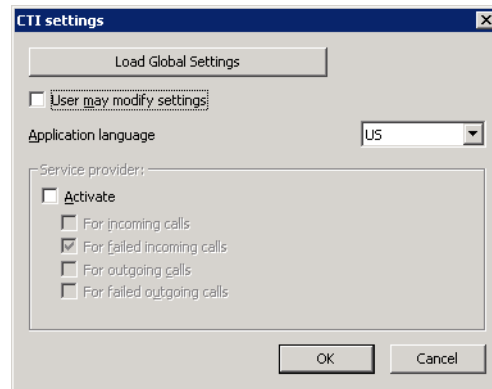
With the **Unified Messaging and telephony features** option it is possible to exclude this user from the features provided on the XPR system. Remove the checkmark to delete the user from the XPR database.

CTI settings

Via the **Activate CTI** checkbox, telephony functions (for the CTI client) can be released for the respective user provided they are implemented and configured. This generates and activates the **CTIJOURNAL** database field for this user on the XPR server.

Advanced CTI settings

Via the **Advanced...** button you reach the **CTI settings** dialog in which you can set a user's CTI functions different from the global settings. The global settings are defaulted via the connector configuration. See [Section 5.3.5.3, “CTI Settings Tab”, on page 241](#).



Via the **Load Global Settings** button you copy the global settings (those defaulted with the connector settings) for this user.

User may modify settings

Setting this option allows the user to change his/her settings for the CTI client.

Application language

Here you can select the language to be used in the CTI client dialogs for this user.

Service provider

The CTI client does not log calls if the program has not been started. Enabling the **Activate** checkbox you can set for all calls that the associated XPR-CTI journal entries are sorted into the corresponding CTI client directories via the service provider.

The behavior can be individually configured for the following call states:

- For incoming calls
- For failed incoming calls
- For outgoing calls
- For failed outgoing calls

XPR user data

These are the database fields that were defined in the LDAP APL via the default setting or after extending the **extensionData** field. You find further information about database fields and how to expand them in the description of the LDAP APL configuration in [Section 5.3.1.7, “The “Attributes” Tab”, on page 220](#).

NOTE: If the **PIN** field remains empty, the default PIN will be used. This PIN is specified via the general voicemail settings in the respectively installed telematics APL. If a PIN is entered in the Exchange user definition that deviates from the default PIN, the relevant user will not be automatically forced anymore to change the PIN assigned here when he/she logs on to his/her voice box for the first time.

Which database fields are available by default and the purposes they serve is described in detail in the Server Administration manual, chapter **User Data Administration**, section **Database Fields Significance**.

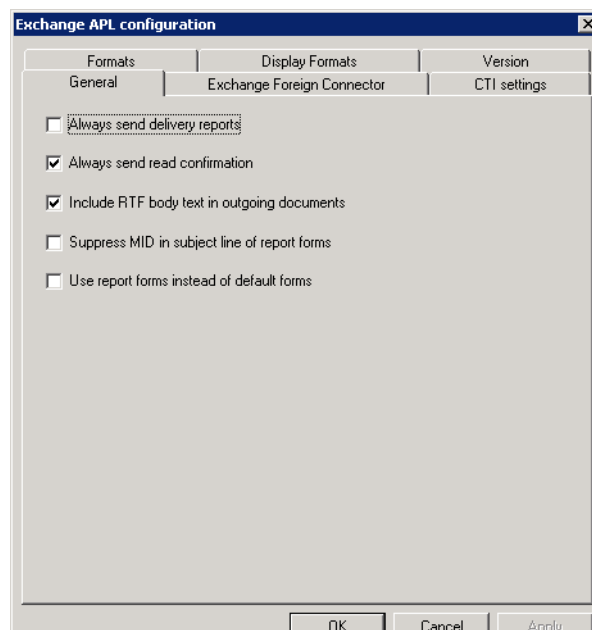
5.3.5 Administration of the XPR Foreign Connector

All connector properties that need to be configured for the XPR server are configured with the new XPR Foreign Connector via the settings dialog of the **ExchAPL** in the monitor. The following connector properties can be set:

- The connections to the transport directories found on the server that has the Mailbox Server Role.
- The global CTI settings.
- The message formats

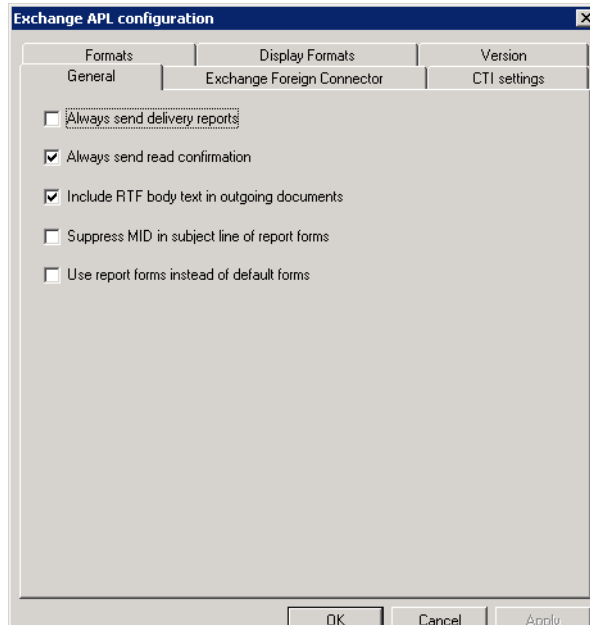
How to edit the settings of the XPR Foreign Connector:

1. Start the XPR monitor.
2. In the **Modules of <XPR server name>** window expand the branch **<XPR server name>**, then the branch **<Settings>** and finally the branch **ExchApl**.
3. Open the **ExchApl** settings dialog with a doubleclick on **Set Options**.
The configuration dialog of the XPR Foreign Connector opens.



5.3.5.1 General Tab

On the **General** tab you perform settings for creating and sending delivery reports.



The **Always send delivery reports** option generates a delivery report for messages that originate from Exchange, even when not explicitly asked for. The **Always send read confirmation** option returns a read report to the MRS originator as soon as messages are read on the Exchange server. The originator on XPR side receives a read report as soon as the Exchange user opens the document.

If you activate the **Include RTF body text in outgoing documents** option, a document in Rich Text Format (RTF) is sent as attachment in addition to the normal text representation. RTF is the official data exchange format used by Microsoft for text files. Text files exchanged in this format retain their formatting e.g. font weight, etc. when being transferred between users.

When the **Suppress MID info in subject line of report forms** option is activated, the message IDs in square brackets are omitted from the subject line. The ID display is of no significance to the normal user, but it helps tracking a routing process. Furthermore, IDs are used to assign a report to a message.

NOTE: In case of default reports it is not possible to suppress the message ID display.

Via **Use report forms instead of default forms** XPR confirmation forms are used instead of the normal Exchange default forms. For a more detailed description of the function and installation of XPR reports refer to the *Unify OpenScape Xpressions V7 Server Administration* manual from the **Automatic Report Transmission per Mail** section.

5.3.5.2 Exchange Foreign Connector Tab

The screenshot shows the 'Exchange APL configuration' dialog box with the 'Exchange Foreign Connector' tab selected. The 'Drop directory' field contains '\\<Hub Transport Server>\<Drop Directory>' and the 'Replay directory' field contains '\\<Hub Transport Server>\Replay'. There is a checkbox for 'Multiple Hub Transport Servers' which is currently unchecked. Below it are fields for 'Replay directory (Server 2)', 'Replay directory (Server 3)', 'Replay directory (Server 4)', 'Replay directory (Server 5)', and 'Replay directory (Server 6)', all of which are empty. At the bottom, there is a note: 'Before saving these values the Apl checks for their validity and logs errors otherwise. Changes take effect after Apl restart.' and buttons for 'OK', 'Cancel', and 'Apply'.

On the **Exchange Foreign Connector** tab, in the **Drop directory** and **Replay directory** entry lines, you specify the path to the shares (drop and replay directory) used for the message transport.

NOTE: If this path is not defined yet, the XPR server name is displayed here as default.

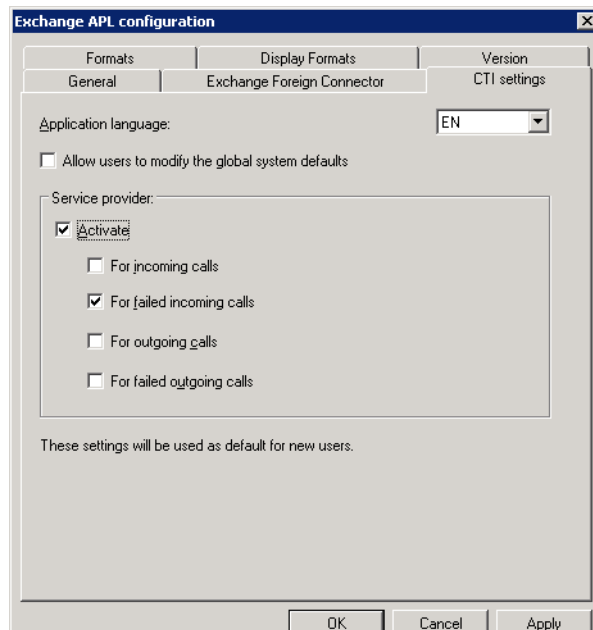
In the **Drop directory** and **Replay directory** specify the path to the shared transport directories according to the following pattern:

- For the **Drop directory**
`\\<Ip address or name of the Exchange server on which the Hub Transport Server operates>\<XPR server name>-<name of the Exchange Server 2010 Mailbox Server Role>`
- For the **Replay directory**
`\\<Ip address or name of the Exchange server on which the Hub Transport Server operates>\Replay`

After you have specified the path click on **Apply** and **OK** to save the modifications.

NOTE: The configuration respectively a modification of the configuration settings does not take effect until the **ExchApl** is rebooted.

5.3.5.3 CTI Settings Tab



On the **CTI settings** tab you find the **global** CTI settings valid for all users. These global defaults may later be customized in the course of the user definition.

Application language

Sets the language to be used in the CTI client dialogs.

Allow users to modify the global system defaults

This option enables all users to change the settings globally defaulted here.

NOTE: The permission to modify global defaults can be individually and belatedly granted as part of the CTI settings on user level. See [Section 5.3.4.1, “CTI settings”, on page 234](#).

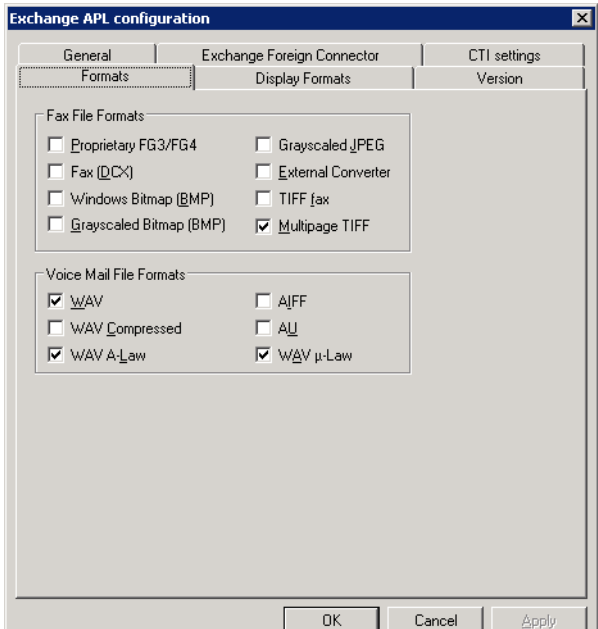
Service provider

The CTI client does not log calls if the program has not been started. Enabling the **Activate** checkbox you can set for all calls that the associated XPR-CTI journal entries are sorted into the corresponding directory via the service provider after the CTI client start.

The behavior can be individually configured for the following call states:

- For incoming calls
- For failed incoming calls
- For outgoing calls
- For failed outgoing calls

5.3.5.4 Formats Tab



On the **Formats** tab you can set the file formats accepted by the XPR Foreign Connector.

The Exchange client should be able to display these formats of course. Documents received by the XPR server that are not in one of the formats selected in this dialog would be converted into one of these formats prior to being sent to the Exchange gateway.

NOTE: A maximum of one conversion is performed, even if several possible target formats are specified. Here, an internal evaluation comes to bear that performs the “cheapest” conversion from the converter’s point of view.

When using the XPR Outlook extensions, the WAV format must be selected for the voicemail feature.

The following **Fax Formats** are available:

File formats for fax messages	Description
Proprietary FG3/FG4	Proprietary fax format (XPR Viewer).
Fax (DCX)	Multi-page PCX graphic format. Used by Microsoft fax.
Windows Bitmap (BMP)	Individual fax pages are converted in a Windows Bitmap.
Grayscale Bitmap (BMP)	Individual fax pages are converted in a Windows Bitmap, where a trilinear grayscale interpolation is performed.

Table 20 File formats for fax messages

File formats for fax messages	Description
Grayscale JPEG	Fax data are converted in a nine-grayscale JPEG format. This format is suitable for viewing with HTML mail clients.
External Converter	When you select this format, a configurable program is called, which executes a conversion from TIFF in an arbitrary format instead (see info box under this table). When you activate this external conversion, further fax formats must not have been selected beforehand.
TIFF Fax	Single-paged, compressed TIFF fax format.
TIFF multipage	Fax data according to TIFF stand (multi-page).

Table 20 File formats for fax messages

External Converter Support

Selecting this option activates an external converter. You find the preferred Fax2PDF converter in the `AddOn` directory on the product data carrier. For this feature you need to perform the following registry entries under the key:

```
[HKLM\SOFTWARE\PPCOM\mrs\Mrs-Globals\Converter\]
```

TiffToExternalConverter REG_SZ *<Program name with parameters>*

TiffToExternalExtension REG_SZ *<Extension>*

Example of *<Program name with parameters>*:

```
D:\XPR\res\convert\Fax2PDF\Fax2Pdf %1 %2
```

Example of *<extension>*:

```
pdf
```

You find further information about the functions of the external converter in the *Server Administration* manual in Appendix A under the caption: *Document Formats*.

The following **voicemail file formats** are available for selection:

Voicemail File Formats	Description
WAV	Windows Audio Format
WAV Compressed	Compressed Windows Audio Format. This format enables direct compression of voicemails that are routed via the Exchange gateway. Further settings, such as the Audio-Codec used for compression, are performed via the maintenance options in the MTA configuration. The appropriate codec to play-back compressed files is also required on the client computer. Note: Besides the subsequent compression for memory-saving storage on the XPR server, the Codecs setting is also responsible for direct compression. Direct compression is available for Integrated as well as for Unified Messaging and applies with the arrival of a message. It is used for all voicemails transmitted by the XPR MTA, i.e. all voicemails recorded by Forward and Guest Access. Direct compression is not used with messages directly created in Microsoft Exchange by True Unified Messaging. These are all messages recorded in Direct Access.
WAV A-Law	European ISDN-voicemail format.
AIFF	Audio format used predominantly on Apple computers.
AU	Unix audio format.
WAV μ-Law	US ISDN-voicemail format.

Table 21

Voicemail File Formats

5.3.5.5 Display Formats Tab

Via definitions in the **Display Formats** tab you can replace formats for message information defaulted by the XPR system with customer-specific defaults in the Outlook journal **Subject** and **From** column. This setting applies system-wide for all Exchange users receiving XPR voice and fax messages.

Formats	Display Formats
From	
From (Fax):	
From (Voice):	
Subject:	
Subject (Fax):	
Subject (Voice):	

To replace the XPR default formats, you need to fill the opposite fields with new format texts, with the generic defaults in the **From** and **Subject** being replaceable with specific defaults.

NOTE: If no configuration is performed here, the standard entries for the **From** and **Subject** columns generated by the XPR server are passed on to Exchange 1:1.

You can set:

- In which of the two Outlook journal columns (**From** and **Subject**) the additional information is to appear.
- For which message types (fax, voicemails or both) the information is to be displayed.
- Which message parameters are to be shown and whether the parameters are to be embedded in an explanatory text.

The top three entry lines are intended for entries in the **From** column in the Outlook journal. The three bottom columns are allocated for the **Subject** column.

If you want to display information for both message types (fax and voicemails), enter the corresponding parameters in the **From:** and **Subject:** entry lines, possibly supplemented with text.

You can display the information separately in the Outlook journal according to fax and voicemails via the **From (Fax)** and **From (Voice)** or **Subject (Fax)** and **Subject (Voice)** entry lines.

NOTE: Please note that entries in these fields will overwrite possible entries in the **From:** and **Subject:** fields, which then become effectless.

Possible parameters include:

Parameter	Description
<i>{originator}</i>	When a message comes in, this parameter is replaced with the XPR originator. Example: <i>FAXG3/01234567</i>
<i>{callername}</i>	When a message comes in, this parameter is replaced with the display name of the originator, provided it has been found in the XPR database. Example: <i>Joe User</i> .
<i>{callernumber}</i>	When a message comes in, this parameter is replaced with the formatted calling number of the caller. Example: <i>447711</i>
<i>{size}</i>	When a message comes in, this parameter is replaced with the number of fax pages or the voicemail message length. Example of fax messages: <i>2</i> (number of pages). Example of voicemails: <i>23</i> (message length in seconds).
<i>{orgnumber}</i>	When a message comes in, this parameter is replaced with the original calling number of the caller. Example: <i>49123987654</i>
<i>{service}</i>	When a message comes in, this parameter is replaced with the service used for transmitting the document. Example: <i>FAXG3</i>

Table 22 *Parameters for additional XPR Information Display in the Outlook Journal*

Examples:

The entry

{service} mail from "{caller name}" <{caller number}> {size} page(s)

either in the **From:** or **From (Fax):** entry line would generate the following text in the **From** journal column with an incoming fax message:

FAXg3 mail from "Joe User" <0240412345678> 2 page(s)

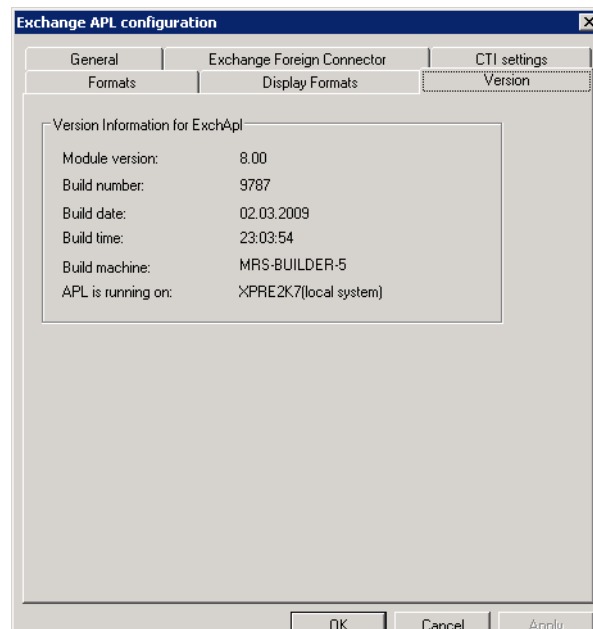
The entry

Voice message from: {caller name} ({caller number}) {size} seconds

either in the **Subject:** or **Subject (Voice):** entry line would generate the following text in the **Subject** journal column in case of an incoming voicemail:

Voice message from: Joe User (0240412345678) 23 seconds

5.3.5.6 Version Tab



The version number of the Exchange APL installed is shown on the **Version** tab. This number should always be entered when reporting errors.

5.4 Multi-Hub Transport Server Support

You can use several hub transport servers to configure a load distribution and to grant high availability. You can connect a maximum of five additional hub transport servers to the system. These servers must have been configured in the network and contain a shared replay directory called **Replay** in the path %ProgramFiles%\Microsoft\Exchange Server\TransportRoles in each case.

IMPORTANT: All hub transport servers additionally connected for this purpose also require access to the drop directory. These additional hub transport servers must therefore be granted the privileges for accessing the drop directory share.

NOTE: You can rename both directories and store them anywhere in the system. If this is desired, adjust the new directory names and the directory paths in the system upon the creation, activation or configuration.

If you use the multi-hub transport server version, the Exchange server and the XPR server require a commonly used and shared resource for the drop directory. Since only one XPR Foreign Connector can be installed on the XPR server, the drop directory must be on the server that all Hub Transport and mail servers as well as the XPR server can access.

Depending on the Exchange environment, the drop directory needs to be configured on the following servers:

- If only one mail server is available for several multi-hub transport servers, the drop directory is created on a commonly used and shared resource of the mail server.
- If the mail server is a clustered server with an SAN drive, the drop directory is created on a commonly used and shared resource of the cluster.
- If the mail server is a clustered server without SAN drive, the drop directory is created on a commonly used and shared resource of the XPR server.

You find more detailed information about adjusting the path and sharing the **drop** and **replay directory** in [Section 5.2.7.1, “Creating the Transport Directories”](#), on [page 198](#).

5.4.1 Configuring the Multi-Hub Server Support

How to configure the multi-hub transport support:

1. Install the Exchange connection pretending that only one Exchange Hub Transport server is available. See [Section 5.2.6.5, "XPR Foreign Connector Installation", on page 185](#).

Besides the mailbox server, select an arbitrary, already existing hub transport server in the Exchange servers' setup dialog. The name of this server is automatically entered as value in the registry key HUBTRANSPORTSERVER.

NOTE: You cannot configure a multi-hub transport support during the setup. This is only possible after the Exchange connection has already been installed. Only then the required **ExchApl** registry branch and the configuration dialog for the **ExchApl** can be accessed on the XPR server.

2. Register all additionally deployed hub transport servers that send messages from the XPR server to the *Exchange Server 2010* via the Exchange Foreign Connector. The server names of all hub transport servers used are entered in the Exchange system in the **SourceTransportServers** parameter.

Proceed as follows:

- Start the *Exchange Server 2010 management shell*.
- Enter the following command in the console:

```
Set-ForeignConnector -Identity
<ForeignConnectorIdParameter>
-SourceTransportServers "<DEFAULT hub transport server
name>",
"<name hub transport server 1>", "<name hub transport server 2>",
... "<name hub transport server 5>"
```

You find further information about the console command `Set-ForeignConnector` in the *Microsoft TechNet*:

<http://technet.microsoft.com/en-us/library/bb123789.aspx>

NOTE: The first line of this command is separated from the second line by a blank

```
(...IdParameter> -SourceTransp...).
```

3. Define where you wish to install the drop directory.

- Follow the instructions given in [Section 5.2.7.1, “Creating the Transport Directories”](#), on page 198 to configure this commonly used and shared resource.
- Set the “RootDropDirectoryPath” path of the hub transport server to zero:

```
Set-TransportServer -identity <hub transport server>  
  
-RootDropDirectoryPath ""
```

NOTE: The first line of this command is separated from the second line by a blank

(...port server> -RootDropDi...).

- Repeat this process for the other available hub transport servers.
- Set the complete UNC path of the commonly used and shared drop directory for the Foreign Connector:

```
Set-ForeignConnector -Identity "MrsConnector (<XPR server  
name>  
:<name of the Exchange Server 2010 Mailbox Server role>)"  
-DropDirectory "\\<UNC path to the commonly used and  
shared drop directory>\<XPR server name>-<name of the  
Exchange Server 2010 Mailbox Server role>" or <name of the  
commonly used and shared drop directory>
```

NOTE: The second line of this command is separated from the third line by a blank

(...Server role>)" -DropDirectory "...).

4. Test the previously performed configuration steps. Use Outlook to check whether messages to be sent via the XPR server are delivered to the new drop directory.
5. Start the XPR server.
6. Expand the registry in the HKLM\Software\Wow6432Node\PP-COM\MRS\ExchApl branch and create manually the corresponding key (HUBTRANSPORTSERVER<1...5>) for each additionally used hub transport server (maximum 5). Enter the server name associated to the respective hub transport server as value.
7. Enter the UNC path names of the replay directories additionally used in the **ExchApl** settings dialog.
8. Open the **ExchApl** settings dialog in the XPR monitor via **ExchApl -> Set Options**.

9. Switch to the **Exchange Foreign Connector** tab.
10. Enable the **Multi Hub Transport Server** option. This activates the entry fields for specifying the UNC names of the replay directories additionally used.
11. In the entry fields, specify the UNC path names of the drop directory used.
12. Enter the UNC path names of the replay directories additionally used in the corresponding fields.

The screenshot shows the 'Exchange API configuration' dialog box with the 'Exchange Foreign Connector' tab selected. The 'General' sub-tab is active. It contains fields for 'Drop directory' and 'Replay directory', both set to '\\<Hub Transport Server>\<Drop Directory>' and '\\<Hub Transport Server>\<Replay>' respectively. The 'Multiple Hub Transport Servers' checkbox is checked. Below it are six 'Replay directory (Server X)' fields, each set to '\\<Hub Transport Server X>\<Replay>'. At the bottom, there is a note: 'Before saving these values the Apl checks for their validity and logs errors otherwise. Changes take effect after Apl restart.' and buttons for 'OK', 'Cancel', and 'Apply'.

13. Click on **Apply** to save the data.
14. Click on **OK** to close the settings dialog.
15. Reboot the **ExchApl**.

NOTE: By monitoring the drop directory, you can now check whether the XPR server retrieves the messages delivered here, thus whether they are removed from the drop directory.

5.5 Using additional Address Spaces for the Exchange Connectors

5.5.1 Overview

In Exchange organizations where you find two or more XPR kernels that provide a connection to this Exchange environment, you need to assign message transmission to a fixed XPR connector that delivers messages to a specific Exchange server. This avoids addressing the wrong Exchange server, which leads to an increased server load and thus to additional message transport efforts.

Because the XPR Foreign Connector designed for *Exchange Server 2010* is no longer capable of configuring message transport restrictions with the help of user lists, the path must lead here via different address space types.

If several Xpressions servers are to connect a single Exchange organization via connectors, a unique MRS proxy ID, thus an individual address space type, is required for each connector.

The default address space type for each Exchange connector is **MRS**. However, you can assign a different address space type to each Exchange connector per configuration. This restricts the message transmission to the connector for which it is configured.

Example:

Address space definition via EXADDRESSTYPE	Assigned users
MRS1	User 11, user 12, ..., user 1n
MRS2	User 21, user 22, ..., user 2n
...	...
MRSn	User n1, user n2, ..., user nn

Defining the address space type for the single Exchange connectors with assignment to the desired Exchange servers then determines the connector to handle the message transport.

5.5.1.1 Configuration Overview

Required configuration steps:

1. Configuring the Address Space on the Exchange Server
2. Creating the required "Active Directory object" using the `CreateProxyAddr.bat` batch file.
3. Copying the DLLs into the corresponding Exchange directories for creating the proxy addresses.
4. Configuring the e-mail address policies.
5. Adding the required **EXADDRESSTYPE** registry key. You need to configure this registry key for the XPR Foreign Connector (Exch APL) as well as for the Unified Messaging Connector (ExUM APL). The additional address spaces are assigned to the respective connectors via this key.

5.5.2 Configuring additional Address Spaces

5.5.2.1 Configuring the Address Space on the Exchange Server

On the Exchange side you need to set the "AddressSpaces" of the XPR Foreign Connectors in such a way that they correspond to those on the "ExAddressType" Xpressions side.

You need to configure the address space type in Exchange manually via the *Exchange Management Shell* (EMS). In this process you need change the default address space type (**MRS:*;1**) on all *Exchange servers 2010* for the second and all further connectors.

The following address space types are assigned to the additional connectors on the Exchange servers:

XPR Server	MRS Address Space Type	Exchange Address Space Value
For the first server	MRS1	MRS1:*;1
For the second server	MRS2	MRS2:*;1
...	...	...
For the n-th server	MRSn	MRSn:*;1

Use the *Exchange Management Shell* command prompt to execute the following command on the Exchange servers for configuring the assignment:

```
Set-Foreignconnector -Identity "MrsConnector (XPRESSIONS:EXCHANGE)" -AddressSpaces "MRSx:*;1"
```

MRS_x with _x= 1, 2, 3,... continually for each additional XPR connector for labeling the connectors uniquely

NOTE: You find additional information about this topic under:
<http://technet.microsoft.com/en-us/library/bb123789.aspx>

5.5.2.2 Creating the “Active Directory Object”

To define a new address space type, a batch file that creates this address space type must be started once for each additional connector.

How to create a new address space type for another connector in the Active Directory:

1. Log on to the Xpressions server with the account under which the Exch APL runs.

NOTE: For this action, the service account must be a domain account that has administrator privileges on the Exchange server.

2. Start the batch file `CreateProxyAddr.bat`
After installing the XPR connectors you find this batch file in the setup directory of the Xpressions server under:

... \xpr\bin

Example:

```
CreateProxyAddr "DC=<MYDOMAIN,DC=COM>" Temp.txt MRS1
```

Replace `<MYDOMAIN,DC=COM>` with the given domain information of the relevant customer environment.

The `MRS1` parameter must match the address space type created in the previous step.

NOTE: You can enter any file name under `Temp.txt`. Merely the `.txt` file extension must be kept. This is a temporary file created by the batch file as auxiliary file. You therefore need not create this file manually.

5.5.2.3 Copying the DLLs into the corresponding Exchange Directories

Creating the proxy addresses must now be harmonized with the new address space type.

This requires copying the DLL that generates the proxy addresses into a new directory. To do this, copy the content of the directory

```
...\Program Files\Microsoft\ExchangeServer\Mailbox\address\MRS
```

into another directory to be newly created:

```
...\Program Files\Microsoft\Exchange Server\Mailbox\address\MRSx
```

NOTE: MRSx with x= 1, 2, 3,... continually for each additional XPR connector for labeling the connectors uniquely. For example, MRS1 for the first XPR connector, MRS2 for the second etc.

Example:

```
...\Program Files\Microsoft\Exchange Server\Mailbox\address\MRS1
```

```
...\Program Files\Microsoft\Exchange Server\Mailbox\address\MRS2
```

```
...
```

```
...\Program Files\Microsoft\Exchange Server\Mailbox\address\MRSn
```

5.5.2.4 Configuring the e-mail Address Policies

The connector e-mail address policy concerned must be adjusted for each new address space type.

Proceed as follows:

1. Start the *Exchange Management Console (EMC)*.
2. Open the configuration dialog for the e-mail address policies

NOTE: You reach this dialog via: **Microsoft Exchange > Organization Configuration > Hub Transport > E-mail Address Policies.**

3. Enter a new address space type according to the sample of the available default address space type **MRS**.

Example:

E-mail address: **@MRS**

E-mail (address)type: **MRS1**

NOTE: If desired, you can remove the default e-mail address policy after adding a new custom address space type (for example **MRS1**). This will not affect this feature's function.

5.5.2.5 Adding the required EXADDRESSTYPE registry key.

The address space types that associate the XPR connectors must be activated on every XPR server. A registry key added to the corresponding registry path is used for this purpose.

For the XPR Foreign Connector (Exch APL):

HKLM\SOFTWARE\Wow6432Node\PP-COM\MRS\ExchAp1

For the XPR True Unified Connector (ExUM APL):

HKLM\SOFTWARE\Wow6432Node\PP-COM\MRS\ExUMAp1

For the Exch APL

EXADDRESSTYPE [REG_SZ]

Default:	-
Possible values:	<address space <i>name</i> >
Example:	MRSn, with n = 1, 2, 3, ...

If several XPR servers and consequently several Exchange connectors are connected to an Exchange environment, this registry key is required for differentiating the Exchange foreign connectors. Assigning special address space names then optimizes message transmission. The foreign connectors are labeled by consecutive numbering.

For the ExUm APL

EXADDRESSTYPE [REG_SZ]

Default:	-
Possible values:	<address space <i>name</i> >
Example:	MRSn, with n = 1, 2, 3, ...

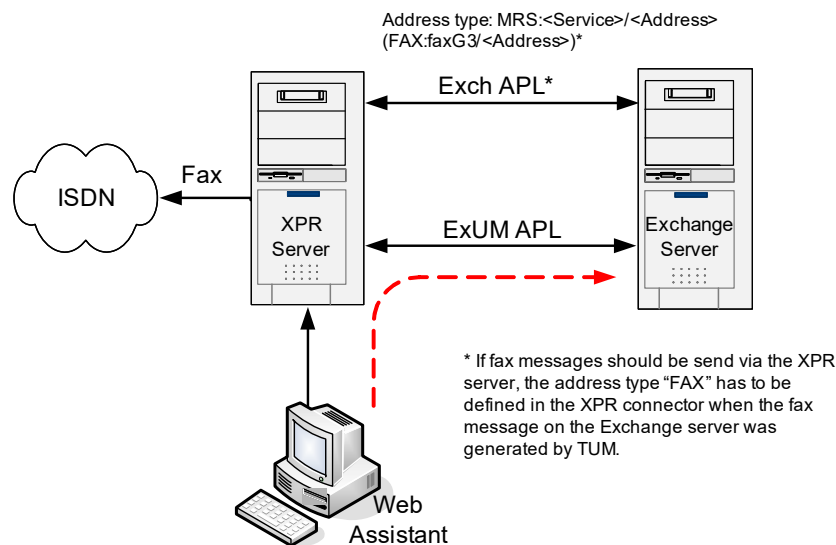
If several XPR servers and consequently several Exchange TUM connectors are connected to an Exchange environment, this registry key is required for differentiating the Exchange TUM connectors. Assigning special address space names then optimizes message transmission. The TUM connectors are labeled by consecutive numbering.

NOTE: Registry entry modifications require a reboot of the concerned Exchange Apl to take effect.

5.6 Fax Message Addressing

When addressing fax messages, the address space in the Exchange foreign connector may have to be extended by the “FAX” address type.

This is always required if fax messages were directly generated on the Exchange server and are to be transmitted via the XPR server. Fax messages are directly stored on the Exchange server e.g. if they are generated by a client that transmits the message by TUM transaction via the ExUM APL to the Exchange server (for example *Web Assistant*).



5.6.1 Definition of the “FAX” Address Type

How to configure the “FAX” address type:

1. Start the *Exchange management shell*.
2. Enter the following command in the command prompt:

```
Set-ForeignConnector "MrsConnector (<XPR-server name>:<name of the Exchange Server 2010 Mailbox Server Role>)"
-AddressSpaces "MRS:*;1","FAX:*;1"
```

The “FAX” address type is now defined for fax transmission via the XPR server.

5.7 Adding and assigning the MRS E-Mail Address Type retrospectively

NOTE: As of Exchange Server 2007 the distribution groups support the **sAMAaccountName**. As a result, all Exchange users with this attribute are replicated as full XPR users to the XPR server. This causes problems when assigning the MRS address type and the number of replicated users exceeds the number of available user licenses. Therefore, the number of user groups to be replicated may have to be restricted beforehand via the LDAP configuration.

If no default policy has been created for the MRS address type upon the installation or further address types are required, this must be done in a retrospective procedure. The MRS address type is required for assigning messages arriving via the XPR server to Exchange users.

How to retrospectively add and assign the MRS address type:

1. Start the Exchange management console.
2. In the left section of the management console expand the object group **Organization Configuration**.
3. From the list of organization objects select **Hub Transport**.
The middle section of the management console now displays the Hub Transport objects.
4. In the middle section of the management console switch to the **E-mail Address Policy** tab.
5. Select the **Default Policy** entry. The right section of the management console now displays the default policy editing features.

NOTE: You can also use the **New E-mail Address Policy** feature to specify a new policy for creating and assigning the MRS address type via this policy.

6. Select **Edit** via the actions section to add the MRS address type to this policy. The wizard for editing the policy will then open with the first dialog **Introduction**.
7. Since no settings need to be made here, push the **Next >** button in this dialog. The **Conditions** dialog opens.
8. Since no settings need to be made here, push the **Next >** button in this dialog. The **E-Mail Addresses** dialog opens.
9. Use here the selection button (next to the **Add** button) to select **Custom Address** for the MRS address.
The Custom Address entry mask opens.

10. In the **E-mail address** field specify the address description (e. g. **@MRS** or, if additional address descriptions are required, **@MRS1** etc.).
11. In the **E-mail type** field specify the address type **MRS**.
12. Complete your entries with **OK**.
You return to the **E-Mail Addresses** dialog. The new address type is displayed here under **Address**.
13. In the **E-Mail Addresses** dialog click on **Next >**.
The **Schedule** dialog opens.
14. In the **Schedule** dialog set the time when the newly defined address type is to be adopted by the system. Then click **Next >**. The **E-mail Address Policy** dialog opens.
15. In the **E-mail Address Policy** dialog click the **Edit** button to continue the address type definition.
The **Completion** dialog opens.
16. In this dialog you can trace the address policy update. When the process is complete, click the **Finish** button.

The definition and assignment of the MRS E-Mail address type is now complete.

5.8 Security Settings for Installation and Live Operation of the E2k7 APL and ExUM APL

To ensure maximum security, various security settings can be reduced **after** the installation for real operation. This section describes which privileges are required for the installation and which privileges can be restricted for real operation.

IMPORTANT: To accomplish its tasks the XPR Foreign Connector uses MAPI access. Since Microsoft have not revealed the MAPI access privilege hierarchy, the connector function can only be granted under an account with Exchange full-admin privileges. The privilege restrictions described in the following have been tested on a system with the default policy by Microsoft. After modifying the default security policy by service packs or corporate security adaptations, the below privilege restrictions may lose their validity.

The test environment is composed of the following elements:

- Windows Server 2003 Enterprise SP2.
- Exchange Server 2010 Enterprise Edition x64.
- Exchange Mailbox Server Role and Exchange Hub Transport Server Role are installed on two physically separated servers.
- The installation is performed with the default security policy

With the installation description for each single XPR component the required privileges are named as well.

5.8.1 Requirements

The following tools are required for displaying and configuring the privileges:

- **ADSI Edit** (contained in the Microsoft Support Tools on the product data carrier for the Windows installation).
- **Exchange management console** and/or **Exchange management shell** on the product data carrier for the Exchange installation.
- The administration program **Active Directory Users and computer**.
- The administration program **Local Security Settings** (from the Windows Admin Pack, if you administer remotely from a workstation).

Definitions

<i><organization></i>	Wildcard for the name of your Exchange organization.
<i><Domain></i>	Wildcard for the name of your domain.
<i>APLSRV</i>	Name of the server on which the ExchApl runs as service.
<i>MBSRV</i>	Name of the Exchange server on which the Mailbox Server Role is installed.
<i>HTSRV</i>	Name of the Exchange server on which the Hub Transport Server Role is installed.

5.8.2 Privileges for the Exch APL Installation

Creating the XPR service account

Generate a user entry in your domain. This user account is required as service account for the Exch APL. In the following we will call this account USER. This USER needs to have a mailbox.

Microsoft demands this USER to be member of the group of domain administrators for the required MAPI access. Therefore, add this USER to the domain administrator group.

Local administrator

Promote the USER on the XPR server, on the *MBSE* and on the *HTSRV* to local administrator.

NOTE: You must be domain administrator for installing the Exch APL. Only then you are entitled to check whether the USER is a member of the domain. If you do not have the corresponding privilege, the installation will fail.

The USER must be assigned further special privileges on the XPR server. This is required for the services to work correctly. Via **Start > Programs > Administrative Tools > Local Security Policy** open the **Local Security Settings** dialog. Select **Local Policy > User Rights Assignment** and assign the corresponding privileges to the USER. The following privileges are to be assigned:

- "Logon on as a service" **1
- "Act as part of operation system" ¹
- "Backup files and directories" ¹
- "Restore files and directories" ¹
- "Logon as a batch job" ¹
- "Adjust memory quotas for a process" ¹

Exchange administrator

Promote the USER to "Exchange administrator with Read Privilege Role". This privilege is required on the Mailbox Server Role as well as on the Hub Transport Server Role.

This setting is required for reading the Exchange objects properties.

1. Such privileges are set with the connector installation. They are also required for the ExUM APL.

MRSProxy64.dll (optional for manual creation)

If you want to use the **MRS Proxy address generation** function, the USER requires “full access” to the Exchange directory \\MBSRV\address. Share this folder with the USER for this purpose (sharing permissions).

Address templates

For the address templates (407 German or 409 English) the USER must have the privilege to “create address template objects” and to “delete address template objects”. To assign these privileges start ADSI Edit and switch to the directory:

```
CN=407|CN=409, CN=Address-Templates, CN=Addressing,  
CN=<Organization>, CN=Microsoft Exchange, CN=Services,  
CN=Configuration, DC=<Domain>.
```

Open the properties dialog here and switch to the **Security Settings** tab. Add the USER via **Add** to the list displayed. Click on the **Advanced** button to change the privilege and assign the “Create address template objects” and “Delete address template objects” privileges to the USER. In the entry line select **Apply onto** “This object only”.

Address types (optional for manual creation)

Creating address types requires the privileges “Create addr type objects” and “Delete addr type objects”. To assign these privileges start ADSI Edit and switch to the directory:

```
CN=Address-Types, CN=Addressing, CN=<Organization>, CN=Microsoft  
Exchange, CN=Services, CN=Configuration, DC=<Domain>.
```

Open the properties dialog here and switch to the **Security Settings** tab. Add the USER via **Add** to the list displayed. Click on the **Advanced** button to change the privilege and assign the “Create addr type objects” and “Delete addr type objects” privileges to the USER. In the entry line select **Apply onto** “This object only”.

Default policy (optional for manual creation)

Adding address types to the default policy requires the read and write privilege. To assign these privileges start ADSI Edit and switch to the directory:

```
CN=Default Policy, CN=Recipient Policies, CN=<Organization>,  
CN=Microsoft Exchange, CN=Services, CN=Configuration,  
DC=<Domain>.
```

Open the properties dialog here and switch to the **Security Settings** tab. Assign the USER read and write privileges here.

MRS container object (1)

To create the MRS container object the USER requires the “Create container objects” privilege. To assign this privilege start ADSI Edit and switch to the directory:

```
CN=<Organization>, CN=Microsoft Exchange, CN=Services,  
CN=Configuration, DC=<Domain>.
```

Open the properties dialog here and switch to the **Security Settings** tab. Add the USER via **Add** to the list displayed. Click the **Advanced** button to change the privilege and assign the USER the “Create container objects” privilege. In the entry line select **Apply onto** “This object only”.

NOTE: As option, you can simultaneously grant the privilege to “Delete container objects” at this point.

MRS container object (2)

Creating the MRS container object additionally requires the privileges “Create directory synchronization objects” and “Delete directory synchronization objects”. To assign these privileges start ADSI Edit and switch to the directory:

CN=<Organization>,CN=Microsoft Exchange, CN=Services,
CN=Configuration, DC=<Domain>.

Open the properties dialog here and switch to the **Security Settings** tab. Add the USER via **Add** to the list displayed. Click on the **Advanced** button to change the privilege and assign the USER the “Create directory synchronization objects” and “Delete directory synchronization objects” privilege. In the entry line select **Apply onto** “Child objects only”.

MRS connector object

Creating the MRS connector object requires the “Create all child objects ” and “Delete all child objects” privileges. To assign these privileges start ADSI Edit and switch to the directory:

CN=Connections, CN=<RG>, CN=Routing Groups, CN=<AG>,
CN=Administrative Groups, CN=<Organization>, CN=Microsoft
Exchange, CN=Services, CN=Configuration, DC=<Domain>.

Open the properties dialog here and switch to the **Security Settings** tab. Add the USER via **Add** to the list displayed. Click on the **Advanced** button to change the privilege and assign the “Create all child objects” and “Delete all child objects” privileges to the USER. In the entry line **Apply onto** select “This and all child objects”.

MRS settings object

The MRS settings object serves as storage location for the connector settings and other XPR settings for the connector. First, it must be defined. The USER of this MRS settings object must then be assigned additional privileges for accessing this object. Start the ADSI Edit and switch to the directory:

CN=Microsoft Exchange, CN=Services, CN=Configuration, DC=<Domain>

Generate a new object “MRS” (object class = container) here.

Open the properties dialog here and switch to the **Security Settings** tab. Add the USER via **Add** to the list displayed. Push the **Advanced** button and assign the USER the following privileges:

- “List Contents”, “Read all properties” and “Write all properties”
- “Delete”, “Read permissions” and “Modify permissions”
- “Create all child objects” and “Delete all child objects”

In the entry line **Apply onto** select “This and all child objects”.

With these privileges the XPR component “Exch APL” can be installed via the XPR setup.

5.8.3 Privileges for the ExUM APL Installation

To set up the ExUM APL the USER must be promoted from domain user to domain administrator.

Subsequently, the ExUM APL can be installed by the XPR setup.

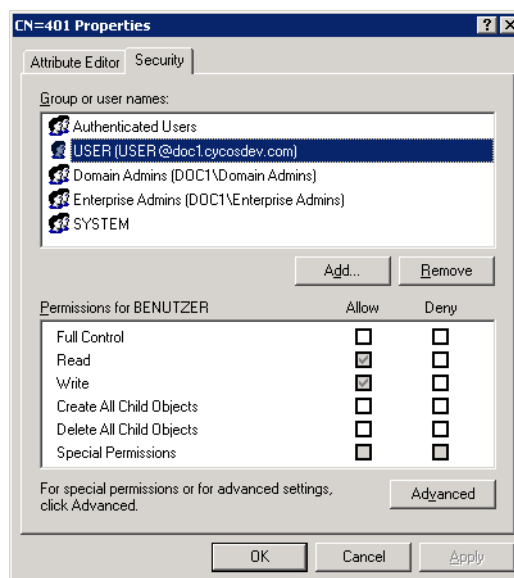
5.8.4 Privileges for the MMC Snap-in Installation

The installing user requires the privileges for modifying the AdminPropertyPages. Otherwise the installation will fail. To check this, start ADSI Edit and change to any directory under DisplaySpecifiers. For example:

CN= <401>, CN=DisplaySpecifiers, CN=Configuration, DC=<Domain>

Open the properties dialog here and switch to the **Security Settings** tab. Check whether the installing user has this right. If not, make the corresponding modifications.

read [inherited] & write [explicit]



Modify the privileges for all speech containers on the `DisplaySpecifiers` level. When you assign the privilege, select “This object and all child objects” under **Apply to**. The rights will be inherited by setting the option “Apply this permission to objects and/or containers within this container only”.

5.8.5 Privilege Restrictions for Live Operation

5.8.5.1 General

The USER can be relegated to the domain user privilege for operating the ExUM APL.

IMPORTANT: If you want to install an update, turn the restricted privileges into the state in which they were “before the installation”. After the update you can restrict the privileges again.

5.8.5.2 MRS Connector Settings

MRS connector settings (1)

The following setting is only required if you want to restrict the privilege assignment for the **MRS Settings Object** (see [Section 5.8.2, “MRS settings object”, on page 264](#)). Start the ADSI Edit and switch to the directory:

```
CN=APLSRV:MBSRV, CN=MRS,CN=Microsoft Exchange, CN=Services,  
CN=Configuration, DC=<Domain>
```

Open the properties dialog here and switch to the **Security Settings** tab. Assign the USER the following privileges:

read [inherited] & write [explicit]

MRS connector settings (2)

This privilege is only required to save administrative settings group-wide. Start the ADSI Edit and switch to the directory:

```
CN=Admin Group (Exchange Administrative Group (FYDIBOHF23SPDLT)),  
CN=MRS, CN=Microsoft Exchange, CN=Services, CN=Configuration,  
DC=<Domain>
```

Open the properties dialog here and switch to the **Security Settings** tab. Assign the USER the following privileges:

read [inherited] & write [explicit]

MRS connector object

The following privilege is required to save connector-specific settings. Start the ADSI Edit and switch to the directory:

CN=MrsConnector (APLSRV:MBSRV), CN=Connections, CN=Exchange Routing Group< (DWBGZMFD01QNBJR), CN=Routing Groups, CN=Exchange Administrative Group (FYDIBOHF23SPDLT), CN=Administrative Groups, CN=<Organization>, CN=Microsoft Exchange, CN=Services, CN=Configuration, DC=<Domain>

Open the properties dialog here and switch to the **Security Settings** tab. Assign the USER the following privileges:

Full control [explicit]

Privilege settings can be withdrawn after the installation for the following objects:

• MRS Proxy.dll	• MRS container (1)
• Address template	• MRS container (2)
• Address types	• MRS connector
• Default policy	• MMC snap-in

All other privileges are required for operating the Exch APL.

5.8.5.3 Assigning the privilege of operating Exch Apl service to any user

In environments where operating the Exch Apl service with “Local Administrator” privileges via the service account is not desired, this privilege can be assigned to another user after the installation. This is necessary, because the Apl does not start anymore after the withdrawal of the “Local Administrator” privilege.

How to assign privileges necessary for starting the Exch Apl service to a user who does not have administrative privileges:

Steps to Run the ExchApl without local admin rights

The ExchApl queries some exchange services. Without the local admin rights the service user must have read/write permissions to query the following services:

Microsoft Exchange RPC Client Access (MSEExchangeRPC)
Microsoft Exchange Transport (MSEExchangeTransport)
Microsoft Exchange System Attendant (MSEExchangeSA)
Microsoft Exchange Information Store (MSEExchangeIS)

Installing GPMC from the Command Line in Windows 2008 R2:

1. Open an elevated command prompt.
2. In the command prompt, type `ServerManagercmd -install gpmc`

XPR and Microsoft Exchange Server 2010

Security Settings for Installation and Live Operation of the E2k7 APL and ExUM APL

3. Start GPMC from the command prompt by typing `start gpmmc.msc`
4. Close the command prompt.

To set GPO in Windows 2008 R2:

To add Read and Write permissions to the service user account that was delegated on the services below,

Microsoft Exchange RPC Client Access (MSEExchangeRPC)
Microsoft Exchange Transport (MSEExchangeTransport)
Microsoft Exchange System Attendant (MSEExchangeSA)
Microsoft Exchange Information Store (MSEExchangeIS)

follow these steps:

1. On the Exchange server, start GPMC.MSC
2. Click on the domain.
3. Right-click Default Domain Policy, and then click Edit to open Group Policy Object Editor.
4. Expand Computer Configuration, expand Policies, expand Windows Settings, expand Security Settings, and then expand System Services.
5. Right-click the Microsoft Exchange System Attendant service, and then click Properties.
6. Click to select the Define this policy setting check box, and then click Edit Security.
7. Click Add, type username, click Check, and then click OK.
8. Click to select the Read check box and the Write check box.
9. Click OK two times, and then quit Group Policy Object Editor.
10. Click OK, and then quit the Active Directory Users and Computers snap-in.

Now you need to update the group policy on the Exchange with the following command:

```
gpupdate /force
```

Allow service control manager access with the following command:

```
sc [<ServerName>] sdset <ServiceName>  
<ServiceSecurityDescriptor>
```

To see the current permissions:

```
sc sdshow SCMANAGER
```

Use the Sc.exe tool to grant sufficient permissions to Authenticated Users


```
sc sdshow SCMANAGER
D: (A;;CCLCRPRC;;;AU) (A;;CCLCRPWPRC;;;SY) (A;;KA;;;BA) S: (AU;
FA;KA;;;WD) (AU;OIIOFA;GA;;;WD)
```

NOTE: The permissions string is specified in Security Descriptor Definition Language (SDDL).

The following permissions are granted after you run the command:

- Discretionary access control list (DACL)
- Allow to Authenticated Users: SDDL_CREATE_CHILD, SDDL_LIST_CHILDREN, SDDL_READ_PROPERTY, SDDL_READ_CONTROL
- Allow to SYSTEM: SDDL_CREATE_CHILD, SDDL_LIST_CHILDREN, SDDL_READ_PROPERTY, SDDL_WRITE_PROPERTY, SDDL_READ_CONTROL
- Allow to Built-in Administrators: SDDL_KEY_ALL
- System access control list (SACL)
- Audit activities of the Everyone group: SDDL_AUDIT_FAILURE, SDDL_KEY_ALL
- Audit activities of the Everyone group: SDDL_INHERIT_ONLY, SDDL_OBJECT_INHERIT, SDDL_AUDIT_FAILURE SDDL_GENERIC_ALL WD

Further details can be found under the following links:

<http://technet.microsoft.com/en-us/library/cc742037.aspx>

<http://msdn.microsoft.com/library/aa379567.aspx>

5.8.5.4 Privilege Overview

Topic	Privilege	Restrictable after the installation	Required for	
			TUM	Exch APL
Configuring a user pool		No	•	•
Local administrator	Inclusive the local security policies	Yes	• *	•
MrsProxy.dll	Sharing the ... \Exchsrvr \ADDRESS folder	Yes		•
Mailbox stores	send as & receive as	No	•	•
Address templates (407 409)	Template generation	Yes		•
Address types	Address type generation	Yes		•
Default policy	Read & write	Yes		•
MRS container (1)	Container object generation	Yes		•
MRS container (2)	Generating & deleting the Directory Synchronization Object	Yes		•
MRS connector	Generating & deleting all child objects	Yes		•
MRS settings object	Creating the XPR object	No		•
MRS connector settings (1)	Read & write	No		•
MRS connector settings (2)	Read & write	No		•
MRS connector settings (3)	Full access	No		•
*) requires special settings. See the explanations.				

Table 23 Privilege Overview

5.9 Migration

NOTE: Users who deployed Integrated Messaging (mailbox replication) so far must be switched to True Unified Messaging users. The users with Integrated Messaging will otherwise only be able to work as voice-only users, since they can only deploy the mailbox on the XPR server.

How to migrate an XPR server from an existing connection to *Exchange Server 2003* to a connection to *Exchange Server 2010*:

1. Uninstall the existing connector (E2kApl) and, if installed, the ExUM Apl. To do this, use the **Modify** option from the XPR server setup.

NOTE: If the ExUM Apl is also installed on the system, it must be uninstalled, since the TUM connection must be established to the new *Exchange Server 2010*. It will later be installed again in the Exchange 2010 connector setup.

IMPORTANT: In case of this system modification the Exchange 2010 connector must not be simultaneously selected for installation. The Exchange 2010 connector must be set up later in a separate step.

2. Uninstall the *Exchange system manager* that supplied the required CDO for the *Exchange Server 2003* connection.
3. Install the **MAPICDO**. Because the *Exchange System Manager* cannot be used in *Exchange Server 2010* any more, the *Microsoft Collaboration Data Object* (CDO) must be installed on the XPR server manually.

The following file is required to install the connectors for the *Exchange Server 2010* connection:

ExchangeMapiCdo.EXE

This file complies with all requirements as regards MAPI and CDO for the **ExchApl** and **ExUMApl**.

The ExchangeMapiCdo.EXE setup file provided by Microsoft for this purpose can be downloaded from the following website:

<http://www.microsoft.com/downloads/details.aspx?FamilyID=e17e7f31-079a-43a9-bff2-0a110307611e&DisplayLang=en>

4. Install the new XPR Foreign Connector **and** the ExUM Apl. To do this, use the **Modify** option from the XPR server setup.

5.10 Integration in Hosted *Exchange* 2010

IMPORTANT: When planning the XPR setup we urgently recommend to discuss the following requirements with the provider to ensure that the provider is willing and able to meet such requirements.

The following requirements must be met for connecting an XPR server to a *Hosted Exchange Server 2010*:

- The XPR server is installed at the customer's and not on the provider side. Thus, it does not share its location with Exchange.
- An XPR satellite, on which the connectors run **within the Exchange domain** on the provider side, must be installed.

NOTE: This does not require a physical server. A virtual server is sufficient.

- This satellite must have been connected to the XPR kernel computer in the customer domain. This connection requires:
 - A VPN connection or a similar network connection between the satellite and the XPR kernel computer.
 - Data traffic on this connection must be allowed in both directions to the destination ports 137, 138, 139, 445 and 13010.
- The services on the satellite and on the XPR kernel computer must be able to access the respectively other computer. In other words, either the domains must trust each other or workgroup authentication must be reverted to.

If you use workgroup authentication, execute the following sub-steps:

1. Create a local user on the XPR kernel computer with the same user name and password that is specified for the domain user account. This user name and password is used for the services of the Exchange satellite.
2. Add this user account to the group of local administrators.
3. Execute the sub-steps 1. and 2. for the reverse direction. That means, create a local user on the satellite with the same user name and password that is specified for the domain user account of the services on the XPR kernel computer. Add this user account to the group of local administrators.
4. Open **Start > Control Panel > Administrative Tools > Local Security Policy > Security Settings > Local Policies > Security Options** and verify that the entry **Network access: Sharing and security model for local accounts** has value **Classic - local users authenticate as themselves**.

5.11 Troubleshooting

5.11.1 Configuration for the CDO in Systems without public Folders

Working in a system environment without public folders may lead to problems with the CDO.

See also:

<http://social.technet.microsoft.com/Forums/exchange/en-US/3a2e9489-6137-42fb-95d1-bebcfe2ea138/mapiefailoneprovider-0x8004011d-error-message-when-you-access-an-exchange-server-2010-mailbox?forum=exchange2010>

How to solve such problems:

1. Open the registry editor (`regedit.exe`).
2. Open the path:

Windows 32-bit version

`HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows Messaging Subsystem`

Windows 64-bit version

`HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows Messaging Subsystem`

3. Create in the opened path the registry directory **CDO** if it is not present there.
4. Create the registry key **Ignore No PF** in **CDO**.
5. Enter the [DWORD] value 1 for the registry key **Ignore No PF**.

The CDO problem as regards missing public folders has now been solved.

6 Connecting Exchange Server 2013 via an Exchange 2007/2010 Domain

If an XPR server connection to an Exchange Server 2007/2010 environment has already been configured, this connection can be used to access the mailboxes of an Exchange Server 2013 to be newly integrated in this domain.

This requires the service account existing for the ExUM Apl in the Exchange 2007/2010 environment to be replaced with a new service account on Exchange Server 2013. This new account must use the same logon data to allow access to both the Exchange Server 2013 mailboxes and those of the older Exchange environment.

The Exch Apl is still used as described in the manual. The service account need not be adjusted for this Apl.

6.1 Overview

With Exchange Server 2013 appearing, some architectural changes have become effective. For compatibility reasons, the components Collaboration Data Objects (CDO) and Messaging API (MAPI) must therefore be updated to allow supporting Exchange Server 2013.

To update these components, the configuration must be additionally adjusted for the MAPI, so that the ExUM Apl can set up the connection to the Exchange server.

You find detailed information about the installation (MAPI Download configuration guidance.docx) under:

<http://www.microsoft.com/en-us/download/details.aspx?id=39045>

6.2 General System Requirements

For Exchange Server 2013:

- Microsoft Exchange 2013 Server with Service Pack 1

Provision under:

<http://www.microsoft.com/en-us/download/details.aspx?id=41994>

For Xpressions V7 R1 FR3 or later

- Exchange MAPICDO download version 08.03.0.8353

Provision under:

<http://www.microsoft.com/en-us/download/details.aspx?id=42040>

- Hotfixes for the Xpressions version 811FR3:
 - ExUmApl-811FR3-17687
 - LdapApl-811FR3-17681
 - MMCEXchSnapIns-811FR3-20140615

NOTE: Please check that the previous **ExchangeMAPICDO** version is no longer present on the system before you start setting up the new or a more recent **ExchangeMAPICDO 6.5.8353** version.

6.3 XPR Service Account Requirements

Two service accounts are required to enable the ExUM Apl accessing the Exchange Server 2013: one service account with a mailbox configured on Exchange Server 2013 and another one with a mailbox configured on the older Exchange server.

Such requirements must be complied with to allow setting up a working connection between the Exchange servers via the service account settings and independently from the Exchange server versions.

XPR service accounts required for accessing:

- Exchange 2007 and/or Exchange 2010

An XPR service account with a mailbox on the Exchange Server 2007/2010. This service account is usually the one that was configured for setting up the connection of the ExUM Apl to the available Exchange 2007/2010 domain.

If this service account has been changed or replaced with another service account for some reason, the following registry keys under `HKLM\SOFTWARE\Wow6432Node\PPCOM\MRS\ExUMAp1` must be checked and corrected if required:

ACCOUNT,
ACCOUNTDN,
ACCOUNTDNFULL and
LEGACYEXCHANGEDN

IMPORTANT: If you cannot exclusively access the mailboxes of the Exchange Server 2007/2010 via the ExUM Apl, the configuration of this service account is most likely to be incorrect.

- Exchange 2013

One XPR service account with a mailbox on the Exchange Server 2013 for accessing the mailboxes of the Exchange Server 2013 users.

How to create and configure this service account is described in the following.

6.4 Creating an XPR Service Account on the Exchange Server 2013

You can use both the EAC (Exchange Admin Center) and the EMS (Exchange Management Shell) for creating the service account. Simply use the administration application most convenient to you. In the following we describe the proceedings using the Exchange Admin Center (EAC).

How to create the new service account on the Exchange Server 2013:

1. Start the **Exchange Admin Center** and log on to it.
2. Click on **Recipients > Mailboxes**
3. Click on **New >**
4. Click on **User mailbox**
5. Specify the logon data for the service account.
6. Complete the process.

The <XPR service account> is thus created.

6.5 Checking the Exchange 2013 Server Configuration

At this point we strongly recommend to first check the configuration and operational capability of the Exchange Server 2013. Proceed as follows:

Via a web browser:

1. Login to the Xpressions machine with the 2013 Service Account.
2. In the Internet Explorer, open the **Internet Options** dialog via **Tools > Internet Options**.
3. Select the **Connections** tab
4. Select **LAN Setting**
5. Uncheck **Automatically detect Settings**

NOTE: This feature could cause delay in EXUMAPL access to Exchange 2013.

6. Access the service account's mailbox via OWA.
To do this, deploy the user data you previously specified for the service account.
7. Check whether you can access the mailbox and send/receive e-mails.

Via an Outlook client:

1. Create an Outlook mail profile on any client.

NOTE: You must not create the Outlook mail profile on the XPR server.

To do this, deploy the user data you previously specified for the service account.

2. Check whether you can access the mailbox and send/receive e-mails.

6.6 Assigning Privileges

6.6.1 Assigning the required Privileges to the Service Account

After making sure that you can access the mailbox and send/receive e-mails, you can assign the required privileges to the service account on the Exchange Server 2013.

To do this you can use both the EAC (Exchange Admin Center) and the EMS (Exchange Management Shell).

How to assign the privileges via the **Exchange Admin Center (EAC)**:

1. Start the **Exchange Admin Center** and log on to it.
2. Click on **Permissions > Admin roles**.
3. Select **View-Only Organization Management**.
4. Click on **Edit**.
5. Click on **Add** in the **Members** section.
6. Select the <XPR service account> from the displayed list.
7. Click on **Add**.
8. Click on **OK**.
9. Add the <XPR service account>.
10. Click on the **Save** button.

The privilege is thus assigned.

How to assign privileges via the **Exchange Management Shell (EMS)**:

1. Start the **Exchange Management Shell (EMS)**.
2. Enter the following command in the command prompt:

```
Add-RoleGroupMember "View-Only OrganizationManagement" -Member "<XPR service account>"
```

This command is used for assigning the **View-Only Administrator rights** to the <XPR service account>.

6.6.2 Exchange Server 2013 Privileges

6.6.2.1 Privileges on Organization and Database Level

The following privileges must be assigned on the organization and database level:

Send as,

Receive as,

ms-exch-store-admin

How to assign the privileges:

1. Start the **Exchange Management Shell (EMS)**.
2. Enter the following commands in the command prompt in succession:

```
Get-OrganizationConfig | Add-ADpermission -User "<XPR service account>"  
-ExtendedRights "ms-Exch-Store-Admin","Send As", "Receive As"
```

```
Get-MailboxDatabase | Add-ADPermission -User "<XPR service account>"  
-ExtendedRights "send as", "receive as", "ms-Exch-Store-Admin"
```

6.6.2.2 Privileges on User Level

The <XPR service account> must be granted full access for the ExUM Apl to access the mailboxes of each user via the service account. In addition, accessing the mailboxes requires the privileges **Send as**, **Receive as** and **Administer Information Store** on the user level.

How to assign the privileges:

1. Start the **Exchange Management Shell (EMS)**.
2. Enter the following commands in the command prompt in succession:

```
Add-MailboxPermission -User "<XPR service account>" -Identity "<TUM USER>"  
-AccessRights fullaccess
```

```
Get-Mailbox "<TUM USER>" | Add-ADPermission -User "<XPR service account>"  
-ExtendedRights "send as", "receive as", "ms-exch-store-admin"
```

6.6.2.3 Configuring a Throttling Policy

The XPR service account requires configuring a Client Throttling Policy.

Proceed as follows:

1. Start the **Exchange Management Shell (EMS)**.
2. Enter the following commands in the command prompt in succession:

```
New-ThrottlingPolicy -Name "XPR Throttling Policy" -RCAMaxConcurrency $null
-RcaMaxBurst unlimited -RcaRechargeRate unlimited -IsServiceAccount:$true

Set-Mailbox Identity <XPR service account> -ThrottlingPolicy "XPR Throttling Policy"
```

3. Restart the **RPC Client Access** service on all Exchange servers.
4. Restart the ExUM Apl.

The new policy is thus configured.

Logging of the throttling events in the **RPC Client Access** service is disabled by default. The **RPC Client Access** log does therefore not display any throttling information. How to activate the throttling event logging:

1. Start any text editor, for example **Notepad**.
2. Open the file:

```
Microsoft.Exchange.RpcClientAccess.Service.exe.config
```

You find this file in path:

```
C:\Program Files\Microsoft\Exchange Server\V14\Bin
```

3. Find the following line in the opened file:

```
<add key="LoggingTag" value="ConnectDisconnect, Logon, Failures,
ApplicationData, Warnings" />
```

4. Add "Throttling" to the comma-separated list of events to be displayed in the log.
5. The relevant line of the above example will then read:

```
<add key="LoggingTag" value="ConnectDisconnect, Logon, Failures,
ApplicationData, Warnings, Throttling" />
```

6. Save the file in the text editor.
7. Close the file:
8. Restart the **RPC Client Access** service.

Logging the throttling events is now active.

You find more detailed information about the "Throttling" subject under:

[http://technet.microsoft.com/en-us/library/dd297964\(v=exchg.141\).aspx](http://technet.microsoft.com/en-us/library/dd297964(v=exchg.141).aspx)

6.6.3 Assigning local Privileges to the XPR Service Account

The <XPR service account> requires some local privileges on the XPR server. Such privileges are in detail:

- Log on as a service
- Act as part of the operating system
- Back up files and directories
- Restore files and directories
- Log on as batch job
- Adjust memory quotas for a process

How to assign these privileges:

1. Click the **Start** button on the system that hosts the XPR server.
2. Click on **Administrative Tools**.
3. Select **Local Security Policy** from the list of administrative tasks.
The **Local Security Policy** dialog opens.
4. Expand the displayed directory path **Security Settings > Local Policies > User Rights Assignment**.
5. Perform here the rights assignment according to the above list.

6.6.4 Switching the ExUM Apl to the new XPR Service Account

The <XPR service account> used so far for logging the ExUM Apl on to the Exchange Server 2007/2010 must be switched to the new <XPR service account> with the mailbox on the Exchange Server 2013.

How to perform this switch:

1. Click the **Start** button on the system that hosts the XPR server.
2. Click on **Administrative Tools**.
3. Select **Services** from the administrative tasks list.
The **Services** dialog opens.
4. Find the “XPR Exchange connector for i386...” service in the list.
5. Click on this entry with the right mouse button to open the associated context menu.

6. Select **Properties** from the context menu.
 7. Switch to the **Log On** tab.
 8. In the **This account** area, change the login data of the old <XPR service account> on the Exchange Server 2007/2010 to the login data of the new <XPR service account> on the Exchange Server 2013.
 9. Click on **OK**.
 10. The new setting is applied and the properties dialog closes.
 11. Restart the "XPR Exchange connector for i386..." service.
- Switching to the new <XPR service account> is now complete.

6.7 Adjusting the LDAP Configuration

Three database fields of the Active Directory must be replicated to the Xpressions server to enable accessing the mailbox of a user on the Exchange Server 2013. This requires three new database fields on the XPR server.

Accessing the corresponding mailboxes is controlled via the new database fields:

- **EXCH_MBX_GUID**
GUID of the Exchange mailbox. This database field is filled with value **msExchMailboxGuid**, which is allocated for this user in the Active Directory.
- **EXCH_VERSION**
Version number of the Exchange server. This database field is filled with value **msExchVersion**, which is allocated for this user in the Active Directory.
- **EXCH_HOMESERVER**
Name of the Exchange home server. This database field is filled with value **msExchHomeVersion**, which is allocated for this user in the Active Directory.

Data is transmitted from the Active Directory by replicating the LDAP APl in the corresponding XPR server database field.

NOTE: Using the **Active Directory Services Interfaces Editor (AdsiEdit)** you can access the Active Directory attributes.

6.7.1 Extending the User Data Mask on the XPR Server

The three database fields must be added on the XPR server manually.

NOTE: You find a detailed description of how to add a database field on the XPR server in the OpenScape Xpressions Web Assistant manual.

How to add the database fields on the XPR server:

1. Enter the IP address of the XPR Web Assistant in your web browser.
The Web Assistant starts.
 2. Log on to the system with administrator privileges.
 3. In the navigation menu on the left, expand the **Special server settings** link.
 4. Click on the **Mask editor** link.
- In the right-hand area, the XPR database settings page is displayed.
5. Select USER as the mask to be edited from the combo box.
 6. Click on the **Edit** button.

The user database definitions are displayed.

7. Enter the character strings specified in the following lines anywhere in the mask description to create the database fields:

```
EXCH_MBX_GUID      #####  
EXCH_VERSION      #####  
EXCH_HOMESERVER    #####
```

NOTE: The empty space between the data field names and the wildcard to indicate the field's width must consist of blanks (no tab!).

8. Click on the **Check mask description** button to test the entries' correctness.
If an error message occurs, correct your entries.
9. If you do not receive an error message, scroll downward on the page and check whether the entries **EXCH_MBX_GUID**, **EXCH_VERSION** and **EXCH_HOMESERVER** are present in the alphabetically sorted list.

NOTE: You need not adjust the field properties.

10. Click on the **Save** button under the field names list.

The database fields are created.

The database fields required for assigning **EXCH_MBX_GUID**, **EXCH_VERSION** and **EXCH_HOMESERVER** to the associated user are thus created.

NOTE: In the Web Assistant you can check once more on the databases' existence as they should be present in the user settings:

1. Expand **Server settings** in the Web Assistant.
2. Click on the **User Administration** link.
3. Open any user definition.

The database fields **EXCH_MBX_GUID**, **EXCH_VERSION** and **EXCH_HOMESERVER** are now additionally available in the user data mask.

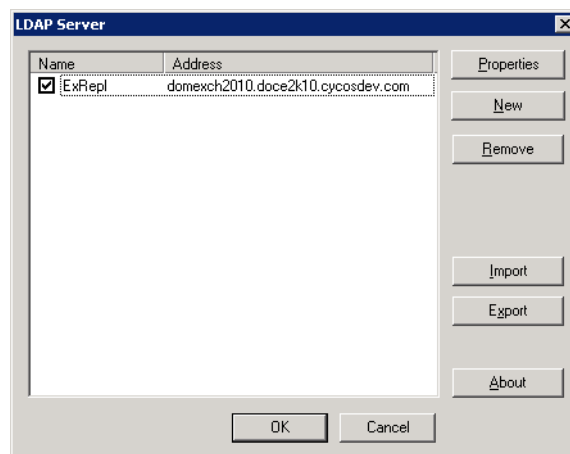
6.7.2 Expanding the LDAP Replication

Allocating the new database fields on the XPR server correctly requires adjusting the data replication of the corresponding fields from the Active Directory.

How to expand the replication via the LDAP Apl configuration dialog:

1. Open the XPR monitor.
2. Expand in the **XPRModules of <XPR server name> window** the **<Settings>** branch. 
3. Expand the  **LdapApl** branch.
4. Double-click **Set Options**.

The LDAP APL settings dialog opens.



5. Click on the **Properties** button.
The **Modify server settings** dialog of the LDAP Apl opens.

Connecting Exchange Server 2013 via an Exchange 2007/2010 Domain

Adjusting the LDAP Configuration

The screenshot shows the 'Modify server settings' dialog box with the 'Login' tab selected. The dialog contains the following fields and options:

- Logical name:** Ex2003
- Server IP address:** domexch2007.doce2k7.cycosdev.com
- Port number:** 389
- Directory type:** Active Directory
- DS User Account:**
 - User Name:** administrator
 - Password:** (masked with dots)
 - Domain:** doce2k7
 - Authentication type:** NTLM

Buttons at the bottom include 'Test connection', 'Query DS Attributes', 'OK', 'Cancel', and 'Apply'. The version number 'Version 8.00.42.9787' is displayed in the bottom left corner.

6. Switch to the **Attributes** tab.

The screenshot shows the 'Modify server settings' dialog box with the 'Attributes' tab selected. The dialog displays a table of attribute bindings between LDAP and MRS servers.

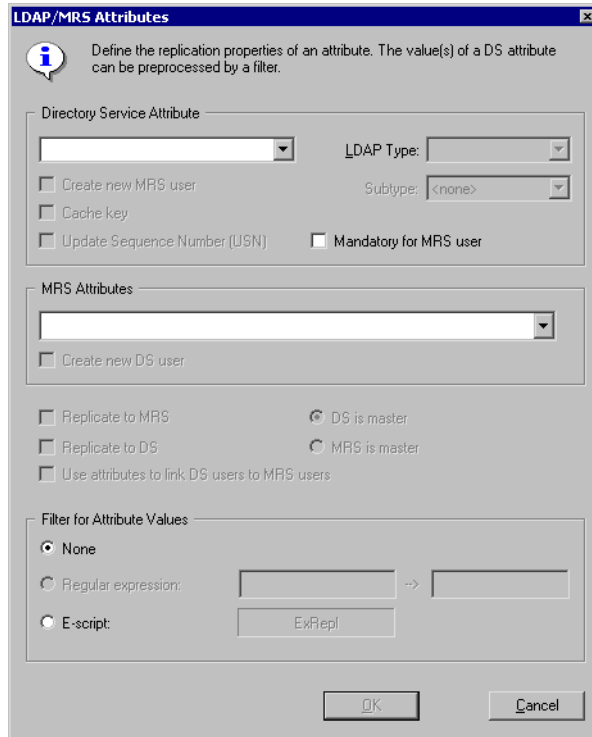
LDAP	Flags	MRS
co	<>	COUNTRY
company	<>	COMPANY
department	<>	DIVISION
description	<>	REMARK
displayName	<>	NAME
extensionData	<>	FAXG3:HEADLINE,FAXG3:ID,GROUP:...
facsimileTelephon...	<>	FAXG3:FAXG4
homePhone	<>	PRIVTEL
l	<>	CITY
mail	<>	SMTP
mobile	<>	GSM;SMS
objectGUID	K	
postOfficeBox	<>	ADDR2
postalCode	<>	ZIP
proxyAddresses	>~	EXCH
sAMAccountName	>	LMACCOUNT
st	<>	STATE
streetAddress	<>	ADDR1
telephoneNumber	<>	PHONE
uSNChanged	#	

Buttons at the bottom include 'Edit', 'Add', 'Remove', 'OK', 'Cancel', and 'Apply'. The version number 'Version 8.00.42.9787' is displayed in the bottom left corner.

7. Click on the **Edit** button.

Connecting Exchange Server 2013 via an Exchange 2007/2010 Domain

Adjusting the LDAP Configuration



The dialog box is titled "LDAP/MRS Attributes". It contains a help icon and a description: "Define the replication properties of an attribute. The value(s) of a DS attribute can be preprocessed by a filter." The dialog is divided into several sections:

- Directory Service Attribute:** A dropdown menu, an "LDAP Type:" dropdown, and a "Subtype:" dropdown (set to "<none>").
- Checkboxes: "Create new MRS user", "Cache key", "Update Sequence Number (USN)", and "Mandatory for MRS user".
- MRS Attributes:** A dropdown menu and a "Create new DS user" checkbox.
- Replication options: "Replicate to MRS", "Replicate to DS", and "Use attributes to link DS users to MRS users".
- Master/Slave options: "DS is master" (selected) and "MRS is master".
- Filter for Attribute Values:** Radio buttons for "None" (selected), "Regular expression:", and "E-script:". There are input fields for the regular expression and E-script, and an "ExRepl" button.
- Buttons: "OK" and "Cancel".

8. Select the **msExchMailboxGuid** attribute from the **Directory Service Attribute** combo box.
9. Link the attribute to the freshly configured XPR database field **EXCH_MBX_GUID** via the **MRS Attributes** combo box.
10. Repeat the steps 8. and 9. for the attributes **msExchVersion** -> **EXCH_VERSION** and **msExchHomeServerName** -> **EXCH_HOMESERVER**.
11. Click on **OK**.
The **LDAP/MRS Attributes** closes and you return to the **Modify server settings** dialog.
12. Switch to the **Login** tab in the **Modify server settings** dialog.
13. Click on the **Query DS Attributes** button to trigger the replication for the new data fields once.

Adjusting the LDAP configuration is now complete.

6.8 Adjusting Registry Settings

6.8.1 Adjusting Registry Settings for the XPR Server

Updating the MAPI was required for supporting an RPC/HTTP connection. It enables connecting the Exchange Server 2013 via RPC/HTTP. The RPC proxy server configuration must be adjusted for those components that require a MAPI update.

The configuration is adjusted by adding a registry key on the XPR server.

The registry key is created in the following registry path:

```
HKCU\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem
```

NOTE: Be sure that you are logged in with the EXCHANGE 2013 SERVICE ACCOUNT.

How to create the registry key:

1. Create the new registry key **RPCHTTPProxyMap_EXUMAPL** with the format **[REG_SZ]** in the above registry path.
2. Double-click the created key and enter the registry value in the following format:

```
<DOMAIN>=<ProxyServer><ProxyServerSettings>
```

The parameters have the following meaning:

<Domain>

The domain name of the RPC/HTTP endpoint of the proxy server used by the MAPI clients, or * (asterisk icon).

<ProxyServer>

The <ProxyServer> parameter contains value <FrontEndPoolFQDN> and must be entered in the format `https://<FrontEndPoolFQDN>`. For example: `https://mail.company.com`

You can use the EMS for having value <FrontEndPoolFQDN> put out. Enter the following command in the command line there:

```
Get-OutlookAnywhere | fl server*, Interna*, identity
```

NOTE: Make sure that the value put out via `Get-OutlookAnywhere` is adopted in <FrontEndPoolFQDN> exactly.

<ProxyServerSettings>

The MAPI profile settings are stored in the <ProxyServerSettings> parameter. It comprises the following further parameters:

- <RpcHttpAuthenticationMethod>,
- <RpcAuthenticationMethod> and
- <IgnoreSslCert>

Inserting the parameter in the underlying abbreviated notation results in the complete value of the registry key:

```
<DOMAIN>=<ProxyServer>,<RpcHttpAuthenticationMethod>,<RpcAuthenticationMethod>,<IgnoreSslCert>
```

You can insert the following valid values for the single parameters:

for <RpcHttpAuthenticationMethod>

- Negotiate
- NTLM
- Basic

for <RpcAuthenticationMethod>

- Negotiate
- NTLM
- Anonymous
- None

for <IgnoreSslCert>

- True
- 1
- Y
- Yes

NOTE: Any other value inserted here is interpreted as False.

Examples:

```
unify.com=https://mail.unify.com,ntlm,ntlm,true
*=https://mail.unify.com,ntlm,ntlm,true
```

You can obtain further information about this subject from the *Configuring the MAPI download for EXCHANGE 2013* instructions. You find these instructions in the Microsoft document *MAPI Download configuration guidance.docx* under:

<http://www.microsoft.com/en-us/download/details.aspx?id=39045>

6.8.2 Checking and configuring Certificates for the RPC Proxy Server

You must access the RPC proxy address via web browser to check and configure the certificates for the RPC proxy server:

NOTE: Execute the following work steps via the <XPR Exchange 2013 Service Account> logged in at the domain.

1. Open the web browser.
If you use the Internet Explorer, access the CAS-URL specified in the **RPCHTTPProxyMap**. The default setting for the CAS-URL is `https://<CAS server address>`
If a certificate error occurs, follow the next steps:
2. In the Internet Explorer, open the **Internet Options** dialog via **Tools > Internet Options**.
3. Select the **Security** tab.
4. Mark the **Local Intranet** icon.
5. Click on the **Sites** button.
6. Add the RPC proxy address
`https://<CAS server address>`
7. Click on **Add**.
8. Click on **Close**.
9. Click on **OK** in the **Internet Options** dialog.
10. Click on **Certificate error** in the address line in the browser window..
11. Click on **View Certificates**.
The **Certificate** dialog opens.
12. Click on the **Install certificate** button.
The **Certificate Import Wizard** dialog opens.
13. Click on **Next** in this dialog.

14. Select the **Place all certificates in the following store** option in the next dialog.
 15. Click on the **Browse** button.
The **Select Certificate Store** dialog opens.
 16. Select **Trusted Root Certification Authorities**.
 17. Click on **OK** in the **Select Certificate Store** dialog.
The dialog closes and you return to the **Certificate Import Wizard**.
 18. Click on **Next** in this dialog.
 19. Click on **Finish** in the next dialog.
- The certificate is now checked and configured.

6.8.3 Registry Settings for the ExUM Apl

To access the mailboxes configured on the Exchange Server 2013 the ExUM Apl requires some control parameters for the Exchange Server 2013 profile to be configured appropriately. These parameters are deposited in various registry keys.

To configure these registry keys correctly, adopt the data exactly as they are put out via the `Get-Mailbox` command of the **Exchange Management Shell (EMS)**.

6.8.3.1 Determining the Registry Values via the EMS

How to determine the registry values:

1. Start the **Exchange Management Shell (EMS)**.
2. Enter the following command in the command prompt:

```
Get-Mailbox "<XPR Service user>" | fl name, identity, alias, ExchangeGuid,  
LegacyExchangeDN, ServerLegacyDN, ServerName
```

The requested parameters are put out.

6.8.3.2 Configuring the Registry Keys for the ExUM Apl

The following registry keys contain the parameters required for the <XPR service account> to access the mailboxes in Exchange Server 2013.

The registry keys must be created in the following registry path:

Connecting Exchange Server 2013 via an Exchange 2007/2010 Domain

Adjusting Registry Settings

HKLM\SOFTWARE\Wow6432Node\PP-COM\MRS\ExUMAp1

E2K13_DOMAIN [REG_SZ]

Default:	-
Possible values:	<Domain name>
Example:	company.com

Domain of the RPC/HTTP endpoint of the proxy server used by the MAPI clients.

E2K13_HOME_SERVER_DN [REG_SZ]

Default:	-
Possible values:	<Distinguished name of the home server>

Defined name of the home server. The name can be retrieved from the `ServerLegacyDN` and `ExchangeGuid` via a `Get-Mailbox` command.

Edit the character string as described in the following:

1. Replace the variable <Exchange 2013 Server> after the character string of the `ServerLegacyDN`

`CN=SERVERS/CN=<EXCHANGE 2013 SERVER>`

with value `ExchangeGuid@<DOMAIN>`.

Example:

```
/o=COMPANY ORG/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/  
cn=Configuration/cn=Servers/cn=fe5f84bf-36f9-42eb-ab2f-9e40e3413bf1@company.com
```

NOTE: The <DOMAIN> portion is replaced with the data from the **E2K13_DOMAIN** registry key.

E2K13_RPC_PROXY_SERVER [REG_SZ]

Default:	-
Possible values:	<server name>
Example:	amb09-exch2k13.company.com

The FQDN of the RPC/HTTP endpoint of the proxy server (of the CAS server) used by the MAPI clients.

E2K13_SERVICEUSER_DN [REG_SZ]

Default:	-
Possible values:	<Distinguished name of the <XPR service account>>

Defined name of the <XPR service account>. The name can be retrieved from the `LegacyExchangeDN` properties via a `Get-Mailbox` command.

Example:

```
/o=COMPANY ORG/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Recipients/
cn=e092feee00504b1ebf88ba3afd6c059e-admine2k13
```

E2K13_UNRESOLVED_NAME [REG_SZ]

Default:	-
Possible values:	<Mailbox alias for the <XPR service account>>
Example:	admine2k13

Mailbox alias name for the <XPR service account> on the Exchange Server 2013. Use the alias name you retrieved from the alias properties via a `Get-Mailbox` command.

E2K13_UNRESOLVED_SERVER [REG_SZ]

Default:	-
Possible values:	<ACCOUNTDNFULL>
Example:	fe5f84bf-36f9-42eb-ab2f-9e40e3413bf1@company.com

Personalized server ID. Use the ID you retrieved from the **ExchangeGuid** properties via a `Get-Mailbox` command, followed by the domain name (format: <ExchangeGuid>@<Domain>).

NOTE: The <DOMAIN> portion is replaced with the data from the **E2K13_DOMAIN** registry key.

LEGACYEXCHANGEDN [REG_SZ]

Default:	-
Possible values:	<Entry of the LegacyExchangeDN object data>
Note:	See registry key ACCOUNTDNFULL

Check this registry key after the first ExUM Apl start. If no value has been entered here, the ExUM Apl will not work correctly. Copy in this case the value from the available registry key

ACCOUNTDNFULL [REG_SZ] as the registry value for this key.

6.9 Log File

To facilitate tracing the processes in the Exchange Server 2013, they are logged. You can use the log data when looking for errors or monitoring server processes. The Exchange Server 2013 stores such data in the following directory:

```
<Microsoft Exchange Server Installation Path>\V15\Logging\RPC Client Access
```

Connecting Exchange Server 2013 via an Exchange 2007/2010 Domain

Log File

7 XPR and Microsoft Exchange Server 2013

7.1 General Considerations

Following the workaround that enables accessing an Exchange Server 2013 via connecting an Exchange 2007/2010 domain you can now also directly connect an Exchange Server 2013 domain by modifying the Exchange connectors.

This chapter describes the connection of an already existing OpenScape Xpressions V7 server to a new Exchange Server 2013 domain.

NOTE: You can obtain all explanations that concern the interaction of the Xpressions server and Microsoft Exchange 2013 from chapter “OpenScape Xpressions V7 and Microsoft Exchange 2010”, because the basic functionality has not changed.

7.2 Overview

With Exchange Server 2013 appearing, some architectural changes have become effective. For compatibility reasons, the components Collaboration Data Objects (CDO) and Messaging API (MAPI) must therefore be updated to allow supporting Exchange Server 2013.

Updating these components requires the configuration to be additionally adjusted for the MAPI, so that the ExUM Apl can set up the connection to the Exchange server.

You find detailed information about the installation (MAPI Download configuration guidance.docx) under:

<http://www.microsoft.com/en-us/download/details.aspx?id=39045>

7.3 General System Requirements

For Exchange Server 2013:

- Microsoft Exchange 2013 Server with Service Pack 1

Provision under:

<http://www.microsoft.com/en-us/download/details.aspx?id=41994>

For Xpressions V7 R1 FR4 or later

- Exchange MAPICDO download version 08.03.0.8353

Provision under:

<http://www.microsoft.com/en-us/download/details.aspx?id=42040>

- The following hotfixes must have been installed on the Xpressions server:
 - E2k7Apl V7 R1 FR4 or later
 - ExUmApl V7 R1 FR4 or later
 - LdapApl V7 R1 FR4 or later
 - MMCExchSnapIns V7 R1 FR4 or later

NOTE: Please check that the previous **ExchangeMAPICDO** version is no longer present on the system before you start setting up the new or a more recent **ExchangeMAPICDO 6.5.8353** version.

7.3.1 Preparations

The following preparatory steps must be executed to set up the XPR Foreign Connector:

- **For migration scenarios only**

Users who deployed Integrated Messaging (mailbox replication) so far must be switched to True Unified Messaging beforehand. The users with Integrated Messaging will otherwise only be able to work as voice-only users, since they can only deploy the mailbox on the XPR server.

- **MAPI and CDO**

Because the *Exchange System Manager* cannot be used in *Exchange Server 2013* any more, the *Microsoft Collaboration Data Object* (CDO) must be installed on the XPR server manually.

You find detailed information about the installation (MAPI Download configuration guidance.docx) under:

<http://www.microsoft.com/en-us/download/details.aspx?id=39045>

- **Configuring a service account**

Configure a user account (service account) in the context of which the connectors are to operate. This service account must have an Exchange mailbox. Under this service account the Exch Apl and ExUM APL service operates on the kernel computer. The privileges assigned to this account enable the operation of the Exchange connector in the system. Using the service account you can easily administer the privileges for operating the connectors.

- **Assigning privileges**

Assigning the privileges for the installation and operation of the connectors has slightly changed with the XPR Foreign Connector. Which privileges are required and how to set them is described further down the text under **"Requirements and privileges for installing the connectors"**.

- **Transport directories**

Message transport between the two systems requires two transport directories (`\<drop directory>` and `\<replay directory>`) on the *Exchange server 2013*. The drop directory serves for transporting messages from Exchange to the XPR server, the replay directory is in charge of transporting in the reverse direction. You find information about the configuration and activation of these transport directories in [Section 7.10.7.1, "Creating the Transport Directories"](#), on page 346.

- **Requirements and privileges for installing the connectors**

Management role groups

The new privilege model in *Microsoft Exchange Server 2013* is called *Role Based Access Control* (RBAC). A method to assign privileges to users of an organization in this new privilege model is to group users in so-called *Management Role Groups*.

Management Role Groups facilitate assigning management roles to a user group considerably, because the same roles are assigned to all members of a role group at the same time.

Administrator and specialist roles are grouped in role groups, for example. This enables combining users for important management tasks such as organization management, recipient management and more in *Exchange Server 2013*.

You find further information about this topic under:

<http://technet.microsoft.com/en-us/library/dd298183.aspx>

Installation Requirements	
☐	The server components Mailbox Server Role and Hub Transport Server Role are installed and active.
☐	The network function as well as the name resolution in the network work correctly. You can use DCDiag and NetDiag (Windows support tools) to check this.
☐	You are logged in at the domain as installing user with domain admin privileges and Exchange admin privileges. This gives you unrestricted access to the service database. This is important with respect to installing and configuring the service.
The service account requires locally the following privileges on the XPR system: Notes: • Privilege assignment occurs via the Security Policies. You reach the corresponding setting dialog via Start > Administrative Tools > Local Security Policy under Local Policies > User Rights Assignment. Under the local security policies you find the locally set and “effective” policies. • Separate policies can be entered for domains and domain controllers. These policies overwrite, as the case may be, the locally defaulted ones. After a policy modification on domain level, a restart of the corresponding computers (domain controllers and Exch APL computers) may be required. • If you plan a system allowing more than 5000 MAPI accesses, use the Multiline Configuration feature. See Section , “Multiline Configuration”, on page 423. ☒ Log on as service – is set upon the connector installation. (Log on as service)	

Table 24

Check List: Installation Requirements for the Exchange -2013 Connectors

Installation Requirements	
☒	Act as part of the operating system – is set upon the connector installation. (Act as part of the operating system)
☒	Back up files and directories – is set upon the connector installation. (Back up files and directories)
☒	Restore files and directories – is set upon the connector installation. (Restore files and directories)
☒	Log on as batch job – is set upon the connector installation. (Log on as batch job)
☒	Adjust memory quotas for a process – is set upon the connector installation. (Adjust memory quotas for a process)
On the organization level of the Exchange server (Active Directory level), the following privileges are required for the service account:	
☐	The installing user must have the “Organization Management” privilege in the Exchange 2013. This provides full access to the Exchange-specific part of the Active Directory for installing and uninstalling various objects (for example: connector, address type, templates, etc.).
☐	User “service account” must belong to the group of “domain administrators”
☐	User “service account” must belong to the group of “domain users”

Table 24

Check List: Installation Requirements for the Exchange -2013 Connectors

Installation Requirements	
☐	The XPR service account requires configuring a Client Throttling Policy. Proceed as follows: – Start the Exchange Management Shell (EMS). – Enter the following commands in the command prompt in succession: <code>New-ThrottlingPolicy -Name "XPR Throttling Policy" -RCAMaxConcurrency unlimited -RcaMaxBurst unlimited -RcaRechargeRate unlimited -IsServiceAccount:\$true</code> <pre>Set-Mailbox -Identity <XPR service account> -ThrottlingPolicy "XPR Throttling Policy"</pre> – Restart the RPC Client Access service on all Exchange servers. – Restart the ExUM Apl. The new policy is thus configured. Logging of the throttling events in the RPC Client Access service is disabled by default. The RPC Client Access log does therefore not display any throttling information. How to activate the throttling event logging: – Start any text editor, for example Notepad. – Open the file: <code>Microsoft.Exchange.RpcClietAccess.Service.exe.config</code> You find this file in path: <code>C:\Program Files\Microsoft\Exchange Server\V15\Bin</code> – Find the following line in the opened file: <code><add key="LoggingTag" value="ConnectDisconnect, Logon, Failures, ApplicationData, Warnings" /></code> – Add "Throttling" to the comma-separated list of events to be displayed in the log. – The relevant line of the above example will then read: <code><add key="LoggingTag" value="ConnectDisconnect, Logon, Failures, ApplicationData, Warnings, Throttling" /></code> – Save the file in the text editor. – Close the file: – Restart the RPC Client Access service. Logging the throttling events is now active. You find more detailed information about the "Throttling" subject under: http://technet.microsoft.com/en-us/library/dd297964(v=exchg.141).aspx

Table 24 Check List: Installation Requirements for the Exchange -2013 Connectors

Installation Requirements	
☐	A service account with Exchange mailbox for operating the Exch and ExUM Apl has been created. The Exch and ExUM APL service runs under this user account on the kernel computer. The privileges assigned to this account enable the operation of the Exchange connector in the system. This also enables the simple administration of the privileges for this service account. Operating the gateway via a service account always requires the following privileges: • View-Only Organization Management role group In the pool that forms the <i>Role Based Access Control (RBAC)</i> privilege model in <i>Microsoft Exchange Server 2013</i>, the <i>View-Only Organization Management role group</i> is one of the <i>Management Role Groups</i> available by default. Administrators or users who belong to this role group can have the properties of every Exchange organization object displayed. The <i>View-Only Organization Management role group</i> in <i>Exchange Server 2013</i> is comparable with the <i>Exchange View-Only Administrators role</i> in <i>Microsoft Exchange Server 2007</i>. You find more information about this topic under: http://technet.microsoft.com/en-us/library/dd351130.aspx The XPR service account must be added to the <i>View-Only Organization Management role group</i>. You may do this via Active Directory Users & Computers. Alternatively you can do this by deploying the Exchange Management Shell, EMS. Execute the following steps for assignments to this <i>Management Role Group</i>: – Start the <i>Exchange management shell</i>. – Enter the following command in the command prompt: <pre>Add-RoleGroupMember "View-Only Organization Management" -Member "<XPR service account>"</pre> Note: You can check whether the assignment for the XPR service account was successful, thus the XPR service account now belongs to the <i>View-Only Organization Management role group</i>, via the following command: <pre>Get-RoleGroupMember "View-Only Organization Management"</pre> You find more information about this topic under: http://technet.microsoft.com/en-us/library/dd638143.aspx
☐	• Local administrator on the Mailbox Server Role as well as on the Hub Transport Server Role.

Table 24

Check List: Installation Requirements for the Exchange -2013 Connectors

Installation Requirements	
☐	• Organization Management role group (required for the setup only) With <i>Exchange Server 2010</i> the <i>Exchange Organization Administrators</i> role has changed to <i>Organization Management</i> role group. The <i>Organization Management</i> role group is comparable to the <i>Exchange Organization Administrators</i> role in <i>Exchange Server 2007</i>. The installing user must belong to the <i>Management Role Group “Organization Management role group”</i> in the <i>Exchange Server 2013</i> organization. This gives the user full access to the Exchange-specific part of the Active Directory for installing/uninstalling different objects such as the connector, the address types and templates etc. You may do this via Active Directory Users & Computers. Alternatively you can do this by deploying the Exchange Management Shell, EMS. Execute the following steps for assignments to this <i>Management Role Group</i>: – Start the <i>Exchange management shell</i>. – Enter the following command in the command prompt: Add-RoleGroupMember “Organization Management” -Member “<XPR service account>” Note: You can check whether the assignment for the XPR service account was successful, thus the XPR service account now belongs to the <i>Organization Management</i> role group, via the following command: <pre>Get-RoleGroupMember “Organization Management”</pre>
☐	• Privileges “Send As”, “Receive As” and “Administer Information Store” on organization level How to assign the XPR service account the privileges <i>Send As</i>, <i>Receive As</i> and <i>Administer Information Store</i> on organization level: – Start the <i>Exchange management shell</i>. – Enter the following command in the command prompt: Get-OrganizationConfig Add-ADpermission -User “<XPR service account>” -ExtendedRights “ms-Exch-Store-Admin”, “Send As”, “Receive As” Note: You can check whether the assignment for the XPR service account was successful, thus the XPR service account now has the privileges <i>ms-Exch-Store-Admin</i>, <i>Send As</i> and <i>Receive As</i> on organization level, via the following command: <pre>Get-OrganizationConfig Get-AdPermission -User <XPR service account> Select -Property User,ExtendedRights, Deny, IsValid”</pre>

Table 24

Check List: Installation Requirements for the Exchange -2013 Connectors

Installation Requirements	
☐	• Explicit privileges “Send As”, “Receive As” and “Administer Information Store” on mailbox database level How to assign the XPR service account the explicit privileges <i>Send As</i>, <i>Receive As</i> and <i>Administer Information Store</i> on mailbox database level: – Start the <i>Exchange management shell</i>. – Enter the following command in the command prompt: <pre>Get-MailboxDatabase Add-ADPermission -User "<XPR service account>" -ExtendedRights "send as", "receive as", "ms-Exch-Store-Admin"</pre> Note: You can check whether the assignment for the XPR service account was successful, thus the XPR service account now has the explicit privileges <i>ms-Exch-Store-Admin</i>, <i>Send As</i> and <i>Receive As</i> on mailbox database level, via the following command: <pre>Get-MailboxDatabase Get-AdPermission -User "<XPR service account>" Select -Property Identity, User,ExtendedRights, Deny, IsValid"</pre>

Table 24

Check List: Installation Requirements for the Exchange -2013 Connectors

Installation Requirements	
☐	• Explicit privilege “Send As” on user mailbox level How to assign the explicit privilege <i>Send As</i> to the MRS user account on user mailbox level: – Start the <i>Exchange management shell</i>. – Enter the following command in the command prompt: For a specific user: <pre>Get-Mailbox -Identity "<Exchange user>" Add-ADpermission -user "<XPR service account>" -ExtendedRights "Send As"</pre> For all users of a specific organization unit: <pre>\$XPRUSERS=Get-User -OrganizationalUnit "<XPR organization unit>"; FOREACH (\$USER in \$XPRUSERS) { Add-ADPermission -User "<XPR service account>" -Identity \$USER.NAME -ExtendedRights "Send As" }</pre> Note: You can check whether the assignment for the XPR service account was successful, thus the XPR service account has the explicit privilege <i>Send As</i> on the user mailbox level, via the following command: <pre>Get-Mailbox -Identity "Exchange User" Get-AdPermission -User "<XPR service account>" Select -Property User,ExtendedRights, Deny"</pre> You find further information about this topic under: http://technet.microsoft.com/en-us/library/bb676368.aspx

Table 24

Check List: Installation Requirements for the Exchange -2013 Connectors

Installation Requirements	
☐	• Explicit privilege “FullAccess” on user mailbox level How to assign the explicit privilege <i>FullAccess</i> to the XPR service account: – Start the <i>Exchange management shell</i>. – Enter the following command in the command prompt: For a specific user: <pre>Add-MailboxPermission -User "<XPR service account>" -Identity "<Exchange user>" -AccessRights FullAccess</pre> For all users of a specific organization unit: <pre>\$XPRUSERS= Get-User -OrganizationalUnit "<XPR organization unit>" FOREACH (\$USER in \$XPRUSERS) { Add-MailboxPermission -User "<XPR service account>" -Identity \$USERS.NAME -AccessRights FullAccess}</pre> Note: The organization unit has a default limit of 1000 users (Exchange). Note: You can check whether the assignment for the XPR service account was successful, thus the XPR service account now has the explicit privilege <i>FullAccess</i> on the user mailbox level, via the following command: <pre>Get-MailboxPermission -Identity "<Exchange user>" -User "MRS Service Account"</pre> You find further information about this topic under: http://technet.microsoft.com/en-us/library/aa996343.aspx for additional details)

Table 24

Check List: Installation Requirements for the Exchange -2013 Connectors

Finally, reboot the service *Microsoft Exchange Information Store* for the privilege assignments to take immediate effect.

7.4 Requirements for a direct Connection

7.4.1 XPR Service Account on Exchange Server 2013

One service account with a mailbox on the Exchange Server 2013 is required for accessing Exchange Server 2013. This service account ensures that a functioning connection can be set up to the Exchange Server 2013 and the profile settings can be adjusted.

How to create and configure this service account is described in the following.

7.4.2 Users on the Exchange Server 2013

All users must have been migrated from the Exchange Server 2007/2010 to the Exchange Server 2013 before the connector connections to the Exchange Server 2013 are configured.

NOTE: To access Exchange Server 2007/2010 and Exchange Server 2013 users, deploy the solution described in the previous chapter: [Chapter 6, “Connecting Exchange Server 2013 via an Exchange 2007/2010 Domain”](#).

7.5 Creating an XPR Service Account on the Exchange Server 2013

You can use both the EAC (Exchange Admin Center) and the EMS (Exchange Management Shell) for creating the service account. Simply use the administration application most convenient to you. In the following we describe the proceedings using the Exchange Admin Center (EAC).

How to create the new service account on the Exchange Server 2013:

1. Start the **Exchange Admin Center** and log on to it.
2. Click on **Recipients > Mailboxes**
3. Click on **New >**
4. Click on **User mailbox**
5. Specify the logon data for the service account.
6. Complete the process.

The *<XPR service account>* is thus created.

7.6 Checking the Exchange 2013 Server Configuration

At this point we strongly recommend to first check the configuration and operational capability of the service account on the Exchange Server 2013. Proceed as follows:

Via a web browser:

1. Access the service account's mailbox via OWA.
To do this, deploy the user data you previously specified for the service account.
2. Check whether you can access the mailbox and send/receive e-mails.

Via an Outlook client:

1. Create an Outlook mail profile for the service account on any client.

NOTE: You must not create the Outlook mail profile on the XPR server.

To do this, deploy the user data you previously specified for the service account.

2. Check whether you can access the mailbox and send/receive e-mails.

7.7 Assigning Privileges

7.7.1 Assigning the required Privileges to the Service Account

After making sure that you can access the mailbox and send/receive e-mails, you can assign the required privileges to the service account on the Exchange Server 2013.

To do this you can use both the EAC (Exchange Admin Center) and the EMS (Exchange Management Shell).

How to assign the privileges via the **Exchange Admin Center (EAC)**:

1. Start the **Exchange Admin Center** and log on to it.
2. Click on **Permissions > Admin roles**.
3. Select **View-Only Organization Management**.
4. Click on **Edit**.
5. Click on **Add** in the **Members** section.
6. Select the *<XPRservice account>* from the displayed list.
7. Click on **Add**.
8. Click on **OK**.
9. Add the *<XPR service account>*.

10. Click on the **Save** button.

The privilege is thus assigned.

How to assign privileges via the **Exchange Management Shell (EMS)**:

1. Start the **Exchange Management Shell (EMS)**.
2. Enter the following command in the command prompt:

```
Add-RoleGroupMember "View-Only Organization Management" -Member "<XPR service account>"
```

This command is used for assigning the **View-Only Administrator rights** to the *<XPRservice account>*.

7.7.2 Exchange Server 2013 Privileges

7.7.2.1 Privileges on Organization and Database Level

The following privileges must be assigned on the organization and database level:

Send as,

Receive as,

ms-exch-store-admin

How to assign the privileges:

1. Start the **Exchange Management Shell (EMS)**.
2. Enter the following commands in the command prompt in succession:

```
Get-OrganizationConfig | Add-ADPermission -User "<XPR service account>"  
-ExtendedRights "ms-Exch-Store-Admin", "Send As", "Receive As"
```

```
Get-MailboxDatabase | Add-ADPermission -User "<XPR service account>"  
-ExtendedRights "send as", "receive as", "ms-Exch-Store-Admin"
```

7.7.2.2 Privileges on User Level

The *<XPRservice account>* must be granted full access for the ExUM Apl to access the mailboxes of each user via the service account. In addition, accessing the mailboxes requires the privileges **Send as**, **Receive as** and **Administer Information Store** on the user level.

How to assign the privileges:

1. Start the **Exchange Management Shell (EMS)**.
2. Enter the following commands in the command prompt in succession:

```
Add-MailboxPermission -User "<XPR service account>" -Identity "<TUM USER>"
    -AccessRights fullaccess
```

```
Get-Mailbox "<TUM USER>" | Add-ADPermission -User "<XPR service account>"
    -ExtendedRights "send as", "receive as", "ms-exch-store-admin"
```

7.7.2.3 Configuring a Throttling Policy

The service account requires configuring a Client Throttling Policy.

Proceed as follows:

1. Start the **Exchange Management Shell (EMS)**.
2. Enter the following commands in the command prompt in succession:

```
New-ThrottlingPolicy -Name "XPR Throttling Policy" -RCAMaxConcurrency Unlimited
    -RcaMaxBurst unlimited -RcaRechargeRate unlimited -IsServiceAccount:$true
```

```
Set-Mailbox Identity <XPR service account> -ThrottlingPolicy "XPR Throttling Policy"
```

3. Restart the **RPC Client Access** service on all Exchange servers.
4. Restart the ExUM Apl.

The new policy is thus configured.

Logging of the throttling events in the **RPC Client Access** service is disabled by default. The **RPC Client Access** log does therefore not display any throttling information. How to activate the throttling event logging:

1. Start any text editor, for example **Notepad**.
2. Open the file:

```
Microsoft.Exchange.RpcClientAccess.Service.exe.config
```

You find this file in path:

```
C:\Program Files\Microsoft\Exchange Server\V15\Bin
```

3. Find the following line in the opened file:

```
<add key="LoggingTag" value="ConnectDisconnect, Logon, Failures,
    ApplicationData, Warnings" />
```

4. Add *<Throttling>* to the comma-separated list of events to be displayed in the log.

5. The relevant line of the above example will then read:

```
<add key="LoggingTag" value="ConnectDisconnect, Logon, Failures,  
ApplicationData, Warnings, Throttling" />
```

6. Save the file in the text editor.
7. Close the file:
8. Restart the **RPC Client Access** service.

Logging the throttling events is now active.

You find more detailed information about the “New Throttling Policy” subject under:

<http://technet.microsoft.com/en-us/library/dd351045%28v=exchg.150%29.aspx>

7.7.3 Configuration of Exchange Server 2013 without public Folders

If the Exchange Server 2013 does not provide a database for public folders, the Xpressions server cannot log on to Exchange Server 2013. If it tries nonetheless, the following error message is issued:

MAPI_E_FAILONEPROVIDER (0x8004011D)

The administrator can evade this problem by changing the configuration:

1. On each system that hosts an Xpressions server click on **Start > Run**.
2. Enter **regedit** in the input line.
3. Click on **OK** to open the registry editor.
4. Navigate to the registry path:
 - If the Xpressions server is present on a 32-bit operating system:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows Messaging Subsystem\CDO
```

- If the Xpressions server is present on a 64-bit operating system:

```
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows Messaging Subsystem\CDO
```

5. Create the **CDO** registry directory if it is not yet available in the above path.
6. Next, or if the **CDO** registry directory is already available, create a registry key in the **CDO** registry directory with the DWORD data type and call it **Ignore No PF**.
7. Change the DWORD value for **Ignore No PF** to **1**.

8. Click on **OK**.

Adjusting the Exchange Server 2013 configuration without public folder is thus performed.

7.7.4 Assigning local Privileges to the XPR Service Account

The <XPR service account> requires some local privileges on the XPR server. Such privileges are in detail:

- Log on as a service
- Act as part of the operating system
- Back up files and directories
- Restore files and directories
- Log on as batch job
- Adjust memory quotas for a process

How to assign these privileges:

1. Click the **Start** button on the system that hosts the XPR server.
2. Click on **Administrative Tools**.
3. Select **Local Security Policy** from the list of administrative tasks.

The **Local Security Policy** dialog opens.

4. Expand the displayed directory path **Security Settings > Local Policies > User Rights Management**.

Perform here the rights assignment according to the above list.

7.8 Adjusting the LDAP Configuration

Three database fields of the Active Directory must be replicated to the Xpressions server to enable accessing the mailbox of a user on the Exchange Server 2013. This requires three new database fields on the XPR server.

Accessing the corresponding mailboxes is controlled via the new database fields:

- **EXCH_MBX_GUID**
GUID of the Exchange mailbox. This database field is filled with value **msExchMailboxGuid**, which is allocated for this user in the Active Directory.

- **EXCH_VERSION**

Version number of the Exchange server. This database field is filled with value **msExchVersion**, which is allocated for this user in the Active Directory.

- **EXCH_HOMESERVER**

Name of the Exchange home server. This database field is filled with value **msExchHomeVersion**, which is allocated for this user in the Active Directory.

Data is transmitted from the Active Directory by replicating the LDAP APl in the corresponding XPR server database field.

NOTE: Using the **Active Directory Services Interfaces Editor (AdsiEdit)** you can access the Active Directory attributes.

7.8.1 Extending the User Data Mask on the XPR Server

The three database fields must be added on the XPR server manually.

NOTE: You find a detailed description of how to add a database field on the XPR server in the OpenScope Xpressions Web Assistant manual.

How to add the database fields on the XPR server:

1. Enter the IP address of the XPR Web Assistant in your web browser.

The Web Assistant starts.

2. Log on to the system with administrator privileges.
3. In the navigation menu on the left, expand the **Special server settings** link.
4. Click on the **Mask editor** link.

In the right-hand area, the XPR database settings page is displayed.

5. Select USER as the mask to be edited from the combo box.

6. Click on the **Edit** button.

The user database definitions are displayed.

7. Enter the character strings specified in the following lines anywhere in the mask description to create the database fields:

```
EXCH_MBX_GUID      #####
EXCH_VERSION      #####
EXCH_HOMESERVER    #####
```

NOTE: The empty space between the data field names and the wildcard to indicate the field's width must consist of blanks (no tab!).

8. Click on the **Check mask description** button to test the entries' correctness. If an error message occurs, correct your entries.
9. If you do not receive an error message, scroll downward on the page and check whether the entries **EXCH_MBX_GUID**, **EXCH_VERSION** and **EXCH_HOMESERVER** are present in the alphabetically sorted list.

NOTE: You need not adjust the field properties.

10. Click on the **Save** button under the field names list.

The database fields are created.

The database fields required for assigning **EXCH_MBX_GUID**, **EXCH_VERSION** and **EXCH_HOMESERVER** to the associated user are thus created.

NOTE: In the Web Assistant you can check once more on the databases' existence as they should be present in the user settings:

1. Expand **Server settings** in the Web Assistant.
2. Click on the **User Administration** link.
3. Open any user definition.

The database fields **EXCH_MBX_GUID**, **EXCH_VERSION** and **EXCH_HOMESERVER** are now additionally available in the user data mask.

7.8.2 Expanding and updating the LDAP Replication

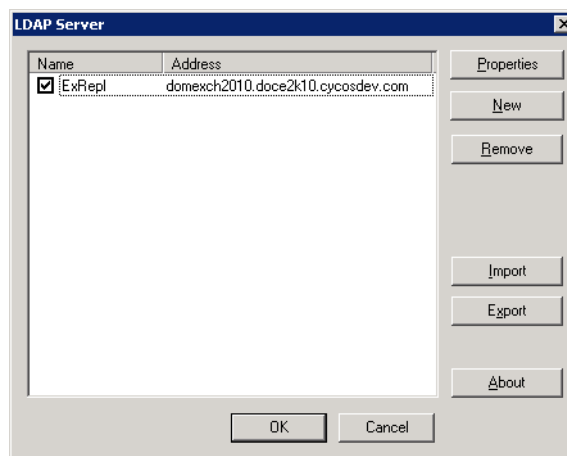
The LDAP replication must first be adjusted for the existing XPR system. This replication will see to the new database fields on the XPR server being described correctly with the corresponding values from the Active Directory. A simple supplementation of the database fields by assigning the corresponding values via the LDAP attributes is not sufficient because the LDAP Apl only replicates those data changed after the last update.

In this case the administrator must configure another LDAP connection to initially start the replication for Exchange Server 2013.

Proceed as follows:

1. Open the XPR monitor.
2. Expand in the **Modules of <XPR server name>** window the  **<Settings>** branch.
3. Expand the  **LdapApI** branch.
4. Double-click **Set Options**.

The LDAP APL settings dialog opens.



1. Create a file called Ex2013.lcf. Save it with the following contents under path "Installation path Xpressions>\Siemens\xpr\res\ldap":

```
DirTyp:ActiveDir
Script:ExRepl
AttMap:6
msExchHomeServerName:EXCH_HOMESERVER:0,str:toM:script
msExchMailboxGuid:EXCH_MBX_GUID:0,octets:toM:script
msExchVersion:EXCH_VERSION:0,int64:toM:none
objectGUID::1,octets:key:none
proxyAddresses:EXCH:0,str:cor:rule:"MRS:%t":%1
uSNChanged::0,int64:usn:none
Folders:2
:(homeMDB=*):2:a:1
CN=Deleted Objects:(objectclass=*):1:7:0
```

2. Click on the **Import** button.

The dialog for selecting files opens.

3. Select the configuration file `Ex2013.lcf`.

After you have made your selection, a new dialog for configuring an LDAP connection opens automatically.

4. Switch to the **Login** tab.
5. Enter the data you have already used for the existing LDAP connection on the **Login** tab.
6. Switch to the **Search** tab.
7. On this tab, select the users to be replicated.
8. Click on the **Replicate now** button.
The relevant database fields are now being replicated.
9. Click on **OK**.
The settings are saved and the configuration dialog closes.
10. Reopen the LDAP configuration when the replication is complete and the database fields have been filled in.
11. Disable (remove the tick that precedes the connection) or remove this LADP connection.

7.8.3 Switching the ExUM Apl to the new XPR Service Account

The *XPR service account* used so far for logging the ExUM Apl on to the Exchange Server 2007/2010 must be switched to the new *<XPR service account>* with the mailbox on the Exchange Server 2013.

How to perform this switch:

1. Click the **Start** button on the system that hosts the XPR server.
2. Click on **Administrative Tools**.
3. Select **Services** from the administrative tasks list.
The **Services** dialog opens.
4. Find the **XPR Exchange UM APL** service in the list
5. Click on this entry with the right mouse button to open the associated context menu.
6. Select **Properties** from the context menu.
7. Switch to the **Log On** tab.
8. In the **This account** area, change the login data of the old *<XPR service account>* on the Exchange Server 2007/2010 to the login data of the new *<XPR service account>* on the Exchange Server 2013.
9. Click on **OK**.

10. The new setting is applied and the properties dialog closes.
 11. Reboot the **XPR Exchange UM APL** service
- Switching to the new *<XPR service account>* is now complete.

7.9 Adjusting Registry Settings

7.9.1 Adjusting Registry Settings for the XPR Server

Updating the MAPI was required for supporting an RPC/HTTP connection. It enables connecting the Exchange Server 2013 via RPC/HTTP. The RPC proxy server configuration must be adjusted for those components that require a MAPI update.

The configuration is adjusted by adding a registry key **RPCHTTPProxyMap_EXUMAPL** on the XPR server.

The registry key is created in the following registry path:

```
HKCU\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem
```

NOTE: Be sure that you are logged in with the EXCHANGE 2013 SERVICE ACCOUNT.

How to create the registry key:

1. Create the new registry key **RPCHTTPProxyMap_EXUMAPL** with the format **[REG_SZ]** in the above registry path.
2. Double-click the created key and enter the registry value in the following format:

```
<DOMAIN>=<ProxyServer><ProxyServerSettings>
```

The parameters have the following meaning:

<Domain>

The domain name of the RPC/HTTP endpoint of the proxy server used by the MAPI clients, or * (asterisk icon).

<ProxyServer>

The **<ProxyServer>** parameter contains value **<FrontEndPoolFQDN>** and must be entered in the format **https://<FrontEndPoolFQDN>**. For example: **https://mail.company.com**

You can use the EMS for having value **<FrontEndPoolFQDN>** put out. Enter the following command in the command line there:


```
Get-OutlookAnywhere | fl server*, Interna*, identity
```

NOTE: Make sure that the value put out via `Get-OutlookAnywhere` is adopted in `<FrontEndPoolFQDN>` exactly.

```
<ProxyServerSettings>
```

The MAPI profile settings are stored in the `<ProxyServerSettings>` parameter. It comprises the following further parameters:

- `<RpcHttpAuthenticationMethod>`,
- `<RpcAuthenticationMethod>` and
- `<IgnoreSslCert>`

Example:

company.com=https://mail.company.com,ntlm,ntlm,true

or

***=https://mail.company.com,ntlm,ntlm,true**

Inserting the parameter in the underlying abbreviated notation results in the complete value of the registry key:

```
<DOMAIN>=<ProxyServer>,<RpcHttpAuthenticationMethod>,  
      <RpcAuthenticationMethod>,<IgnoreSslCert>
```

You can insert the following valid values for the single parameters:

for `<RpcHttpAuthenticationMethod>`

- Negotiate
- NTLM
- Basic

for `<RpcAuthenticationMethod>`

- Negotiate
- NTLM
- Anonymous
- None

for `<IgnoreSslCert>`

- True
- 1
- Y

- Yes

NOTE: Any other value inserted here is interpreted as `False`.

Examples:

```
unify.com=https://mail.unify.com,ntlm,ntlm,true  
*=https://mail.unify.com,ntlm,ntlm,true
```

You can obtain further information about this subject from the *Configuring the MAPI download for EXCHANGE 2013* instructions. You find these instructions in the Microsoft document *MAPI Download configuration guidance.docx* under:

<http://www.microsoft.com/en-us/download/details.aspx?id=39045>

7.9.2 Checking and configuring Certificates for the RPC Proxy Server

You must access the RPC proxy address via web browser to check and configure the certificates for the RPC proxy server:

NOTE: Execute the following work steps via the *<XPR Exchange 2013 Service Account>* logged in at the domain.

1. Login to the Xpressions machine with the 2013 Service Account.
2. In the Internet Explorer, open the **Internet Options** dialog via **Tools > Internet Options**.
3. Select the **Connections** tab
4. Select **LAN Setting**
5. Uncheck **Automatically detect Settings**

NOTE: This feature could cause delay in EXUMAPL access to Exchange 2013.

6. Open the web browser.
If you use the Internet Explorer, access the CAS-URL specified in the **RPCHTTpProxyMap**. The default setting for the CAS-URL is `https://<CAS server address>`
If a certificate error occurs, follow the next steps:

7. In the Internet Explorer, open the **Internet Options** dialog via **Tools > Internet Options**.
 8. Select the **Security** tab.
 9. Mark the **Local Intranet** icon.
 10. Click on the **Sites** button.
 11. Add the RPC proxy address
`https://<CAS server address>`
 12. Click on **Add**.
 13. Click on **Close**.
 14. Click on **OK** in the **Internet Options** dialog.
 15. Click on **Certificate error** in the address line in the browser window..
 16. Click on **View Certificates**.
The **Certificate** dialog opens.
 17. Click on the **Install certificate** button.
The **Certificate Import Wizard** dialog opens.
 18. Click on **Next** in this dialog.
 19. Select the **Place all certificates in the following store** option in the next dialog.
 20. Click on the **Browse** button.
The **Select Certificate Store** dialog opens.
 21. Select **Trusted Root Certification Authorities**.
 22. Click on **OK** in the **Select Certificate Store** dialog.
The dialog closes and you return to the **Certificate Import Wizard**.
 23. Click on **Next** in this dialog.
 24. Click on **Finish** in the next dialog.
- The certificate is now checked and configured.

7.10 Installing the Connectors

7.10.1 General Considerations

NOTE: For an already existing Xpressions system to be freshly connected to an Exchange Server 2013 the old connectors must first be uninstalled by a run-through of **Modify**.

7.10.2 Installation of the XPR Components for the Connection to *Exchange Server 2013*

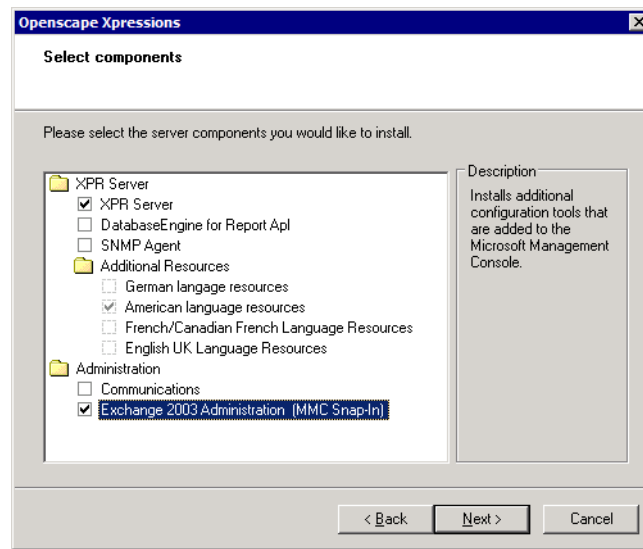
7.10.2.1 Selecting the Components

In the XPR server setup, after the license service installation, the language selection as well as reading the release notes you reach the setup dialogs for the Exchange connection.

After you have confirmed to have taken notice of the release notes you perform a first selection of components for the XPR server in the following dialog. Here you can also select the MMC Snap-in for installation on the XPR server. This, however, is only required if the XPR user administration is to occur from the XPR server.

NOTE: Managing users with help of the Active Directory Users and Computers program is normally not performed via the XPR server. Therefore, the MMC Snap-in must be manually installed on the server from which the user administration occurs. You find the setup file on the product data carrier in the directory <X>:\...\Addon\Client\Exchange\MMCSnapIns.
X corresponds to the current letter of the device that holds your product data carrier.

If you want to install the Snap-in on the XPR server, select the **Exchange 2003 Administration (MMC Snap-In)** option. The installation is then automatically started at the end of the server installation.



NOTE: If you do not see the MMC Snap-in component in this dialog, a license is likely to be missing. In this case please check the licenses and restart the setup program.

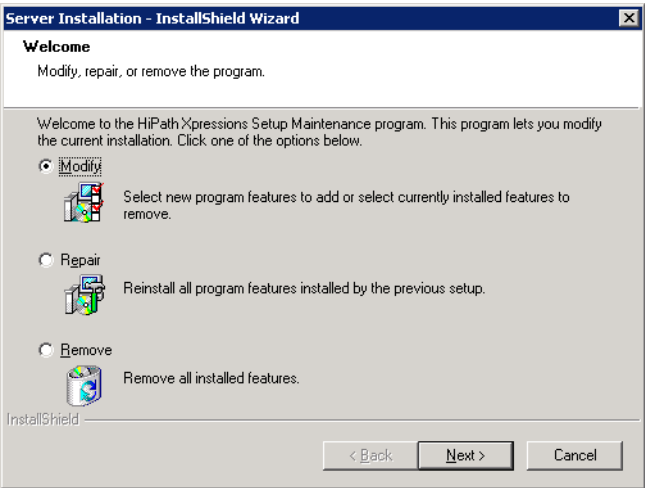
Exchange 2003 administration (MMC Snap-in extension)

users are still administered via the MMC Snap-in extension for Active Directory Users and Computers.

The MMC Snap-in displays the XPR-specific administration dialog **MRS Settings** for the XPR users (see [Section 4.3.4, “User Administration”, on page 114](#)).

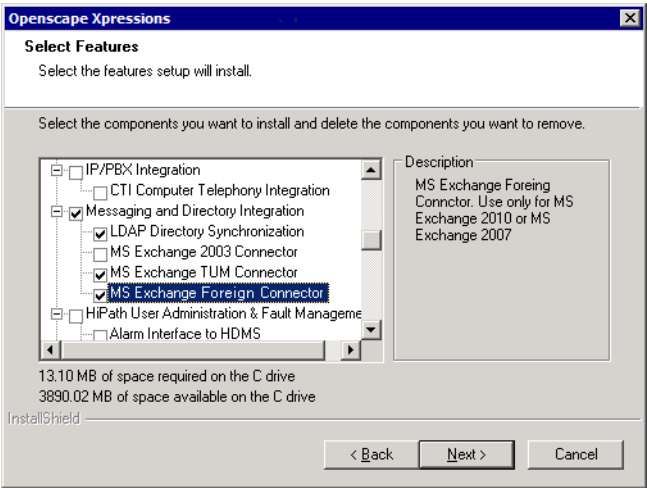
NOTE: A 64-bit operating system supports the available 32-bit XPR MMC Snap-in without restriction. This requires starting the XPR MMC Snap-in in 32-bit mode (`mmc /32`).

After the setup dialogs for the client components, external software, documentation and ASR components, you reach the selection of the desired installation scenario. Select **Modify** to install the Exchange components of the XPR server.



In the next dialog, select the following additional components from the **Messaging and Directory Integration** branch:

- LDAP directory synchronization (with a fresh OpenScope Xpressions V7 server installation only)
- MS Exchange TUM Connector
- MS Exchange Foreign Connector



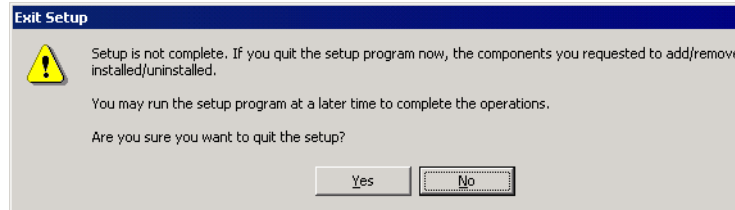
7.10.3 Components Installation Procedure

7.10.3.1 Starting the Installation

Installing the Exchange components in the running XPR setup starts with dialogs invoked for the preparative LDAP APL configuration when the XPR server is freshly installed. If only the two connectors for connecting an Exchange Server 2013 domain directly, Setup starts with the ExUM Apl installation. The steps executed from the setup start up to here serve for installing other XPR server. The respective settings are comprehensively described in the *Server Installation* manual.

7.10.3.2 General Considerations

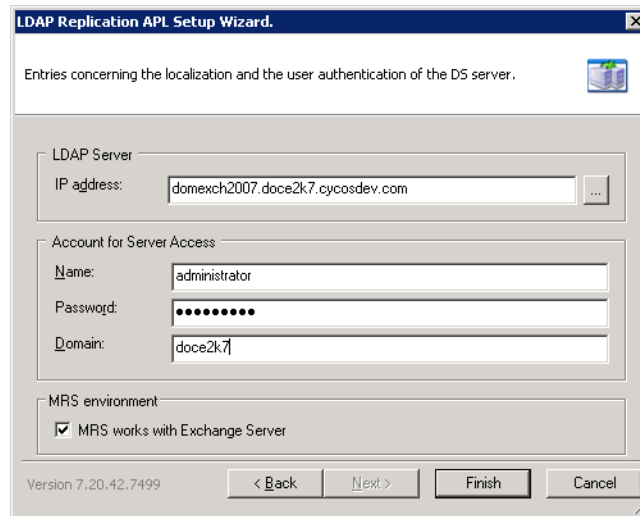
Pushing the **Cancel** button in the installation dialogs delivers the information that Setup has not been duly accomplished yet. If you select **Yes** here, only the installation of the current component is terminated – the XPR setup will then be continued with the next component. With **No** you return to the currently running setup.



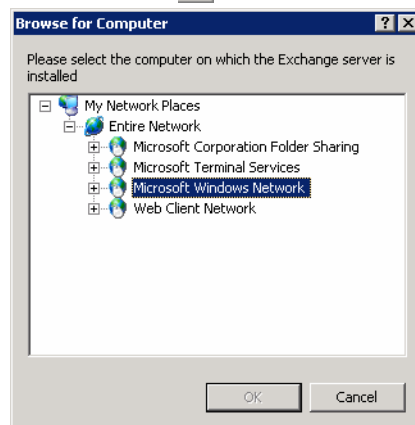
7.10.3.3 Installing the LDAP APL (for a fresh OpenScape Xpressions V7 Server Setup)

Setting up all components for connecting an Exchange Server 2013 freshly starts in the XPR server setup with installing the LDAP directory synchronization (the LDAP APL). The LDAP setup wizard first appears in its welcome window.

With a click on Next the dialog opens in which you find the **IP Address** entry field (**LDAP Server** section) to specify the name of the computer that the LDAP APL is to access for data replication. This is in most cases the Primary Domain Controller computer (PDC), which contains the Global Catalog of the Active Directory.



This can either be done by directly entering the server name in this entry line or via the **Browse for Computer** dialog. This dialog opens when you enable the selection icon ... next to the entry line.



Now create the **Account for Server Access**. In doing so, select a user account that has read as well as write privileges for the Active Directory. This is usually the domain administrator. You can also use the service account if it has the corresponding privileges.

In the **MRS environment** section, via the **MRS works with Exchange Server** check box, you integrate the configuration file required for *Exchange Server 2013*. It is called `Ex2013.lcf`.

The **Active Directory** option is intended for accessing other Active Directory directory services via LDAP. The `AdRepl.lcf` configuration file is then integrated by default. It enables LDAP access to other directory services similar to the Active Directory if no *Exchange server* has been installed.

Finish completes the entries and the LDAP setup.

Via **Back** you return to the LDAP APL setup welcome window again.

Cancel terminates the LDAP APL setup and initiates the installation of the next server component.

How to configure the LDAP APL is described in [Section 7.11.1, “Configuring the LDAP Apl”, on page 353](#).

7.10.4 Installing the OpenScape Xpressions V7 True Unified Messaging Connector (ExUm Apl)

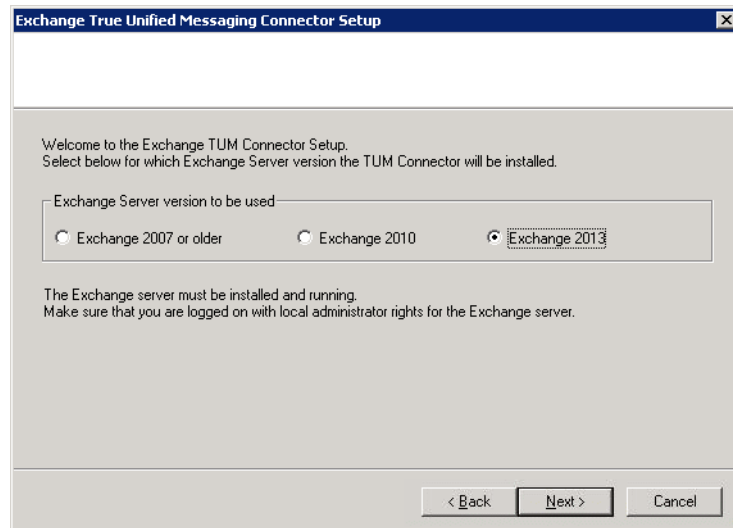
After setting up the LDAP Apl in case of a fresh OpenScape Xpressions V7 server installation or after selecting the components for the two connectors to connect an already installed OpenScape Xpressions V7 server to an Exchange Server 2013 domain, the connectors are installed in the setup.

During the installation all required registry keys but one are automatically created during the ExUM Apl setup. Only the value for the registry key **E2k13_RPC_PROXY_SERVER** must be configured manually during the installation in the **Exchange 2013 setup parameters** dialog via the **RPC proxy server** input line.

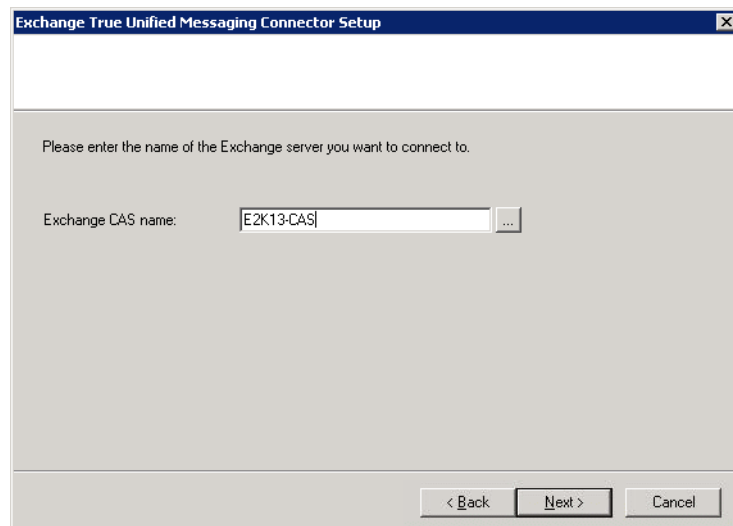
In the first setup step you select the version of the Exchange server to which the TUM connection is to be established. Select here the **Exchange Server 2013** option.

XPR and Microsoft Exchange Server 2013

Installing the Connectors



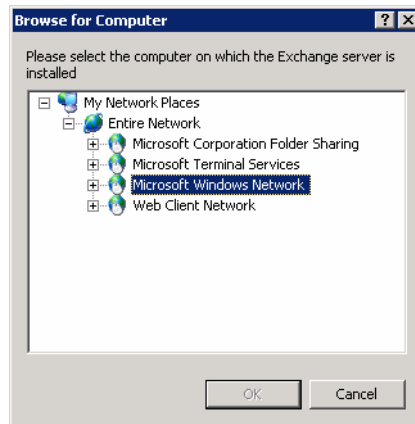
Click on **Next**.



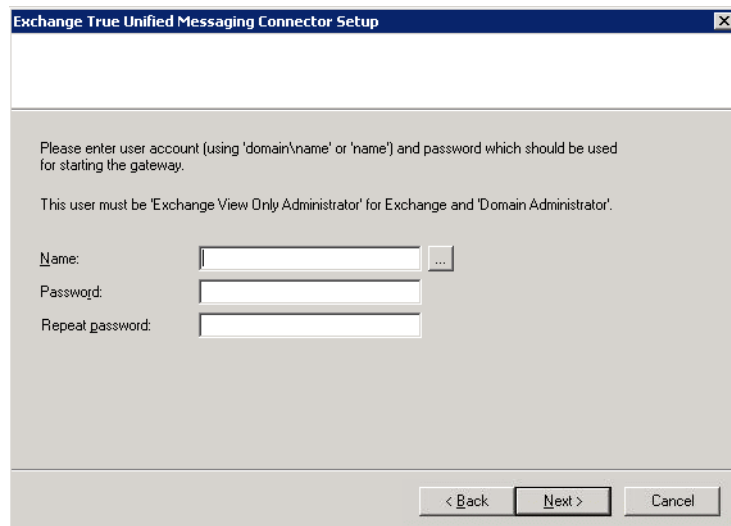
In the next dialog define the Exchange Client Server Role the ExUM APL is to establish a connection to. In a modular Exchange Server 2013 environment structure this is the server that has the Client Access Server (CAS) role.

NOTE: In case of an Exchange Server 2013 with monolithic structure the connection is set up to the server on which the Exchange Server 2013 is installed.

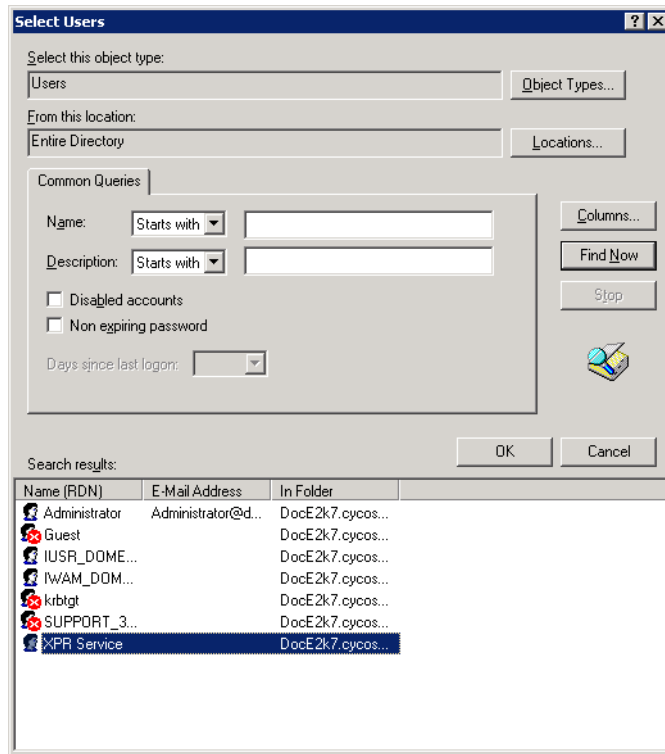
You can do this by directly entering the server name. You can also use the  button to look for the corresponding server in the network. A click on this button opens a dialog for selecting the Exchange Server 2013.



If you have configured the connection to the Exchange Client Access Server, a click on **Next** takes you to the dialog for defining the user account under which the ExUM APL is to run.



Here you can directly enter the name of the OpenScape Xpressions V7 service account in the format `<domain\name>`. You can also use the  button to select the service account.

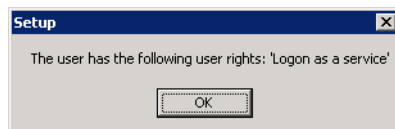


You can proceed as follows to transmit the service account to the ExUM APL configuration page via the user selection dialog:

- By means of a double-click on the selected user name.
- Via direct entry of the name in the lower portion of the dialog. Then verify the name by pressing the **Check Names** button.
- Through selection of the name in the list. Then click the **Add** button.

Click **OK** to complete this process.

Then enter the password to legitimate this service account. If the specified service account is valid, the user privileges assigned by Setup are displayed in a message.

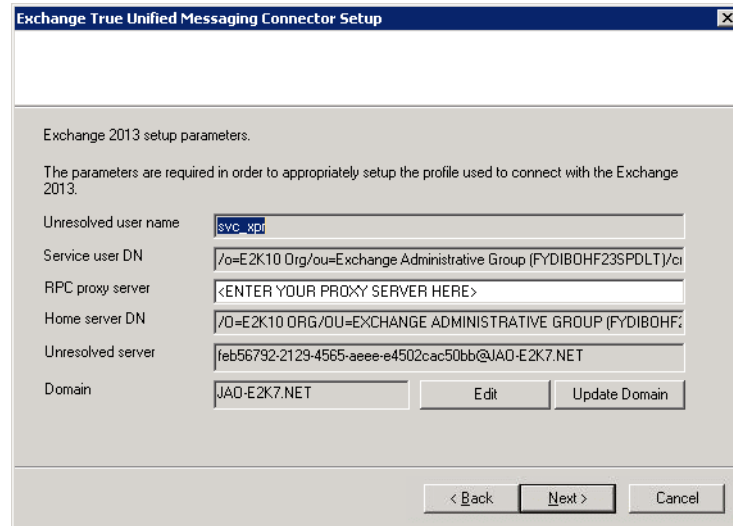


Confirm this message with **OK**. You are then informed that the entered password cannot be checked for validity. If you are not sure at this point, enable **No** to return to the password entry for making an alteration if necessary.

Click on **Next**.

The next dialog displays the required parameters with the settings the ExUM Apl needs for establishing a connection to the mailboxes of the Exchange Server 2013. Here, you must enter the value for the RPC proxy server manually.

Each of these parameters is stored in the registry. You find further information about the registry keys used in [Section 7.10.4.2, "Registry Settings of the ExUM Apl"](#), on page 330.



Exchange True Unified Messaging Connector Setup

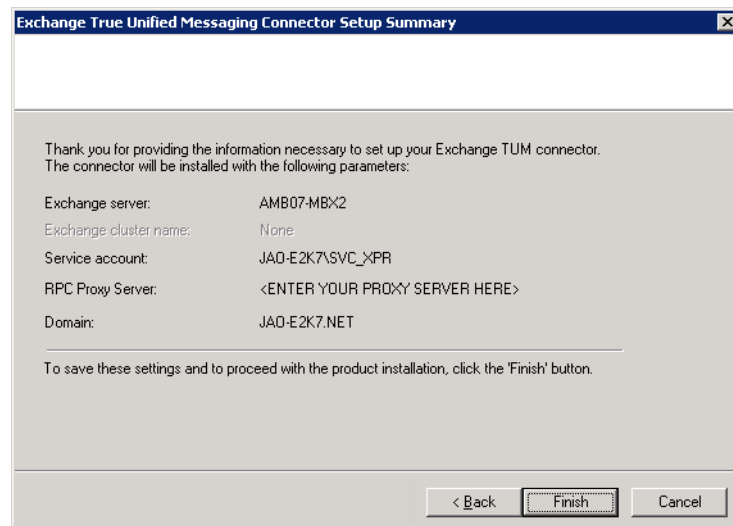
Exchange 2013 setup parameters.

The parameters are required in order to appropriately setup the profile used to connect with the Exchange 2013.

Unresolved user name	svc_xpr
Service user DN	/o=E2K10 Org/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=...
RPC proxy server	<ENTER YOUR PROXY SERVER HERE>
Home server DN	/O=E2K10 ORG/OU=EXCHANGE ADMINISTRATIVE GROUP (FYDIBOHF23SPDLT)/CN=...
Unresolved server	feb56792-2129-4565-aaaa-e4502cac50bb@JAD-E2K7.NET
Domain	JAD-E2K7.NET

Buttons: < Back, Next >, Cancel

If you continue the ExUM APL setup with **Next**, the Summary window displays the entered parameters once again.



Exchange True Unified Messaging Connector Setup Summary

Thank you for providing the information necessary to set up your Exchange TUM connector. The connector will be installed with the following parameters:

Exchange server:	AMB07-MBX2
Exchange cluster name:	None
Service account:	JAD-E2K7\SVC_XPR
RPC Proxy Server:	<ENTER YOUR PROXY SERVER HERE>
Domain:	JAD-E2K7.NET

To save these settings and to proceed with the product installation, click the 'Finish' button.

Buttons: < Back, Finish, Cancel

A click on **Finish** will only save your entries. The ExUM APL installation is thus accomplished.

7.10.4.1 Log Files for installing the ExUM Apl

The installation processes are stored in the following log directories during the ExUM Apl installation:

- %TEMP% directory folder\mrsExch.log
- <Installation path of the XPR server>\log\msExch.log

7.10.4.2 Registry Settings of the ExUM Apl

To enable accessing the mailboxes created on the Exchange Server 2013, some additional registry keys are required for configuring the ExUM Apl profile appropriately. These registry keys are automatically configured by the ExUM installer. Only the value of the registry key **E2K13_RPC_PROXY_SERVER** must be entered manually during the installation.

If these registry values have to be edited, you can use the `Get-Mailbox` command of the **Exchange Management Shell (EMS)** for this purpose.

7.10.4.3 Determining the Registry Values via the EMS

How to determine the registry values:

1. Start the **Exchange Management Shell (EMS)**.
2. Enter the following command in the command prompt:

```
Get-Mailbox "<XPR service account>" | fl name, identity, alias, ExchangeGuid,  
LegacyExchangeDN, ServerLegacyDN, ServerName
```

The requested parameters are put out.

7.10.4.4 Configuring the Registry Keys for the ExUM Api

The following registry keys contain the parameters required for the service account to access the mailboxes in Exchange Server 2013.

The registry keys must be created in the following registry path:

HKLM\SOFTWARE\Wow6432Node\PPCOM\MRS\ExUMApi

E2K13_DOMAIN [REG_SZ]

Default:	-
Possible values:	<Domain name>
Example:	company.com

Domain of the RPC/HTTP endpoint of the proxy server used by the MAPI clients.

E2K13_HOME_SERVER_DN [REG_SZ]

Default:	-
Possible values:	<Distinguished name of the home server>

Defined name of the home server. The name can be retrieved from the ServerLegacyDN and ExchangeGuid via a Get-Mailbox command.

Edit the character string as described in the following:

1. Replace the variable <Exchange 2013 Server> after the character string of the ServerLegacyDN
CN=SERVERS/CN=<EXCHANGE 2013 SERVER>
with value ExchangeGuid@<DOMAIN>.

Example:

```
/o=COMPANY ORG/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/
cn=Configuration/cn=Servers/cn=fe5f84bf-36f9-42eb-ab2f-9e40e3413bf1@company.com
```

NOTE: The <DOMAIN> portion is replaced with the data from the **E2K13_DOMAIN** registry key.

E2K13_RPC_PROXY_SERVER [REG_SZ]

Default:	-
Possible values:	<server name>
Example:	amb09-exch2k13.company.com

The FQDN of the RPC/HTTP endpoint of the proxy server used by the MAPI clients.

E2K13_SERVICEUSER_DN [REG_SZ]

Default:	-
Possible values:	<Distinguished name of the <XPR service account>>

Defined name of the <XPR service account>. The name can be retrieved from the LegacyExchangeDN properties via a Get-Mailbox command.

Example:

```
/o=COMPANY ORG/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Recipients/  
cn=e092feee00504b1ebf88ba3afd6c059e-admine2k13
```

E2K13_UNRESOLVED_NAME [REG_SZ]

Default:	-
Possible values:	<Mailbox alias for the <XPR service account>>
Example:	admine2k13

Mailbox alias name for the <XPR service account> on the Exchange Server 2013. Use the alias name you retrieved from the alias properties via a Get-Mailbox command.

E2K13_UNRESOLVED_SERVER [REG_SZ]

Default:	-
Possible values:	<Personalized server ID>
Example:	fe5f84bf-36f9-42eb-ab2f-9e40e3413bf1@company.com

Personalized server ID. Use the ID you retrieved from the ExchangeGuid properties via a Get-Mailbox command, followed by the domain name (format: <ExchangeGuid>@<Domain>).

NOTE: The <DOMAIN> portion is replaced with the data from the E2K13_DOMAIN registry key.

7.10.4.5 Making the ExUM Apl failsafe on the Exchange Server 2013

With Exchange Server 2013, Microsoft changed the server architecture as they removed the CAS array object. Consequently, it can no longer be used for client access. A new mechanism for providing an alternative failover was therefore implemented in the ExUM Apl. This feature is enabled via three registry keys that must be configured manually.

NOTE: DAGs without an administrative access point can be created only on servers running Exchange 2013 Service Pack 1 or later on Windows Server 2012 R2 Standard or Datacenter edition.

Creating DAGs without cluster administrative access points leads to the situation that the Xpressions Exchange Apl cannot connect to Exchange. This is a restriction.

You find additional information about this topic under:

[https://technet.microsoft.com/en-us/library/dd979799\(v=exchg.150\).aspx](https://technet.microsoft.com/en-us/library/dd979799(v=exchg.150).aspx)

These registry keys must be created in the following registry path:

HKLM\SOFTWARE\Wow6432Node\PPCOM\MRS\ExUMAp1

POLLING_INTERVAL [REG_DWORD]

Default:	-
Possible values:	<0, 60 or higher (value in seconds)>

Interval in seconds in which the ExUMAp1 checks whether the connection to the Exchange server is still up. You can determine the behavior triggered with an interrupted connection via the registry key **STOPONFAILURE**.

STOPONFAILURE [REG_DWORD]

Default:	-
Possible values:	<0 or 1>

If activating **POLLING_INTERVAL** detects an interrupted connection to the Exchange server, you can specify the ExUMAp1's behavior for this case via this registry key.

0: No action; the ExUMAp1 will not be rebooted.

1: The ExUMAp1 will be rebooted. This reboot is triggered by initiating the kernel watchdog.

E2K13_RPC_ALTERNATIVE_SERVERS [REG_MULTI_SZ]

Default:	-
Possible values:	<Exchange CAS server name>
Example:	ExchCAS_1,ExchCAS_2,ExchCAS_3...

This registry key must contain the names (non-FQDN) of the Exchange CAS servers that the ExUm Apl attempts to reconnect in case of an error. In this process, the specified Exchange CAS servers are addressed in succession until a connectable one is found.

7.10.5 Installing the OpenScape Xpressions V7 Foreign Connector

NOTE: If you install the XPR Foreign Connector for an *Exchange Database Availability Group* please heed the modified setup routine.

The ExUM APL installation is automatically followed by the XPR Foreign Connector setup if this component was previously selected.

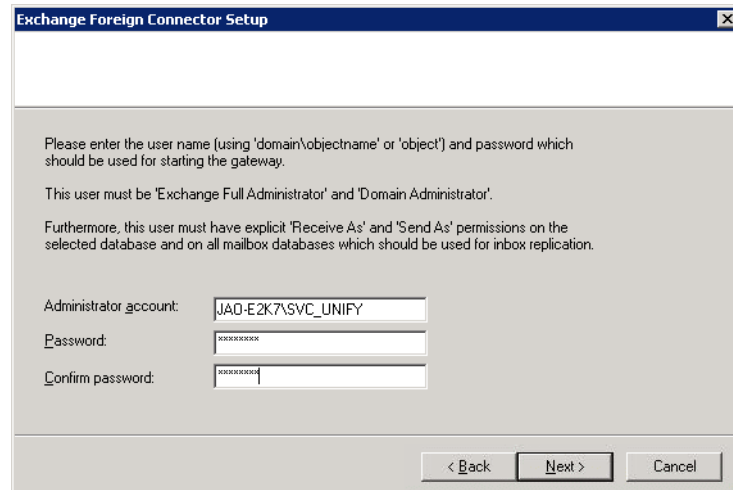
The welcome dialog of the Exch APL installation once again points to the requirements that must be met for a successful installation.

After you have clicked on **Next** in the welcome dialog, you reach the dialog for selecting the Exchange server. Here you determine the Exchange server version that the XPR Foreign Connector is to connect. Select Exchange Server 2013 here.



Then click on the **Next** button.

In the next dialog you need to enter the service account under which the Exch APL is to operate. You specify the service account under Name in the format *<domain\name>*. Then enter the service account password twice.



The dialog box is titled "Exchange Foreign Connector Setup". It contains the following text:

Please enter the user name (using 'domain\objectname' or 'object') and password which should be used for starting the gateway.

This user must be 'Exchange Full Administrator' and 'Domain Administrator'.

Furthermore, this user must have explicit 'Receive As' and 'Send As' permissions on the selected database and on all mailbox databases which should be used for inbox replication.

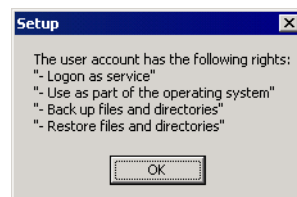
Administrator account: JAO-E2K7\SVC_UNIFY

Password: [masked]

Confirm password: [masked]

At the bottom, there are three buttons: "< Back", "Next >", and "Cancel".

Since the Exchange gateway cannot link up with *Exchange Server 2013* when a wrong password has been specified, the entry must occur twice to rule out typing errors as source of error. A correct entry opens an information dialog as confirmation and to display a list of the user privileges assigned to the user account by Setup.



The dialog box is titled "Setup". It contains the following text:

The user account has the following rights:

- "- Logon as service"
- "- Use as part of the operating system"
- "- Back up files and directories"
- "- Restore files and directories"

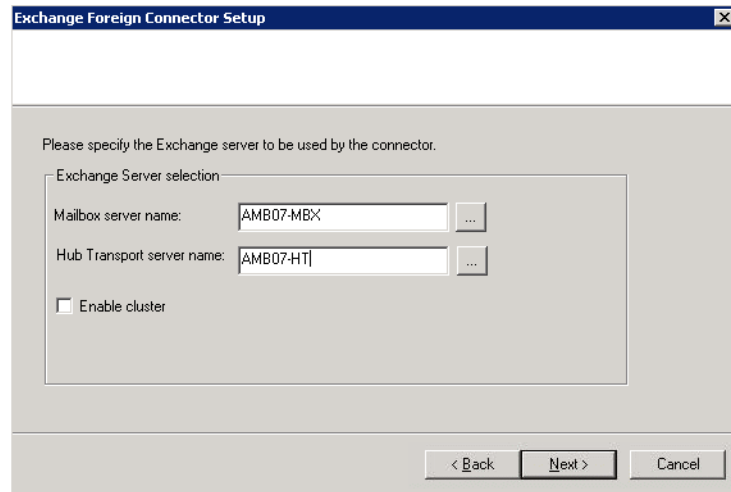
At the bottom, there is an "OK" button.

Confirm the user privilege information display with **OK**.

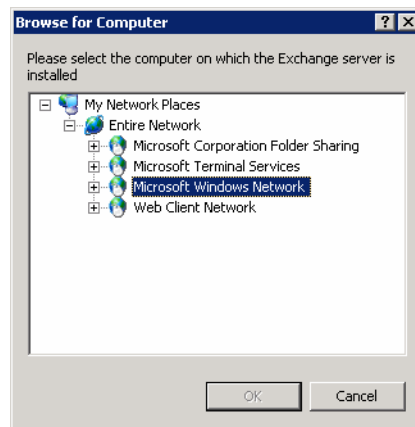
Setup is then continued with entering the computer name for the connection to *Exchange Server 2013*.

In case of a modular *Exchange Server 2013* environment structure the XPR Foreign Connector must establish a connection from the XPR server to the Mailbox Server Role **and** to the Hub Transport Server Role. The connection to the Exchange Mailbox Server Role is required for opening a MAPI connection to resolve addresses. The connection to the Exchange Hub Transport Server Role serves for transporting messages from/to the XPR server.

NOTE: If the *Exchange Server 2013* has a monolithic structure, specify the name of the *Exchange Server 2013* in both entry lines.



Here you can either directly enter the server name or use the ... button to look for the relevant servers in the network.



In the first setup dialog, select the **Enable Cluster** option if you wish to connect an *Exchange Database Availability Group*.

Installing the XPR Foreign Connector at an *Exchange Server 2013* with DAG

After the setup start you need to execute the following worksteps for the XPR Foreign Connector:

1. Select the **Enable cluster** option for choosing the Exchange Server Roles in the setup dialog. Using this option you can install the XPR Foreign Connector at an Exchange Server 2013 with Database Availability Group (DAG).

2. Enter the required Exchange server DAG name in the **Mailbox server name** input field.
3. Enter the name of the Hub Transport server in the **Hub Transport server name** input field.
4. Select the desired address templates after the found database and mailbox data list have been displayed.

5. Configuration of the XPR Foreign Connector for the *Database Availability Group*.

Setting up the XPR Foreign Connector creates the **DAGONES** key in the **HKLM\SOFTWARE\Wow6432Node\PP-COM\MRS\ExchApl** registry path. Enter the names of the servers that form the *Database Availability Group*.

DAGNODES [REG_MULTI_SZ]

Default:	-
Possible values:	NODE1, NODE2,...NODEn
Remark:	NODE1..NODEn are the names of the servers that form the Database Availability Group.

You find additional information about the concept and management of a *Database Availability Group (DAG)* on the following web pages:

Understanding Database Availability Groups

[http://technet.microsoft.com/en-us/library/dd979799\(EXCHG.140\).aspx](http://technet.microsoft.com/en-us/library/dd979799(EXCHG.140).aspx)

Managing High Availability and Site Resilience

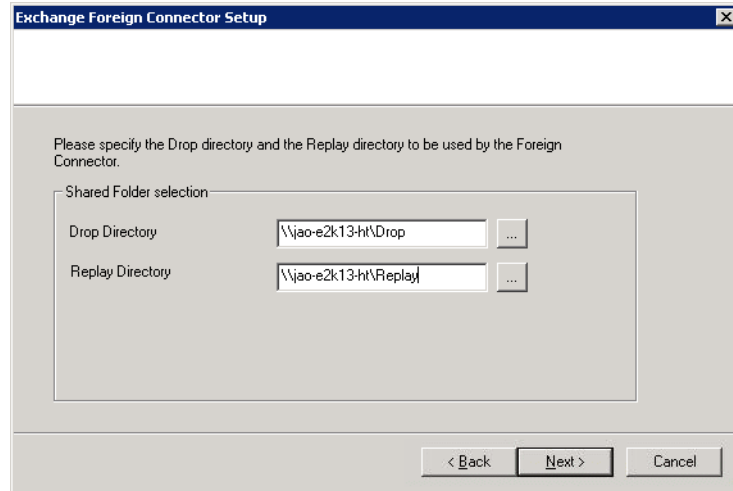
<http://technet.microsoft.com/en-us/library/dd638215.aspx>

Managing Database Availability Groups

<http://technet.microsoft.com/en-us/library/dd351172.aspx>

After you have entered the mailbox server of the Exchange server via the mailbox server name or the DAG name or selected the mailbox server in the network, click on **Next**.

You reach the dialog in which you have selected the transport directories.



In the **Drop directory** and **Replay directory** specify the path to the shared transport directories according to the following pattern:

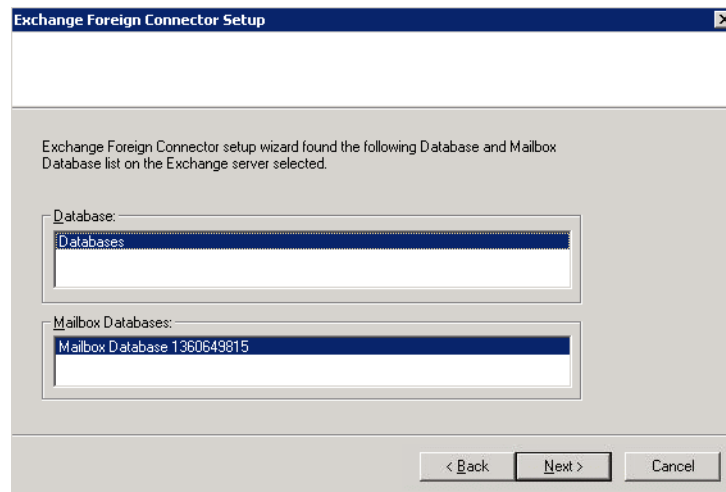
- For the **Drop directory**
`\\<Ip address or name of the Exchange server on which the Hub Transport Server operates>\<XPR server name>-<name of the Exchange Server 2013 Mailbox Server Role>`
- For the **Replay directory**
`\\<Ip address or name of the Exchange server on which the Hub Transport Server operates>\Replay`

You can also use the browse button  to look for the corresponding shares in the network. In the latter case a window opens for selecting the corresponding shares.

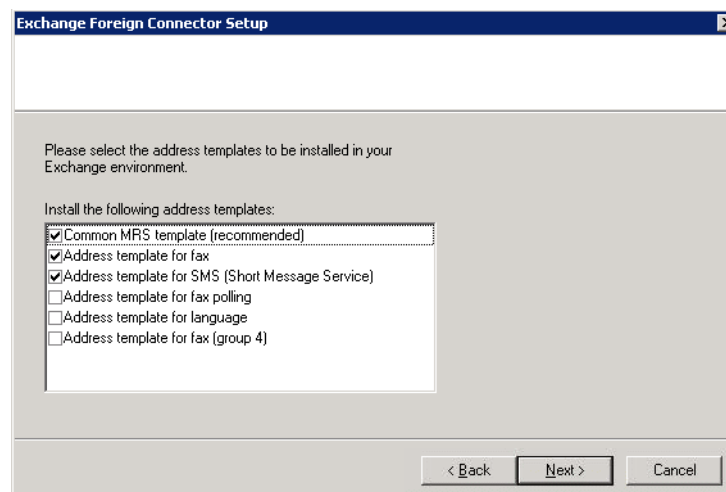
NOTE: The settings performed here during the installation for the paths of the transport directories can later be changed via the **ExchApl** configuration dialogs in the XPR monitor (**Exchange Foreign Connector** tab).

After you have selected the drop directory and the replay directory, click on **Next**.

The next dialog confirms the successful localization of the two specified servers by displaying the **Database** and the **Mailbox Database**.



Click on **Next**. The installation continues with the **address template** configuration.



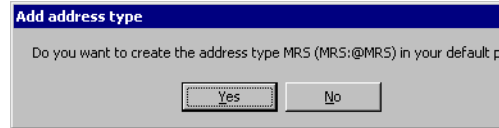
Here you can have **address templates** installed in your Exchange environment for various services offered by the XPR server.

In this way you can later generate e.g. a new address for the address book in the client, so that you only need to enter the corresponding number and select the desired service in there instead of working with the somewhat cryptic default Exchange addressing.

After you have clicked on **Finish**, the dialog for creating the MRS address type (MRS:@MRS) opens. This address type is globally created in the Default Policy.

NOTE: As of Exchange Server 2007 the distribution groups support the **sAMAaccountName**. As a result, all Exchange users with this attribute are replicated as full XPR users to the XPR server. This causes problems when assigning

the MRS address type and the number of replicated users exceeds the number of available user licenses. Therefore, the number of user groups to be replicated may have to be restricted beforehand via the LDAP configuration.



Yes starts the address assignment and immediately defines an MRS address for each Exchange user.

NOTE: In large system environments, address assignment may take a while.

If not all Exchange users are to be assigned the MRS address, click the **No** button in this dialog.

This will directly resume the setup process with the installation of the next XPR component. The MRS address type will not be specified then and there is no assignment of the MRS address to the Exchange users either. The MRS address type must then be manually defined afterwards. See [Section 5.7, “Adding and assigning the MRS E-Mail Address Type retrospectively”](#), on page 258.

A subsequent manual definition of the MRS address type is useful if only specific users are to use this address type. After that, the MRS address can be assigned to users via the definition of filter rules in the Default Policy (or in a newly created policy).

The installation of the XPR components for connecting *Exchange Server 2013* is now complete.

If the ExchAPL does not start when the XPR server is booted, a privilege problem is in most cases responsible for this. You may then see an error message on the XPR monitor like:

```
Exchange Server seems not to be running <0x80004005>
```

In this case check whether the service account was assigned the required privileges or whether the service account was added on all system components to the local administrators.

7.10.5.1 Log Files for installing the E2k7 Apl

The installation processes are stored in the following log directories during the E2k7 Apl installation:

- %TEMP% directory folder\mrsExch.log

- <Installation path of the XPR server>\log\msExch.log

7.10.6 Installation of the MMC Snap-in

Administering the XPR user data requires the MMC Snap-in. It displays the **MRS Settings** tab in the properties dialog for the AD users. To this the MMC Snap-in that was already deployed with *Exchange Server 2003* is used.

NOTE: The MMC Snap-in can be installed on a 32-bit as well as on a 64-bit system. When using a 64-bit system, start this application in 32-bit mode (`mmc / 32`).

You find further information in the Microsoft KB article [http://msdn.microsoft.com/en-us/library/ms692753\(VS.85\).aspx](http://msdn.microsoft.com/en-us/library/ms692753(VS.85).aspx)

The MMC Snap-in can be integrated in a new installation of the XPR server if the XPR users are to be administered from the XPR server. In the first installation dialog, after invoking the server setup, select the **Exchange 2003 Administration (MMC Snapin)** component. See also [Section 7.10.2.1, "Selecting the Components"](#), on page 320.

If the MMC Snap-in is required on another system, the installation must occur manually and belatedly from the XPR product data carrier. You find the setup file on this carrier in the directory: `X:\AddOn\Client\Exchange\MMCSnapIns` (X corresponds to the current letter of the device that holds your product data carrier).

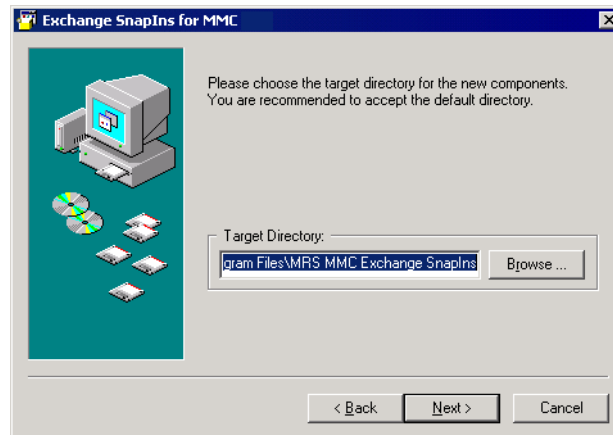
How to manually install the MMC Snap-in:

1. Start the setup by executing the `setup.exe` from the above directory.
A welcome dialog opens. It points out that all running applications should be terminated before Setup is started. So, if any applications are still open, close them after selecting **Cancel**. Setup is left then and active programs can be shut down. Subsequently, it must be started again.
2. Click the **Next** button in the welcome dialog.
The dialog for defining the target directory opens.

During the installation, the following files are created in the `%ProgramFiles%\MMC Exchange SnapIns` directory by default:

```
ExtInst.MMCExchSnapIns.ini
setup.MMCExchSnapIns.ini
Uninstall.MMCExchSnapins.exe
Uninstall.MMCExchSnapins.exe
```

In addition, the `ExtInst.log` log file that logs the setup process is created in the `X:\Documents and Settings\<installing user>\Local Settings\Temp` directory.

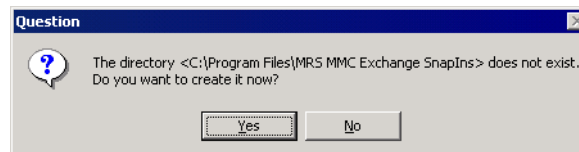


You can also push **Browse...** to specify or newly define a directory to which the program files are then copied. A file selection dialog opens after you have pushed this button. However, we recommend to copy the preset directory since the program components are then easier to find when the necessity arises.

NOTE: The **Back** button takes you back to the welcome dialog and via **Cancel** you can terminate the setup after a security prompt.

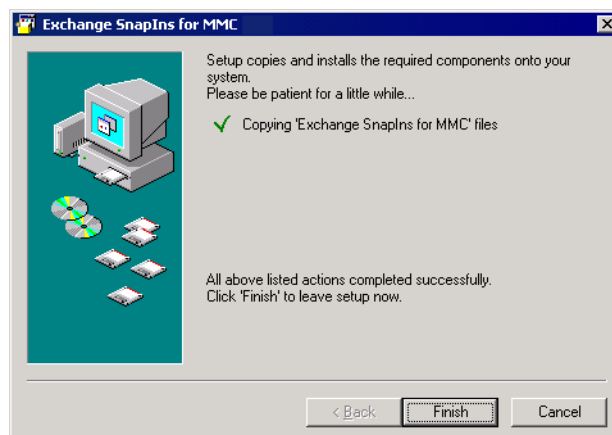
3. Click on the **Next** button after you have made your selection for the target directory.

If this directory does not exist yet, you are asked as to whether or not you want to have the directory defined. Confirm this query with **Yes** if you want to perform the installation.



The program files are being copied to the specified directory.

You can follow the progress of the copying and installation process in the next window by the icon next to **Copying 'Exchange SnapIns for MMC' files**. While the activities continue, a black cross precedes the “Copying 'Exchange SnapIns for MMC' files:” line. After completion of the data transmission, a green tick replaces the black cross.



4. Click **Finish** to complete the installation.

The MMC Snap-in installation is now complete.

7.10.6.1 Error Analysis during the Installation

In the event that an error has occurred during the installation, the cause of a termination can be detected in the log file automatically created with the installation.

Depending on the suggested setup directory, the log file is stored in the following directories:

- If the installation is performed in the directory suggested by Setup, you find the log file in the directory:

```
... \xpr\logs
```

- If the installation is performed in a directory that you determine, you find the log file in the temporary directory of the installing user.

In the log file (`MrsEXCH.log`) all setup steps are itemized and classified with a status description.

Example:

```
...
ExchangeUpdate HrInstallAddressTemplates successful
EnterpriseGDI successfully read
Successfully remove Exchange 2000 Gateway object.
Successfully got MRS-Container-Object (LDAP://AD1DOC/
CN=XPR,CN=Microsoft Exchange,CN=Services,CN=Configuration,
DC=doc-test,DC=alsdorf,DC=cycos,DC=local) Settings Object
(C) successfully removed.
MrsExchSetup HrInstallService successful
Active Directory Object successfully installed.
Successfully got MRS-Container-Object (LDAP://AD1DOC/
CN=XPR,CN=Microsoft Exchange Gateway,CN=Services,
CN=Configuration,Settings Object (<XPR server name>)
<CN=<XPR server name>:AD1DOC> successfully installed
ExchangeUpdate HrInstallGateway successful
Registering Extensions Successfully registered Admin
Extension
Successfully registered User Extension
ExchangeUpdate completed and successful
MaintProxy finished ...
```

If an error has occurred, the corresponding installation step is followed by “failed” instead of “successful”.

Example:

```
MrsExchSetup HrInstallService failed
```

When solving setup problems, the Event Viewer under Windows, which you can use for diagnosis, comes in handy (**Start** > rightclick on **Computer** > select **Manage** from the context menu > expand **Computer Management** > **System Tools** > open the **Event Viewer**).

In there all running processes are logged. When you select the desired protocol or service, the events that happened therein are displayed.

7.10.7 Working on the Exchange Server

7.10.7.1 Creating the Transport Directories

The transport of messages from the XPR server to Exchange and vice versa requires two directories, the drop and replay directory. These two directories serve to buffer the messages in a waiting loop until they are processed, meaning, sent to the respective target server. Storing the messages in these directories depends on the transmission direction.

Both directories are created on the server on which the Hub Transport Server Role operates.

NOTE: If the Exchange environment has a monolithic structure, the directories are created on the server on which the *Exchange server 2013* is installed.

Activating the transport directories requires configurations on the server with the Hub Transport Server Role (in case of a monolithic structure on the *Exchange server 2013*) as well as for the settings of the **ExchApl** on the XPR server.

- The drop directory

This directory serves for delivering messages sent from the Exchange server to the XPR server. The messages are retrieved and further processed by the XPR server.

During the **ExchAPL** installation this object is created as “DropDirectory” object. It contains by default the name:

<XPR server name>-<name of the Exchange Server 2013 Mailbox Server Role>

NOTE: Due to the system, the object name for the Foreign Connector is created using the Mailbox Server Name instead of the Hub Transport Server Name.

You can have the drop directory name put out by entering the following command in the *Exchange management shell*:

```
get-foreignconnector|fl
```

The listing entry you look for has the format:

```
DropDirectory      :  <XPR server name>-<name of the Exchange
                        Server 2013 Mailbox Server Role>
```

NOTE: In case of a modular *Exchange Server 2013* installation distributed among several servers, the drop directory must be reachable via a UNC path in the network. Only then this directory can be accessed from the Hub Transport server (or from all further Hub Transport servers, if available). This is not required if the system has a monolithic structure.

- The replay directory
This directory buffers the messages sent by message servers different from Exchange to the Exchange organization. Exchange retrieves the messages from there and delivers them to the mailbox of the Exchange user.

NOTE: You can rename both directories and store them anywhere in the system. If this is desired, adjust the new directory names and the directory paths in the system upon the creation, activation or configuration.

How to create and activate these directories:

Creating and activating the drop directory

1. Using the Hub Transport Server Role create a directory with the following properties on the server:

Path:

```
%ProgramFiles%\Microsoft\Exchange Server\V15
```

Directory name:

```
<XPR server name>-<name of the Exchange Server 2013 Mailbox Server
Role>
```

The path is defaulted as the drop directory is expected at this point. If several servers with the Hub Transport Role are available, select the one for which the XPR Foreign Connector is installed.

Example:

```
%ProgramFiles%\Microsoft\Exchange Server\V15
\<XPR server name>-<name of the Exchange Server 2013
Mailbox Server Role>
```

NOTE: In case of an *Exchange server 2013* with monolithic structure, the **drop directory** is created in the following path of the server on which the *Exchange server 2013* is installed:

%ProgramFiles%\Microsoft\Exchange Server\V15

NOTE: Please note that the drop directory may only be configured on one Hub Transport server and that there is only one path to the drop directory.

2. Set the following access privileges:
 - Grant the XPR service account under which the Exchange APLs operate **Full Control** of this directory share. Proceed as follows:
 - Invoke the context menu for the drop directory.
 - Change to the **Sharing** tab in the configuration dialog.
 - Enable here the **Permissions** button.
 - Add the XPR service account as user via the **Add** button.
 - Assign the **Full Control** privilege to the XPR service account.
 - Grant the XPR service account **Full Control** of the drop directory for the NTFS authentication. Proceed as follows:
 - Invoke the context menu for the drop directory.
 - Change to the **Security** tab in the properties dialog.
 - Add the XPR service account as user via the **Add** button.
 - Assign the **Full Control** privilege to the XPR service account.
 - Grant the NETWORKSERVICE on the server with the Hub Transport Server Role **Full Control** of the drop directory. Proceed as follows:
 - Invoke the context menu for the drop directory.
 - Change to the **Security** tab in the properties dialog.
 - Add the NETWORKSERVICE as user via the **Add** button.
 - Assign the **Full Control** privilege to the NETWORKSERVICE.

- Grant the Hub Transport server **Full Control** of this directory share.

NOTE: If several Hub Transport servers have been installed, this must occur for every single Hub Transport server.

Proceed as follows:

- Invoke the context menu for the drop directory.
 - Change to the **Security** tab in the properties dialog.
 - Use the **Add** button to add the Hub Transport server(s) as computer.
 - Assign the **Full Control** privilege to the Hub Transport server(s).
3. In case of several Hub Transport servers set the UNC path to the drop directory.

Use the Exchange management shell command:

```
Set-ForeignConnector -Identity "MrsConnector (<XPR server
name>:<name of the Exchange Server 2013
Mailbox Server Role>)" -DropDirectory "\\<Hub Transport
server name>\<XPR server name>-<name of the Exchange Server
2013 Mailbox Server Role>" for this purpose
```

The creation of the drop directory is now complete.

NOTE: If you do not use the default path for the drop directory you need to reconfigure your individual path in the system. When you configure the path the drop directory is simultaneously activated. To modify the directory path start the *Exchange management shell*.

Enter the following command in the *Exchange management shell*:

```
Set-TransportServer <hub transport server>
-RootDropDirectoryPath "<drive>:\<path>"
```

The first line of this command is separated from the second line by a blank (...port server> -RootDropDir...).

In the *Exchange management shell* you can check whether the activation has been successful with the following command:

```
Get-TransportServer <Hub Transport Server>|fl
```

In the subsequently displayed list the previously empty `RootDropDirectoryPath`: entry must now feature the entered path specification.

Creating or activating the replay directory

In the list put out by the

```
Get-TransportServer <your Hub Transport Server>|fl
```

command you find the defaulted path to the replay directory. It reads:

```
ReplayDirectoryPath      : %ProgramFiles%\Microsoft\  
                           Exchange Server\TransportRoles\Replay
```

NOTE: You can create the replay directory anywhere on the server that has the Hub Transport Server Role. In doing so you need to adjust the path, though. You do this via the command:

```
Set-TransportServer <hub transport server>  
-ReplayDirectoryPath "<path>"
```

The first line of this command is separated from the second line by a blank (`...port server> -ReplayDir...`).

1. Set the following privileges for accessing the “Replay” replay directory:

- Grant the XPR service account under which the Exchange APLs operate full access to this directory share. Proceed as follows:
 - Invoke the context menu for this directory.
 - Change to the **Sharing** tab in the configuration dialog.
 - Enable here the **Permissions** button.
 - Add the XPR service account as user via the **Add** button.
 - Assign the **Full Control** privilege to the XPR service account.
- Grant the XPR service account **Full Control** of the drop directory for the NTFS authentication. Proceed as follows:
 - Invoke the context menu for the replay directory.
 - Change to the **Security** tab in the properties dialog.
 - Add the XPR service account as user via the **Add** button.
 - Assign the **Full Control** privilege to the XPR service account.

- Grant the NETWORKSERVICE on the server with the Hub Transport Server Role **Full Control** of the replay directory. Proceed as follows:
 - Invoke the context menu for the replay directory.
 - Change to the **Security** tab in the properties dialog.
 - Add the NETWORKSERVICE as user via the **Add** button.
 - Assign the **Full Control** privilege to the NETWORKSERVICE.

Creating the replay directory is now complete.

Configuration of the ExchApl for access to the transport directories

The transport directories on the XPR side must now be configured.

1. In the XPR monitor open the configuration dialog of the **ExchApl**.
2. Switch to the **Exchange Foreign Connector** tab.
The entry lines for **Drop directory** and **Replay directory** display the XPR server name as default.
3. In the **Drop directory** and **Replay directory** specify the path to the shared transport directories according to the following pattern:

For the **Drop directory**

\\<Ip address or name of the Exchange server on which the Hub Transport Server operates>\<XPR server name>-<Exchange2013 mailbox server name>

For the **Replay directory**

\\<Ip address or name of the Exchange server on which the Hub Transport Server operates>\Replay

4. Click on **Apply** and **OK** to save the modifications.

The entered values are stored in the XPR server registry:

Registry path:

HKLM\SOFTWARE\Wow6432Node\PP-COM\MRS\ExchApl

Key:

DropDirectory and ReplayDirectory).

The configuration of the XPR Foreign Connector on the side is thus complete.

The **ExchApl** must be rebooted for the configuration settings to take effect.

NOTE: If the default logging window of the monitor displays an error message after you have saved the modifications, the system is unable to locate the two directories via the specified path. Open the ExchAPL settings dialog again and correct your path specifications.

7.11 Configuration

7.11.1 Configuring the LDAP Api

7.11.1.1 General Considerations

With Windows 2000, Microsoft have introduced the Active Directory Concept which allows a much more flexible administration of any kind of user data. Browsing the Active Directory requires a protocol, specially developed for this purpose. This protocol is called Lightweight Directory Access Protocol, LDAP for short. It is a further development of the access protocol Directory Access Protocol (DAP), based on the X.500 Directory Service, since the DAP could not meet the demands in terms of speed and overhead any more.

Active directory

The Active Directory Service¹ (DS) is understood as a scalable directory service structured similarly to a folder directory in a file system. However, here we do not deal with a file hierarchy (e.g. nested directories as with the complete path: `c:\Company\Site\Department\Group...`) but with an object hierarchy. An object is in this context a unit described by a unique, named set of attributes. With folder directories, the Explorer would principally be the counterpart to the LDAP protocol, used for Active Directory display and editing.

During log-in to the network and the search for released resources, Active Directory clients must be able to communicate with computers on which Active Directory is executed. This means that extraneous access to the domain control and global catalogs has to be performed using LDAP (Lightweight Directory Access Protocol).

LDAP (Lightweight Directory Access Protocol)

LDAP² is a communication protocol developed for TCP/IP networks. The LDAP protocol defines in which way directory clients access directory servers, carry out directory actions and make use of shared directory data. LDAP standards are established by IETF (Internet Engineering Task Force) working parties. In Active Directory the LDAP specifications for attributes and the IETF standards for the LDAP versions 2 and 3 are implemented.

-
1. See also the five-volume reference by Microsoft:
Active Directory Developer's Reference Library, David Iseminger,
Microsoft Press 2000, ISBN 0-7356-0993-6
 2. Further literature to deepen the LDAP subject:
Implementing LDAP, Mark Wilcox, Wrox Press Ltd.-1999, ISBN 1-861002-21-1

As the name already suggests, LDAP is an efficient method to access directory services without the complexity of other directory protocols. Since the LDAP protocol defines which processes are permitted in querying and modifying directory information and how to perform safe access, you can list directory objects, execute queries or administer Active Directory with LDAP.

LDAP and interoperability

LDAP is an open Internet standard. The use of LDAP enables cooperation of Active Directory with the directory services of other suppliers. As component of Active Directory Interfaces (DSI), the Active Directory support of LDAP comprises an LDAP supplier object. The Active Directory interfaces support the LDAP application programming interfaces for C defined in the internet standard RFC 1823. You can easily adjust other applications for directory services to access Active Directory information via DSI and LDAP.

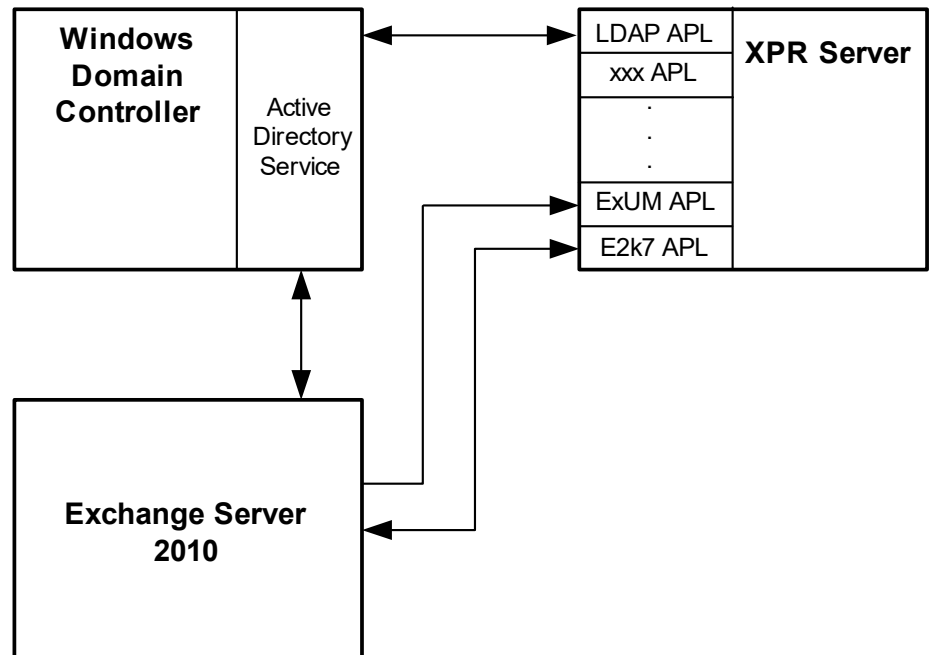
Active Directory and Exchange Server

In the course of standardization and a stronger integration of Exchange in the operating system Windows 2000, Exchange Server (from version Exchange 2000 Server) has been completely adapted to cooperation with the directory service Active Directory introduced in Windows 2000. This means that now all Exchange directory information is stored in Active Directory, too. Thus the individual Exchange directory used in previous versions to centrally store objects of an organization (e.g. addresses, mail boxes, distribution lists and public folders...) has been replaced. Among other things it was necessary to install a special directory service to administer data replication between individual Exchange servers. Connecting Exchange to the Active Directory Service of Windows has the following advantages:

- Enabling a centralized object administration.
This means that the directory objects can be administered from one place with only one management tool as of operating system version Windows 2000 Server.
- Security management simplification.
Because *Exchange Server 2003, 2007, 2010* and *2013* uses the same security functions as Windows, all security regulation modifications (user or group accounts) apply to data stored in Exchange and Windows as well.
- Efficient creation of distribution lists.
The security groups defined in Windows are automatically used as distribution lists by *Exchange Server 2003, 2007, 2010* and *2013*.
- Simplified access to directory information.
By creating an LDAP interface you can display and edit the Active Directory data via the native LDAP protocol.

7.11.1.2 Active Directory and XPR Server

In order to meet future requirements and to ensure the interplay with *Exchange Server 2003*, *Exchange Server 2007*, *Exchange Server 2010*, and *Exchange Server 2013*, the Active Directory (DS) directory service was integrated in the XPR system with the help of the LDAP APL.



For this purpose a separate connection to the Active Directory via the LDAP APL is required. The function of this is to enable a mapping between the attributes of the Active Directory and the data relevant for XPR, in other words to establish correct assignment. Since manual adaption of the database fields is relatively laborious, the effort is minimized by performing the basic configuration via the import of a standard configuration file (`xxx.lcf`).

Miscellaneous

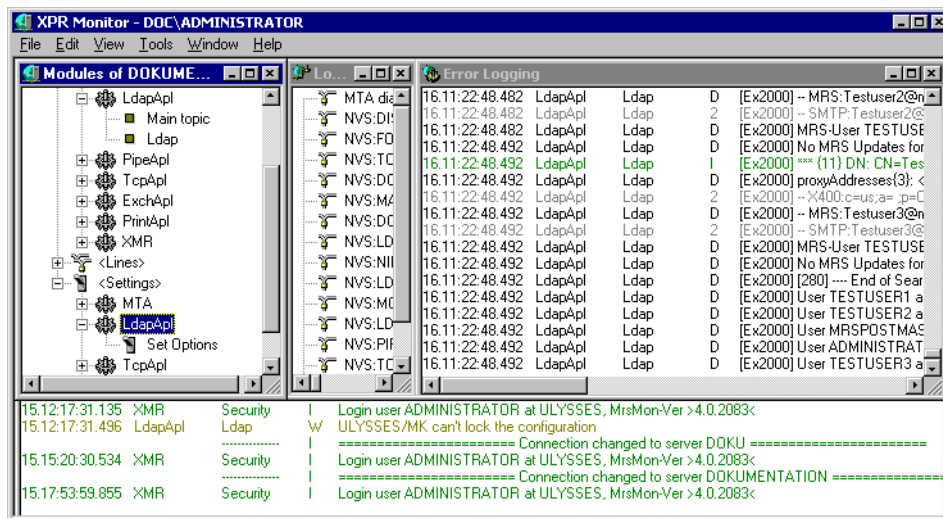
1. The LDAP APL only serves to replicate user data - the DS pattern is not extended or modified.
2. The LDAP port used is configured on 389 by default.
3. The LDAP APL is so conceived that it can additionally access other systems supporting the LDAP protocol.

7.11.1.3 Installing the LDAP APL

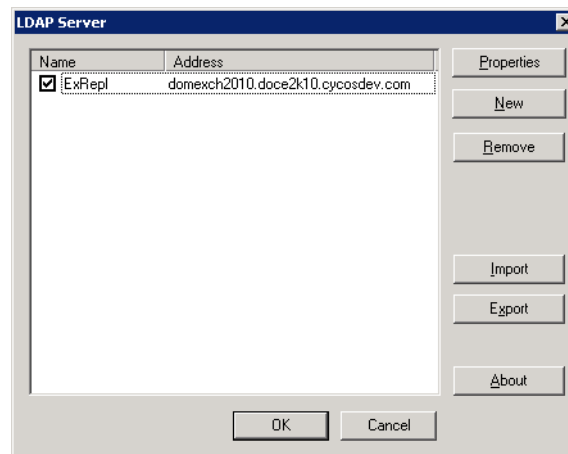
Installation via the XPR setup

Installation of the LDAP APL is embedded in the XPR server setup. If a new XPR server is to be set up for *Exchange Server 2013*, the LDAP APL must be integrated in the installation for selecting the Exch APL. The LDAP APL installation procedure in the XPR setup is described in [Section 7.10.3.3](#), “Installing the LDAP APL (for a fresh OpenScale Xpressions V7 Server Setup)”, on page 324.

7.11.1.4 Editing LDAP Settings



All LDAP settings are performed from within the XPR monitor. You reach the setting options via the **Modules of <XPR server name>** window. Expand the branch next to **<Settings>**. Then open the subtree **LdapApl**. Subsequently, double-click **Set Options** to open the LDAP APL settings dialog.



This first dialog **LDAP Servers** serves general administration purposes. The names and IP addresses of already existing LDAP configurations are listed here. From here you can define further LDAP configurations (LDAP links) and edit already existing ones. In use is the server that features a check mark before the name entry.

The buttons in this dialog have the following significance:

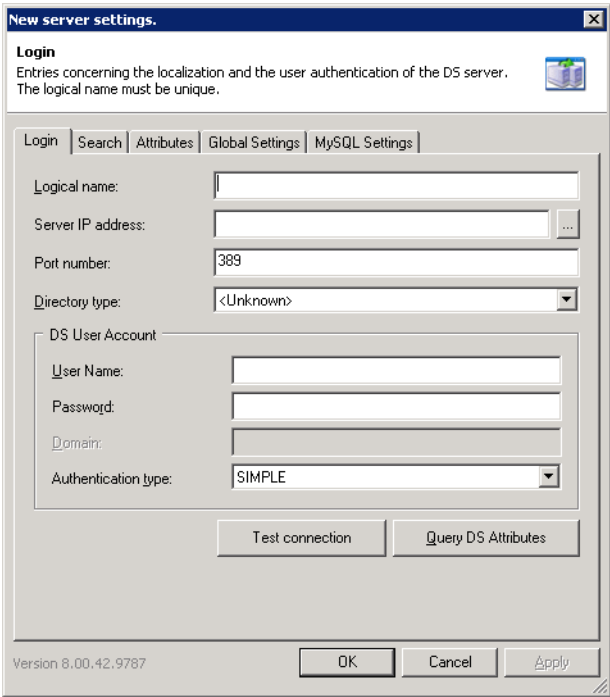
Properties

When you select an arbitrary configuration entry, the **Properties** button takes you to the configuration dialog **Edit server settings**. In there you find four setting tabs used for changing the LDAP configuration.

New

Via the **New** button you can add further LDAP configurations. When you enable it you are taken to the **New server settings** configuration dialog. To define a new LDAP configuration here, fill in the four tabs **Login**, **Search**, **Attributes** and **Global Settings**.

The significance of the individual entry lines can be gathered from the **Properties** button description further below.

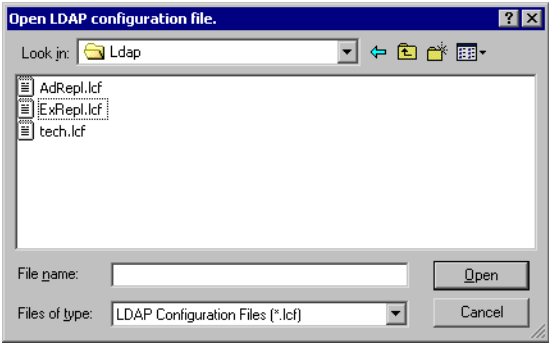


Remove

Deletes a selected LDAP configuration file.

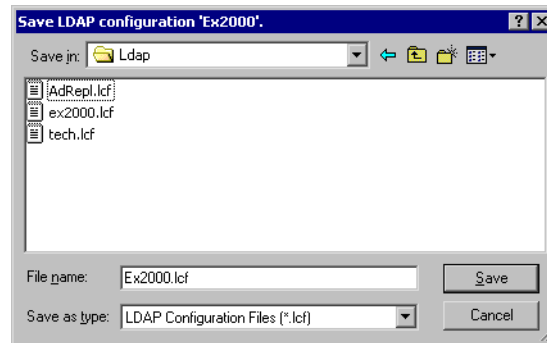
Import

Branches to the file selection window **Open LDAP configuration file**. Here you can enter an existing configuration file (format: xxx.lcf). In this way it is possible to implement different configuration files. Completing this step takes you to the **Login** tab in the **Edit server settings** window where you can perform modifications.



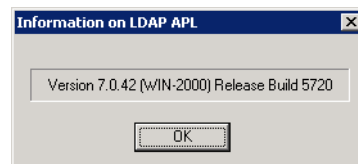
Export

If stored as `xxx.lcf` file, a configuration file can be created, which includes all current settings of the selected server.



Info

The About button opens an information dialog that displays the currently active LDAP APL version. With a click on **OK** you leave this dialog again.



OK

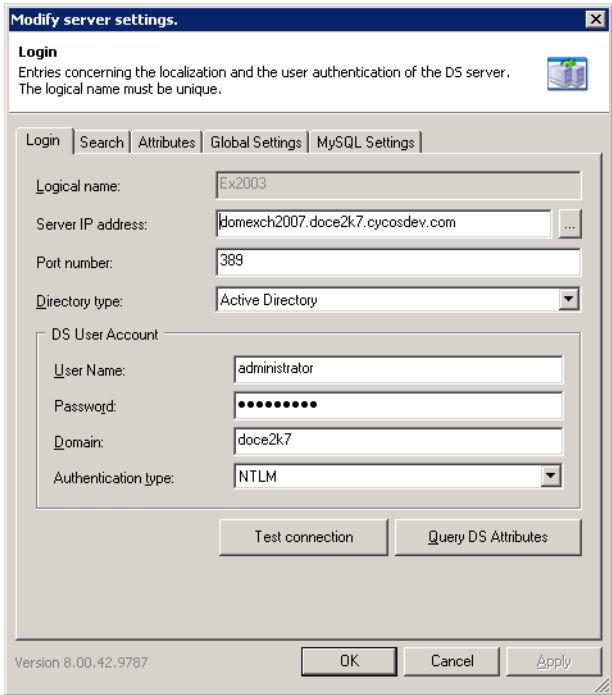
Copies the entries made in the **Edit server settings** tab and closes the LDAP APL setting dialog.

Cancel

Terminates the LDAP APL configuration without copying modifications previously made.

7.11.1.5 The “Login” Tab

Here all information on this DS server is displayed. In the upper section you find the assigned LDAP configuration name and the entry lines for the IP address, the port number and the directory type of the LDAP server. Thereunder, entry lines for user identification data are available. With the exception of the short name (name of the LDAP connection) assigned upon the reconfiguration you can now edit settings for DS server localization and the access privileges.



NOTE: The LDAP configuration name (**Logical name**) is only possible via a redefinition of the configuration settings.

The functions of the input fields on the **Login** tab are as follows:

Dialog Entry	Description
Logical name:	Here you can assign an arbitrary name to a new LDAP configuration. This name must be unique since it is used for registry entry replication. If you open an already existing DS server configuration via the Properties button, the previously assigned name is displayed. It can, however, not be changed in this form.

Table 25 Entry Fields in the LDAP Settings Tab “Login”

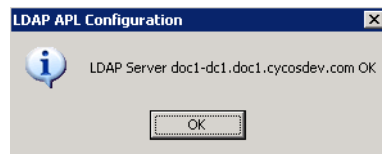
Dialog Entry	Description
Server IP address:	In this entry line you can specify the valid DS server IP address (either the qualified host name or the numeric address), or the IP address of the selected entry is displayed. If you have opened an existing configuration, the IP address of the selected configuration is displayed. To simplify things you can use the  button (to the right of the entry line) to search the entire network for the desired DS server.
Port number	Entry field for displaying the currently set port or to modify the port number. Note: Ports 3268 cannot be used for searching the Active Directory. Via port 3268 the global catalog (thus the entire forest) is searched for a specific attribute, with only reading access being possible. In addition, the global catalog only holds a subset of the AD attributes. The extensionData attribute does not belong to this subset. Consequently, the extensionData attribute cannot be read out or written via this port. The following warning is issued via the LDAP APL in this case: <i>LdapApl Ldap W [Ex2003] ldap_modify [1 attributes]: Unwilling To Perform</i>
Directory type:	This menu allows selection of either Active Directory, <unknown> or DirX. For our purposes set Active Directory here. The other options refer to LDAP connections to other systems.
In the DS User Account section	
User name	Here, the name of the user account is entered/displayed that is furnished with the corresponding privileges for the AD access. The AD access is possible if this user account belongs to the group of domain administrators or to the group of Builtin account administrators.
Password	This entry field is for definition of the password associated with the above user account.
Domain	Field for entry (or display) of the domain name associated to the above user account.
Authentication type	The definition of the authentication type must be set to NTLM (NT Lan Manager) for connecting the Active Directory Service. The alternatives SIMPLE and Negotiate are intended for other directory systems. Annotation: When you log in with the authentication type SIMPLE , the user name must be entered in the LDAP format, i.e. as "Distinguished Name" (DN). Example: uid=admin,ou=administrators,ou=TopologyManagement,o=NetscapeRoot

Table 25 Entry Fields in the LDAP Settings Tab "Login"

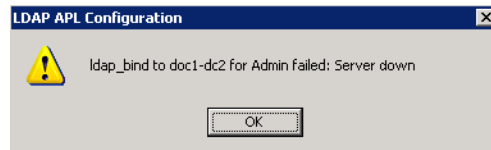
The data relevant for the DS server selection are now entered.

Testing the connection

Via the **Test connection** button you can verify the entered connection data. You are informed about the status of the connection to the DS server by a message shown in the below illustration.



In case of an error (the connection cannot be established), the same dialog appears with a special text message that, if possible, contains details on the problem occurred.



Polling DS attributes

Via this button you can manually trigger the initial transmission of the DS attributes. Otherwise, the selected DS server reads out the DS attributes by way of a periodically occurring query and lists them in the **Attributes** tab (see **Polling interval** and **Schedule** in the **Search** tab). You can watch this process on the XPR monitor as well. See also [Section 7.11.2, “Monitoring the LDAP APL Activities”](#), on page 378.

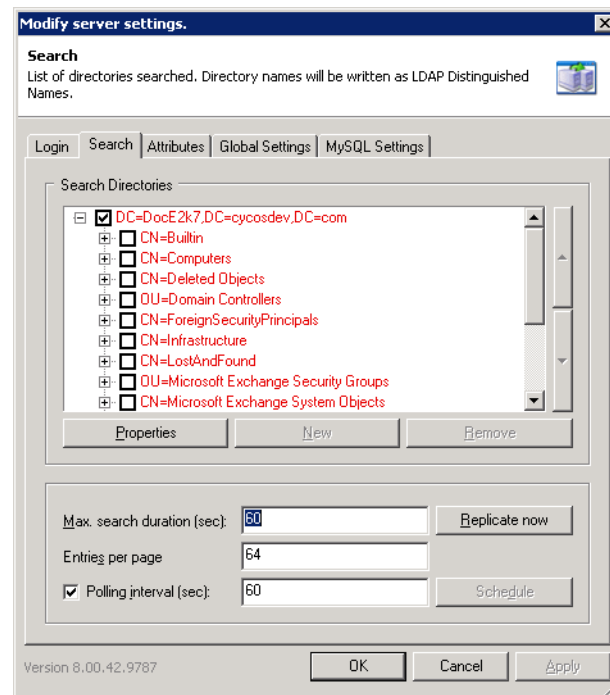
7.11.1.6 The “Search” Tab

General

The **Search** tab is used to define directories or user entries that are to be integrated in the replication process. Here you must explicitly select the containers that include users whose attributes are to be replicated.

NOTE: Make sure to only select containers that include real users. Otherwise unwanted entries (for example the Exchange system mailbox) may be integrated in the replication process. A new user “system mailbox” would then be generated on the XPR server with each replication process.

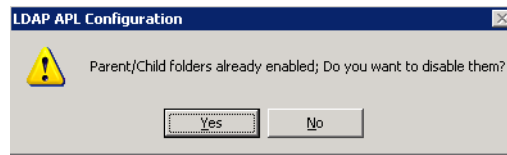
The containers or user entries in the search directory are color highlighted according to the search depth.



The **Search Directories** section displays the directories of the entire DS tree. You can expand the tree (click the [+] icons) to display the single user entries. To select a directory, place a check mark in the corresponding box next to the branching nodes of the tree.

- **Black entry:** Only the attributes of the users defined in the respective container object are replicated.
- **Blue entry:** Only the user attributes of the first level below the selected container will be replicated.
- **Red entry:** The entire subtree will be included in the replication.

An implemented logic prevents a redundant replication. An error message is issued when a new selection includes an already existing one.



If you confirm this message with **Yes**, the new setting becomes active and the old one is automatically adapted. **No** restores the state before the modification.

NOTE: Annotation on selecting users whose attributes are to be replicated: If in a larger organization all users have been defined in one container and attribute replication is only required for a subset of these users, the selection process may become relatively protracted when all users have to be selected individually. In this case filter rule definition can be applied to specify the selection. Another option is to define the users intended of replication in a special container.

The two arrow icons on the right margin of this window display serve to modify the directory sequence in the list represented. Select the container or container object to be moved with a click and move it up or down according to the new position desired. In this way you can customize the replication priority since otherwise, with several selected directories, the processing sequence is from top to bottom.

Replication settings

The buttons and entry fields in the bottom section of the dialog define the temporal replication process.

- **Polling interval**

IMPORTANT: Default after the installation is 0 seconds. Thus replication is at first deactivated so that it does not occur uncontrolled.

Each entered number value *x* starts the replication after *x* seconds (for example: with an entry of 12 the next replication starts after 12 seconds). Instead of via a polling interval, replication can also be performed via a schedule definition. Deactivate the checkbox next to the **Polling interval** entry to automatically activate the **Schedule** button. Schedule definition is described further below. If you want regular replication via a polling interval and no valid time value has been entered yet, an error message informs you accordingly.

- **Max. search duration** (Default 60 seconds)

This value determines the maximum duration of a replication. Any numeric value x ($x > 0$) entered there terminates the replication when this value has been reached after x seconds.

- **Entries per page**

Since timeout problems may occur when extremely large amounts of data have to be replicated, you can determine the number of data records to be transferred per transmission unit via the **Entries per page** field. 0 means that all data records are to be transmitted in one go; any other value restricts the number of data records. For example, 128 data records are sent per transmission unit with the entry 128.

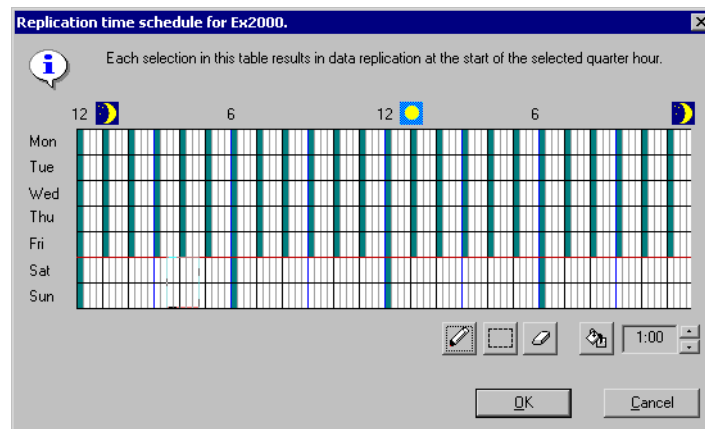
- **Replicate now**

Via the **Replicate now** button you can start this process manually.

- **Schedule**

With a click on the **Schedule** button you can create a replication week profile. Replication can be set in 15-minute steps for each weekday.

NOTE: Replication does not occur if it is to be performed via a schedule but no settings have been made there. No error message is issued on this.



After opening the schedule you can edit the replication times. The following tools are available:

Tool	Description
	Serves to arbitrarily enter replication times in the schedule.
	Selection tool for marking sections in the week profile.

Table 26

Tools to create a Replication Schedule

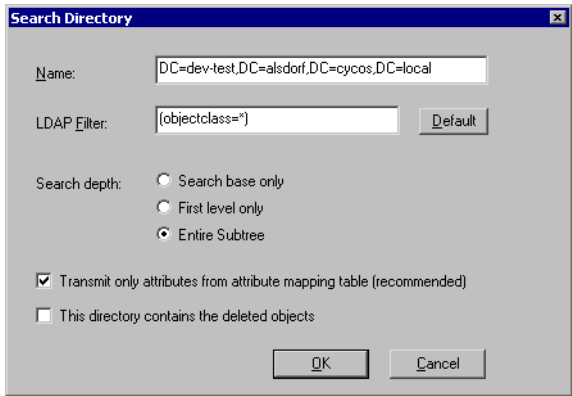
Tool	Description
	With the eraser function you can remove single replication times from the week profile. If an entire area has previously been selected with the selection tool, the replication marks within the marked area are maintained in case of replication mark deletion.
	Is used to define a replication time for a whole week if replication is to occur each day at the same time in the same interval. The intervals can be specified in the entry field next to this icon.

Table 26 Tools to create a Replication Schedule

The Properties, New, and Remove buttons

The **New** and **Remove** buttons are intended for manual configuration (directory type “unknown”). In the *Exchange Server 2013* connection context (directory type “Active Directory”) they are meaningless and therefore inactive.

After clicking on **Properties** you can view and modify the search directory settings.



The **Name** specifies the **search base** or the starting point of the search run within the directory hierarchy. Under **Name** the search base is displayed as node of the DS branch.

The **LDAP Filter** field specifies the **search filter** that determines the conditions for searching the data records (objects). This filtering also enables looking for special criteria of the user data replication. In the **LDAP Filter** field the search filter can be restricted to specific attributes. The default filter `objectclass=*` replicates all entries. Any complex logical filter¹ is conceivable.

NOTE: As of Exchange Server 2007 the distribution groups support the **sAMAaccountName**. As a result, all Exchange users with this attribute are replicated as full XPR users to the XPR server. This causes problems when assigning the MRS address type and the number of replicated users exceeds the number of available user licenses. Applying suitable filtering here, for example via `(&(objectclass=*)(!objectClass=group))`, you may restrict the users to

1. For more information see: Implementing LDAP, Mark Wilcox, Wrox Press Ltd. 1999, ISBN 1-861002-21-1

be replicated. In the above filtering example this would concern users who do not have an `ObjectClass=Group`. In the single case the filter to be defined depends on the structure in which the users are implemented in the Active Directory.

After changing the filter you can click on the **Default** button to switch to the `objectclass=*` filter again.

The **search area** indicates which part of the directory starting from the search base is to be searched. The search area can be set for the selected object via the **Search depth** option:

- **Search base only**
Only the attributes of the users defined in this container object are replicated.
- **First level only**
Only the user attributes of the first level below the selected container will be replicated.
- **Entire Subtree**
The entire subtree is included in the replication.

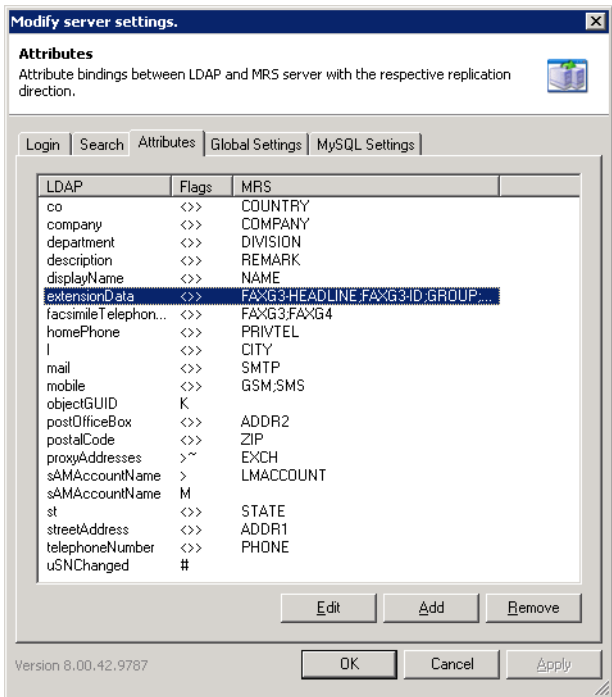
By means of the checkbox **Transmit only attributes from attribute mapping table (recommended)** you can define that only the entries listed on the **Attributes** tab are transmitted. This setting is recommended since it optimizes IP transmission (only attributes needed most are transmitted).

When the checkbox **This directory contains the deleted objects** is active, the elements of the folder entered in the **Name** field are interpreted as “deleted”. The expression “deleted” is somewhat inaccurate here since objects thus defined are not removed but only hidden.

The settings become valid with **OK**; **Cancel** terminates the previously described process without performing any modifications. Simultaneously you are taken back to the **Search** tab.

7.11.1.7 The “Attributes” Tab

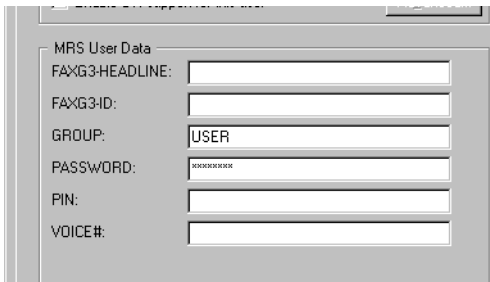
The central window of the **Attributes** tab lists the DS attributes, the corresponding XPR data fields and the set flags. They are already defaulted by the basic setting respectively by importing the configuration file for the *Exchange Server 2013* connection (*ExRepl1.lcf*).



Of the listed attributes the **extensionData** attribute is especially significant. The XPR data fields assigned to this DS attribute are exactly those you find in the Exchange users' properties dialog on the **MRS Settings** tab, where they are configured.

The configuration of the **extensionData** LDAP attribute is stored in the “MRS Setting Object” in the Active Directory. The MRS Setting Object for the LDAP configuration is available only once for the entire Exchange environment.

Via editing this attribute you can add further fields on the **MRS Settings** tab. See [Section 7.11.1.7, “Extending XPR attributes”, on page 372](#).



When you click on the **Edit** button, settings for selected attributes can be changed and via **Add** further attributes are selected, assigned and various attribute parameters set.

The following illustration shows the empty form to select a new attribute and the required mapping as well as settings of the individual parameters (usage of attributes, replications etc.).

The attribute to which the following settings relate is selected and displayed in a combo box in the **Directory Service Attribute** section. Next to this name field, the data type is specified in the field with the gray background under **LDAP Type**. Thus you are informed whether the type is a string variable (**str**), an integer variable (**int**) etc. Thereunder, another field is placed to display the **Subtype**: if there is another differentiation in subtypes as e.g. with an Octets type.

The checkboxes included in this portion have the following functions:

Checkbox	Description
Create new MRS user Sets Flag: M	Use this attribute if a new XPR user is to be defined. The value of this LDAP attribute is used as user ID on the definition of new XPR users. If the Use attributes to link DS users to XPR users option is not active, this value also serves to directly link an LDAP data record to the data of an XPR user of this name.

Table 27 Settings for the LDAP Directory Service Attribute

Checkbox	Description
Cache key Sets Flag: K	Integrates an attribute in the cache (for faster access). Once an XPR user has been found, he/she is then directly found via the cache key in each following search and his/her data are available faster.
Update Sequence Number (USN) Sets Flag: #	The USN is an update ID incremented from XPR attributes to DS attributes with every search request. When this checkbox is active, only records that have a larger USN-ID than the one generated with the last search run are replicated.
Mandatory for MRS user	Defines that this attribute is mandatory for an XPR user. If this option is set, a user is only defined if the attribute is filled in. In other words, if the attribute entry is deleted, all users that do not have this attribute entry will be deleted with the next replication.

Table 27 Settings for the LDAP Directory Service Attribute

Thereunder you find the **XPR Attributes** selection field to assign the above selected DS attribute to the corresponding XPR database field. All XPR database fields are listed here so that each DS attribute can be mapped on each XPR field (and vice versa).

The associated checkbox allows using this attribute when a new **DS user** is to be created (sets flag: **D**). This option is presently not available but will be implemented for future applications.

The checkboxes coming next determine the replication direction. You can alternatively replicate to the XPR server (**Replicate to XPR**, sets flag: **>**), to the domain server (**Replicate to DS**, sets flag: **<**) or to both simultaneously (both flags are set: **< >**). If a reciprocative replication is desired, you need to define one of the two servers as the superordinate one. This is done via activation of the **DS is master** or **XPR is master** switches.

Through activating the checkbox **Use attributes to link DS users to XPR users** (sets flag **~**) you can directly relate a DS user to an XPR user via attributes. Indirect linkages can thus be defined. For example, with DS attribute *proxyAddresses*, XPR attribute *EXCH* and activated option, all DS data of a user are assigned via the value of the DS attribute *proxyAddresses* to the XPR user who has the same contents in the *EXCH* database field.

The switches in the **Filter for Attribute Values** section can be set to manipulate attributes in various manners (for example, to quickly determine a user etc.). Depending on the complexity of the manipulation, this can either be done by a regular expression or by an e-Script. E-Scripts are programs for establishing e.g. complex filters.

The following setting options are available:

Filter setting	Description
None	The filter function is deactivated.
Regular expression:	Entry fields for regular expressions.
E-Script	Entry field for the name of the e-Script to be applied to the DS attribute.

Table 28 Filter Settings for the LDAP Attribute Values

Definition example of an attribute's replication properties with usage of the **Regular expression** filter function.

The entries in the above dialog have the following significance:

- All entries of the directory attribute *proxyAddresses* are filtered.
- When an entry matches the regular expression *XPR:%t*, it is replaced with the expression on the right and copied; all other are rejected. *%t* serves as wild card for an arbitrary, not empty chain of characters without blanks entered in the right field for *%1*. You can generally enter several sub-patterns in the regular expression field on the left-hand side; on the right-hand side you can then indicate the *n*th sub-pattern with *%n*. You find more information on regular expressions in the **E Programming Language** and **XPR Server Administration** manual, chapter "LDAP APL".

The settings performed are copied with **OK**. You are simultaneously taken back to the **Attributes** tab. Newly selected and edited attributes are added at the bottom of the list.

Extending XPR attributes

An additional example explains how to add new fields to user data (in **Active Directory Users and Computers**) on the **MRS Settings** configuration tab.

IMPORTANT: If additional XPR attributes are defined here for the DS server, data replication to the XPR server may lead to the deletion of XPR-significant data fields. If an XPR data field is replicated when empty, then a completed data field may be deleted (overwritten by the empty data field). Data fields must consequently not be left empty with defining a user.

1. In the XPR monitor under LDAP APL select the **Set Options** function.
2. Next, mark the desired server in the list of possible LDAP servers and enable the **Properties** button.
3. In the **Edit server settings** dialog then open switch to the **Attributes** tab.
4. Select the **extensionData** entry from the attribute list.
5. Click **Edit**.

The **XPR Attributes** combination field displays all entries of the **extensionData** directory attribute.

6. You can now select additional data fields via the associated checkboxes in the **XPR Attributes** selection dialog. These fields are then additionally integrated after a click on **OK** in the user settings with **Active Directory Users and Computers**.

Cancel terminates the process and modifications already performed are disregarded. A click on either button simultaneously takes you back to the **Attributes** tab.

If the attributes are defined by the configuration file, they are listed on the **Attributes** tab with the already existing assignment to the XPR system. This means that with the represented attribute the corresponding XPR data field on which this attribute has been mapped is displayed. There are various flag symbols between the attribute name and the XPR data fields which already provide information about how certain attribute or replication parameters are set. The following flags or combinations of them can be set:

Flag Symbol	Significance for the selected attribute
M	The attribute is used when a new XPR user is to be defined.
D	The attribute is used when a new DS user is to be defined (this option is presently not available).
K	Integrating the attribute in the cache (for faster access).
#	This flag indicates that the search run is only performed from the last replicated records.

Table 29 *List of possible Attribute Flags*

Flag Symbol	Significance for the selected attribute
<	Replicates this attribute to the DS server (with XPR as master). This setting can be used if e.g. a new <i>Exchange Server 2013</i> is to be coupled to an existing XPR server to replicate all XPR data to the AD.
>	Replicates this attribute to the XPR server (AD is master).
<>	Replication in both directions.
<>>	Replication in both directions with AD as master.
<<>	Replication in both directions with XPR as master.
~	This flag shows that the directory service user is linked directly with an XPR user by means of the attribute.

Table 29 *List of possible Attribute Flags*

The **Edit** button enables the modification of the attribute parameters of a selected entry at a later date. When you click it, the **LDAP/XPR Attributes** dialog opens with the entries made for the selected attribute. You can adapt entries and save them as described above.

Replication of XPR multivalued fields

The XPR server database can be so extended that for some entries so-called multivalued entries can be generated. In this way it is possible to define several phone numbers for one database entry. The field **VOICE** or **PHONE** can be intended for this purpose, if several phones or voiceboxes are needed for one user. The fields are stored in the database consecutively numbered: **PHONE** (primary field), **PHONE.01** (the first non-primary field) etc.

However, since the AD does not provide any number of attributes for phone numbers, these fields cannot be directly replicated to the AD in this format. The phone number entries in the AD are so organized that only the first phone number (primary) can be replicated via the *telephoneNumber* attribute, all other phone numbers (non-primary) are replicated via the *otherTelephone* attribute.

So that these fields can be integrated in replication to the AD server, an additional field is offered (for example **PHONE.***). This field serves exclusively for replicating non-primary fields, thus for example the database fields **PHONE.01**, **PHONE.02** etc. It is possible to replicate the multivalued fields in different ways:

- LDAP single value to XPR multivalued field.

Example: *telephoneNumber* to *PHONE*

Only the primary entry is replicated to the XPR server.

- LDAP multivalued to XPR multivalued field.

Example: *otherTelephone* to *PHONE*

All multivalued entries are replicated to the XPR server 1:1.

- LDAP multivalued to XPR multivalued fields without the primary field

Example: *otherTelephone* to *PHONE.**

All multivalued entries, except for the primary field, are replicated to the XPR server.

Attribute settings for additional LDAP servers (e.g. subdomains)

As attributes for additional LDAP servers, e.g. additional subordinate domains, are not automatically preset, these must be set as follows:

1. Select the first server in the **LDAP Servers** window and export its settings to a file by means of the Export button. The changes for the new server must now be made in this file.
2. Open this file with the editor, change the entries for the Domain Controller **DC** and for the Container **CN** and, where applicable, **OU** to be replicated and save your changes in a file.

```
dirType:ActiveDir
Script:EXRep1
AttMap:21
co:COUNTRY:0, str:toM, toD:none
company:COMPANY:0, str:toM, toD:none
department:DIVISION:0, str:toM, toD:none
description:REMARK:0, str:toM, toD:none
displayName:NAME:0, str:toM, toD:none
extensionData:FAXG3-HEADLINE;FAXG3-ID;GROUP;PASSWORD;PIN;VOICE#:2, octets:toM, toD:none
facsimileTelephoneNumber:FAXG3#;FAXG4#:0, str:toM, toD:none
homePhone:PRIVTEL#:0, str:toM, toD:none
l:CITY:0, str:toM, toD:none
mail:SMTP:0, str:toM, toD:none
mobile:GSM#;SMS#:0, str:toM, toD:none
objectGUID::1, octets:key:none
postOfficeBox:ADDR2:0, str:toM, toD:none
postalCode:ZIP:0, str:toM, toD:none
proxyAddresses:EXCH:0, str:toM, cor:rule:"MRS:%t":%l
sAMAccountName:LMACCOUNT:0, str:toM:script
sAMAccountName::0, str:newM:none
st:STATE:0, str:toM, toD:none
streetAddress:ADDR1:0, str:toM, toD:none
telephoneNumber:PHONE#:0, str:toM, toD:none
uSNCchanged::0, int64:usn:none
Folders:3
DC=doc-test, DC=aisdorf, DC=cycos, DC=local:(objectclass=):2:a:2
OU=Test_UO:(objectclass=):0:3:0
CN=Users:(objectclass=):0:3:0
```

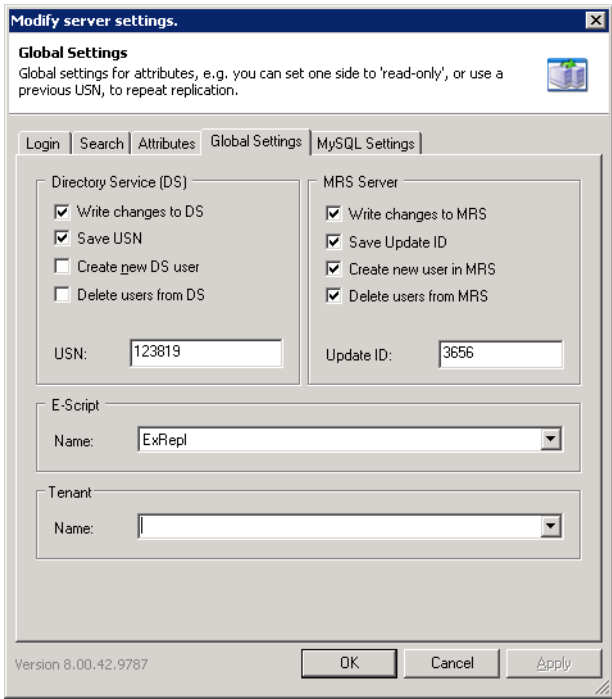
3. This file is now imported into the LDAP Servers window.
In the following the same specifications are demanded for the new server as already described in section 2.4.3.1, “The “Login” Tab”, on page 281. The **Search** and **Global Settings** tabs must now be filled out. Enter the same settings here as for the first server.

7.11.1.8 The “Global Settings” Tab

On the **Global Settings** tab you can perform additional, more detailed settings.

The **Global Settings** tab consists of four sections.

- Settings that refer to the Directory Service (DS),
- Settings that concern XPR (**MRS Server**) and
- a selection dialog to pick an e-script and



Settings in the **Directory Service** and **XPR Server** section are performed analog for the Active Directory and XPR side. You can perform the following settings:

Dialog Function	Description
Write changes to DS and Write changes to MRS	Modifications can either be saved in the Active Directory, on the XPR system or in both.
Save USN and Save Update ID	With the modifications copied upon LDAP APL shutdown, the USN (Update Sequence Number) and/or the UID (Update ID) is incremented. Here you can determine whether this is desired for one of the two or for both. The corresponding values are stored in the registry. Both IDs make sure that replication processes performed at a later date can start from a certain flag rather than all over again.

Table 30 Global Directory Service Settings for the LDAP APL

Dialog Function	Description
Create new user in MRS	Depending on the preset replication directions, creation of a user entry can be suppressed for testing purposes by deactivating the checkbox .
Delete users from MRS	Via this checkbox deletion of user entries can be suppressed for testing purposes (resetting the checkbox).
Entry fields: USN and Update ID	By means of these entry fields, a replication can be started from a certain USN (Update ID). In doing so it should always be clear what has been replicated with the entered USD. In this context it is useful to keep a log on the replication processes.

Table 30 Global Directory Service Settings for the LDAP APL

E-Script

You can select an e-script in the corresponding section used for automatic attribute editing. The defaulted e-script **ExRepl** active for the Exchange connection sets the predefined values for the standard replication.

An e-script can act as complex filter allowing e.g. telephone number normalization or special actions upon creating a new XPR user. Selection of e-scripts is performed via the pull-down list. Existing e-scripts are generally contained in the . . . \XPR\res\Ldap directory.

Tenant (with Exchange Server 2003 only)

NOTE: Here you can select one of the defaulted tenants for a multi-tenant scenario with several Exchange organizations.

7.11.1.9 “My SQL Settings” Tab

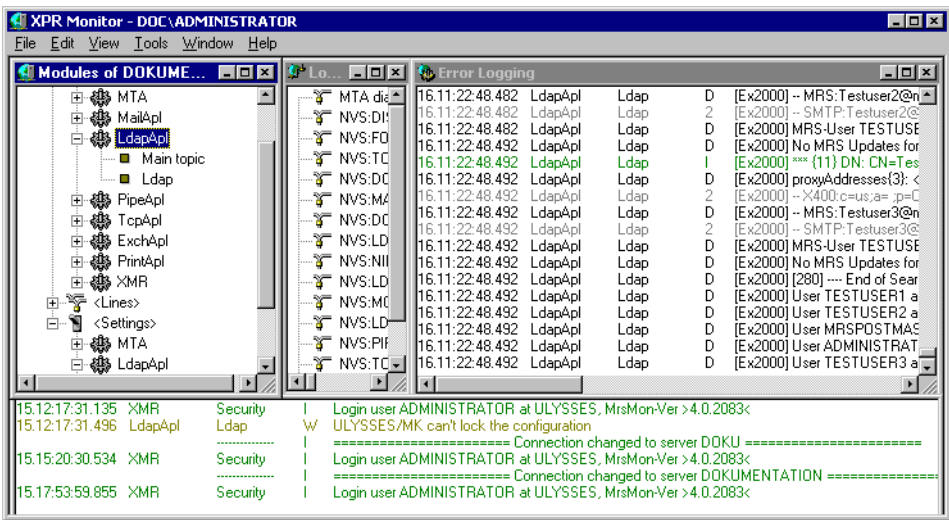
No settings need to be performed here for connecting the Active Directory to the XPR server in an Exchange scenario. The **MySQL Settings** tab serves for configuring another deployment scenario for the LDAP Apl.

7.11.2 Monitoring the LDAP APL Activities

Via the XPR monitor you can precisely observe which actions are currently carried out by the LDAP APL. The following short instruction shows you the path to this display:

1. In the XPR monitor access the **Modules of <XPR server name>** window and drag the gear wheel icon  LdapApl named "LdapApl" from the <Topics>  branch to the **Error Logging** window per Drag&Drop.
2. Adapt the parameters for the data to be displayed in the **Logging Monitor Properties** window.
3. Verify your settings with the **Copy** button.
4. Confirm your selection with **OK**.

The selected LDAP APL activities are now logged in the **LdapApl-All Topics** window (see next figure).



The **XPR Monitor** chapter of the **XPR Server Administration** manual informs you about further monitoring and logging options.

7.11.3 Uninstalling the LDAP APL

Analog to the uninstallation of other XPR components, you can uninstall these from the command line with the following command:

```
LdapApl remove.
```

The running component must previously be closed down via the *Service Control Manager*. You do this by selecting the component in the services list and a click on **Stop**.

You can also close the LDAP service via the DOS console. Enter the following command in the command line:

```
LdapApl stop
```

7.11.4 User Administration

The XPR MMC Snap-in installation extends the **Properties of <user>** register in **Active Directory Users and Computers** with the **MRS Settings** tab.

NOTE: Users who do not have an Exchange mailbox cannot see the **MRS Settings** tab.

If the XPR MMC Snap-in is installed on a 32-bit operating system you reach this settings page as follows:

1. Start the administration program **Active Directory Users and Computers** via **Start > Programs > Administrative Tools**.
2. Select the corresponding user directory there.
3. Open the associated properties dialog with a doubleclick on the desired user entry.

NOTE: You can also reach the **Properties** dialog through opening the context menu.

4. Switch to the **MRS Settings** tab.
On this tab, XPR-relevant settings are performed individually for each user.

If the XPR MMC Snap-in is installed on a 64-bit operating system, you must start the XPR MMC Snap-in in 32-bit mode (`mmc /32`).

NOTE: You find further information in the Microsoft KB article [http://msdn.microsoft.com/en-us/library/ms692753\(VS.85\).aspx](http://msdn.microsoft.com/en-us/library/ms692753(VS.85).aspx)

Proceed as follows:

1. Open the application start-up panel via **Start > Run**.
2. Enter the following command:

```
dsa.msc /32
```

The managing program **Active Directory Users and Computers** opens in 32-bit mode.

3. Select the corresponding user directory there.
4. Open the associated properties dialog with a doubleclick on the desired user entry.

NOTE: You can also reach the **Properties** dialog through opening the context menu.

5. Switch to the **MRS Settings** tab.
On this tab, XPR-relevant settings are performed individually for each user.

7.11.4.1 “MRS Settings” Tab

The screenshot shows the 'Test User 1 Properties' dialog box with the 'MRS Settings' tab selected. The dialog has a tabbed interface with the following tabs: Member Of, Dial-in, Environment, Sessions, General, Address, Account, Profile, Telephones, Organization, Remote control, Terminal Services Profile, COM+, and MRS Settings. The 'MRS Settings' tab is active, showing a checkbox for 'Unified Messaging and telephony features' which is checked. Below this is a section for 'CTI settings' with a checkbox for 'Activate CTI' which is also checked, and an 'Advanced...' button. The 'MRS User data' section contains several text boxes: 'FAXG3-HEADLINE:', 'FAXG3-ID:', 'GROUP:' (containing 'USER'), 'PASSWORD:' (containing 'XXXXXXXX'), 'PIN:', and 'VOICE:' (containing '101'). At the bottom, it says 'Data last modified: 05.12.2007 17:08:41' and has 'OK', 'Cancel', 'Apply', and 'Help' buttons.

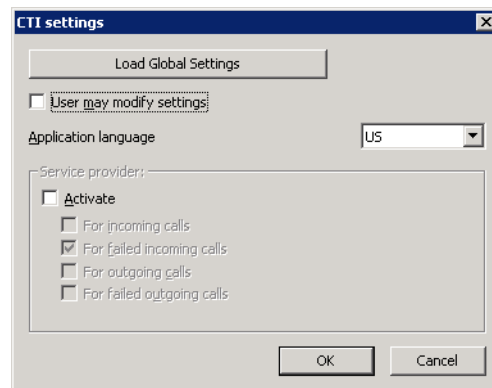
With the **Unified Messaging and telephony features** option it is possible to exclude this user from the features provided on the XPR system. Remove the checkmark to delete the user from the XPR database.

CTI settings

Via the **Activate CTI** checkbox, telephony functions (for the CTI client) can be released for the respective user provided they are implemented and configured. This generates and activates the **CTIJOURNAL** database field for this user on the XPR server.

Advanced CTI settings

Via the **Advanced...** button you reach the **CTI settings** dialog in which you can set a user's CTI functions different from the global settings. The global settings are defaulted via the connector configuration. See [Section 7.11.5.3, “CTI Settings Tab”, on page 389](#).



Via the **Load Global Settings** button you copy the global settings (those defaulted with the connector settings) for this user.

User may modify settings

Setting this option allows the user to change his/her settings for the CTI client.

Application language

Here you can select the language to be used in the CTI client dialogs for this user.

Service provider

The CTI client does not log calls if the program has not been started. Enabling the **Activate** checkbox you can set for all calls that the associated XPR-CTI journal entries are sorted into the corresponding CTI client directories via the service provider.

The behavior can be individually configured for the following call states:

- For incoming calls
- For failed incoming calls
- For outgoing calls
- For failed outgoing calls

XPR user data

These are the database fields that were defined in the LDAP APL via the default setting or after extending the **extensionData** field. You find further information about database fields and how to expand them in the description of the LDAP APL configuration in [Section 7.11.1.7, “The “Attributes” Tab”, on page 368](#).

NOTE: If the **PIN** field remains empty, the default PIN will be used. This PIN is specified via the general voicemail settings in the respectively installed telematics APL. If a PIN is entered in the Exchange user definition that deviates from the default PIN, the relevant user will not be automatically forced anymore to change the PIN assigned here when he/she logs on to his/her voice box for the first time.

Which database fields are available by default and the purposes they serve is described in detail in the Server Administration manual, chapter **User Data Administration**, section **Database Fields Significance**.

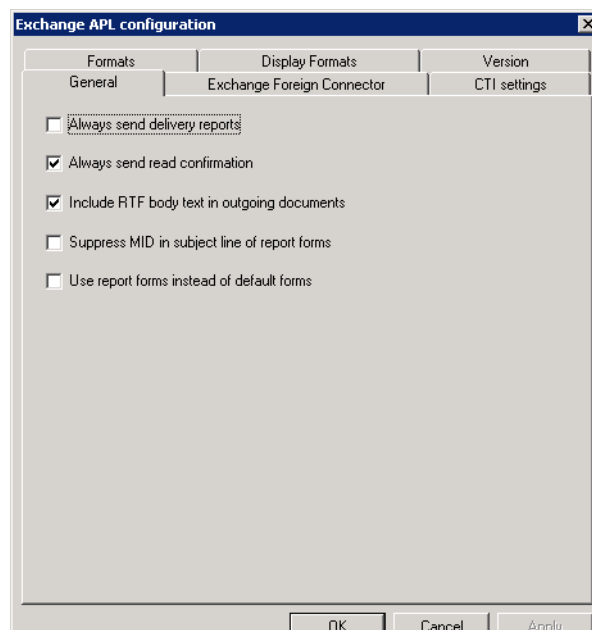
7.11.5 Administration of the XPR Foreign Connector

All connector properties that need to be configured for the XPR server are configured with the new XPR Foreign Connector via the settings dialog of the **ExchAPL** in the monitor. The following connector properties can be set:

- The connections to the transport directories found on the server that has the Mailbox Server Role.
- The global CTI settings.
- The message formats

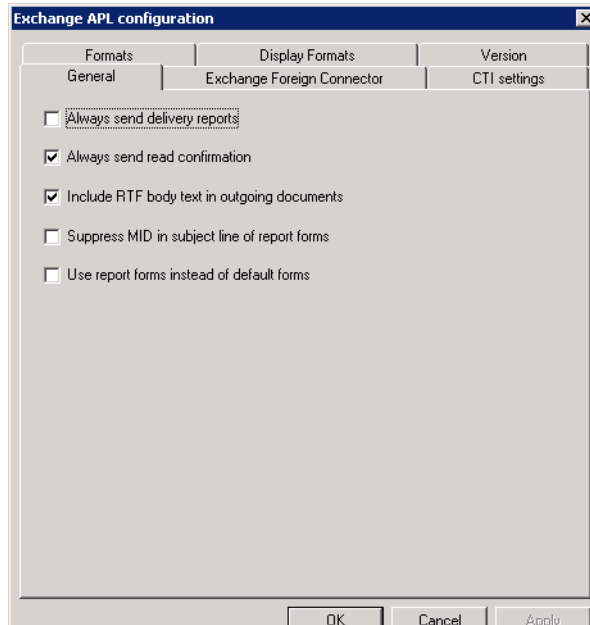
How to edit the settings of the XPR Foreign Connector:

1. Start the XPR monitor.
2. In the **Modules of <XPR server name>** window expand the branch **<XPR server name>**, then the branch **<Settings>** and finally the branch **ExchApl**.
3. Open the **ExchApl** settings dialog with a doubleclick on **Set Options**.
The configuration dialog of the XPR Foreign Connector opens.



7.11.5.1 General Tab

On the **General** tab you perform settings for creating and sending delivery reports.



The **Always send delivery reports** option generates a delivery report for messages that originate from Exchange, even when not explicitly asked for. The **Always send read confirmation** option returns a read report to the MRS originator as soon as messages are read on the Exchange server. The originator on XPR side receives a read report as soon as the Exchange user opens the document.

If you activate the **Include RTF body text in outgoing documents** option, a document in Rich Text Format (RTF) is sent as attachment in addition to the normal text representation. RTF is the official data exchange format used by Microsoft for text files. Text files exchanged in this format retain their formatting e.g. font weight, etc. when being transferred between users.

When the **Suppress MID info in subject line of report forms** option is activated, the message IDs in square brackets are omitted from the subject line. The ID display is of no significance to the normal user, but it helps tracking a routing process. Furthermore, IDs are used to assign a report to a message.

NOTE: In case of default reports it is not possible to suppress the message ID display.

Via **Use report forms instead of default forms** XPR confirmation forms are used instead of the normal Exchange default forms. For a more detailed description of the function and installation of XPR reports refer to the *Unify OpenScape Xpressions V7 Server Administration* manual from the **Automatic Report Transmission per Mail** section.

7.11.5.2 Exchange Foreign Connector Tab

The screenshot shows the 'Exchange APL configuration' dialog box with the 'Exchange Foreign Connector' tab selected. The 'Drop directory' field contains '\\<Hub Transport Server>\<Drop Directory>'. The 'Replay directory' field contains '\\<Hub Transport Server>\Replay'. There is a checkbox for 'Multiple Hub Transport Servers' which is currently unchecked. Below it are fields for 'Replay directory (Server 2)', 'Replay directory (Server 3)', 'Replay directory (Server 4)', 'Replay directory (Server 5)', and 'Replay directory (Server 6)', all of which are empty. At the bottom, there is a note: 'Before saving these values the Apl checks for their validity and logs errors otherwise. Changes take effect after Apl restart.' and buttons for 'OK', 'Cancel', and 'Apply'.

On the **Exchange Foreign Connector** tab, in the **Drop directory** and **Replay directory** entry lines, you specify the path to the shares (drop and replay directory) used for the message transport.

NOTE: If this path is not defined yet, the XPR server name is displayed here as default.

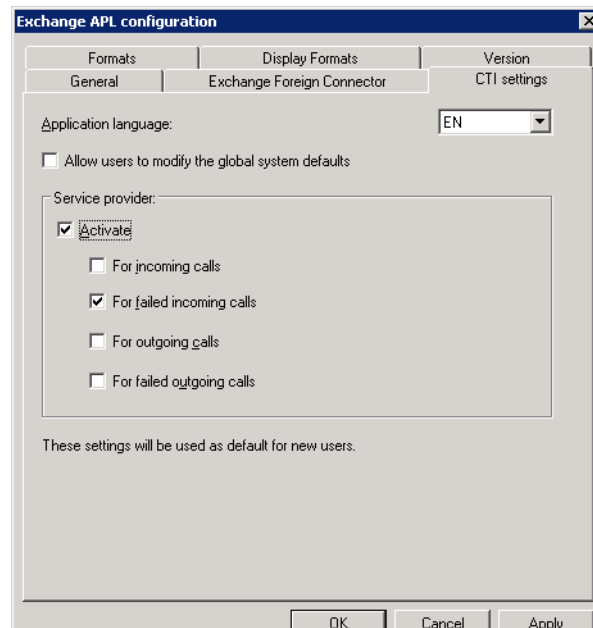
In the **Drop directory** and **Replay directory** specify the path to the shared transport directories according to the following pattern:

- For the **Drop directory**
`\\<Ip address or name of the Exchange server on which the Hub Transport Server operates>\<XPR server name>-<name of the Exchange Server 2013 Mailbox Server Role>`
- For the **Replay directory**
`\\<Ip address or name of the Exchange server on which the Hub Transport Server operates>\Replay`

After you have specified the path click on **Apply** and **OK** to save the modifications.

NOTE: The configuration respectively a modification of the configuration settings does not take effect until the **ExchApl** is rebooted.

7.11.5.3 CTI Settings Tab



On the **CTI settings** tab you find the **global** CTI settings valid for all users. These global defaults may later be customized in the course of the user definition.

Application language

Sets the language to be used in the CTI client dialogs.

Allow users to modify the global system defaults

This option enables all users to change the settings globally defaulted here.

NOTE: The permission to modify global defaults can be individually and belatedly granted as part of the CTI settings on user level. See [Section 7.11.4.1, “CTI settings”, on page 382](#).

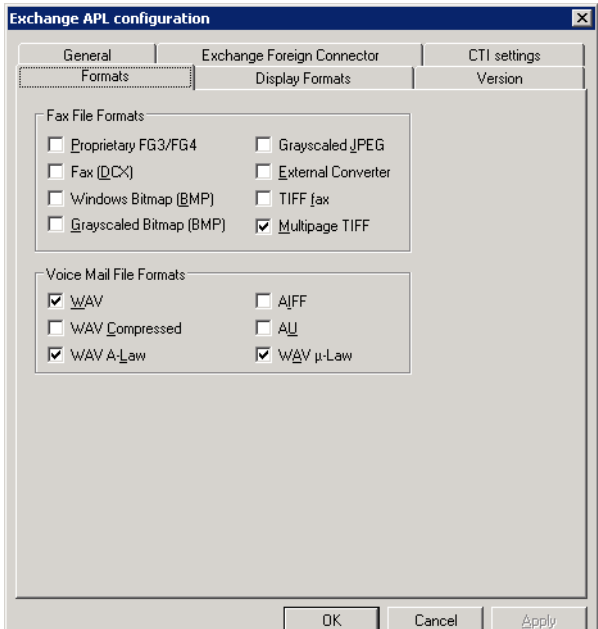
Service provider

The CTI client does not log calls if the program has not been started. Enabling the **Activate** checkbox you can set for all calls that the associated XPR-CTI journal entries are sorted into the corresponding directory via the service provider after the CTI client start.

The behavior can be individually configured for the following call states:

- For incoming calls
- For failed incoming calls
- For outgoing calls
- For failed outgoing calls

7.11.5.4 Formats Tab



On the **Formats** tab you can set the file formats accepted by the XPR Foreign Connector.

The Exchange client should be able to display these formats of course. Documents received by the XPR server that are not in one of the formats selected in this dialog would be converted into one of these formats prior to being sent to the Exchange gateway.

NOTE: A maximum of one conversion is performed, even if several possible target formats are specified. Here, an internal evaluation comes to bear that performs the “cheapest” conversion from the converter’s point of view.

When using the XPR Outlook extensions, the WAV format must be selected for the voicemail feature.

The following **Fax Formats** are available:

File formats for fax messages	Description
Proprietary FG3/FG4	Proprietary fax format (XPR Viewer).
Fax (DCX)	Multi-page PCX graphic format. Used by Microsoft fax.
Windows Bitmap (BMP)	Individual fax pages are converted in a Windows Bitmap.
Grayscale Bitmap (BMP)	Individual fax pages are converted in a Windows Bitmap, where a trilinear grayscale interpolation is performed.

Table 31 File formats for fax messages

File formats for fax messages	Description
Grayscale JPEG	Fax data are converted in a nine-grayscale JPEG format. This format is suitable for viewing with HTML mail clients.
External Converter	When you select this format, a configurable program is called, which executes a conversion from TIFF in an arbitrary format instead (see info box under this table). When you activate this external conversion, further fax formats must not have been selected beforehand.
TIFF Fax	Single-paged, compressed TIFF fax format.
TIFF multipage	Fax data according to TIFF stand (multi-page).

Table 31 File formats for fax messages

External Converter Support

Selecting this option activates an external converter. You find the preferred Fax2PDF converter in the `AddOn` directory on the product data carrier. For this feature you need to perform the following registry entries under the key:

```
[HKLM\SOFTWARE\PPCOM\mrs\Mrs-Globals\Converter\]
```

TiffToExternalConverter REG_SZ *<Program name with parameters>*

TiffToExternalExtension REG_SZ *<Extension>*

Example of *<Program name with parameters>*:

```
D:\XPR\res\convert\Fax2PDF\Fax2Pdf %1 %2
```

Example of *<extension>*:

```
pdf
```

You find further information about the functions of the external converter in the *Server Administration* manual in Appendix A under the caption: *Document Formats*.

The following **voicemail file formats** are available for selection:

Voicemail File Formats	Description
WAV	Windows Audio Format
WAV Compressed	Compressed Windows Audio Format. This format enables direct compression of voicemails that are routed via the Exchange gateway. Further settings, such as the Audio-Codec used for compression, are performed via the maintenance options in the MTA configuration. The appropriate codec to play-back compressed files is also required on the client computer. Note: Besides the subsequent compression for memory-saving storage on the XPR server, the Codecs setting is also responsible for direct compression. Direct compression is available for Integrated as well as for Unified Messaging and applies with the arrival of a message. It is used for all voicemails transmitted by the XPR MTA, i.e. all voicemails recorded by Forward and Guest Access. Direct compression is not used with messages directly created in Microsoft Exchange by True Unified Messaging. These are all messages recorded in Direct Access.
WAV A-Law	European ISDN-voicemail format.
AIFF	Audio format used predominantly on Apple computers.
AU	Unix audio format.
WAV μ-Law	US ISDN-voicemail format.

Table 32

Voicemail File Formats

7.11.5.5 Display Formats Tab

Via definitions in the **Display Formats** tab you can replace formats for message information defaulted by the XPR system with customer-specific defaults in the Outlook journal **Subject** and **From** column. This setting applies system-wide for all Exchange users receiving XPR voice and fax messages.

From	Subject

To replace the XPR default formats, you need to fill the opposite fields with new format texts, with the generic defaults in the **From** and **Subject** being replaceable with specific defaults.

NOTE: If no configuration is performed here, the standard entries for the **From** and **Subject** columns generated by the XPR server are passed on to Exchange 1:1.

You can set:

- In which of the two Outlook journal columns (**From** and **Subject**) the additional information is to appear.
- For which message types (fax, voicemails or both) the information is to be displayed.
- Which message parameters are to be shown and whether the parameters are to be embedded in an explanatory text.

The top three entry lines are intended for entries in the **From** column in the Outlook journal. The three bottom columns are allocated for the **Subject** column.

If you want to display information for both message types (fax and voicemails), enter the corresponding parameters in the **From:** and **Subject:** entry lines, possibly supplemented with text.

You can display the information separately in the Outlook journal according to fax and voicemails via the **From (Fax)** and **From (Voice)** or **Subject (Fax)** and **Subject (Voice)** entry lines.

NOTE: Please note that entries in these fields will overwrite possible entries in the **From:** and **Subject:** fields, which then become effectless.

Possible parameters include:

Parameter	Description
{originator}	When a message comes in, this parameter is replaced with the XPR originator. Example: FAXG3/01234567
{callername}	When a message comes in, this parameter is replaced with the display name of the originator, provided it has been found in the XPR database. Example: Joe User.
{callernumber}	When a message comes in, this parameter is replaced with the formatted calling number of the caller. Example: 447711
{size}	When a message comes in, this parameter is replaced with the number of fax pages or the voicemail message length. Example of fax messages: 2 (number of pages). Example of voicemails: 23 (message length in seconds).
{orgnumber}	When a message comes in, this parameter is replaced with the original calling number of the caller. Example: 49123987654
{service}	When a message comes in, this parameter is replaced with the service used for transmitting the document. Example: FAXG3

Table 33 Parameters for additional XPR Information Display in the Outlook Journal

Examples:

The entry

{service} mail from "{caller name}" <{caller number}> {size} page(s)

either in the **From:** or **From (Fax):** entry line would generate the following text in the **From** journal column with an incoming fax message:

FAXg3 mail from "Joe User" <0240412345678> 2 page(s)

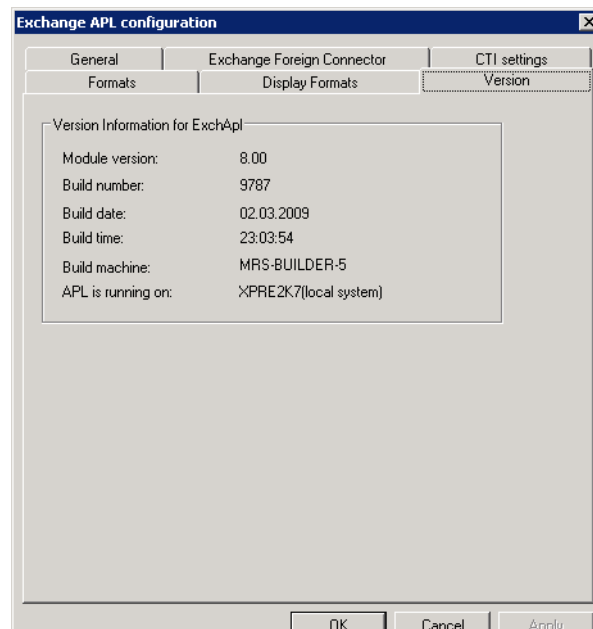
The entry

Voice message from: {caller name} ({caller number}) {size} seconds

either in the **Subject:** or **Subject (Voice):** entry line would generate the following text in the **Subject** journal column in case of an incoming voicemail:

Voice message from: Joe User (0240412345678) 23 seconds

7.11.5.6 Version Tab



The version number of the Exchange APL installed is shown on the **Version** tab. This number should always be entered when reporting errors.

7.12 Multi-Hub Transport Server Support

You can use several hub transport servers to configure a load distribution and to grant high availability. You can connect a maximum of five additional hub transport servers to the system. These servers must have been configured in the network and contain a shared replay directory called **Replay** in the path `%ProgramFiles%\Microsoft\Exchange Server\TransportRoles` in each case.

IMPORTANT: All hub transport servers additionally connected for this purpose also require access to the drop directory. These additional hub transport servers must therefore be granted the privileges for accessing the drop directory share.

NOTE: You can rename both directories and store them anywhere in the system. If this is desired, adjust the new directory names and the directory paths in the system upon the creation, activation or configuration.

If you use the multi-hub transport server version, the Exchange server and the XPR server require a commonly used and shared resource for the drop directory. Since only one XPR Foreign Connector can be installed on the XPR server, the drop directory must be on the server that all Hub Transport and mail servers as well as the XPR server can access.

Depending on the Exchange environment, the drop directory needs to be configured on the following servers:

- If only one mail server is available for several multi-hub transport servers, the drop directory is created on a commonly used and shared resource of the mail server.
- If the mail server is a clustered server with an SAN drive, the drop directory is created on a commonly used and shared resource of the cluster.
- If the mail server is a clustered server without SAN drive, the drop directory is created on a commonly used and shared resource of the XPR server.

You find more detailed information about adjusting the path and sharing the **drop** and **replay directory** in [Section 7.10.7.1, “Creating the Transport Directories”](#), on [page 346](#).

7.12.1 Configuring the Multi-Hub Server Support

How to configure the multi-hub transport support:

1. Install the Exchange connection pretending that only one Exchange Hub Transport server is available. See [Section 7.10.5, "Installing the OpenScape Xpressions V7 Foreign Connector", on page 334](#).

Besides the mailbox server, select an arbitrary, already existing hub transport server in the Exchange servers' setup dialog. The name of this server is automatically entered as value in the registry key HUBTRANSPORTSERVER.

NOTE: You cannot configure a multi-hub transport support during the setup. This is only possible after the Exchange connection has already been installed. Only then the required **ExchApl** registry branch and the configuration dialog for the **ExchApl** can be accessed on the XPR server.

2. Register all additionally deployed hub transport servers that send messages from the XPR server to the *Exchange Server 2013* via the Exchange Foreign Connector. The server names of all hub transport servers used are entered in the Exchange system in the **SourceTransportServers** parameter.

Proceed as follows:

- Start the *Exchange Server 2013 management shell*.
- Enter the following command in the console:

```
Set-ForeignConnector -Identity
<ForeignConnectorIdParameter>
-SourceTransportServers "<DEFAULT hub transport server
name>",
"<name hub transport server 1>", "<name hub transport server 2>",
... "<name hub transport server 5>"
```

You find further information about the console command `Set-ForeignConnector` in the *Microsoft TechNet*:

<http://technet.microsoft.com/en-us/library/bb123789.aspx>

NOTE: The first line of this command is separated from the second line by a blank

```
(...IdParameter> -SourceTransp...).
```

3. Define where you wish to install the drop directory.

- Follow the instructions given in [Section 7.10.7.1, “Creating the Transport Directories”](#), on page 346 to configure this commonly used and shared resource.

- Set the “RootDropDirectoryPath” path of the hub transport server to zero:

```
Set-TransportServer -identity <hub transport server>
-RootDropDirectoryPath ""
```

NOTE: The first line of this command is separated from the second line by a blank

```
(...port server> -RootDropDi...).
```

- Repeat this process for the other available hub transport servers.

- Set the complete UNC path of the commonly used and shared drop directory for the Foreign Connector:

```
Set-ForeignConnector -Identity "MrsConnector (<XPR server
name>
:<name of the Exchange Server 2013 Mailbox Server role>)"
-DropDirectory "\\<UNC path to the commonly used and
shared drop directory>\<XPR server name>--<name of the
Exchange Server 2013 Mailbox Server role>" or <name of the
commonly used and shared drop directory>
```

NOTE: The second line of this command is separated from the third line by a blank

```
(...Server role>)" -DropDirectory "...).
```

4. Test the previously performed configuration steps. Use Outlook to check whether messages to be sent via the XPR server are delivered to the new drop directory.
5. Start the XPR server.
6. Expand the registry in the HKLM\Software\Wow6432Node\PP-COM\MRS\ExchApl branch and create manually the corresponding key (HUBTRANSPORTSERVER<1...5>) for each additionally used hub transport server (maximum 5). Enter the server name associated to the respective hub transport server as value.
7. Enter the UNC path names of the replay directories additionally used in the **ExchApl** settings dialog.
8. Open the **ExchApl** settings dialog in the XPR monitor via **ExchApl -> Set Options**.

9. Switch to the **Exchange Foreign Connector** tab.
10. Enable the **Multi Hub Transport Server** option. This activates the entry fields for specifying the UNC names of the replay directories additionally used.
11. In the entry fields, specify the UNC path names of the drop directory used.
12. Enter the UNC path names of the replay directories additionally used in the corresponding fields.

The screenshot shows the 'Exchange API configuration' dialog box with the 'Exchange Foreign Connector' tab selected. The 'General' sub-tab is active. It contains the following fields and options:

- Drop directory:** A text box containing '\\<Hub Transport Server>\<Drop Directory>'.
- Replay directory:** A text box containing '\\<Hub Transport Server>\<Replay>'.
- ☒ **Multiple Hub Transport Servers**
- Replay directory (Server 2):** A text box containing '\\<Hub Transport Server 2>\<Replay>'.
- Replay directory (Server 3):** A text box containing '\\<Hub Transport Server 3>\<Replay>'.
- Replay directory (Server 4):** A text box containing '\\<Hub Transport Server 4>\<Replay>'.
- Replay directory (Server 5):** A text box containing '\\<Hub Transport Server 5>\<Replay>'.
- Replay directory (Server 6):** A text box containing '\\<Hub Transport Server 6>\<Replay>'.

At the bottom, there is a note: 'Before saving these values the Apl checks for their validity and logs errors otherwise. Changes take effect after Apl restart.' and three buttons: 'OK', 'Cancel', and 'Apply'.

13. Click on **Apply** to save the data.
14. Click on **OK** to close the settings dialog.
15. Reboot the **ExchApl**.

NOTE: By monitoring the drop directory, you can now check whether the XPR server retrieves the messages delivered here, thus whether they are removed from the drop directory.

7.13 Using additional Address Spaces for the Exchange Connectors

7.13.1 Overview

In Exchange organizations where you find two or more XPR kernels that provide a connection to this Exchange environment, you need to assign message transmission to a fixed XPR connector that delivers messages to a specific Exchange server. This avoids addressing the wrong Exchange server, which leads to an increased server load and thus to additional message transport efforts.

Because the XPR Foreign Connector designed for *Exchange Server 2013* is no longer capable of configuring message transport restrictions with the help of user lists, the path must lead here via different address space types.

If several Xpressions servers are to connect a single Exchange organization via connectors, a unique MRS proxy ID, thus an individual address space type, is required for each connector.

The default address space type for each Exchange connector is **MRS**. However, you can assign a different address space type to each Exchange connector per configuration. This restricts the message transmission to the connector for which it is configured.

Example:

Address space definition via EXADDRESSTYPE	Assigned users
MRS1	User 11, user 12, ..., user 1n
MRS2	User 21, user 22, ..., user 2n
...	...
MRSn	User n1, user n2, ..., user nn

Defining the address space type for the single Exchange connectors with assignment to the desired Exchange servers then determines the connector to handle the message transport.

7.13.1.1 Configuration Overview

Required configuration steps:

1. Configuring the Address Space on the Exchange Server
2. Creating the required "Active Directory object" using the `CreateProxyAddr.bat` batch file.
3. Copying the DLLs into the corresponding Exchange directories for creating the proxy addresses.
4. Configuring the e-mail address policies.
5. Adding the required **EXADDRESSTYPE** registry key. You need to configure this registry key for the XPR Foreign Connector (Exch APL) as well as for the Unified Messaging Connector (ExUM APL). The additional address spaces are assigned to the respective connectors via this key.

7.13.2 Configuring additional Address Spaces

7.13.2.1 Configuring the Address Space on the Exchange Server

On the Exchange side you need to set the "AddressSpaces" of the XPR Foreign Connectors in such a way that they correspond to those on the "ExAddressType" Xpressions side.

You need to configure the address space type in Exchange manually via the *Exchange Management Shell* (EMS). In this process you need change the default address space type (**MRS:*;1**) on all *Exchange servers 2013* for the second and all further connectors.

The following address space types are assigned to the additional connectors on the Exchange servers:

XPR Server	MRS Address Space Type	Exchange Address Space Value
For the first server	MRS1	MRS1:*;1
For the second server	MRS2	MRS2:*;1
...	...	...
For the n-th server	MRSn	MRSn:*;1

Use the *Exchange Management Shell* command prompt to execute the following command on the Exchange servers for configuring the assignment:

```
Set-Foreignconnector -Identity "MrsConnector (XPRESSIONS:EXCHANGE)" -AddressSpaces "MRSx:*;1"
```

MRS_x with _x= 1, 2, 3,... continually for each additional XPR connector for labeling the connectors uniquely

NOTE: You find additional information about this topic under:
<http://technet.microsoft.com/en-us/library/bb123789.aspx>

7.13.2.2 Creating the “Active Directory Object”

To define a new address space type, a batch file that creates this address space type must be started once for each additional connector.

How to create a new address space type for another connector in the Active Directory:

1. Log on to the Xpressions server with the account under which the Exch APL runs.

NOTE: For this action, the service account must be a domain account that has administrator privileges on the Exchange server.

2. Start the batch file `CreateProxyAddr.bat`
After installing the XPR connectors you find this batch file in the setup directory of the Xpressions server under:

... \xpr\bin

Example:

```
CreateProxyAddr "DC=<MYDOMAIN,DC=COM>" Temp.txt MRS1
```

Replace `<MYDOMAIN,DC=COM>` with the given domain information of the relevant customer environment.

The `MRS1` parameter must match the address space type created in the previous step.

NOTE: You can enter any file name under `Temp.txt`. Merely the `.txt` file extension must be kept. This is a temporary file created by the batch file as auxiliary file. You therefore need not create this file manually.

7.13.2.3 Copying the DLLs into the corresponding Exchange Directories

Creating the proxy addresses must now be harmonized with the new address space type.

This requires copying the DLL that generates the proxy addresses into a new directory. To do this, copy the content of the directory

```
...\Program Files\Microsoft\ExchangeServer\Mailbox\address\MRS
```

into another directory to be newly created:

```
...\Program Files\Microsoft\Exchange Server\Mailbox\address\MRSx
```

NOTE: MRSx with x= 1, 2, 3,... continually for each additional XPR connector for labeling the connectors uniquely. For example, MRS1 for the first XPR connector, MRS2 for the second etc.

Example:

```
...\Program Files\Microsoft\Exchange Server\Mailbox\address\MRS1
```

```
...\Program Files\Microsoft\Exchange Server\Mailbox\address\MRS2
```

```
...
```

```
...\Program Files\Microsoft\Exchange Server\Mailbox\address\MRSn
```

7.13.2.4 Configuring the e-mail Address Policies

The connector e-mail address policy concerned must be adjusted for each new address space type.

Proceed as follows:

1. Start the *Exchange Management Console (EMC)*.
2. Open the configuration dialog for the e-mail address policies

NOTE: You reach this dialog via: **Microsoft Exchange > Organization Configuration > Hub Transport > E-mail Address Policies.**

3. Enter a new address space type according to the sample of the available default address space type **MRS**.

Example:

E-mail address: **@MRS**

E-mail (address)type: **MRS1**

NOTE: If desired, you can remove the default e-mail address policy after adding a new custom address space type (for example **MRS1**). This will not affect this feature's function.

7.13.2.5 Adding the required EXADDRESSTYPE registry key.

The address space types that associate the XPR connectors must be activated on every XPR server. A registry key added to the corresponding registry path is used for this purpose.

For the XPR Foreign Connector (Exch APL):

HKLM\SOFTWARE\Wow6432Node\PP-COM\MRS\ExchAp1

For the XPR True Unified Connector (ExUM APL):

HKLM\SOFTWARE\Wow6432Node\PP-COM\MRS\ExUMAp1

For the Exch APL

EXADDRESSTYPE [REG_SZ]

Default:	-
Possible values:	<address space <i>name</i> >
Example:	MRSn, with n = 1, 2, 3, ...

If several XPR servers and consequently several Exchange connectors are connected to an Exchange environment, this registry key is required for differentiating the Exchange foreign connectors. Assigning special address space names then optimizes message transmission. The foreign connectors are labeled by consecutive numbering.

For the ExUm APL

EXADDRESSTYPE [REG_SZ]

Default:	-
Possible values:	<address space <i>name</i> >
Example:	MRSn, with n= 1, 2, 3, ...

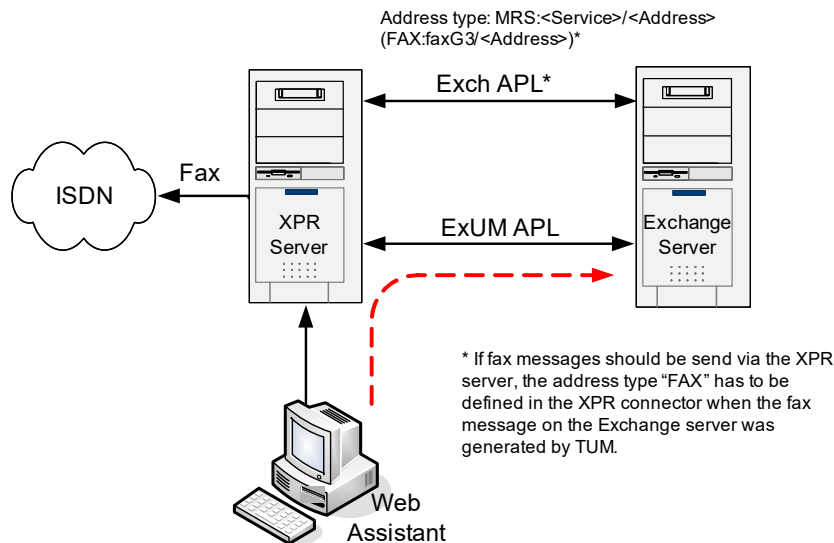
If several XPR servers and consequently several Exchange TUM connectors are connected to an Exchange environment, this registry key is required for differentiating the Exchange TUM connectors. Assigning special address space names then optimizes message transmission. The TUM connectors are labeled by consecutive numbering.

NOTE: Registry entry modifications require a reboot of the concerned Exchange Apl to take effect.

7.14 Fax Message Addressing

When addressing fax messages, the address space in the Exchange foreign connector may have to be extended by the “FAX” address type.

This is always required if fax messages were directly generated on the Exchange server and are to be transmitted via the XPR server. Fax messages are directly stored on the Exchange server e.g. if they are generated by a client that transmits the message by TUM transaction via the ExUM APL to the Exchange server (for example *Web Assistant*).



7.14.1 Definition of the “FAX” Address Type

How to configure the “FAX” address type:

1. Start the *Exchange management shell*.
2. Enter the following command in the command prompt:


```
Set-ForeignConnector "MrsConnector (<XPR-server name>:<name of the Exchange Server 2013 Mailbox Server Role>)"
-AddressSpaces "MRS:*;1", "FAX:*;1"
```

The “FAX” address type is now defined for fax transmission via the XPR server.

7.15 Adding and assigning the MRS E-Mail Address Type retrospectively

NOTE: As of Exchange Server 2007 the distribution groups support the **sAMAaccountName**. As a result, all Exchange users with this attribute are replicated as full XPR users to the XPR server. This causes problems when assigning the MRS address type and the number of replicated users exceeds the number of available user licenses. Therefore, the number of user groups to be replicated may have to be restricted beforehand via the LDAP configuration.

If no default policy has been created for the MRS address type upon the installation or further address types are required, this must be done in a retrospective procedure. The MRS address type is required for assigning messages arriving via the XPR server to Exchange users.

How to retrospectively add and assign the MRS address type:

1. Start the Exchange management console.
2. In the left section of the management console expand the object group **Organization Configuration**.
3. From the list of organization objects select **Hub Transport**.
The middle section of the management console now displays the Hub Transport objects.
4. In the middle section of the management console switch to the **E-mail Address Policy** tab.
5. Select the **Default Policy** entry. The right section of the management console now displays the default policy editing features.

NOTE: You can also use the **New E-mail Address Policy** feature to specify a new policy for creating and assigning the MRS address type via this policy.

6. Select **Edit** via the actions section to add the MRS address type to this policy. The wizard for editing the policy will then open with the first dialog **Introduction**.
7. Since no settings need to be made here, push the **Next >** button in this dialog. The **Conditions** dialog opens.
8. Since no settings need to be made here, push the **Next >** button in this dialog. The **E-Mail Addresses** dialog opens.
9. Use here the selection button (next to the **Add** button) to select **Custom Address** for the MRS address.
The Custom Address entry mask opens.

10. In the **E-mail address** field specify the address description (e. g. **@MRS** or, if additional address descriptions are required, **@MRS1** etc.).
11. In the **E-mail type** field specify the address type **MRS**.
12. Complete your entries with **OK**.
You return to the **E-Mail Addresses** dialog. The new address type is displayed here under **Address**.
13. In the **E-Mail Addresses** dialog click on **Next >**.
The **Schedule** dialog opens.
14. In the **Schedule** dialog set the time when the newly defined address type is to be adopted by the system. Then click **Next >**. The **E-mail Address Policy** dialog opens.
15. In the **E-mail Address Policy** dialog click the **Edit** button to continue the address type definition.
The **Completion** dialog opens.
16. In this dialog you can trace the address policy update. When the process is complete, click the **Finish** button.

The definition and assignment of the MRS E-Mail address type is now complete.

7.16 Security Settings for Installation and Live Operation of the E2k7 APL and ExUM APL

To ensure maximum security, various security settings can be reduced **after** the installation for real operation. This section describes which privileges are required for the installation and which privileges can be restricted for real operation.

IMPORTANT: To accomplish its tasks the XPR Foreign Connector uses MAPI access. Since Microsoft have not revealed the MAPI access privilege hierarchy, the connector function can only be granted under an account with Exchange full-admin privileges. The privilege restrictions described in the following have been tested on a system with the default policy by Microsoft. After modifying the default security policy by service packs or corporate security adaptations, the below privilege restrictions may lose their validity.

The test environment is composed of the following elements:

- Windows Server 2003 Enterprise SP2.
- Exchange Server 2010 Enterprise Edition x64.
- Exchange Mailbox Server Role and Exchange Hub Transport Server Role are installed on two physically separated servers.
- The installation is performed with the default security policy

With the installation description for each single XPR component the required privileges are named as well.

7.16.1 Requirements

The following tools are required for displaying and configuring the privileges:

- **ADSI Edit** (contained in the Microsoft Support Tools on the product data carrier for the Windows installation).
- **Exchange management console** and/or **Exchange management shell** on the product data carrier for the Exchange installation.
- The administration program **Active Directory Users and computer**.
- The administration program **Local Security Settings** (from the Windows Admin Pack, if you administer remotely from a workstation).

Definitions

<i><organization></i>	Wildcard for the name of your Exchange organization.
<i><Domain></i>	Wildcard for the name of your domain.
<i>APLSRV</i>	Name of the server on which the ExchApl runs as service.
<i>MBSRV</i>	Name of the Exchange server on which the Mailbox Server Role is installed.
<i>HTSRV</i>	Name of the Exchange server on which the Hub Transport Server Role is installed.

7.16.2 Privileges for the Exch APL Installation

Creating the XPR service account

Generate a user entry in your domain. This user account is required as service account for the Exch APL. In the following we will call this account USER. This USER needs to have a mailbox.

Microsoft demands this USER to be member of the group of domain administrators for the required MAPI access. Therefore, add this USER to the domain administrator group.

Local administrator

Promote the USER on the XPR server, on the *MBSE* and on the *HTSRV* to local administrator.

NOTE: You must be domain administrator for installing the Exch APL. Only then you are entitled to check whether the USER is a member of the domain. If you do not have the corresponding privilege, the installation will fail.

The USER must be assigned further special privileges on the XPR server. This is required for the services to work correctly. Via **Start > Programs > Administrative Tools > Local Security Policy** open the **Local Security Settings** dialog. Select **Local Policy > User Rights Assignment** and assign the corresponding privileges to the USER. The following privileges are to be assigned:

- “Logon on as a service” **1
- “Act as part of operation system” ¹
- “Backup files and directories” ¹
- “Restore files and directories” ¹
- “Logon as a batch job” ¹
- “Adjust memory quotas for a process” ¹

Exchange administrator

Promote the USER to “Exchange administrator with Read Privilege Role”. This privilege is required on the Mailbox Server Role as well as on the Hub Transport Server Role.

This setting is required for reading the Exchange objects properties.

1. Such privileges are set with the connector installation. They are also required for the ExUM APL.

MRSProxy64.dll (optional for manual creation)

If you want to use the **MRS Proxy address generation** function, the USER requires “full access” to the Exchange directory \\MBSRV\address. Share this folder with the USER for this purpose (sharing permissions).

Address templates

For the address templates (407 German or 409 English) the USER must have the privilege to “create address template objects” and to “delete address template objects”. To assign these privileges start ADSI Edit and switch to the directory:

```
CN=407|CN=409, CN=Address-Templates, CN=Addressing,  
CN=<Organization>, CN=Microsoft Exchange, CN=Services,  
CN=Configuration, DC=<Domain>.
```

Open the properties dialog here and switch to the **Security Settings** tab. Add the USER via **Add** to the list displayed. Click on the **Advanced** button to change the privilege and assign the “Create address template objects” and “Delete address template objects” privileges to the USER. In the entry line select **Apply onto** “This object only”.

Address types (optional for manual creation)

Creating address types requires the privileges “Create addr type objects” and “Delete addr type objects”. To assign these privileges start ADSI Edit and switch to the directory:

```
CN=Address-Types, CN=Addressing, CN=<Organization>, CN=Microsoft  
Exchange, CN=Services, CN=Configuration, DC=<Domain>.
```

Open the properties dialog here and switch to the **Security Settings** tab. Add the USER via **Add** to the list displayed. Click on the **Advanced** button to change the privilege and assign the “Create addr type objects” and “Delete addr type objects” privileges to the USER. In the entry line select **Apply onto** “This object only”.

Default policy (optional for manual creation)

Adding address types to the default policy requires the read and write privilege. To assign these privileges start ADSI Edit and switch to the directory:

```
CN=Default Policy, CN=Recipient Policies, CN=<Organization>,  
CN=Microsoft Exchange, CN=Services, CN=Configuration,  
DC=<Domain>.
```

Open the properties dialog here and switch to the **Security Settings** tab. Assign the USER read and write privileges here.

MRS container object (1)

To create the MRS container object the USER requires the “Create container objects” privilege. To assign this privilege start ADSI Edit and switch to the directory:

```
CN=<Organization>, CN=Microsoft Exchange, CN=Services,  
CN=Configuration, DC=<Domain>.
```

Open the properties dialog here and switch to the **Security Settings** tab. Add the USER via **Add** to the list displayed. Click the **Advanced** button to change the privilege and assign the USER the “Create container objects” privilege. In the entry line select **Apply onto** “This object only”.

NOTE: As option, you can simultaneously grant the privilege to “Delete container objects” at this point.

MRS container object (2)

Creating the MRS container object additionally requires the privileges “Create directory synchronization objects” and “Delete directory synchronization objects”. To assign these privileges start ADSI Edit and switch to the directory:

CN=<Organization>,CN=Microsoft Exchange, CN=Services,
CN=Configuration, DC=<Domain>.

Open the properties dialog here and switch to the **Security Settings** tab. Add the USER via **Add** to the list displayed. Click on the **Advanced** button to change the privilege and assign the USER the “Create directory synchronization objects” and “Delete directory synchronization objects” privilege. In the entry line select **Apply onto** “Child objects only”.

MRS connector object

Creating the MRS connector object requires the “Create all child objects ” and “Delete all child objects” privileges. To assign these privileges start ADSI Edit and switch to the directory:

CN=Connections, CN=<RG>, CN=Routing Groups, CN=<AG>,
CN=Administrative Groups, CN=<Organization>, CN=Microsoft
Exchange, CN=Services, CN=Configuration, DC=<Domain>.

Open the properties dialog here and switch to the **Security Settings** tab. Add the USER via **Add** to the list displayed. Click on the **Advanced** button to change the privilege and assign the “Create all child objects” and “Delete all child objects” privileges to the USER. In the entry line **Apply onto** select “This and all child objects”.

MRS settings object

The MRS settings object serves as storage location for the connector settings and other XPR settings for the connector. First, it must be defined. The USER of this MRS settings object must then be assigned additional privileges for accessing this object. Start the ADSI Edit and switch to the directory:

CN=Microsoft Exchange, CN=Services, CN=Configuration, DC=<Domain>

Generate a new object “MRS” (object class = container) here.

Open the properties dialog here and switch to the **Security Settings** tab. Add the USER via **Add** to the list displayed. Push the **Advanced** button and assign the USER the following privileges:

- “List Contents”, “Read all properties” and “Write all properties”
- “Delete”, “Read permissions” and “Modify permissions”
- “Create all child objects” and “Delete all child objects”

In the entry line **Apply onto** select “This and all child objects”.

With these privileges the XPR component “Exch APL” can be installed via the XPR setup.

7.16.3 Privileges for the ExUM APL Installation

To set up the ExUM APL the USER must be promoted from domain user to domain administrator.

Subsequently, the ExUM APL can be installed by the XPR setup.

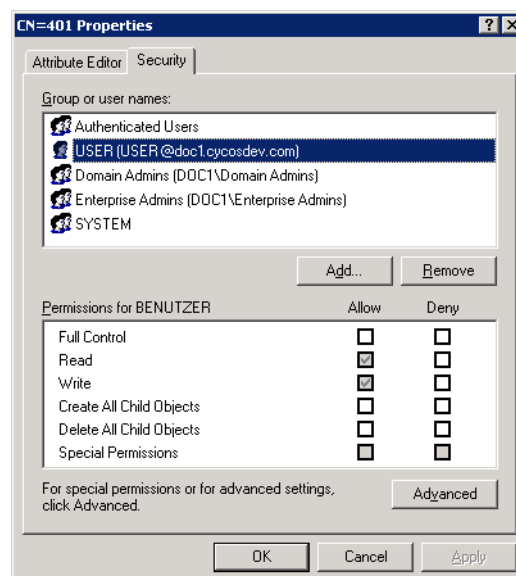
7.16.4 Privileges for the MMC Snap-in Installation

The installing user requires the privileges for modifying the AdminPropertyPages. Otherwise the installation will fail. To check this, start ADSI Edit and change to any directory under DisplaySpecifiers. For example:

CN= <401>, CN=DisplaySpecifiers, CN=Configuration, DC=<Domain>

Open the properties dialog here and switch to the **Security Settings** tab. Check whether the installing user has this right. If not, make the corresponding modifications.

read [inherited] & write [explicit]



Modify the privileges for all speech containers on the `DisplaySpecifiers` level. When you assign the privilege, select “This object and all child objects” under **Apply to**. The rights will be inherited by setting the option “Apply this permission to objects and/or containers within this container only”.

7.16.5 Privilege Restrictions for Live Operation

7.16.5.1 General

The USER can be relegated to the domain user privilege for operating the ExUM APL.

IMPORTANT: If you want to install an update, turn the restricted privileges into the state in which they were “before the installation”. After the update you can restrict the privileges again.

7.16.5.2 MRS Connector Settings

MRS connector settings (1)

The following setting is only required if you want to restrict the privilege assignment for the **MRS Settings Object** (see [Section 7.16.2, “MRS settings object”, on page 412](#)). Start the ADSI Edit and switch to the directory:

```
CN=APLSRV:MBSRV, CN=MRS,CN=Microsoft Exchange, CN=Services,  
CN=Configuration, DC=<Domain>
```

Open the properties dialog here and switch to the **Security Settings** tab. Assign the USER the following privileges:

read [inherited] & write [explicit]

MRS connector settings (2)

This privilege is only required to save administrative settings group-wide. Start the ADSI Edit and switch to the directory:

```
CN=Admin Group (Exchange Administrative Group (FYDIBOHF23SPDLT)),  
CN=MRS, CN=Microsoft Exchange, CN=Services, CN=Configuration,  
DC=<Domain>
```

Open the properties dialog here and switch to the **Security Settings** tab. Assign the USER the following privileges:

read [inherited] & write [explicit]

MRS connector object

The following privilege is required to save connector-specific settings. Start the ADSI Edit and switch to the directory:

CN=MrsConnector (APLSRV:MBSRV), CN=Connections, CN=Exchange Routing Group< (DWBGZMFD01QNBJR), CN=Routing Groups, CN=Exchange Administrative Group (FYDIBOHF23SPDLT), CN=Administrative Groups, CN=<Organization>, CN=Microsoft Exchange, CN=Services, CN=Configuration, DC=<Domain>

Open the properties dialog here and switch to the **Security Settings** tab. Assign the USER the following privileges:

Full control [explicit]

Privilege settings can be withdrawn after the installation for the following objects:

• MRS Proxy.dll	• MRS container (1)
• Address template	• MRS container (2)
• Address types	• MRS connector
• Default policy	• MMC snap-in

All other privileges are required for operating the Exch APL.

7.16.5.3 Assigning the privilege of operating Exch Apl service to any user

In environments where operating the Exch Apl service with “Local Administrator” privileges via the service account is not desired, this privilege can be assigned to another user after the installation. This is necessary, because the Apl does not start anymore after the withdrawal of the “Local Administrator” privilege.

How to assign privileges necessary for starting the Exch Apl service to a user who does not have administrative privileges:

Steps to Run the ExchApl without local admin rights

The ExchApl queries some exchange services. Without the local admin rights the service user must have read/write permissions to query the following services:

Microsoft Exchange RPC Client Access (MSExchangeRPC)
Microsoft Exchange Transport (MSExchangeTransport)
Microsoft Exchange System Attendant (MSExchangeSA)
Microsoft Exchange Information Store (MSExchangeIS)

Installing GPMC from the Command Line in Windows 2008 R2:

1. Open an elevated command prompt.
2. In the command prompt, type `ServerManagercmd -install gpmc`

XPR and Microsoft Exchange Server 2013

Security Settings for Installation and Live Operation of the E2k7 APL and ExUM APL

3. Start GPMC from the command prompt by typing `start gpmmc.msc`
4. Close the command prompt.

To set GPO in Windows 2008 R2:

To add Read and Write permissions to the service user account that was delegated on the services below,

Microsoft Exchange RPC Client Access (MSEExchangeRPC)
Microsoft Exchange Transport (MSEExchangeTransport)
Microsoft Exchange System Attendant (MSEExchangeSA)
Microsoft Exchange Information Store (MSEExchangeIS)

follow these steps:

1. On the Exchange server, start GPMC.MSC
2. Click on the domain.
3. Right-click Default Domain Policy, and then click Edit to open Group Policy Object Editor.
4. Expand Computer Configuration, expand Policies, expand Windows Settings, expand Security Settings, and then expand System Services.
5. Right-click the Microsoft Exchange System Attendant service, and then click Properties.
6. Click to select the Define this policy setting check box, and then click Edit Security.
7. Click Add, type username, click Check, and then click OK.
8. Click to select the Read check box and the Write check box.
9. Click OK two times, and then quit Group Policy Object Editor.
10. Click OK, and then quit the Active Directory Users and Computers snap-in.

Now you need to update the group policy on the Exchange with the following command:

```
gpupdate /force
```

Allow service control manager access with the following command:

```
sc [<ServerName>] sdset <ServiceName>  
<ServiceSecurityDescriptor>
```

To see the current permissions:

```
sc sdshow SCMANAGER
```

Use the Sc.exe tool to grant sufficient permissions to Authenticated Users

```
sc sdshow SCMANAGER
D: (A;;CCLCRPRC;;;AU) (A;;CCLCRPWPRC;;;SY) (A;;KA;;;BA) S: (AU;
FA;KA;;;WD) (AU;OIIOFA;GA;;;WD)
```

NOTE: The permissions string is specified in Security Descriptor Definition Language (SDDL).

The following permissions are granted after you run the command:

- Discretionary access control list (DACL)
- Allow to Authenticated Users: SDDL_CREATE_CHILD, SDDL_LIST_CHILDREN, SDDL_READ_PROPERTY, SDDL_READ_CONTROL
- Allow to SYSTEM: SDDL_CREATE_CHILD, SDDL_LIST_CHILDREN, SDDL_READ_PROPERTY, SDDL_WRITE_PROPERTY, SDDL_READ_CONTROL
- Allow to Built-in Administrators: SDDL_KEY_ALL
- System access control list (SACL)
- Audit activities of the Everyone group: SDDL_AUDIT_FAILURE, SDDL_KEY_ALL
- Audit activities of the Everyone group: SDDL_INHERIT_ONLY, SDDL_OBJECT_INHERIT, SDDL_AUDIT_FAILURE SDDL_GENERIC_ALL WD

Further details can be found under the following links:

<http://technet.microsoft.com/en-us/library/cc742037.aspx>

<http://msdn.microsoft.com/library/aa379567.aspx>

7.16.5.4 Privilege Overview

Topic	Privilege	Restrictable after the installation	Required for	
			TUM	Exch APL
Configuring a user pool		No	•	•
Local administrator	Inclusive the local security policies	Yes	• *	•
MrsProxy.dll	Sharing the ... \Exchsrvr \ADDRESS folder	Yes		•
Mailbox stores	send as & receive as	No	•	•
Address templates (407 409)	Template generation	Yes		•
Address types	Address type generation	Yes		•
Default policy	Read & write	Yes		•
MRS container (1)	Container object generation	Yes		•
MRS container (2)	Generating & deleting the Directory Synchronization Object	Yes		•
MRS connector	Generating & deleting all child objects	Yes		•
MRS settings object	Creating the XPR object	No		•
MRS connector settings (1)	Read & write	No		•
MRS connector settings (2)	Read & write	No		•
MRS connector settings (3)	Full access	No		•
*) requires special settings. See the explanations.				

Table 34 Privilege Overview

7.17 Migration

NOTE: Users who deployed Integrated Messaging (mailbox replication) so far must be switched to True Unified Messaging users. The users with Integrated Messaging will otherwise only be able to work as voice-only users, since they can only deploy the mailbox on the XPR server.

How to migrate an XPR server from an existing connection to *Exchange Server 2003* to a connection to *Exchange Server 2013*:

1. Uninstall the existing connector (E2kApl) and, if installed, the ExUM Apl. To do this, use the **Modify** option from the XPR server setup.

NOTE: If the ExUM Apl is also installed on the system, it must be uninstalled, since the TUM connection must be established to the new *Exchange Server 2013*. It will later be installed again in the Exchange 2013 connector setup.

IMPORTANT: In case of this system modification the Exchange 2013 connector must not be simultaneously selected for installation. The Exchange 2013 connector must be set up later in a separate step.

2. Uninstall the *Exchange system manager* that supplied the required CDO for the *Exchange Server 2003* connection.
3. Install the **MAPICDO**. Because the *Exchange System Manager* cannot be used in *Exchange Server 2013* any more, the *Microsoft Collaboration Data Object* (CDO) must be installed on the XPR server manually.

The following file is required to install the connectors for the *Exchange Server 2013* connection:

ExchangeMapiCdo.EXE

This file complies with all requirements as regards MAPI and CDO for the **ExchApl** and **ExUMApl**.

The ExchangeMapiCdo.EXE setup file provided by Microsoft for this purpose can be downloaded from the following website:

<http://www.microsoft.com/downloads/details.aspx?FamilyID=e17e7f31-079a-43a9-bff2-0a110307611e&DisplayLang=en>

4. Install the new XPR Foreign Connector **and** the ExUM Apl. To do this, use the **Modify** option from the XPR server setup.

7.18 Integration in Hosted *Exchange* 2013

IMPORTANT: When planning the XPR setup we urgently recommend to discuss the following requirements with the provider to ensure that the provider is willing and able to meet such requirements.

The following requirements must be met for connecting an XPR server to a *Hosted Exchange Server 2013*:

- The XPR server is installed at the customer's and not on the provider side. Thus, it does not share its location with Exchange.
- An XPR satellite, on which the connectors run **within the Exchange domain** on the provider side, must be installed.

NOTE: This does not require a physical server. A virtual server is sufficient.

- This satellite must have been connected to the XPR kernel computer in the customer domain. This connection requires:
 - A VPN connection or a similar network connection between the satellite and the XPR kernel computer.
 - Data traffic on this connection must be allowed in both directions to the destination ports 137, 138, 139, 445 and 13010.
- The services on the satellite and on the XPR kernel computer must be able to access the respectively other computer. In other words, either the domains must trust each other or workgroup authentication must be reverted to.

If you use workgroup authentication, execute the following sub-steps:

1. Create a local user on the XPR kernel computer with the same user name and password that is specified for the domain user account. This user name and password is used for the services of the Exchange satellite.
2. Add this user account to the group of local administrators.
3. Execute the sub-steps 1. and 2. for the reverse direction. That means, create a local user on the satellite with the same user name and password that is specified for the domain user account of the services on the XPR kernel computer. Add this user account to the group of local administrators.

Open **Start > Control Panel > Administrative Tools > Local Security Policy > Security Settings > Local Policies > Security Options** and verify that the entry **Network access: Sharing and security model for local accounts** has value **Classic - local users authenticate as themselves**.

7.19 Troubleshooting

7.19.1 Configuration for the CDO in Systems without public Folders

Working in a system environment without public folders may lead to problems with the CDO.

See also:

<http://social.technet.microsoft.com/Forums/exchange/en-US/3a2e9489-6137-42fb-95d1-bebcfe2ea138/mapiefailoneprovider-0x8004011d-error-message-when-you-access-an-exchange-server-2010-mailbox?forum=exchange2010>

How to solve such problems:

1. Open the registry editor (`regedit.exe`).
2. Open the path:

Windows 32-bit version

`HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows Messaging Subsystem`

Windows 64-bit version

`HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows Messaging Subsystem`

3. Create in the opened path the registry directory **CDO** if it is not present there.
4. Create the registry key **Ignore No PF** in **CDO**.
5. Enter the [DWORD] value 1 for the registry key **Ignore No PF**.

The CDO problem as regards missing public folders has now been solved.

7.20 Log File

To facilitate tracing the operational processes in the Exchange Server 2013, they are logged. You can use the log data when looking for errors or monitoring server processes. The Exchange Server 2013 stores such data in the following directory:

`<Microsoft Exchange Server Installation Path>\V15\Logging\RPC Client Access`

8 Multiline Configuration

NOTE: Xpressions uses a Microsoft MAPICDO component for message retrieval and notification. Xpressions uses a wrapper around Microsoft's MAPICDO. The MAPICDO integrates between Microsoft Exchange and third party applications such as Blackberry and Xpressions.

The ExUmApl uses the MAPI to do message retrieval and message notification. The Xpressions notification uses a MAPI call "Advise()" for every mailbox in the system. It is this function that has the limitation with-in the MAPI. MAPI only supports a finite number of concurrent advise targets (i.e. mailboxes of unified users). Xpressions was design to adhere to fix value of 5,000 which would guarantee MAPI support.

The ExUmApl creates 1 threads/sessions during it activity. Once the ExUmApl starts a thread is created to poll the Exchange server. Secondly for each mailbox in Xpressions that is Unified a call to Exchange is used to provide mailbox changes that will turn on or off MWI on these mailboxes.

A new request from Xpressions to Exchange during a request to retrieve mailbox messages out of Exchange. The session is terminated once the phone access is terminated.

For Xpressions to handle advisory limits it allows multiple ExUmApl in different Xpressions servers to provide specific mailbox support. This means by adding more ExUmApl and creating rules to specify which mailbox are supported in which Alp we can distribute the mailbox base.

Without a distributed implementation the ExUmApl will stop processing notification and message retrieval.

An example of MTA routing rule and ExUmApl registry configuration:

this is what the MTA rule will look like

```
"NVS:EXCH/[A-D].+@MRS.?"[TYPE=TRANS]=NVS:EXCH1/*
"NVS:EXCH/[E-H].+@MRS.?"[TYPE=TRANS]=NVS:EXCH2/*
```

the MTA rule goes above "extended rules"

And for every ExUmApl registry key you must specify which letters are supported as an example:

```
(hklm\software\pp-com\mrs\exumapl)[for Windows 2003 32 bit]:
(hklm\software\wow6432node\pp-com\mrs\exumapl)[for Windows 2008
64 bit]:
```

```
LINE_PROXY_PATTERN = (REG_SZ) [A-D]*@MRS.?
```

```
(hklm\software\pp-com\mrs\exumapl)[for Windows 2003 32 bit]:
```

```
(hklm\software\wow6432node\pp-com\mrs\exumapl)[for Windows 2008  
64 bit]:
```

```
LINE_PROXY_PATTERN = (REG_SZ) [E-H]*@MRS.?
```

NOTE: Need to set on all Xpressions servers that run the ExUmApl and the ExchApl the following registry key and value:

Create SharedMemMaxSize/DWORD/0x800000 inside of

```
HKEY_LOCAL_MA-
```

```
CHINE\SOFTWARE\WOW6432Node\Microsoft\Windows Messaging  
Subsystem
```

```
HKEY_LOCAL_MA-
```

```
CHINE\SOFTWARE\WOW6432Node\Microsoft\Windows Messaging  
Subsystem\Applications\ExUmApl
```

```
HKEY_LOCAL_MA-
```

```
CHINE\SOFTWARE\WOW6432Node\Microsoft\Windows Messaging  
Subsystem\Applications\E2k7Apl
```

This will prevent any E_OUTOFMEMORY(8007000E) errors on these systems. See Microsoft KB

<http://support.microsoft.com/kb/269794> or any additional reference.

Via the multiline configuration it is possible to install several Exch or ExUM connectors in an Exchange environment. This enables installations such as the connection of an XPR server to several Exchange organizations or a multi-tenant scenario.

In a distributed XPR system, a distinction is made between a kernel system, of which there is only one, and one or more associated satellite systems. Depending on the solution, a maximum of up to nine satellites, and thus nine connections to further Exchange servers, can be configured.

Example cases realized via such a configuration are:

- Multiline configuration for independent Exchange servers with Exchange Server 2003, 2007, 2010 and 2013.
- The standard multiline configuration for a distributed installation with Exchange Server 2003.
- Multiline configuration for associated message delivery with Exchange Server 2003.
- Multi-tenant solution. You find details of a multi-tenant solution configuration in the *OpenScape Xpressions Multi Tenancy* manual.

8.1 Multiline Configuration for independent Exchange Servers

NOTE: Configuring a multiline environment for Exchange Server 2003, 2007, 2010 and 2013 is identical as far as possible. The configuration description points to deviations wherever they may occur.

8.1.1 General Considerations

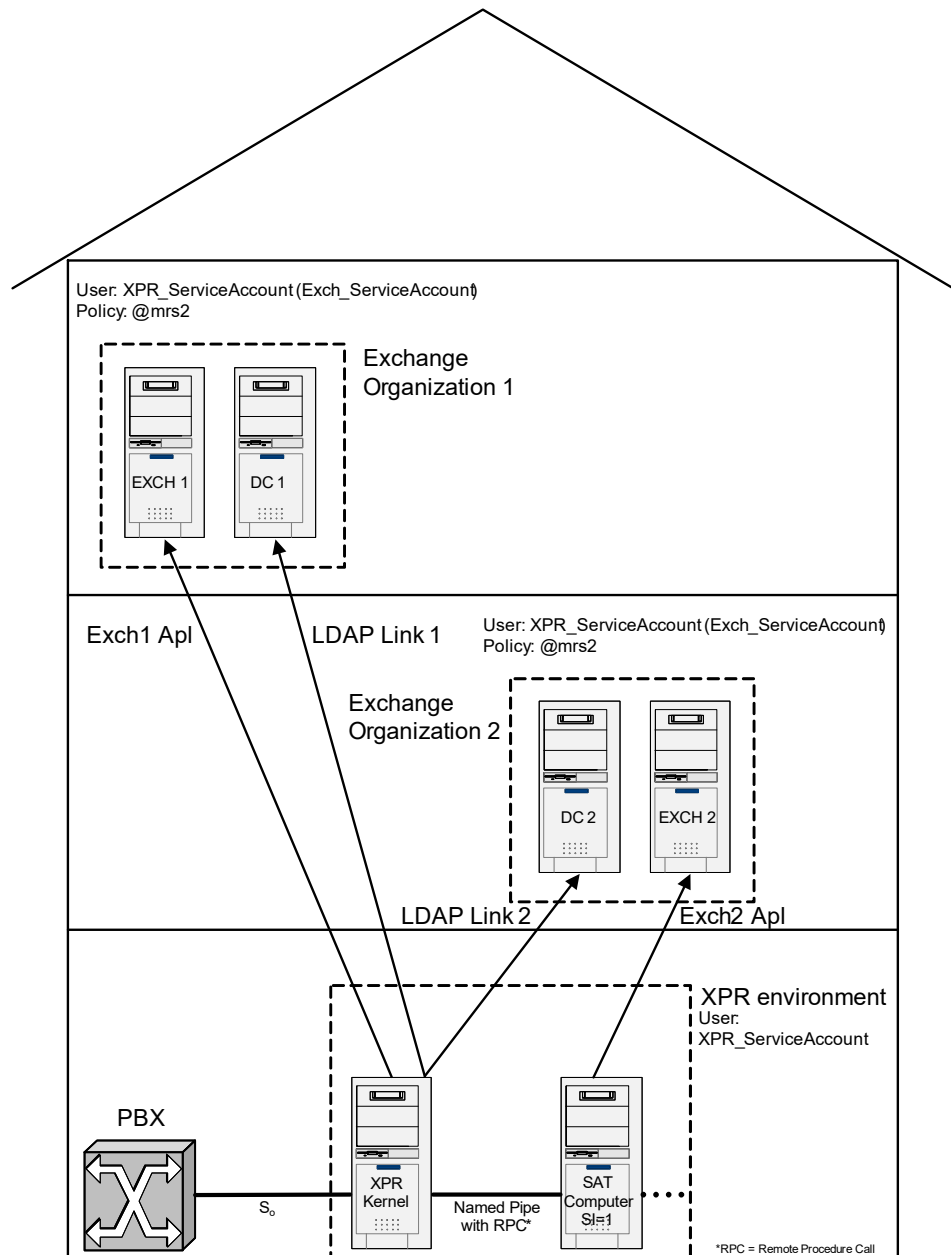
The system does not allow several installations of APLs on one XPR server. But for specific installation requirements, optimizing the XPR server usage via a distributed installation of further APLs would be ideal.

The deployment represents such a requirement in the following forest:

Two independent organizations (in their own domains) with one Exchange server each are to share an XPR server also present in an individual domain and a PBX.

Multiline Configuration

Multiline Configuration for independent Exchange Servers



This deployment scenario with the XPR server can be realized via a distributed installation. XPR server components needed multiple times are additionally outsourced to another computer (satellite). Via multiline configuration you can install several Exchange or TUM connectors in an Exchange environment. This enables setups such as connecting an XPR server to several Exchange organizations.

In a distributed XPR system, a distinction is made between a kernel system, of which there is only one, and one or more associated satellite systems. Depending on the solution, a maximum of up to nine satellites, and thus nine connections to further Exchange servers, can be configured.

A multiline environment for several independent Exchange servers is characterized by:

- One Exchange connector (Exch APL) for each Exchange server domain.
- One TUM connector (ExUM APL) for each Exchange server domain.
- One LDAP APL for each domain.

NOTE: An appropriate configuration allows using only one LDAP APL. The LDAP APL must be configured in such a way that it can access the user data of the different domains. Read and write access to the Active Directories must be possible.

8.1.2 Configuration Requirements

The following requirements must be complied with for a multiline configuration:

- The complete XPR environment for the multiline configuration must be provided. In other words, the XPR server and XPR satellite with the required Exchange APLs and LDAP APLs have been installed.

NOTE: Providing an XPR environment with satellite server is comprehensively described in the *OpenScape Xpressions Server Installation* manual.

- A trust relationship must exist between the domains.
- The service account under which the APLs operate must have the same name, the same password and the same privileges in all domains.
Example:
 - Service account name in the kernel domain: *svc_xpr*
 - Service account name in the satellite domain: *svc_xpr*
- The service account on the Exchange server must have a mailbox.
- The satellite server must be in the domain that hosts the Exchange server to which the connectors and, if required, the LDAP APL are installed. This domain will be called satellite domain in the following.
- The name resolution between both domains (kernel and satellite domain) must work.

Note: It may happen that a new user is defined in an organization whose name is already present in another organization. Since upon the user definition it is possible to allocate the user ID, make sure that the new user is not assigned the same ID as the user previously defined. If you leave the user ID assignment to the system, a USER-ID is automatically customized by attaching some numbers.
Example:

Organization	Name	User ID
org1	Testuser	Testuser
org2	Testuser	Testuser0041

Heed this with the definition of client profiles.

8.1.3 Defining Service Accounts

In each domain and on the XPR server a login account (service account) must be created for the XPR service. All XPR services must run in the context of this service account. These service accounts must conform to the following requirements:

- Each service account must have the same name in all domains.
- Each service account must have the same password in all domains.
- Assign the Exchange privileges to the service account on the Exchange server as described in the following chapters.
 - For Exchange 2007 in [Section 4.8, “Security Settings for Installation and Live Operation of the E2k7 APL and ExUM APL”](#), on page 142.
 - For Exchange 2010 in [Section 5.8, “Security Settings for Installation and Live Operation of the E2k7 APL and ExUM APL”](#), on page 260.
- The service account on the XPR servers must have local admin privileges. This applies for both the XPR kernel and XPR satellites.

Assign these service accounts to all XPR services.

8.1.4 Multiline Configuration

You need to execute the following steps for configuring the multiline scenario:

- [Editing Registry Keys](#)
- [Adding Routing Rules](#)
- [Adding/editing a Policy](#)
- [Adding XPR User Database Fields](#)
- [Supplementing LDAP Attributes](#)
- [Assigning Privileges](#)
- For Exchange Server 2007: [Configuring the Cross-Forest Administration](#)
- For Exchange Server 2010: [Creating Linked Role Groups](#)
- [Further Configuration Steps](#)

8.1.4.1 Editing Registry Keys

You need to edit two registry keys for multiline operation:

- Multiline_Support
- PreferredTransactionAddresses

Multiline_Support

To support multiline, a registry entry must be set for each installed Exch Apl. You need to do this on every computer on which an Exch Apl is installed.

This registry key is created in the following registry path:

```
HKLM\SOFTWARE\Wow6432Node\PP-COM\MRS\ExchApl
```

MULTILINE_SUPPORT [REG_DWORD]

You need to set the value of this registry key to 1.

PreferredTransactionAddresses

In addition, you need to enter the Exchange APLs on the kernel computer (for example: EXCH, EXCH1, EXCH2). This reports these connector addresses to the MTA as valid transaction addresses.

This registry key is created in the following registry path:

```
HKLM\Software\Wow6432Node\PP-COM\MRS\MTA
```

PreferredTransactionAddresses [REG_SZ]

Enter here the ExchApls used, for example: EXCH, EXCH1, EXCH2.

8.1.4.2 Adding Routing Rules

The following routing rules must be added on the kernel computer to the routing rule list under the PREFERRED rule (NVS:.*/*=<PREFERRED>):

```
NVS:EXCH/*@mrs1=NVS:EXCH1/*@mrs1
```

```
NVS:EXCH/*@mrs2=NVS:EXCH2/*@mrs2
```

8.1.4.3 Adding/editing a Policy

For each connector, new proxy addresses must be assigned via a policy.

The MRS addresses are assigned as follows:

MRS Address	Connector	Exchange Server
@mrs1	ExchAPL	EXCH1
@mrs2	ExchApl2	EXCH2

How to proceed is described in the following chapters.

- For Exchange 2007 in [Section 4.7, “Adding and assigning the MRS E-Mail Address Type retrospectively”](#), on page 140.
- For Exchange 2010 in [Section 5.7, “Adding and assigning the MRS E-Mail Address Type retrospectively”](#), on page 258.

8.1.4.4 Adding XPR User Database Fields

On the kernel computer the Correlation Database must be extended so that the XPR server can assign the two ExchApls. Copy the available EXCH field and EXCH renamed to EXCH1 or EXCH2. How to perform this modification:

1. Open the DB tool
2. In the database look for the line

```
<Server>/$SYSTEM      MASK      USER      EXCH
```

3. Copy the complete line and paste it thereunder twice in addition
4. Rename EXCH in the first pasted line to EXCH1
5. Rename EXCH in the second pasted line to EXCH2

The database must subsequently contain the following lines:

```
<Server>/$SYSTEM      MASK      USER      EXCH
<Server>/$SYSTEM      MASK      USER      EXCH1
<Server>/$SYSTEM      MASK      USER      EXCH2
```

6. Save the modification.

The required database fields are thus created.

8.1.4.5 Supplementing LDAP Attributes

For each domain controller an LDAP link must be established and the attribute mapping of both links customized.

Example:

LDAP link to the DC1 (ORG1)

For this link the **EXCH1** attribute must be additionally added to the XPR attribute **EXCH** in the LDAP attribute **proxyAddresses**.

LDAP link to the DC2 (ORG2)

For this link the **EXCH2** attribute must be additionally added to the XPR attribute **EXCH** in the LDAP attribute **proxyAddresses**.

8.1.4.6 Assigning Privileges

The following privileges need to be assigned on the single servers:

- Privileges for the service account on the satellite server in the satellite domain:
 - Add the service account of the kernel domain (trusted domain) to the local administrator group of the satellite server.
 - Add the service account of the kernel domain to the local security policy of the satellite server.
- Privileges for the service account on the kernel server in the kernel domain:
 - Add the service account of the kernel domain to the local administrator group of the kernel server.
 - Add the service account of the kernel domain to the local security policy of the kernel server.
- Privileges for the service account on the Exchange server in the satellite domain:
 - Add the service account of the kernel domain to the local administrator group of the Exchange server in the satellite domain. This allows the service account to access services though the service account is in another domain.
 - Assign the following privileges to the service account of the kernel domain. To do this use the following commands as local user:
 - For the privilege "send as", "receive as", "ms-exch-store-admin"


```
GetOrganizationConfig
```

Multiline Configuration

Multiline Configuration for independent Exchange Servers

- For the privilege "send as", "receive as", "ms-exch-store-admin"
`GetMailboxDatabase`
- To add "send as" for each mailbox
`GetMailbox`
- To add "Full Access" for each mailbox
`AddMailboxPermission`

8.1.4.7 Configuring the Cross-Forest Administration

The service account must be able to access all Exchange servers across the forest. In case of Exchange Server 2007, this requires activating the administrative access of the service account to the cross-forest administration.

How to configure a cross-forest administration is described in the following Microsoft article:

[http://technet.microsoft.com/en-us/library/bb232078\(v=exchg.80\).aspx](http://technet.microsoft.com/en-us/library/bb232078(v=exchg.80).aspx)

8.1.4.8 Creating Linked Role Groups

Execute the steps described in the following to add the privileges “View-Only” and “Organization Management” for the standard roles as Linked Role Groups for Exchange Server 2010:

1. Create Linked Role Groups for Exchange Server 2010.

You need to create such groups because this is the only option to allow a user (here service account in the kernel domain) to accomplish management jobs on an Exchange server in another domain (here the satellite domain). The service account must be in the kernel domain, first for the setup, and then for live operation at a later date. In case of the Linked Role Groups this occurs by replicating the administrative groups with their privileges to the single domains.

Application scenario:

You are logged in on the satellite server (domain **B**) with a user account of domain **B**. You wish to install the APLs via the service account in domain **A**, because the service account for the setup and under which the service shall operate at a later date must be in domain **A**. If the administrative privileges have not been assigned via Linked Role Groups, no setup is possible.

How to configure Linked Role Groups for several Exchange Server 2010 domains is described in the following Microsoft article:

<http://technet.microsoft.com/en-us/library/dd876918.aspx>

- Create a Universal Security Group (USG) in the kernel domain. Add the service account of the kernel domain to administer the satellite domain at a later date to the Universal Security Group. To do this use the following commands:
 1. `$ForeignCredential = Get-Credential`
 2. `$OrgMgmt = Get-RoleGroup "Organization Management"`
 3. `New-RoleGroup "Organization Management - Linked"`
`-LinkedForeignGroup <Name of foreign USG>`
`-LinkedDomainController <FQDN of foreign ExADNoMk DC>`
`-LinkedCredential $ForeignCredential`
`-Roles $OrgMgmt.Role`
 4. `Get-ManagementRoleAssignment`
`-RoleAssignee "Organization Management`
`- Linked" -Role My* | Remove-ManagementRoleAssignment`
 5. `Get-ManagementRole | New-ManagementRoleAssignment`
`-SecurityGroup "Organization Management`
`- Linked" -Delegating`

8.1.4.9 Further Configuration Steps

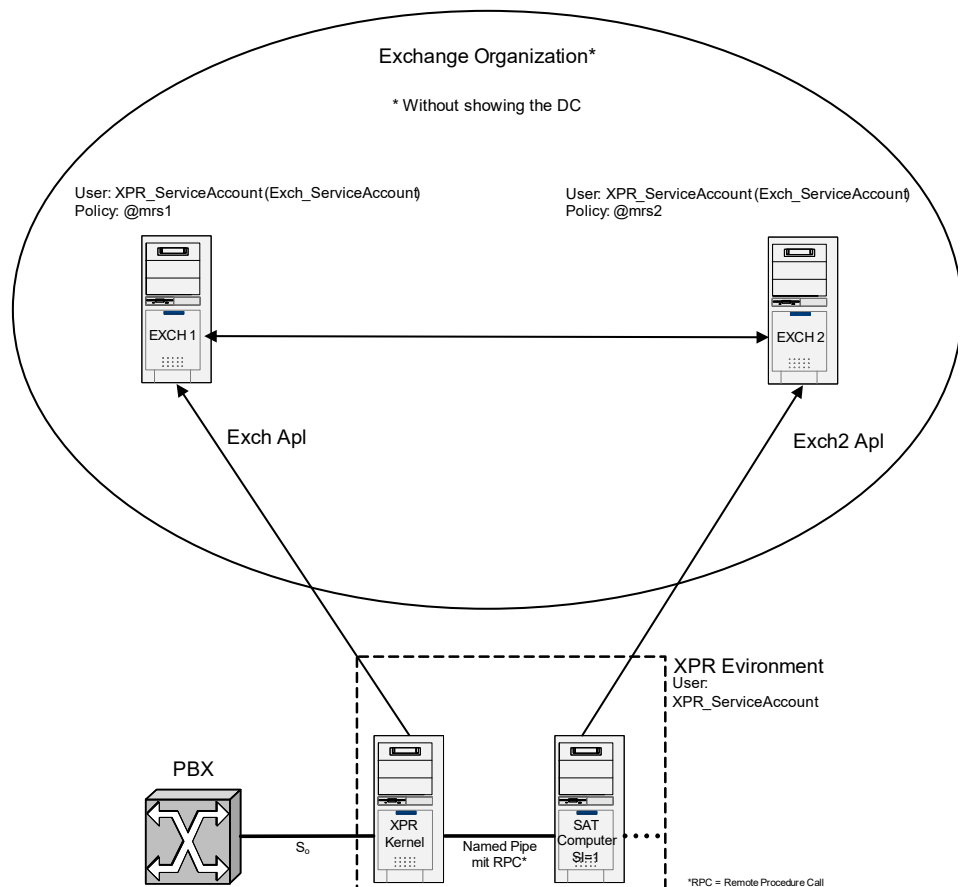
- An additional privilege for the Exch APL is required on the Primary Domain Controller (PDC) of the satellite domain. Add the privilege “Administer information store”, “read” and “write” to the Microsoft Exchange organization.

This eliminates the start-up problem that occurs when reading data of the MRS Connector Object out of the Active Directory of the satellite domain. The MRS Connector Object of the satellite domain can now be read by the service account of the kernel domain.

- Disable the internet protocol IPv6.
This is required on the grounds of persisting Exchange Server 2010 problems with MAPI and IPv6. See also:
http://blogs.msdn.com/b/stephen_griffin/archive/2009/01/28/more-issues-with-mapi-and-ipv6.aspx
- Disable the User Account Control (UAC) on the Windows server 2008 R2.
 1. To do this, open via **Start > Administrative Tools > Local Security Policy> Local Policy > Security Options**.
 2. Select **User Account Control: Run all administrators in Admin Approval Mode**.
 3. Open the context menu **Properties** for this policy.
 4. Select in the **Local Security Setting** dialog the **Disabled** option.

8.1.5 Standard Multiline Configuration for a distributed Installation with Exchange Server

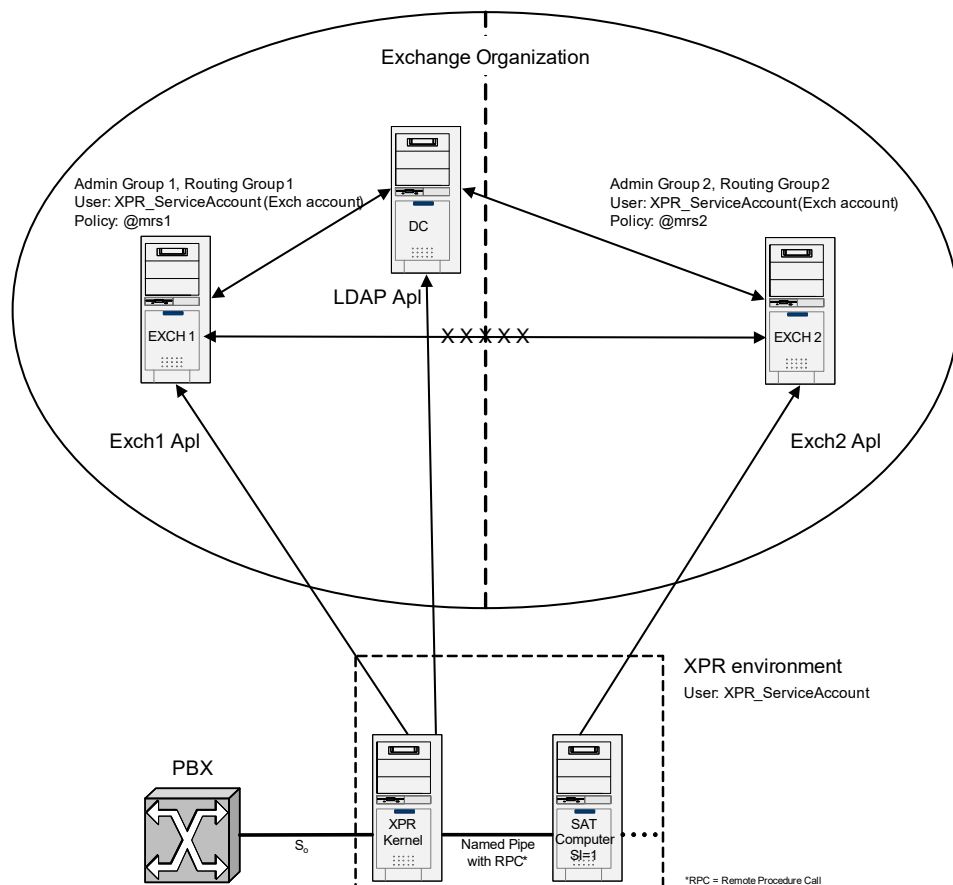
- An organization uses several Exchange servers in a domain forest. A network connection between the two Exchange servers is available and used. The main advantage of distributed XPR systems is the scalability of their hardware resources. In such an organization environment e.g. the message routing can be optimized to achieve a better load distribution. This version will not be dealt with in the following. You find a detailed description of this installation version in the *Server Installation* manual.



8.1.6 Multiline Configuration for associated Message Delivery with Exchange Server

With the same requirements as for multiline configuration for separated Exchange environments, multiline can also be configured for an Exchange environment where the Exchange servers are in one domain. The inbox replication routing must be customized here in addition since for one OU exactly one connector may be in charge.

An organization uses several Exchange servers in a domain forest. The message exchange between the two Exchange servers is not to be used. In other words, a message transmission is required that allows to consider a permanent assignment. This enables the delivery of messages coming in via the XPR server to the users on the corresponding Exchange servers. The availability of several separated admin and routing groups is to be considered here. For these systems as well a XPR server can be integrated via a satellite installation with multiline configuration.



5.

8.1.7 True Unified Messaging (TUM) in Multiline Environments

If True Unified Messaging (TUM) is to be used in multiline environments, ExUM APLs are to be installed to the kernel computer as well as to the satellite in parallel to the Exchange connectors (Exch APL).

For TUM almost the same configuration steps are to be performed as described in [Section 8.1, “Multiline Configuration for independent Exchange Servers”, on page 425](#).

The following installation steps are additionally required:

- Two new registry keys must be inserted/set
- The routing rules in the XPR-MTA must be expanded

Registry keys

To support multiline, the following registry values must be set for each installed ExUM Apl.

NOTE: You need to do this on the computers on which an ExUM Apl is installed.

The registry keys are created in the following registry path:

HKLM\Software\Wow6432Node\PP-COM\MRS\ExUmApl

MULTILINE_SUPPORT [REG_DWORD]

You need to set the value of this registry key to 1.

LINE_PROXY_PATTERN (REG_SZ)

Enter the regular expression for the routing in charge of distributing the users among the available TUM connectors in this registry key.

Example:

***@mrs1**

or for the second routing rule

***@mrs2**

MTA routing rules

The routing rules for the Exch Apl are to be supplemented by those required for the ExUM Apl in the following format:

```
NVS:.*/*=<PREFERRED>
NVS:EXCH/*@mrs1=NVS:EXCH1/*@mrs1
NVS:EXCH/*@mrs1[TYPE=TRANS]=NVS:EXCH1/*@mrs1
NVS:EXCH/*@mrs2=NVS:EXCH2/*@mrs2
NVS:EXCH/*@mrs2[TYPE=TRANS]=NVS:EXCH2/*@mrs2
```

NOTE: The regular expression may be arbitrarily adapted according to the applicable conventions. Via this filter rule it is possible to manage the distribution of users among the TUM connectors.

As regards the routing rules and filter expressions of the ExUM Apl it does not matter whether they refer to the portion after or before the @. A differentiation can be made via the front as well as rear address portion.

Example:

We suppose that the proxy addresses in an Exchange environment have the general format Y[number]@mrs.

To optimize load balancing, the Kernel ExUM Apl shall be made to serve users whose proxy address begins with number 0, 1 and 2. The satellite ExUM Apl then serves the remaining users.

The conceivable routing rule is in such a case for example:

```
"NVS:EXCH/Y[0-2].*@mrs" [TYPE=TRANS]=NVS:EXCH1/@mrs
"NVS:EXCH/Y[3-9].*@mrs" [TYPE=TRANS]=NVS:EXCH2/@mrs
```

and the additional registry values for the ExUM Apls

```
LINE_PROXY_PATTERN (REG_SZ) = "Y[0-2].*@mrs"
```

or for the second ExUM Apl

```
LINE_PROXY_PATTERN (REG_SZ) = "Y[3-9].*@mrs"
```

Users Y0xxxx@mrs to Y2xxxx@mrs are routed via the first ExUM Apl and users Y3xxxx@mrs to Y9xxxx@mrs via the second ExUM Apl.

IMPORTANT: The quotation marks must be specified as well. They are required to tell apart "wildcards" (* represents any string) and "regular expressions" (.* represents any string).

MTA routing rules

The routing rules for the Exch Apl are to be supplemented by those required for the ExUM Apl in the following format:

```
NVS:*.*/*=<PREFERRED>  
NVS:EXCH/*@mrs1=NVS:EXCH1/*@mrs1  
NVS:EXCH/*@mrs1 [TYPE=TRANS]=NVS:EXCH1/*@mrs1  
NVS:EXCH/*@mrs2=NVS:EXCH2/*@mrs2  
NVS:EXCH/*@mrs2 [TYPE=TRANS]=NVS:EXCH2/*@mrs
```

Multiline Configuration

Multiline Configuration for independent Exchange Servers

9 Microsoft Exchange Server 2016/2019/Office 365 (EWS)

9.1 General Considerations

This chapter describes the procedures to configure the connection of an already existing OpenScape Xpressions V7 server to an Exchange Server 2016 domain or to an Office 365 Exchange.

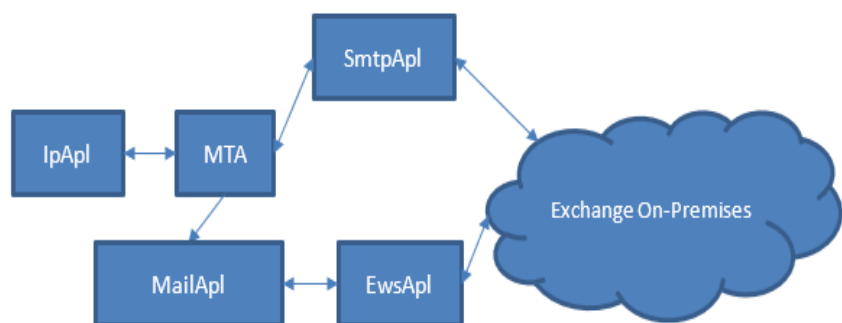
9.2 Overall Architecture

The Xpressions solution to support Exchange 2016/2019 and Office 365 uses the SMTP and Exchange Web Services interface to perform mailbox synchronization.

9.2.1 Exchange 2016 / 2019

On Exchange Server 2016/2019 Microsoft discontinued the Messaging API (MAPI) support. Therefore, to support this Exchange Server versions, architectural changes have been performed on Xpressions side.

The messages are now kept on both Exchange Server and Xpressions' mailbox databases and their statuses are synchronized according to the user changes.



Messages (voicemail and fax) are delivered to the recipient (MailApl) and via a carbon copy rule, they are sent (using SmtmApl) to the recipient's Exchange 2016/2019 mailbox.

When messages are read or deleted on XPR side, MailApl notifies EwsApl which in turn marks the message as read or deletes the message on/from the Exchange side.

When messages are read or deleted on the Exchange side, EwsApl is notified and then notifies MailApl which in turn marks the message as read or deletes the message on XPR side.

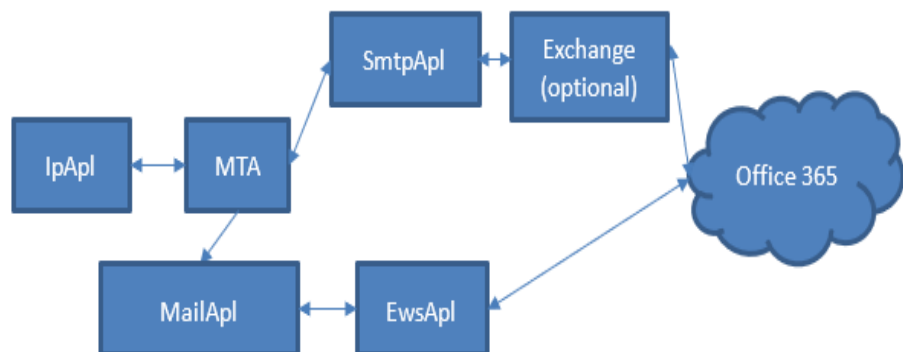
For sending faxes:

A fax message created on Outlook/Outlook Web Access will be delivered by the Exchange server (configuration needed) to Xpressions (via SMTP) and then it is delivered to MTA for conversion and then routed to IpApl for transmission.

9.2.2 Office 365

Like the Exchange Server 2016, the Exchange Online on Office 365 doesn't support Messaging API (MAPI).

On the Xpressions side, the implemented solution works in a similar way.



Messages (voicemail and fax) are delivered to the recipient (MailApl) and via a carbon copy rule, they are sent (using SmtmApl) to the recipient's Office 365 Exchange mailbox.

NOTE: When the SmtmApl is not exposed to the internet, it is possible to use an Exchange server on premises as a relay.

In this case, the messages (voicemail and fax) are delivered to the recipient (MailApl) and via a carbon copy rule are sent (SmtmApl) to MS Exchange on-premises in a hybrid configuration. The MS Exchange then relays the messages to Office 365.

When messages are read or deleted on XPR side, MailApl notifies EwsApl which in turn marks the message as read or deletes the message on/from the Exchange side.

When messages are read or deleted on the Exchange side, EwsApl is notified and then notifies MailApl which in turn marks the message as read or deletes the message on XPR side.

For sending faxes:

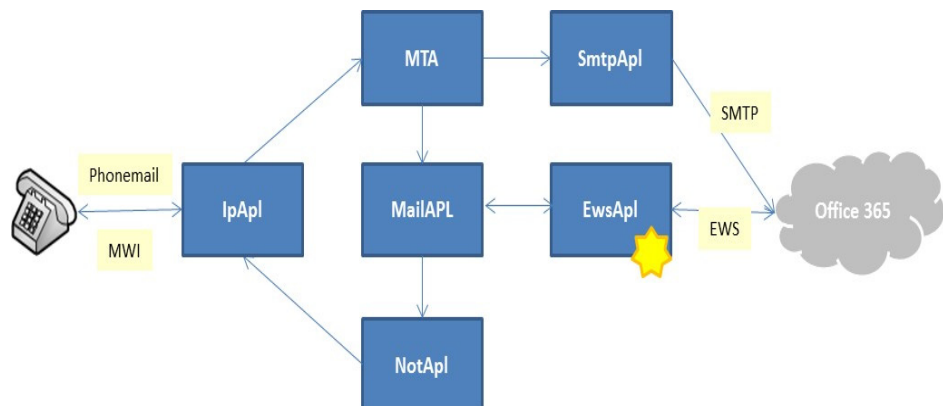
A fax message created on Outlook/Outlook Web Access will be delivered by the Exchange server (configuration needed) to Xpressions (via SMTP) (or to an MS Exchange on -premises) and then it is delivered to MTA for conversion and then routed to IpApl for transmission.

9.3 Installation and Configuration

9.3.1 Preparation/Configuration

- Message flow overview
- Installing .Net Framework 3.5;
- Required hotfixes;
- User mask configuration;
- Users synchronization between Xpressions and Active Directory (via LDAP);
- Importing Exchange users from Active Directory (via script);
- Configuring users;
- Exchange On-Premises service user configuration (Send As permission) [1];
- Configuring SmtplApI;
- Configuring MTA routing rules;
- Configuring EwsApI;
- Sending Faxes to XPR
- Troubleshooting

9.3.2 Message Flow Overview



Message delivery:

Phone>Phonemail (IpApl) -> MTA -> MailApl (Mailbox) (CC-Message)MTA -> SmtplApl -> Exchange > Outlook

Message access:

Phone>Phonemail (IpApl) or Browser> WebAssistant-> MailApl (Mailbox)

Notification (MWI):

read/unread in Outlook >Exchange 2016/2019 -> EwsApl -> MailApl -> NotApl -> IpApl >PBX(Phone)

Message status:

read/unread via Phonemail/Webassistant -> MailApl -> EwsApl -> Exchange(Outlook)

read/unread in Outlook>Exchange 2016/2019 Exchange Online -> EwsApl -> MailApl (Mailbox)

IMPORTANT NOTE: Migrating existing systems limitations:

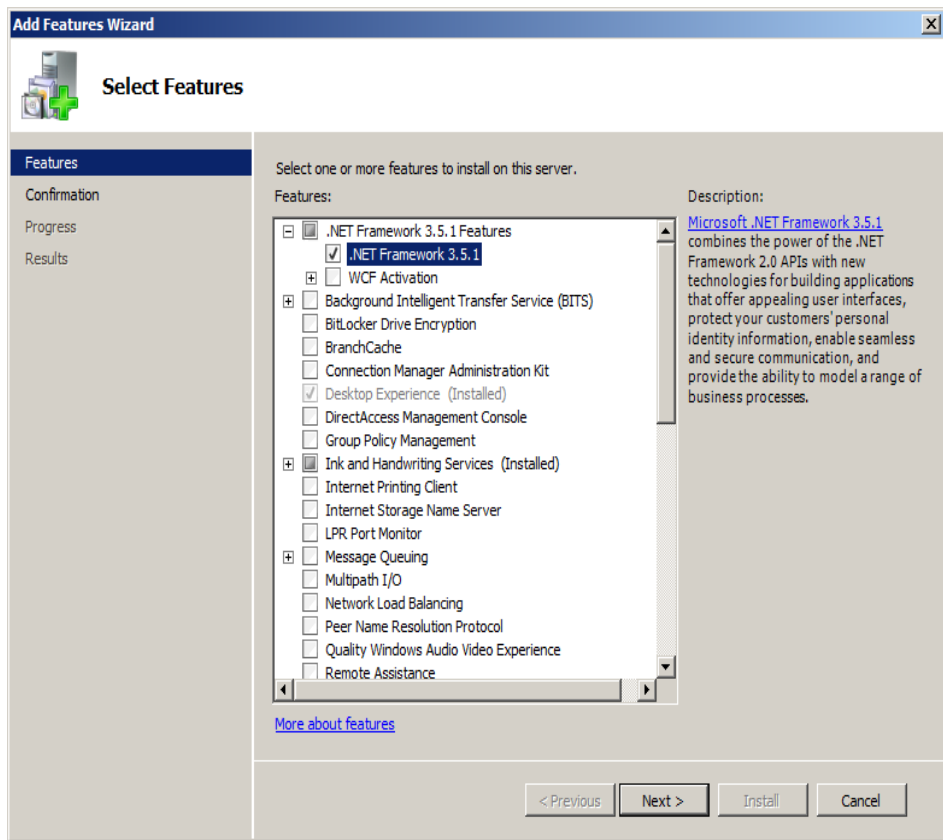
On the scenario where the customer already had the former Xpressions Exchange connector (E2k7Apl/ExUmApl) installed, there may be some limitations:

1. Messages created with the previous solution will only be available on the Exchange Mailbox. Therefore, they will not be available for TUI or WebAssistant access.
2. Such messages will not be monitored, changed or deleted by the new Exchange 2016/2019/Office 365 connector.
3. There is no update scenario from ExchApl and ExUmApl to EWS.

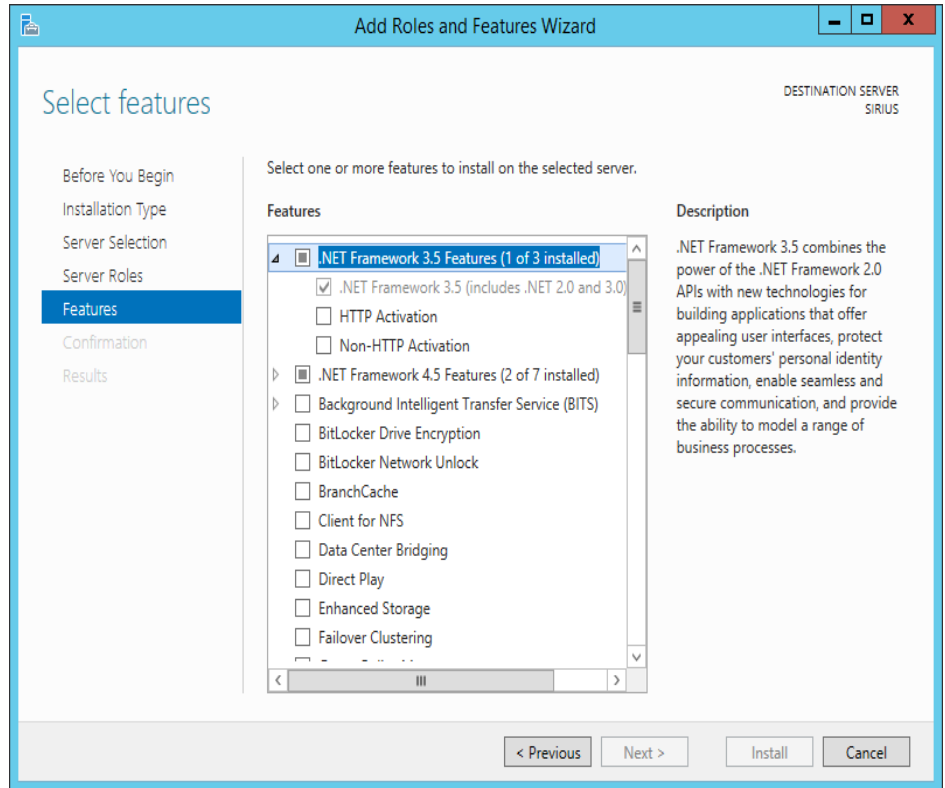
During migration the ExUmApl should be removed in the first step. The ExchApl can be used in parallel but needs to be configured without ExUmApl

9.3.3 Installing the .Net Framework 3.5

9.3.3.1 Windows 2008 R2



9.3.3.2 Windows 2012/ Windows 2012 R2/ Windows 2016/2019



9.3.4 Required Version/ hotfixes on XPR system

The following hotfixes versions (or newer) are mandatory for this feature:

- CycosOpenSSL-811FR5-18885.exe
- EwsApIInstaller-811FR5-18968.exe
- MailApI-811FR5-18818.exe
- Mta-811FR5-18885.exe
- SmtPApI-811FR5-18843.exe
- FiApI-811FR5-18409.exe

9.3.5 TLS 1.2

EwsApi uses Microsoft Windows settings to connect to the Exchange server via HTTPS protocol and uses TLS 1.2 by default.

On Windows Server 2012 or higher it will use TLS 1.2 by default.

On Windows Server 2008 R2 you need the following registry settings to be changed in order to enable TLS 1.2:

1. On .Net framework 3.5

```
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v2.0.50727]
"SystemDefaultTlsVersions"=dword:00000001
```

```
[HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\.NETFramework\v2.0.50727]
"SystemDefaultTlsVersions"=dword:00000001
```

2. On Secure Channel (Schannel) TLS 1.2 registry keys

```
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.2\Client]
"DisabledByDefault"=dword:00000000
"Enabled"=dword:00000001
```

```
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.2\Server]
"DisabledByDefault"=dword:00000000
"Enabled"=dword:00000001
```

3. On .Net framework 4 or higher

```
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319]
"SystemDefaultTlsVersions"=dword:00000001
```

```
[HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\.NETFramework\v4.0.30319]
"SystemDefaultTlsVersions"=dword:00000001
```

9.3.6 EWSApi installation for Exchange 2016/2019/On-Premises

During the EwsApiInstaller setup, the user will have to provide some configurations for the EwsApi:

- Service User section:
 - **User Name:** Exchange user account with impersonation rights on the user's mailbox. (i.e. *adm2016*)
 - **Password:** Password for the account.
 - **Exchange On-Premises:** enables/disables the connection with Exchange On-Premises (should be enabled in this case)
 - **Domain:** Domain which the service user belongs to. Only available when option "Exchange On-Premises" is selected.
- Autodiscover section:
 - **Enable Autodiscover:** If the Exchange on-premises autodiscover is correctly configured, this option may be checked to autofill the "URL" field.
 - **Service URL:** If the autodiscover doesn't work, this field has to be filled with the URL for the Exchange Online EWS:
i.e.: *https://2016exch.domain2016.net/ews/exchange.asmx*

- **O365 default URL button:** fills the URL entry with the default O365 default service URL. *(It should not be used on premise systems)

9.3.7 EWSApi installation for Exchange Online (Office 365)

During the EwsApiInstaller setup, the user will have to provide some configurations for the EwsApi:

- Service User section:
 - **UPN:** Office365 account which will have impersonation rights on the user's mailbox. (i.e. *administrator@unifyoffice365.com*)
 - **Password:** Password of the account.
 - **Exchange On-Premises:** enables/disables the connection with Exchange On-Premises (should be disabled in this case)
- Autodiscover:
 - **Enable Autodiscover:** If the Exchange autodiscover is correctly configured, this option may be checked to autofill the "URL" field.

- **URL:** If the autodiscover does not work, this field has to be filled with the URL for the Exchange Online EWS:
<https://outlook.office365.com/ews/exchange.asmx>
- **O365 default URL button:** fills the URL entry with the default O365 default service URL.

Note: After installation of the EwsApIInstaller hotfix the setup can be also started by running the following command at the Windows cmd:

ExchApIConfigurator /ewsapi

The following additional options are available to the ExchApIConfigurator:

EwsApi

Install the EWSApi service.

IgnoreServiceCheck

nameloc and XPR Configuration Service (cfgsvc).

Registry

Just create/populate the registry. Do not attempt to install the EWSApi service.

9.3.8 EWSApl: OAuth authentication

To enable EWSApl to use OAuth authentication with Office 365 it is necessary to perform a registration in the Microsoft Entra admin center.

IMPORTANT: The endpoints related at the following Microsoft page should be reachable for customers using Office 365.

Please configure your network proxy and firewall to allow the connection to the listed Addresses and ports according to you country region.

For more information please refer to:

<https://docs.microsoft.com/en-us/microsoft-365/enterprise/urls-and-ip-address-ranges?view=o365-worldwide>

General Considerations

This session contains the instructions for configuring the EWSApl for connecting to the Microsoft Exchange Server Online.

NOTE: The EWSApl hotfix must be installed only for the customers that will perform the migration for the new authentication method. Customers that did not performed all the necessary adjusts in the Microsoft Entra admin center, must keep with the previous hotfix version until all the necessary adjusts listed in this document are done.

Use the **EwsAplInstaller-FR5-20967** or a newer one.

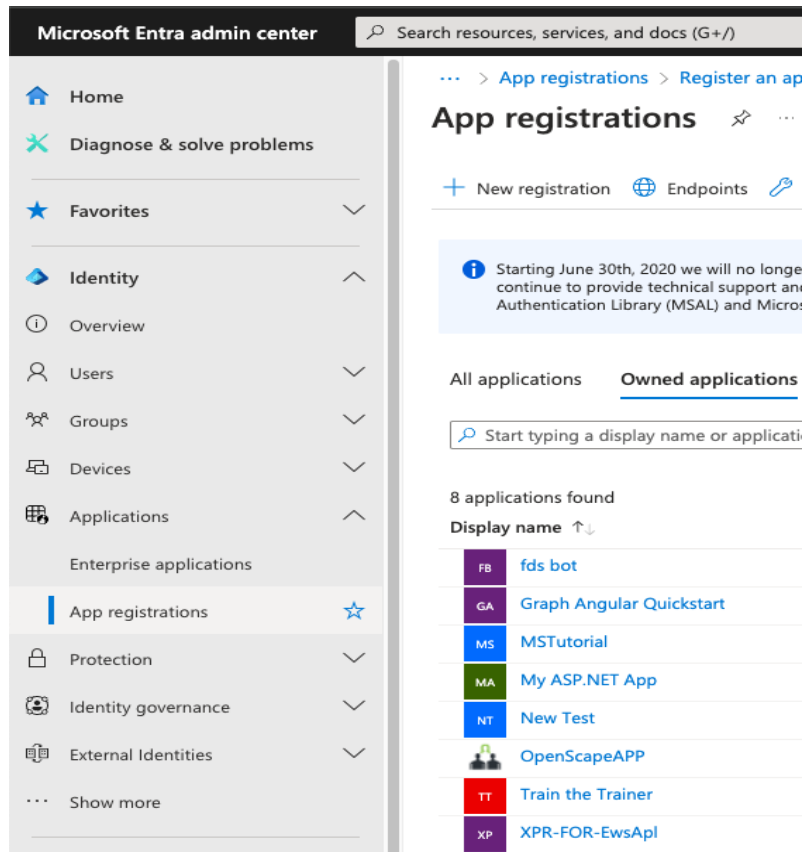
The sections below describe the steps necessary to follow:

9.3.8.1 Microsoft Entra configuration

UI Configuration:

In the Microsoft Entra:

1. Search and open the [Microsoft Entra admin center](#).
2. Navigate to **Applications > App registrations** from the left side menu.



3. Click on **+ New Registration** and enter the following information in the form fields:

a) **Name:**

Enter a name for the application:

e.g. **XPR-EWSApl**

b) **Redirect URI (optional):**

In the selection options available, choose **Public client/native (mobile & desktop)** and use the following URI:

`urn:ietf:wg:oauth:2.0:oob`

Microsoft Exchange Server 2016/2019/Office 365 (EWS)

Installation and Configuration

Home
Diagnose & solve problems
Favorites
Identity
Overview
Users
Groups
Devices
Applications
Enterprise applications
App registrations
Protection
Identity governance
External Identities
Show more

Register an application

Name
The user-facing display name for this application (this can be changed later).
XPR-EWSAp

Supported account types
Who can use this application or access this API?
☒ Accounts in this organizational directory only (CITS only - Single tenant)
☐ Accounts in any organizational directory (Any Microsoft Entra ID tenant - Multitenant)
☐ Accounts in any organizational directory (Any Microsoft Entra ID tenant - Multitenant) and personal Microsoft accounts (e.g. Skype, Xbox)
☐ Personal Microsoft accounts only
Help me choose...

Redirect URI (optional)
We'll return the authentication response to this URI after successfully authenticating the user. Providing this now is optional and it can be changed later, but a value is required for most authentication scenarios.
Public client/native (mobile ... urn:ietf:wg:oauth:2.0:oob

4. Click the **Register** button at the bottom of the page.
5. On this page select **API permissions** on the left side menu.
6. In **Configured permissions** section, click on **+ Add a permission** to open **Request API permissions** page.
7. Go to the **APIs my organization uses** tab and search for **Office 365 Exchange Online**.
8. Click on the **Office 365 Exchange Online**.

Microsoft Entra admin center Search resources, services, and docs (G+)

App registrations XPR-EWSAp

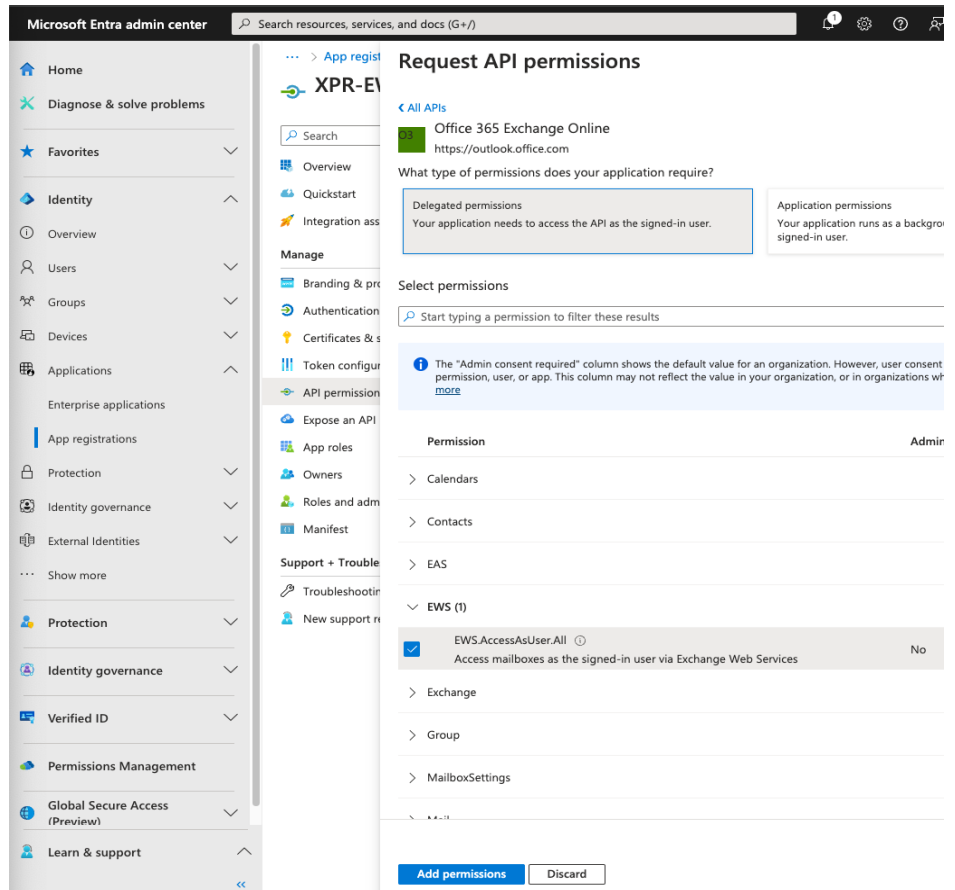
Request API permissions

Select an API
Microsoft APIs APIs my organization uses My APIs

Apps in your directory that expose APIs are shown below

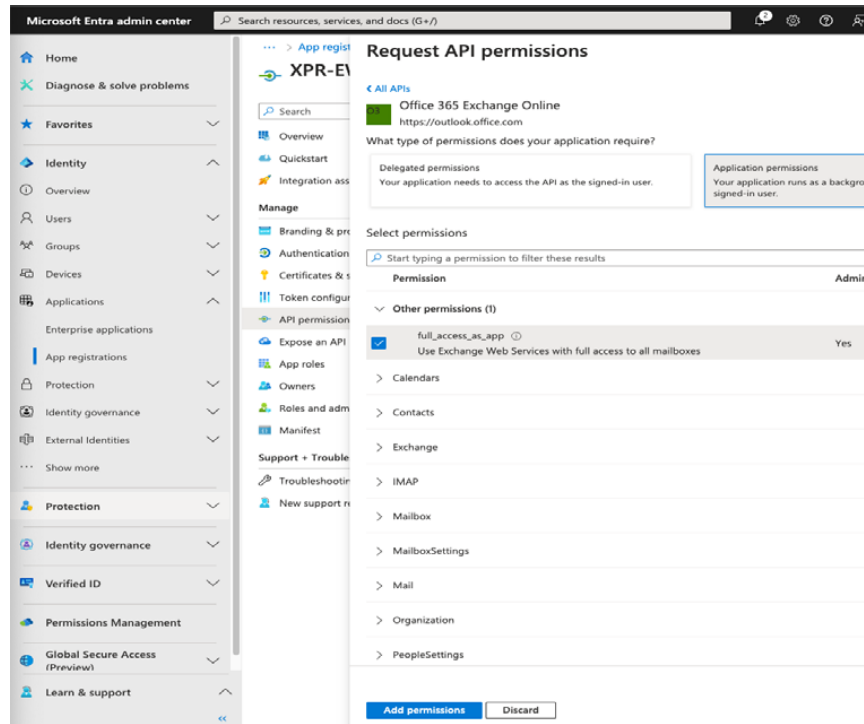
Name	Application (client) ID
Office 365 Exchange Online	00000002-0000-0000-0000-000000000000

9. On the **Request API permissions** for **Office 365 Exchange Online** page click on **Delegated permissions** option and search for **EWS** permission
10. Expand the **EWS** permissions and enable **EWS.AccessAsUser.All**
11. Click on the **Add permissions** button to add this permission and return to the previous screen.

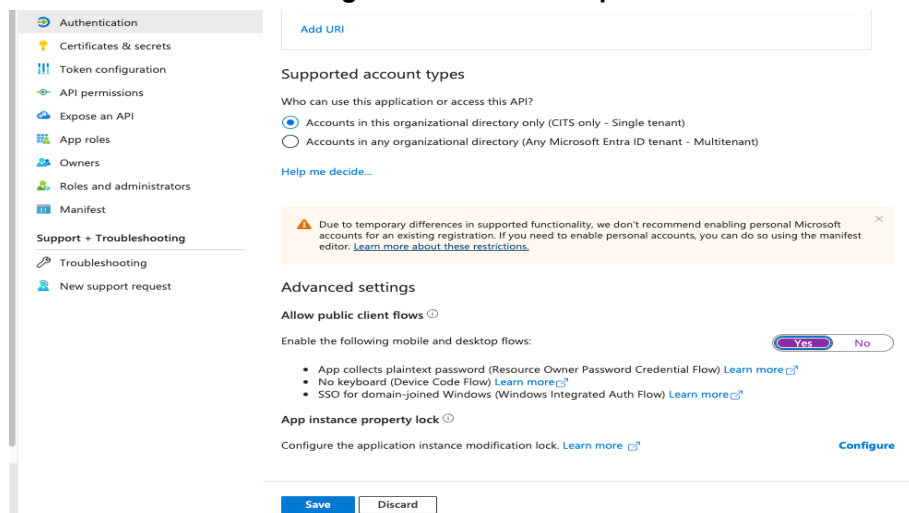


12. Repeat the steps 6, 7 and 8 to add a new permission.
On the **Request API permissions** page, navigate to **APIs my organization uses**, search for and select **Office 365 Exchange Online**. This time, click on the **Application permissions** option and search for **Other permissions**.
13. Expand **Other permissions** and enable **full_access_as_app**.

Microsoft Exchange Server 2016/2019/Office 365 (EWS) Installation and Configuration

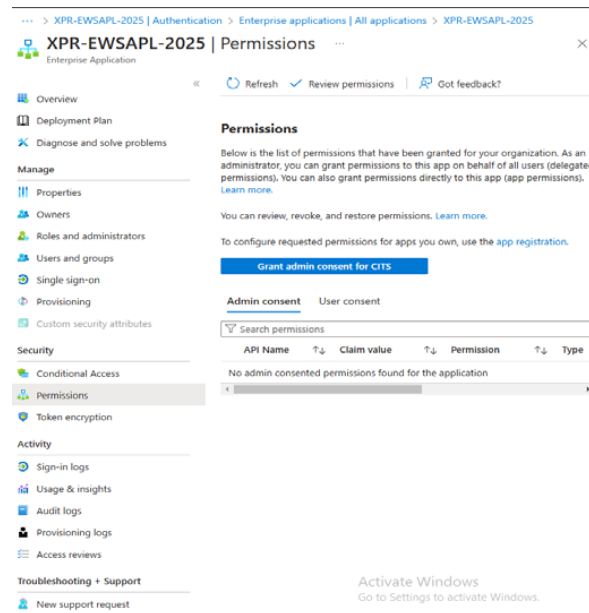


14. Click on the **Add permissions** button to add this permission and return to the previous screen.
15. Select the **Authentication** option on the left side menu.
16. In the **Advanced settings** section, change the **Allow public client flows** setting.
17. Set **Enable the following mobile and desktop flows** to **Yes**.

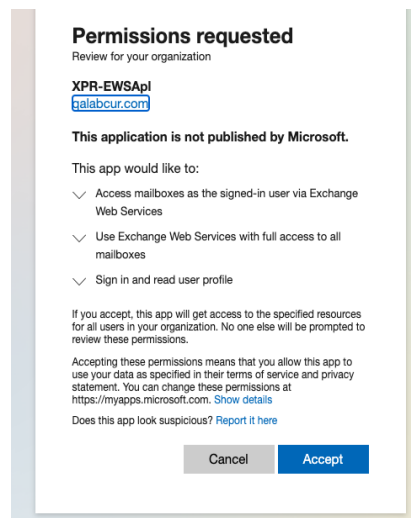


18. Click **Save**.

19. Navigate to **Applications** on the left **Home** menu and go to **Enterprise applications**
20. On **Manage** section, click on **All Applications**
21. Select the application you have created (e.g. **XPR-EWSApi**) from the application list
22. On the left side menu on **Security** section, click on the **Permissions** option.

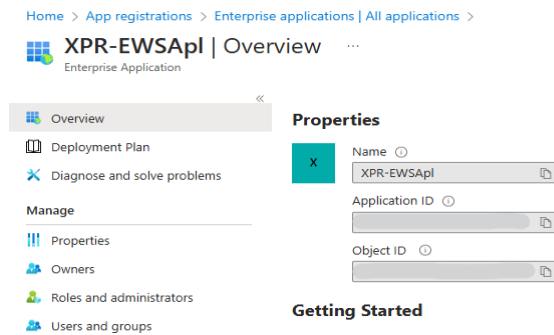


23. Click on **Grant admin consent for ...** button
24. Enter login of the user that has permissions for allowing the application to be used in the organization



25. Click on **Accept** button

26. Click on **Overview** on the left side menu of your interface and copy both the **Application ID** and **Object ID**. This information will be used on EWSApI settings to connect to the Exchange Server.



9.3.8.2 Powershell Configuration

First, use powershell to connect to the Office 365 tenant.

For more details, refer to: [Microsoft Documentation](#).

Then execute the steps below:

1. Create a new Service principal

```
New-ServicePrincipal -AppId <Application ID> -ObjectId  
<Object ID> -DisplayName "SP_XPR_EWSAPL"
```

More details at: [New Service Principal](#).

2. Create a new Role Assignment

```
New-ManagementRoleAssignment -App "SP_XPR_EWSAPL" -Role  
"Application EWS.AccessAsApp"
```

More details at: [New Role Assignment](#).

3. Test the Service principal access

```
Test-ServicePrincipalAuthorization -Identity  
"SP_XPR_EWSAPL" -Resource <user to test>
```

More details at: [Test Service Principal Access](#).

i.e. Testing if the example user [boline1@qalabcur.com](#) can be accessed using the SP_XPR_EWSAPL service principal:

```
Test-ServicePrincipalAuthorization -Identity  
"SP_XPR_EWSAPL" -Resource boline1@qalabcur.com
```


Cmd-let output:

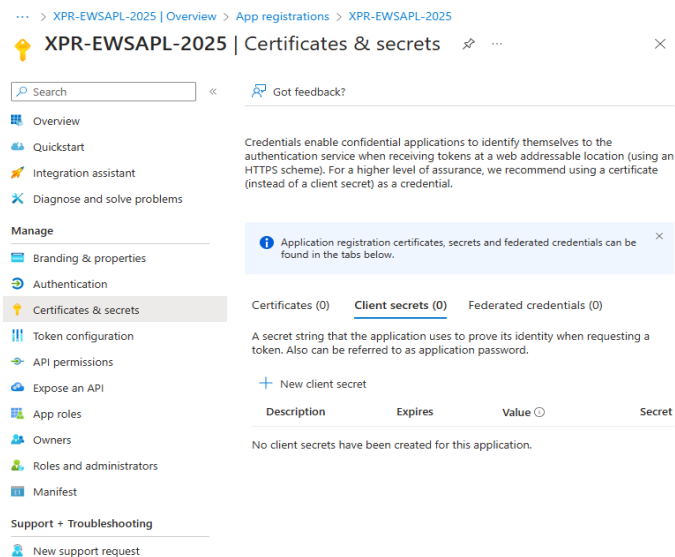
```
PS C:\Windows\system32> Test-ServicePrincipalAuthorization -Identity SP_XPR_EWSAPL_2025 -Resource online1@qalabcur.com

RoleName      GrantedPermissions      AllowedResourceScope      ScopeType      InScope
-----      -
Application  EWS.AccessAsApp        EWS.AccessAsApp           Organization    Organization    True
```

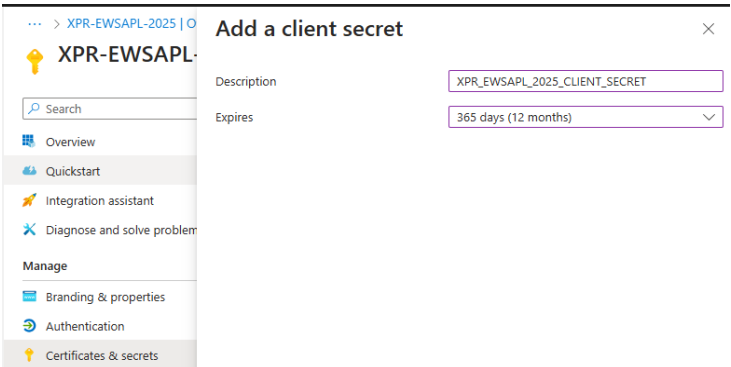
9.3.8.3 Client Secret Configuration

Return to Microsoft Entra admin center page then follow the steps below to set the Client Secret.

1. Go to **App registrations** under **Applications** on the left side menu and select your application.
2. From the left-hand side navigation panel, select **Certificates & secrets** under **Manager** section+

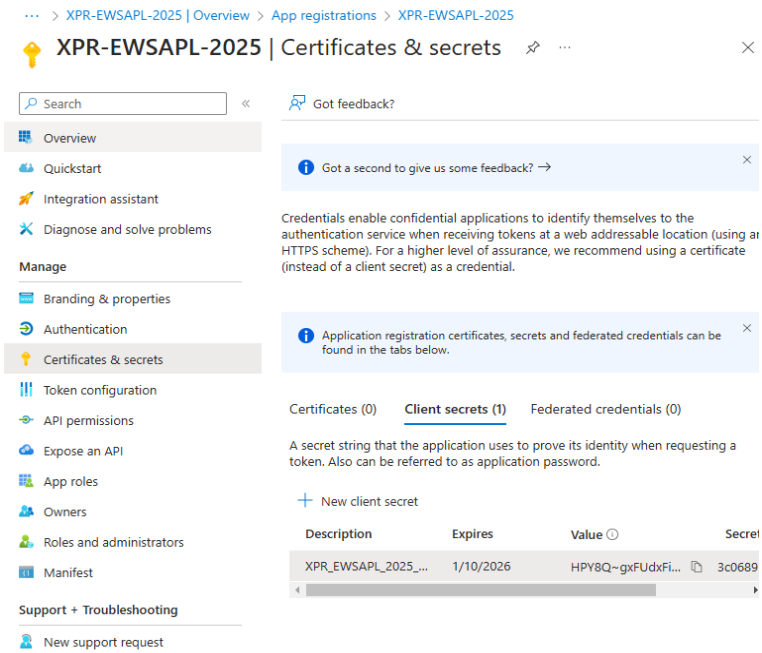


3. Under **Client secrets**, select **+ New client secret** to create a new client secret.
4. Enter a **Description** and specify the client secret **expiration** period desired and click on **Add** button.



5. Copy the content of the client secret **Value** to be used on the **EWSAPL Client Secret** setting.

NOTE: Please be aware that it is not the Secret ID that is used, but the **Value** field. And if this **Value** is not copied when the secret is created, it will not be possible to be copied after this time. You will need to create a new secret to be able to access the client secret **Value**.



Remarks:
According to Microsoft documentation: Changes to app permissions are subject to cache maintenance that varies between 30 minutes and 2 hours depending on

the app's recent usage. When testing configurations, the test command bypasses this cache. An app with no inbound calls to APIs will have its cache reset in 30 minutes, whereas an actively used app will keep its cache alive for up to 2 hours.

More details at: [Role Based Access Control for Applications in Exchange Online](#).

9.3.8.4 EWSApl Hotfix installation

IMPORTANT: The EWSApl hotfix must be installed only for the customers that already performed all the necessary adjusts in the Microsoft Entra admin center listed in the previous sections.

Do not apply EWSAplInstaller-FR5-20967 hotfix or newer if all the necessary changes were not performed.

After installing the latest version of EWSAPL the **Tenant ID** and **Client Secret** additional mandatory entries will be available for the new RBAC authentication method and also the **Test User** entry which is optional.

Microsoft Exchange Online Connection Configuration

Microsoft Exchange Online Connection Configuration

Service User

☐ Use Default credentials

☐ Use the following credentials

UPN: xprservice2022@qalabcu.com

Password:

☒ Use OAuth (Registration must have been completed first)

Redirect URI: urn:ietf:wg:oauth:2.0:oob

Client App ID: <Include your Application (Client) ID here>

Server Name: https://outlook.office365.com

Auth Authority: https://login.windows.net/common

Tenant ID: <Include your Directory (Tenant) ID here>

Client Secret: <Include your Application Client Secret here>

Test User: <Include an User e-mail address here to test the App access>

OAuth default settings

☐ Exchange On-Premises

Autodiscover

☐ Enable Autodiscover

Service URL: https://outlook.office365.com/EWS/Exchange.asmx O365 default URL

Example: https://mail.unifyoffice365.com/EWS/Exchange.asmx

Test Connection Restart Subscriptions More Options

Version 8.11.5.20961 OK Cancel Apply

To configure EWSAPL for Exchange online, please follow the steps below:

1. Open the XPR Monitor, login and navigate to **EwsApi > Edit Settings**.
2. On **Service User** select Use **OAuth (registration must have been completed first)**.
You can click on **OAuth default settings** button in order to fill the OAuth fields with the default settings.
3. Then specify the following mandatory information registered in the **Microsoft Entra admin center > App Registrations** page as described in the previous section:
 - **Client App ID** using the **Application (client) ID** from the MS Entra > **Overview** section
 - **Tenant ID** using the **Directory (tenant) ID** from the MS Entra > **Overview** section
 - **Client Secret** using the **Value** field of the Secret ID from the MS Entra > **Manage > Certificates & Secrets** section
4. **Test User** using a user from the MS Entra > **Users > All Users** section.

NOTE: In case of empty **test user** field, the UPN e-mail address value will be used for **Test Connection** button. To have a successful test connection result, the test user must have a mailbox.

5. Click **Apply**.

Note: You can check if the connection was successful by using the **Test Connection** button.

9.3.9 EWSApi "Service User" configuration

The following permissions must be granted to the Exchange service user:

<Send as> permission

The service user needs to have <Send As> permission on the Exchange On-Premises / Office 365 mailbox for the users to be integrated.

Exchange On-Premises

Please, check the following article (Example 1) to perform this step:

<https://technet.microsoft.com/en-us/library/bb124403%28v=exchg.160%29.aspx?f=255&MSPPErr=-2147217396>

Also, please, find below an example on how to set this permission for all users inside an Organizational Unit:

Get-Mailbox -OrganizationalUnit <OU name> | Add-ADPermission -User username -AccessRights ExtendedRight -ExtendedRights "send as"

Clutter

In order to ensure the clutter feature will not move our messages to the Clutter folder, follow the steps below:

1. On Exchange Admin Center, navigate to:
mail flow > rules > Create a new rule...
2. Name: ByPass Clutter for Xpr messages
3. Click **More options...**
 - a) Apply this rule if...: The sender's... domain is
 - b) Type the domain name of which **SMTPApi** is configured to send messages
(i.e. domain2016.com)
4. In the section **Do the following...** modify the Message properties
 - a) Set a message header
 - b) Type **X-MS-Exchange-OrganizationByPassClutter** in the message header
 - c) Type **true** in the header value
5. Audit this rule with severity level: Low
6. Leave the other fields with their default values
7. Click in the Save button.

https://2016exch.domain2016.net/?pwmcid=4&ReturnObjectType=1&id=4e9a73e8-e0b9-435d-8...

Xpressions ByPass Clutter

Name:
Xpressions ByPass Clutter

*Apply this rule if...
The sender's domain is... 'domain2016.net'
add condition

*Do the following...
Set the message header to this value... Set the message header 'X-MS-Exchange-OrganizationByPassClutter' to the value 'true'
add action

Except if...
add exception

Properties of this rule:
Priority:
3

☒ Audit this rule with severity level:
Low

Choose a mode for this rule:

Save Cancel

Additional details can be found:

[https://technet.microsoft.com/en-us/library/dn896639\(v=exchg.150\).aspx](https://technet.microsoft.com/en-us/library/dn896639(v=exchg.150).aspx)

NOTE: It is not mandatory that the service user account has a license assigned in Exchange On-Premises / Office 365 if the service account is able to perform log in and have the all the necessary permissions.

Throttling Policies

The <XPR service user> requires the creation of a client throttling policy:

On Exchange Management shell

- To create a Throttling Policy:

```
New-ThrottlingPolicy "XPR Throttling Policy" -
EWSThrottlingPolicy 3000 -EWSThrottlingPolicy Unlimited -
MessageRateLimit Unlimited -RecipientRateLimit Unlimited
```

```
New-ThrottlingPolicy "XPR Throttling Policy" -EWSThrottlingPolicy 3000 -
EWSThrottlingPolicy Unlimited -MessageRateLimit Unlimited -
RecipientRateLimit Unlimited
```

- 2 - To associate the Throttling policy to the service user

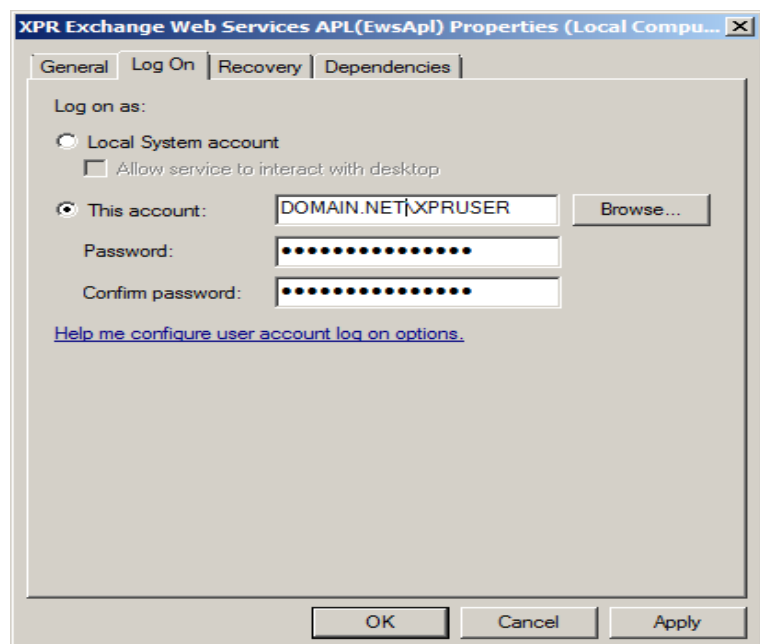
```
Set-Mailbox <XPR service user> -ThrottlingPolicy "XPR
Throttling Policy"
```

More details about throttling limits can be found

<https://msdn.microsoft.com/en-us/library/office/jj945066%28v=exchg.150%29.aspx?f=255&MSPPErr=-2147217396>

9.3.10 "Windows Service" Configuration

The user configured to run EwsApl service can be the same user other Xpressions services run under.



9.3.11 Configuring SmtplApi

Configure on the 'Microsoft Exchange Web Services' tab the service user account of the MS Exchange Online/On-Premises server:

The screenshot shows the 'SMTP APL configuration' dialog box with the 'Microsoft Exchange Web Services' tab selected. The 'Exchange Service User' section contains the following fields:

Field	Value
User:	newadm2016@domain2016.net
Password:	••••••••
Server:	2016exch.domain2016.net
Port:	25

At the bottom of the dialog, there are 'OK', 'Cancel', and 'Apply' buttons, and a version number 'Version 8.11.5.18729'.

NOTE: Only for User who has configured the OFF365 field the "Microsoft Exchange Web Services" setting will be used to send messages via SMTP.

For User without a value in OFF365 the default values from SmtplApi for outbound mails will be used.

NOTE: "Secure Sockets" (TLS) must be setup in additional depending on the requirements from the Exchange Server. See also Exchange Connector Settings.

NOTE: To enable Office 365 integration, the user specified on the Microsoft Exchange Web Services tab must have a valid Microsoft Office 365 license assigned in the Microsoft 365 admin center. Without this license, synchronization between Xpressions and Office 365 will fail, as the user's SmtplApi authentication in Office 365 cannot be performed.

9.3.12 Configuring MTA Routing Rules

SmtpApl will route Voicemails and Faxes to Exchange Online using the MTA Carbon Copy rules. The following CC rules have to be configured for that purpose:

CC rule for VoiceMails:

```
NVS:*/*[ORG=NVS:VOICE/*]=NVS:SMTP/  
<DB,MAILBOX,OFF365>[FLAG=NOPREFERRED]
```

CC rule for Faxes:

```
NVS:*/*[ORG=NVS:FAXG3/*]=NVS:SMTP/  
<DB,MAILBOX,OFF365>[FLAG=NOPREFERRED]
```

Important Note:

When the 'CarbonMode' registry entry in

```
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\PP-COM\MRS\MTA\Rules
```

is set to **DOC,REPORT**, it is necessary to modify the **CarbonCopy Rules** for Ews-Users to CC rule for VoiceMails:

```
NVS:*/*[ORG=NVS:VOICE/*;TYPE!=REPORT]=NVS:SMTP/  
<DB,MAILBOX,OFF365>[FLAG=NOPREFERRED]
```

CC rule for Faxes:

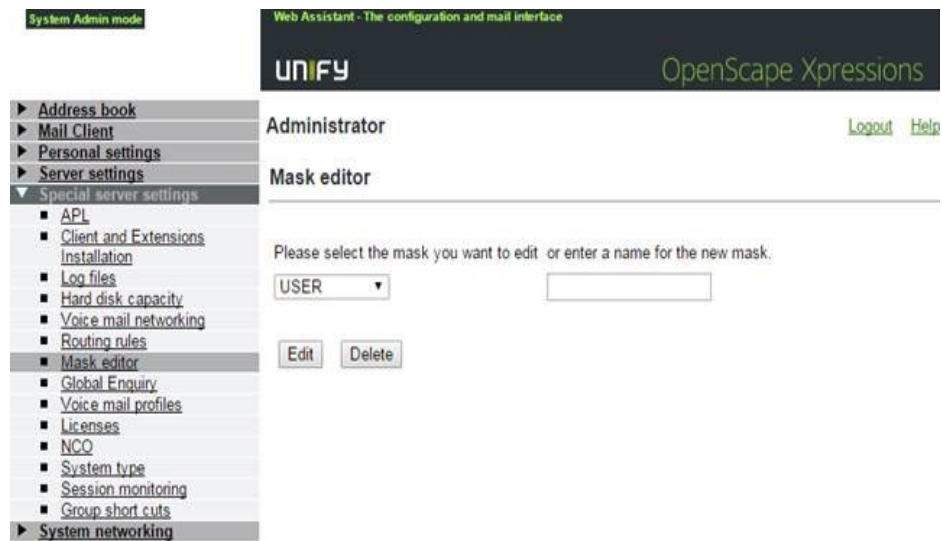
```
NVS:*/*[ORG=NVS:FAXG3/*;TYPE!=REPORT]=NVS:SMTP/  
<DB,MAILBOX,OFF365>[FLAG=NOPREFERRED]
```

9.3.13 User Mask Configuration

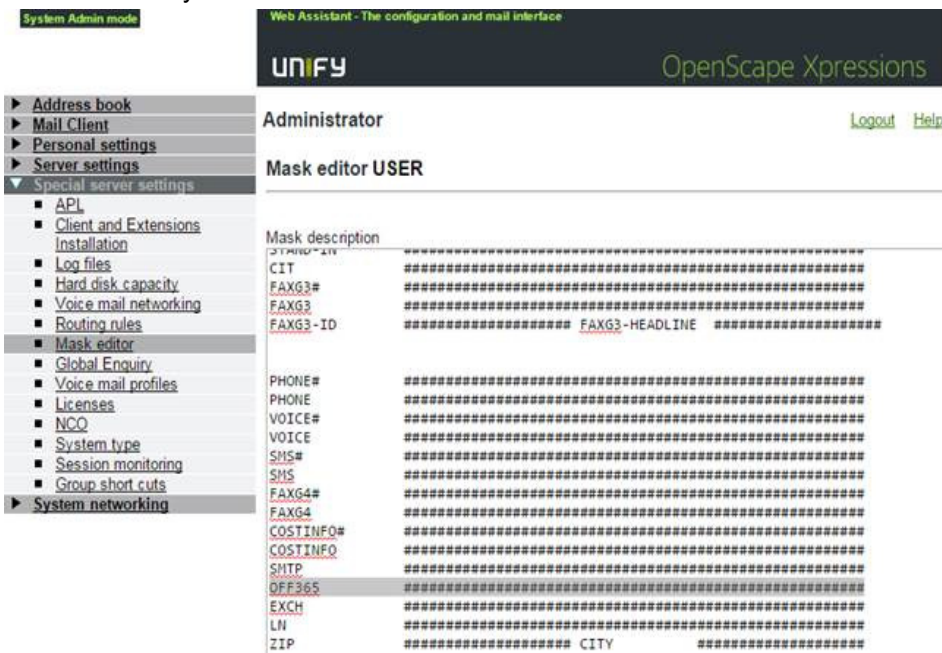
To configure User Mask, follow the steps below:

1. On WebAssistant log on as **ADMINISTRATOR**;
2. Select **Special Server Settings**;
3. Select **Mask Editor**;
4. In the mask combo box select **USER** and click **Edit**:

Microsoft Exchange Server 2016/2019/Office 365 (EWS)
Installation and Configuration



5. Add an entry for **OFF365** field:



6. Scroll down and click **Check mask description**:

Microsoft Exchange Server 2016/2019/Office 365 (EWS)

Installation and Configuration

System Admin mode

Web Assistant - The configuration and mail interface

UNIFY OpenScape Xpressions

Administrator [Logout](#) [Help](#)

COMPANY #####
 DIVISION #####
 ADDR1 #####
 ADDR2 #####
 REMARK #####
 PRIVTEL# #####
 PRIVTEL #####
 PRIVFAX# #####
 PRIVFAX #####
 GSM# #####
 GSM #####
 KEYWORD #####
 TCP/IP #####
 PRINTER #####
 PMI-SCHEDULE #####
 PMI-HOSTNAME #####
 PMI-USERNAME #####
 PMI-PASSWORD #####

Field attributes

Field name	Upper/lower case	Dial number	Privilege	Hide	Encrypt

- Look for **OFF365** entry and select **LOWER** in the first combo box:

System Admin mode

Web Assistant - The configuration and mail interface

UNIFY OpenScape Xpressions

Administrator [Logout](#) [Help](#)

LN UPPER

LOGON_MODE UPPER PSUPER

MAILBOX UPPER

MAX_MONITOR PSUPER

NAME

NCO_GUI_CONN_PT PSUPER

NCO_GUI_PREFIX PSUPER

NCO_LOCATION PSUPER

NCO_TUI_CONN_PT PSUPER

NCO_TUI_PREFIX PSUPER

NO_REPLICATION PSUPER

OFF365 LOWER

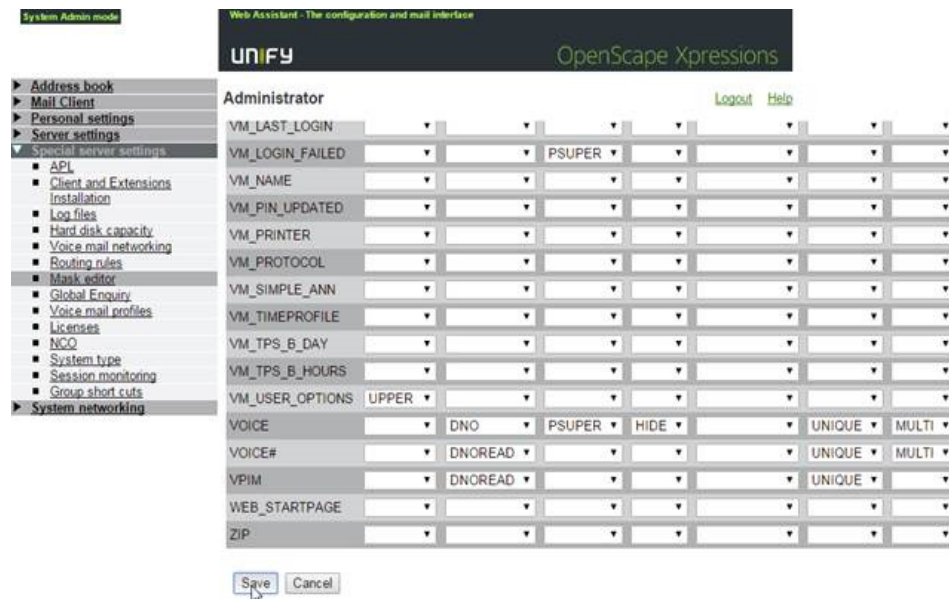
OS_SPEECHENABLE LOWER

PAGERSET_01 UPPER PSUPER

PAGERSET_02 PSUPER

PAGERSET_03 PSUPER

- Click **Save**



9.3.14 Configuring Users

If the users already exist on the XPR system and have been migrated from Exchange Online/Exchange 2016/2019, some configurations must be changed for the new integration.

The users which will use the Exchange Online/On-Premises integration should have the notification and MWI activated for at least one type of message and the Preferred Address must be changed to <Internal Mailbox>.

Also, the new field <OFF365> has to contain the Exchange Online/On-Premises e-mail address for this user (i.e. *user1@domain2016.com*)

9.3.14.1 Users synchronization between Xpressions and Active Directory (via LDAP)

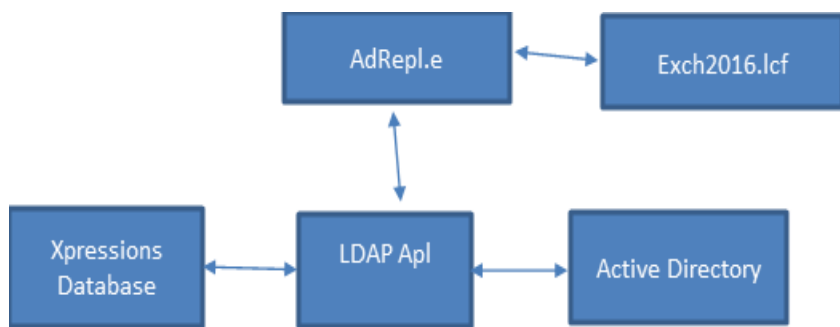
Automatic users replication between the Active Directory and the Xpressions System may be implemented using the LDAPApI. For that purpose, there are some adjustments to be done on the LDAPApI configuration.

The Exch2016.lcf configuration file, created for that purpose, along with the Exch2016repl.e script is the suggested way to perform the mapping of the Active Directory user properties with the correspondent correlation database entries on the Xpressions system.

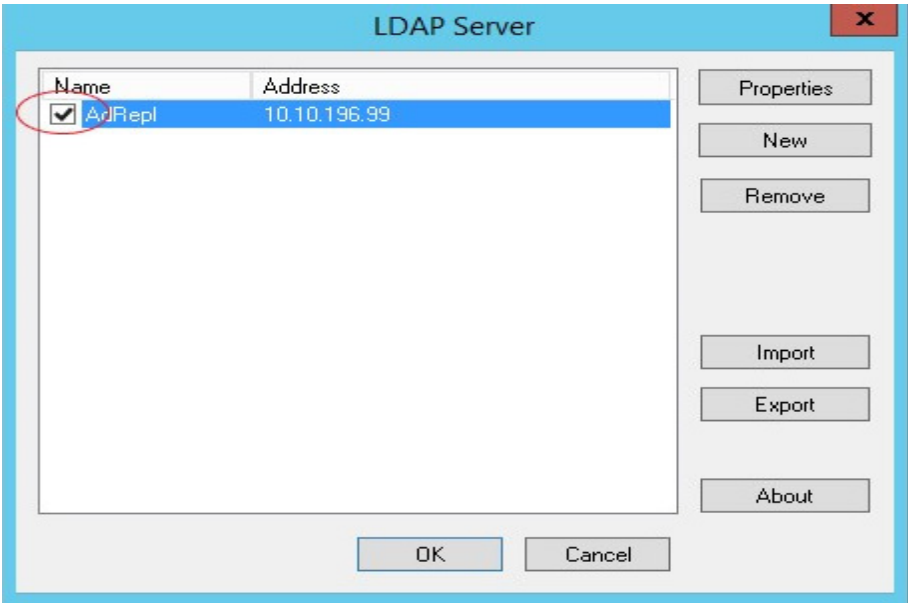
NOTE: Mapping ExtensionData within an office 365 environment and smtp connector doesn't make sense and should not be used. Without an existing ExchApl the Extensions-Data (MRS-Tab) cannot be used.

NOTE: The Exch2016.lcf use **exch2016repl.e** instead of **adrepl.e**.

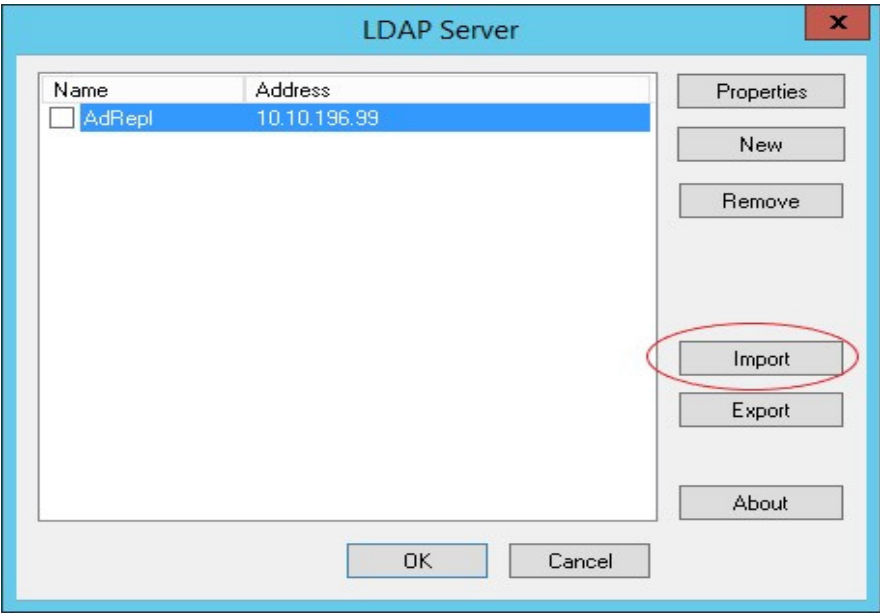
The following steps detail the procedure to configure the LDAPApl for integration of the Exchange 2016/2019 On-Premises for new users and/or migrated users from previous versions of Exchange Servers to the Exchange 2016/2019 On-Premises.



1. Install **LDAPApl** hotfix (LdapApl-811FR5-20005 or newer);
2. On **LdapApl** configuration, disable the current replication script:



3. Import the **Exch2016.lcf** configuration file
(Installed by the LdapApl hotfix on the path `xpr\res\ldap`):



4. Configure the respective connection parameters:

New server settings (imported).

Login
Entries concerning the localization and the user authentication of the DS server. The logical name must be unique.

Logical name: Exchange 2016

Server IP address: 10.10.196.99

Port number: 389 ☐ Secure

Directory type: Active Directory

DS User Account

User Name: administrator

Password: ••••••••

Domain: XPR_DOMAIN

Authentication type: NTLM

Test connection Query DS Attributes

Version 8.11.42.20005 OK Cancel Apply

- Specify the users that will be synchronized on the **Search** tab and configure the replication parameters

Search
List of directories searched. Directory names will be written as LDAP Distinguished Names.

Search Directories

- ☐ OU=XPR
 - ☐ CN=User 7000
 - ☐ CN=User 8000
 - ☐ CN=User 8001
 - ☒ CN=User 8002
 - ☐ CN=User 8003
 - ☐ CN=User 8004
 - ☐ CN=User 8005
 - ☐ CN=User 8006
 - ☐ CN=User 8007

Properties New Remove

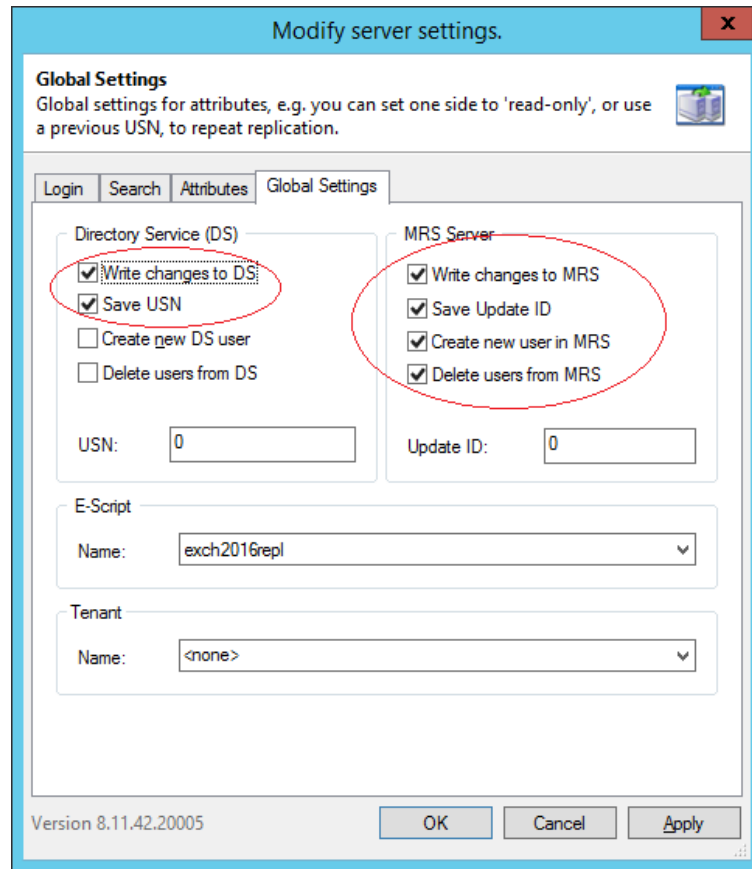
Max. search duration (sec): 120 Replicate now

Entries per page: 64

☒ Polling interval (sec): 0 Schedule

Version 8.11.42.20005 OK Cancel Apply

6. Set the **LdapApi** Global Settings as desired:



9.3.14.2 Importing Exchange Users from Active Directory

If the Exchange users are not on a reachable Active Directory (i.e. Office 365), there is an alternative way to import those users to the Xpressions database. However, there will be no synchronization between original users and the imported ones. Therefore, this should be used only as a temporary solution.

The users may be gathered using powershell scripts provided along with the EwsApi

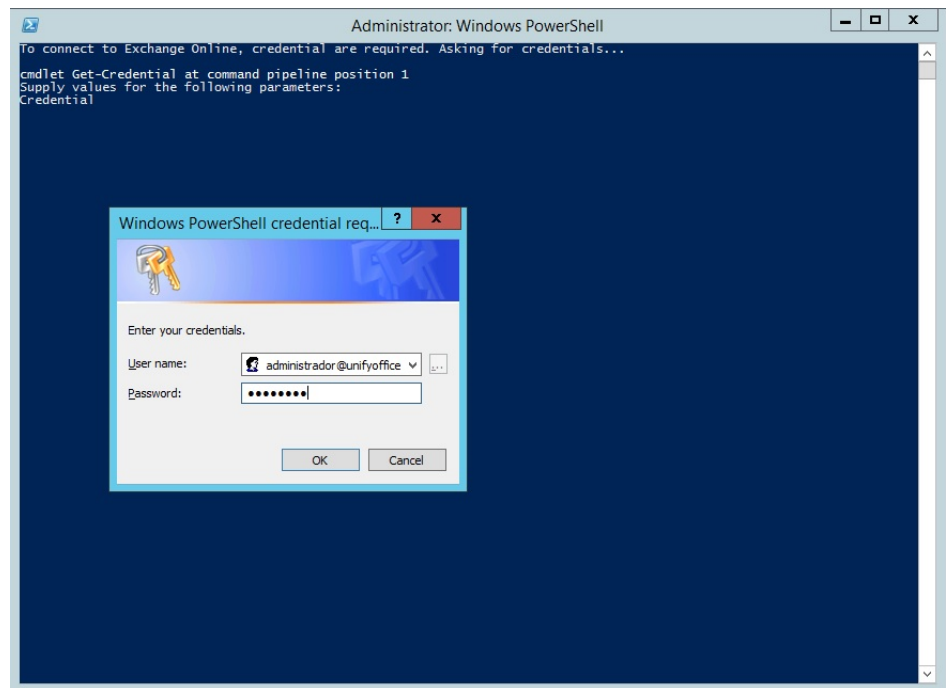
9.3.14.3 Importing users using Powershell scripts

After installing the EwsApiInstaller hotfix on the system, the scripts

- Connect-OnPremises.ps1
- Get-OnPremises-Users.ps1

- Connect-O365.ps1
- Get-O365-Users.ps1
will be available on the path <XPRInstall>\xpr\bin.

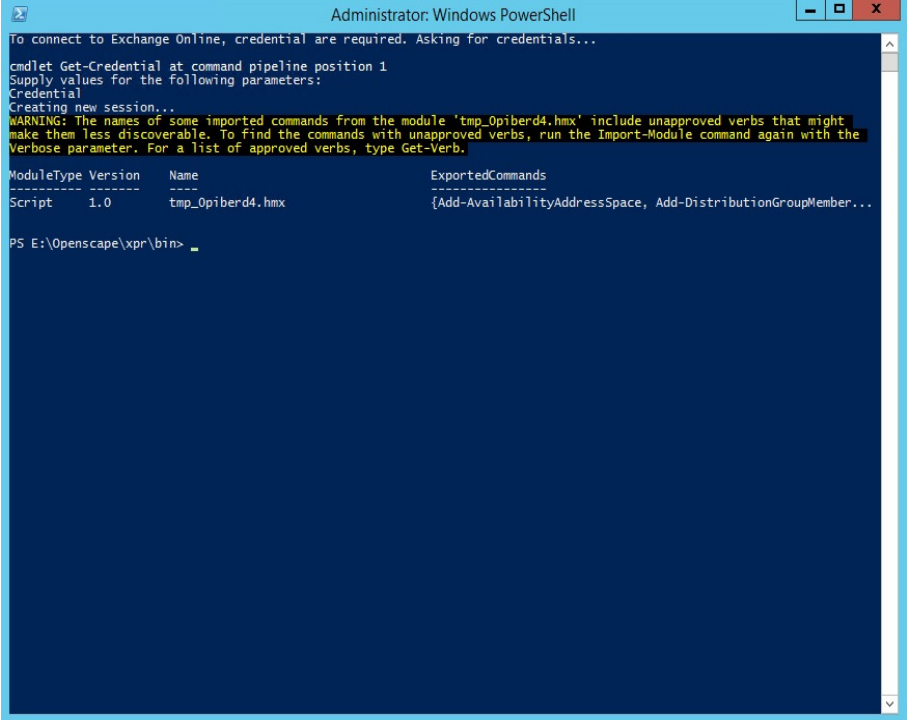
To collect the users from the Exchange server, please, open a PowerShell instance and run the scripts according to your environment.



Then, the user will be prompted to enter the credentials for an Office 365/Exchange 2016/2019 On-Premises administrator user.

If the user has the required rights, the following prompt should be presented to the user:

Microsoft Exchange Server 2016/2019/Office 365 (EWS) Installation and Configuration



```
Administrator: Windows PowerShell

To connect to Exchange Online, credential are required. Asking for credentials...

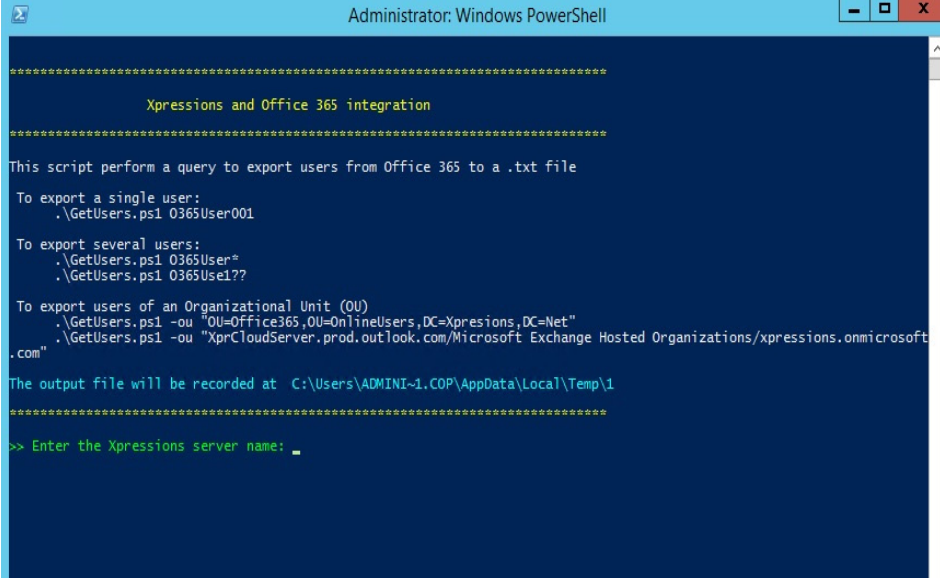
cmdlet Get-Credential at command pipeline position 1
Supply values for the following parameters:
Credential
Creating new session...
WARNING: The names of some imported commands from the module 'tmp_Opiberd4.hmx' include unapproved verbs that might make them less discoverable. To find the commands with unapproved verbs, run the Import-Module command again with the Verbose parameter. For a list of approved verbs, type Get-Verb.

ModuleType Version      Name                               ExportedCommands
-----
Script      1.0          tmp_Opiberd4.hmx                  {Add-AvailabilityAddressSpace, Add-DistributionGroupMember...

PS E:\Openscape\xpr\bin>
```

At this point, the PowerShell is connected to the Exchange Online/On-Premises and may run commands directly on the Exchange Server.

Now, on the same PowerShell instance, run the
<Get- Get-OnPremises|OFF365-Users.ps1>
script, which should result in the following screen:



```
Administrator: Windows PowerShell

*****
Xpressions and Office 365 integration
*****

This script perform a query to export users from Office 365 to a .txt file

To export a single user:
.\GetUsers.ps1 0365User001

To export several users:
.\GetUsers.ps1 0365User*
.\GetUsers.ps1 0365Use1??

To export users of an Organizational Unit (OU)
.\GetUsers.ps1 -ou "OU=Office365,OU=OnlineUsers,DC=Xpressions,DC=Net"
.\GetUsers.ps1 -ou "XprCloudServer.prod.outlook.com/Microsoft Exchange Hosted Organizations/xpressions.onmicrosoft.com"

The output file will be recorded at C:\Users\ADMINI~1\COP\AppData\Local\Temp\1

*****
>> Enter the Xpressions server name: _
```

Follow the script instructions:

```

Administrator: Windows PowerShell

*****
Xpressions and Office 365 integration
*****

This script perform a query to export users from Office 365 to a .txt file

To export a single user:
.\GetUsers.ps1 0365User001

To export several users:
.\GetUsers.ps1 0365User*
.\GetUsers.ps1 0365Use1??

To export users of an Organizational Unit (OU)
.\GetUsers.ps1 -ou "OU=Office365,OU=OnlineUsers,DC=Xpresions,DC=Net"
.\GetUsers.ps1 -ou "XprCloudServer.prod.outlook.com/Microsoft Exchange Hosted Organizations/xpressions.onmicrosoft.com"

The output file will be recorded at C:\Users\ADMINI~1\COP\AppData\Local\Temp\1

*****
>> Enter the Xpressions server name: XPR0365
>> Select an option:
-OU
or [enter] for default option (single or several users): -ou

The following Organizational Units are available:

LAMP80A002.prod.outlook.com/Microsoft Exchange Hosted Organizations/xprdev.onmicrosoft.com
LAMP80A002.prod.outlook.com/Microsoft Exchange Hosted Organizations/xprdev.onmicrosoft.com/Soft Deleted Objects

>> Enter the Name of the Organization Unity (OU) to import: LAMP80A002.prod.outlook.com/Microsoft Exchange Hosted Organizations/xprdev.onmicrosoft.com
OU option selected

There were 42 entries found

To create the file E:\Openscape\xpr\bin\EWSapUsersToImport.txt
Press [ enter ] or press [ ctrl + c ] to end the script
-
  
```

Output file default option

If you chose the default option, the result of this process should be a text file like this:

Microsoft Exchange Server 2016/2019/Office 365 (EWS)

Installation and Configuration

```
EWSApiUsersToImport - Notepad
File Edit Format View Help
XPRO365 USER E2K1340 MAILBOX E2K1340
XPRO365 USER E2K1340 NAME E2K1340
XPRO365 USER E2K1340 PASSWORD RIAQaHY9aaCvTfg1l4mwV+ifQGr15h4F7vI9Ovtp3G0,2015.09.28 22:08:21
XPRO365 USER E2K1340 NOT_ACTIVE 2
XPRO365 USER E2K1340 NOT_LAG 5
XPRO365 USER E2K1340 NOT_SHORTLAG 1
XPRO365 USER E2K1340 NOT_MWI.01 VOICE
XPRO365 USER E2K1340 PREFERRED MAILBOX
XPRO365 USER E2K1340 OFF365 E2K1340@unifyoffice365.com
XPRO365 USER E2K1340 GROUP USER
XPRO365 USER E2K1341 MAILBOX E2K1341
XPRO365 USER E2K1341 NAME E2K1341
XPRO365 USER E2K1341 PASSWORD RIAQaHY9aaCvTfg1l4mwV+ifQGr15h4F7vI9Ovtp3G0,2015.09.28 22:08:21
XPRO365 USER E2K1341 NOT_ACTIVE 2
XPRO365 USER E2K1341 NOT_LAG 5
XPRO365 USER E2K1341 NOT_SHORTLAG 1
XPRO365 USER E2K1341 NOT_MWI.01 VOICE
XPRO365 USER E2K1341 PREFERRED MAILBOX
XPRO365 USER E2K1341 OFF365 E2K1341@unifyoffice365.com
XPRO365 USER E2K1341 GROUP USER
XPRO365 USER E2K1342 MAILBOX E2K1342
XPRO365 USER E2K1342 NAME E2K1342
XPRO365 USER E2K1342 PASSWORD RIAQaHY9aaCvTfg1l4mwV+ifQGr15h4F7vI9Ovtp3G0,2015.09.28 22:08:21
XPRO365 USER E2K1342 NOT_ACTIVE 2
XPRO365 USER E2K1342 NOT_LAG 5
XPRO365 USER E2K1342 NOT_SHORTLAG 1
XPRO365 USER E2K1342 NOT_MWI.01 VOICE
XPRO365 USER E2K1342 PREFERRED MAILBOX
XPRO365 USER E2K1342 OFF365 E2K1342@unifyoffice365.com
XPRO365 USER E2K1342 GROUP USER
XPRO365 USER E2K1343 MAILBOX E2K1343
XPRO365 USER E2K1343 NAME E2K1343
XPRO365 USER E2K1343 PASSWORD RIAQaHY9aaCvTfg1l4mwV+ifQGr15h4F7vI9Ovtp3G0,2015.09.28 22:08:21
XPRO365 USER E2K1343 NOT_ACTIVE 2
XPRO365 USER E2K1343 NOT_LAG 5
XPRO365 USER E2K1343 NOT_SHORTLAG 1
XPRO365 USER E2K1343 NOT_MWI.01 VOICE
```

Use the infotool to import this information into the XPR system.

CSV option

If you select the option -CSV, a new csv file containing the selected users will be created at the specified folder.

```
PREFERRED MAILBOX
OFF365 user1097@domain2016.net
GROUP USER
NOT_SHORTLAG 1
PASSWORD RIAQaHY9aaCvTfg1l4mwV+ifQGr15h4F7vI9Ovtp3G0,2015.09.28 22:08:21

Server: XPR2016
ClassName: USER
Class: DOMAIN2016.NET/USERS/USER1098
MAILBOX DOMAIN2016.NET/Users/user1098
NAME user1098
NOT_ACTIVE 2
NOT_LAG 5
NOT_MWI.01 VOICE
PREFERRED MAILBOX
OFF365 user1098@domain2016.net
GROUP USER
NOT_SHORTLAG 1
PASSWORD RIAQaHY9aaCvTfg1l4mwV+ifQGr15h4F7vI9Ovtp3G0,2015.09.28 22:08:21

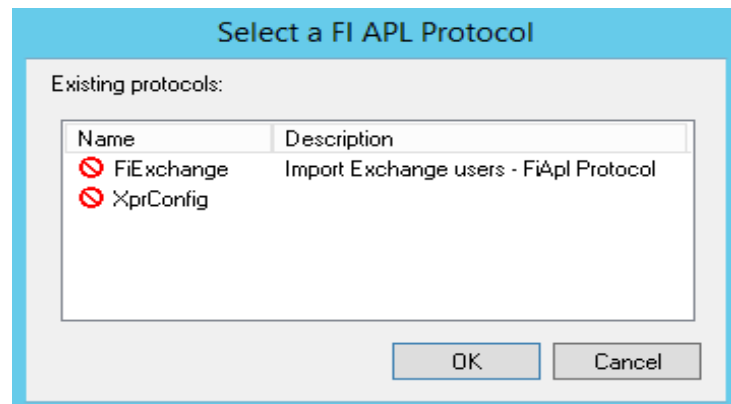
Server: XPR2016
ClassName: USER
Class: DOMAIN2016.NET/USERS/USER1099
MAILBOX DOMAIN2016.NET/Users/user1099
NAME user1099
NOT_ACTIVE 2
NOT_LAG 5
NOT_MWI.01 VOICE
PREFERRED MAILBOX
OFF365 user1099@domain2016.net
GROUP USER
NOT_SHORTLAG 1
PASSWORD RIAQaHY9aaCvTfg1l4mwV+ifQGr15h4F7vI9Ovtp3G0,2015.09.28 22:08:21

File EWSApiUsersToImport.csv recorded with 10 users
To open the file C:\OpenScope\xpr\bin\EWSApiUsersToImport.csv
Press [ enter ] to open the file or press [ ctrl + c ] to end the script
```

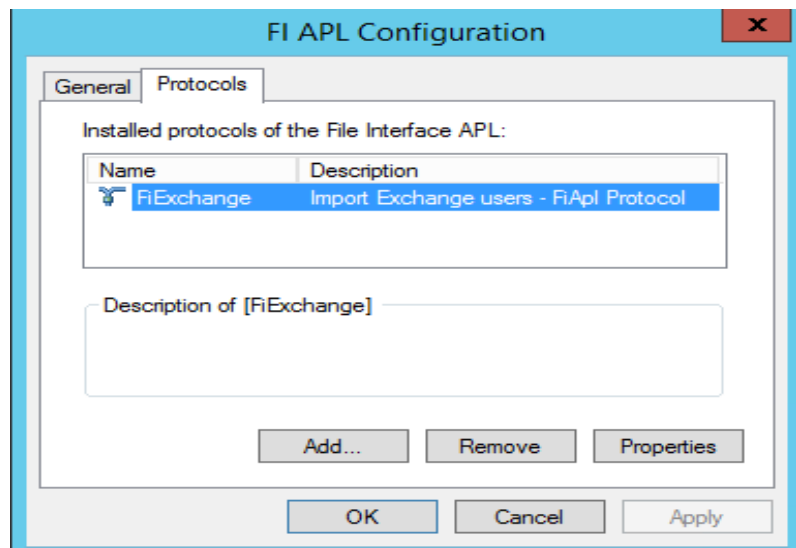
9.3.14.4 Importing users with FiApl

To import a user with **FiApl**, follow the steps below:

1. Open **FI APL Configuration**
2. Navigate to the **Protocols** section.
3. Click **Add**.
4. Select the option **FiExchange**



5. Click the **Apply** button
6. Select the **FiExchange** protocol and click **Properties**



7. Specify the poll directory

The screenshot shows a Windows-style dialog box titled "Properties of [FiExchange]". It is divided into two main sections: "Host -> FI APL" and "FI APL -> Host".

Host -> FI APL section:

- Poll directory:** Text box containing "C:\Temp\NewUsers\"
- Body directory:** Text box containing "C:\Temp\NewUsers\"
- Poll rate (sec.):** Text box containing "30"
- Max. docum. per poll:** Text box containing "128"
- Header pattern:** Text box containing "*.csv"
- Check privileges:** Unchecked checkbox
- Delete header:** Unchecked checkbox
- Edit script:** Button

FI APL -> Host section:

- Incoming messages:**
 - Activate:** Checked checkbox
 - Suffix:** Text box
 - Fax format:** Dropdown menu showing "TIFF Fax"
- Reports:**
 - Filter:** Dropdown menu showing "All"
 - Suffix:** Text box
- Header directory:** Text box
- Body directory:** Text box

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

8. Click **OK**.

9.3.15 Registry Settings (Additional setting of EwsApi)

Autodiscover / REG_DWORD

Default Value: 0

Description: Specify if autodiscover will be used to get the office365/Exchange On-Premises service URL.

Autodiscover_URL / REG_SZ

Default Value: none.

Description: service URL Office 365/Exchange On-Premises used to communicate with Exchange Web Services.

Credentials / REG_SZ

Default Value: Web

Description: Specify which kind of credentials are used to communicated with Office 365/Exchange On-Premises.

Service_User / REG_SZ

Default Value: None.

Description: E-mail of the service user used to authenticate with Office 365/Exchange On-Premises.

SubscriptionTimeout / DWORD

Default Value: 1440

Description: value (in minutes) the subscriptions must be renewed. The maximum time accepted is 24 horas (1440 minutes).

WaitTimeAfterSubscriptionExpire / DWORD

Default Value: 30

Description: value (in seconds) the EwsApl waits before getting events from Office 365 inbox changes.

WaitTimeBetweenCheckHealth / DWORD (default value 20)

Used to specify the interval (in minutes) the Apl will check the delay of the transaction that were not processed yet

MaxDelayTransaction / DWORD (default value 30)

Used to specify the maximum acceptable time (in minutes) for the transaction processing. The time starts counting when the Apl receives the transaction until the transaction is processed completely (i.e. set the message as read in the Exchange Server). If the system is overloaded or the Exchange Server is taking too much time to answer the requests it can be used to identify the system is degraded.

MaxTransactionsDelaySize / DWORD (default value 10)

Used to specify the maximum quantity of transactions the system can continue to run. If there are **MaxTransactionsDelaySize** transactions that were not answered by up to **MaxDelayTransaction**, the restart procedure of the Apl will be initiated.

NumberOfThreads / DWORD

Default Value: Number of monitored users divided by 50. If the result is lower than the number of cores of the machine, the number of cores of the machine will be used as default parameter.

Description: amount of connections that will be created to check notifications events in Exchange Online/Exchange On-Premises. Calculate around 50 users per thread. E.g: if you have 1000 users, 20 threads are recommended.

TransactionThreads / DWORD

Default Value: number of cores of the system.

Description: number of threads that will be used for handling transactions received from the backend (MailApl). The default value is the number of the cores of the system.

MonitorJunkFolder / DWORD

Default Value: false

Description: If true, EWSApl monitors changes in the junk folder of the Exchange 2016/2019 users.

DisableMailboxRules / DWORD

Default Value: false

Description: If enabled (true), all folders used in the user's Inbox rules will be monitored. The default value is false.

EWSTraceEnable / DWORD

Default Value: 0

Description: enable traces of Web Services HTTPS requests/responses. When enabled, the traces are stored at <XPR Installation Folder>\Log\EWSTraces\<DATE_HOUR_MILLISECOND> log folder.

Important Note:

the Web Services HTTPS requests/responses **must only be enabled** for advanced troubleshooting purposes due to the high number of created files.

NewMailEvent/ DWORD

Default Value: false

Description: If enabled (true), all the event for NewMail received in the user's folders monitored will generate a notification to the EWSApl. The default value is false.

Note: this setting is recommended for troubleshooting purposes due to the high number of generated events.

OAuth_AuthAuthority

Type: REG_SZ

Default Value: none,

Description: Azure active directory authorization endpoint uRI.

OAuth_CliApplId

Type: REG_SZ

Default Value: none

Description: The client id assigned to the registered application.

OAuth_RedirURI

Type: REG_SZ

Default Value: none

Description: Developer defined redirect Uri.

OAuth_Server

Type: REG_SZ

Default Value: none

Description: Connection Uri.

OnPremises/ DWORD

Default Value: false

Description: If enabled (true), it indicates the connection will be done to Exchange server 2016. The default value is false.

CycleCount / DWORD

Default value: 3

Description: this is an internal configuration. Please change it only with development advice.

WaitTimeBeforeCallGC/ DWORD

Default value: 15

Description: this is an internal configuration. Please change it only with development advice.

WaitTimeBetweenGetEvent/ DWORD

Default value: 200

Description: this is an internal configuration. Please change it only with development advice.

WaitTimeAfterTimeOut/ DWORD

Default value: 60

Description: this is an internal configuration. Please change it only with development advice.

9.4 Distributed EWSApls

The EWSApl can be installed on the kernel and on Satellites.

To specify which users will be associated with the Apls, it is necessary to specify in the correlation database the index of the Apl the user is associated with.

The following correl entry must be created for that purpose:

<SYSTEM_NAME> USER<USERNAME> SAT_IDX<Index>

<SYSTEM_NAME>	USER	<USERNAME>	SAT_IDX	<Index>

i.e.

XPR0365	USER	XPRUSER1	SAT_IDX	1

If the user does not have the SAT_IDX correlation entry or the value is 0, it will be associated with the EwsApl located at the Xpressions Kernel.

NOTE: EWSApl uses pull subscriptions to keep Xpressions and Exchange On-Premises mailboxes synchronized. The subscription can be alive up to 1440 minutes (24 hours) without the need of renewing the subscription. Microsoft recommends pull subscription for loosely coupled clients, where the client is not reliably connected to the network.

Although EWSApl can handle up to 5000 users , we recommend a maximum of 3000 users per EWSApl/Service user to receive the Exchange On-Premises events in an acceptable time.

CC rule for Distributed Smtpl

Example with 5 Smtpl: kernel and 4 satellites:

; VOICE CC Rules

```
NVS:*/*[ORG=NVS:VOICE/*;RECDB(PREFERRED)=MAILBOX;RECDB(SAT_IDX)=]=NVS:SMTP/<DB,MAILBOX,OFF365>[FLAG=NOPREFERRED] "VOICE rule Kernel without SAT_IDX entry"
```

```
NVS:*/*[ORG=NVS:VOICE/*;RECDB(PREFERRED)=MAILBOX;RECDB(SAT_IDX)=0]=NVS:SMTP/<DB,MAILBOX,OFF365>[FLAG=NOPREFERRED] "VOICE rule Kernel"
```

```
NVS:*/*[ORG=NVS:VOICE/*;RECDB(PREFERRED)=MAILBOX;RECDB(SAT_IDX)=1]=NVS:SMTP.1/<DB,MAILBOX,OFF365>[FLAG=NOPREFERRED] "VOICE rule Satellite 1"
```

```
NVS:*/*[ORG=NVS:VOICE/*;RECDB(PREFERRED)=MAILBOX;RECDB(SAT_IDX)=2]=NVS:SMTP.2/<DB,MAILBOX,OFF365>[FLAG=NOPREFERRED] "VOICE rule Satellite 2"
```

```
NVS:*/*[ORG=NVS:VOICE/*;RECDB(PREFERRED)=MAILBOX;RECDB(SAT_IDX)=3]=NVS:SMTP.3/<DB,MAILBOX,OFF365>[FLAG=NOPREFERRED] "VOICE rule Satellite 3"
```

```
NVS:*/*[ORG=NVS:VOICE/*;RECDB(PREFERRED)=MAILBOX;RECDB(SAT_IDX)=4]=NVS:SMTP.4/<DB,MAILBOX,OFF365>[FLAG=NOPREFERRED] "VOICE rule Satellite 4"
```

; FAX CC Rules

```
NVS:*/*[ORG=NVS:FAX/*;RECDB(PREFERRED)=MAILBOX;RECDB(SAT_IDX)=]=NVS:SMTP/<DB,MAILBOX,OFF365>[FLAG=NOPREFERRED] "FAX rule Kernel without SAT_IDX entry"
```

```
NVS:*/*[ORG=NVS:FAX/*;RECDB(PREFERRED)=MAILBOX;RECDB(SAT_IDX)=0]=NVS:SMTP/<DB,MAILBOX,OFF365>[FLAG=NOPREFERRED] "FAX rule Kernel"
```

```
NVS:*/*[ORG=NVS:FAX/*;RECDB(PREFERRED)=MAILBOX;RECDB(SAT_IDX)=1]=NVS:SMTP.1/<DB,MAILBOX,OFF365>[FLAG=NOPREFERRED] "FAX rule Satellite 1"
```

```
NVS:*/*[ORG=NVS:FAX/*;RECDB(PREFERRED)=MAILBOX;RECDB(SAT_IDX)=2]=NVS:SMTP.2/<DB,MAILBOX,OFF365>[FLAG=NOPREFERRED] "FAX rule Satellite 2"
```

```
NVS:*/*[ORG=NVS:FAX/*;RECDB(PREFERRED)=MAILBOX;RECDB(SAT_IDX)=3]=NVS:SMTP.3/<DB,MAILBOX,OFF365>[FLAG=NOPREFERRED] "FAX rule Satellite 3"
```

```
NVS:*/*[ORG=NVS:FAX/*;RECDB(PREFERRED)=MAILBOX;RECDB(SAT_IDX)=4]=NVS:SMTP.4/<DB,MAILBOX,OFF365>[FLAG=NOPREFERRED] "FAX rule Satellite 4"
```


10 Sending Faxes from Exchange to Xpressions

To send faxes from accounts hosted on Exchange 2016/2019/Exchange Online into the Xpressions system, some extra configurations are mandatory, as follows.

Supposing the syntax of fax recipient is:

FAXG3/<fax number>@<FAX domain>

Example:

FAXG3/+4989700712345@fax.unifyOffice365.com

or

FAXG3/+4989700712345@XPRESSIONS.DOMAIN.NET

10.1 Exchange 2016/2019

To create a new send Connector follow the steps below:

1. On the on-premises Exchange server, create a new **Send Connector**. Name the connector and choose Type: "Custom":

new send connector

Create a Send connector.

There are four types of send connectors. Each connector has different permissions and network settings. [Learn more...](#)

*Name:
XPR2

Type:

- ☒ Custom (For example, to send mail to other non-Exchange servers)
- ☐ Internal (For example, to send intranet mail)
- ☐ Internet (For example, to send internet mail)
- ☐ Partner (For example, to route mail to trusted third-party servers)

next cancel

Sending Faxes from Exchange to Xpressions

Exchange 2016/2019

2. Choose between "MX record" (in that case an internal MX record pointing to the XPR server shall be created) or "Route mail through smart hosts" where the XPR server IP or FQDN may be configured:

Send Connector - Google Chrome

<https://10.10.110.17/ecp/ConnectorMgmt/NewSendConnector.aspx?pwmcid=2&ReturnObject1>

new send connector [Help](#)

A send connector can route mail directly through DNS or redirect it to a smart host. [Learn more...](#)

*Network settings:
Specify how to send mail with this connector.

☒ MX record associated with recipient domain
☐ Route mail through smart hosts

+ edit -

SMART HOST
10.10.158.10

☐ Use the external DNS lookup settings on servers with transport roles

[back](#) [next](#) [cancel](#)

3. Configure the domain that will be routed to the XPR server:

new send connector

A Send connector routes mail to a specified list of domains. These domains can be an SMTP address space or a custom type. [Learn more...](#)

*Address space:
Specify the address space or spaces to which this connector will route mail.

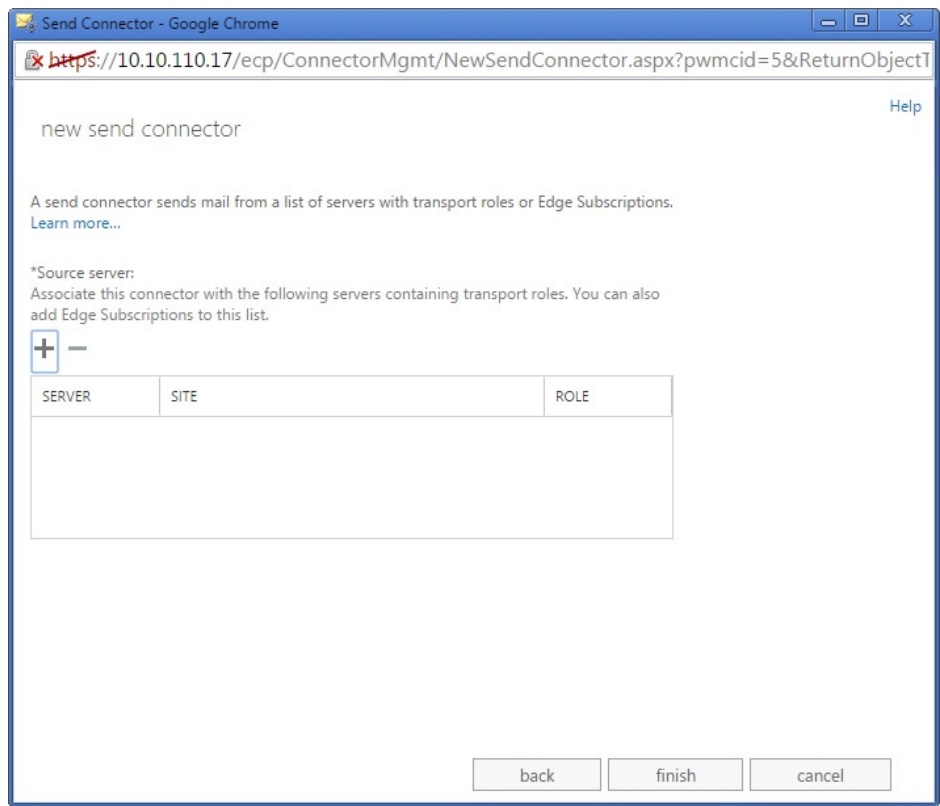
+ ✎ -

TYPE	DOMAIN	COST
SMTP	XPRESSIONS.DOMAIN.NET	1

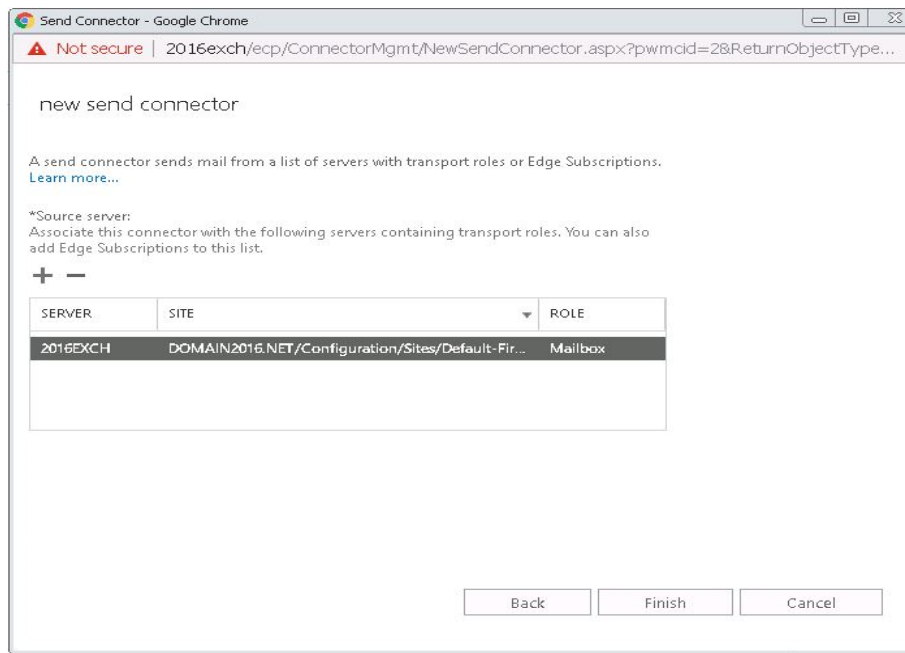
☐ Scoped send connector

Back Next Cancel

4. Choose the on-premises Exchange servers that will route those messages by choosing the Source server.



5. Click **Finish**.



Send Connector has now been created.

The screenshot shows the Exchange Admin Center interface. The top navigation bar includes 'Enterprise Office 365' and 'Administrator'. The left sidebar lists various management areas, with 'mail flow' selected. The main content area shows the 'send connectors' page, which includes a table of connectors. One connector, 'XPR', is listed with a status of 'Enabled'. To the right of the table, detailed information for the selected connector is displayed, including its last modified date, connector status, logging settings, and maximum send message size.

NAME	STATUS
XPR	Enabled

1 selected of 1 total

Connector Details:

- Name: XPR
- Last modified: 12/4/2019 12:02:06 PM
- Connector status: Enabled
- Disable (link)
- Logging: Off
- On (link)
- Maximum send message size (MB): 35

10.2 Exchange Online (Office 365)

10.2.1 SmtplApi accessible via Internet

In this scenario, the Exchange administrator must configure a send connector on the Exchange online side which forwards the configured fax domain (i.e. fax.unifyOffice365.com) to the Xpressions SmtplApi internet address.

Also, the fax domain must be added to the **Local Domains** on Xpressions **SmtplApi** configuration as described in [Section 10.2.2, “Using Exchange on-premises as relay on a hybrid deployment”](#).

Exchange Online side

Create a connector (in this example, it is named XPR) on Exchange online follow the steps below:

Office 365Administrador

Exchange admin center

dashboard
recipients
permissions
compliance management
organization
protection
mail flow
mobile
public folders
unified messaging

rulesmessage tracemessage traceaccepted domainsremote domainsconnectors

Connectors help control the flow of email messages to and from your Office 365 organization. However, because most organizations don't need to use connectors, we recommend that you first d
Want to help us improve connectors? Just [send us feedback](#) and let us know what you liked, didn't like, or what we can do to make your experience better.

+✎🗑️🔗

STATUS	NAME	FROM	TO
On	Inbound from c967cbe6-a523-42ea-8ff9-c0424ef425b4	Your organization's email server	Office 365
On	XPR	Office 365	Your organization's email server
On	Outbound to c967cbe6-a523-42ea-8ff9-c0424ef425b4	Office 365	Your organization's email server

XP
Ma
Fro
To:

De
Noi

Sta
On
Tur
Val

494

OpenScape Xpressions V7 Microsoft Exchange Gateway, Installation and Administration Manual

A31003-S2370-M101-45-76A9, 05/2025

1. On the first screen on the connector creation wizard, choose to send message from "Office 365" to "Your organization's email server":

New Connector - Google Chrome

https://outlook.office365.com/ecp/Connectors/ConnectorSelection.aspx?reqId=14491484514

Select your mail flow scenario

Specify your mail flow scenario, and we'll let you know if you need to set up a connector.
[Learn more](#)

From:
Office 365 ▼

To:
Your organization's email server ▼

You need to create a connector for this mail flow scenario. Because your domain's MX record points to Office 365, you must set up an alternative server (called a smart host) so that Office 365 can send email to your organization's email server (also called on-premises server). To complete the scenario, you might need to configure your email server to accept messages delivered by Office 365. [Learn more about configuring your email server](#)

Next Cancel

Sending Faxes from Exchange to Xpressions
Exchange Online (Office 365)

2. Enter a name for the connector:

New Connector - Google Chrome

https://outlook.office365.com/ecp/Connectors/OutboundConnector.aspx?ConnectorType=Onl

New connector

This connector lets Office 365 deliver messages to your organization's email server.

*Name:
XPR2

Description:

What do you want to do after connector is saved?

☒ Turn it on

☒ Retain internal Exchange email headers (recommended)

Next Cancel

3. Choose the option "Only when email messages are sent to these domains". Also, configure the domain name the users will add to the fax number to send it to Xpressions:

New Connector - Google Chrome

https://outlook.office365.com/ecp/Connectors/OutboundConnector.aspx?ConnectorType=Onl

New connector

When do you want to use this connector?

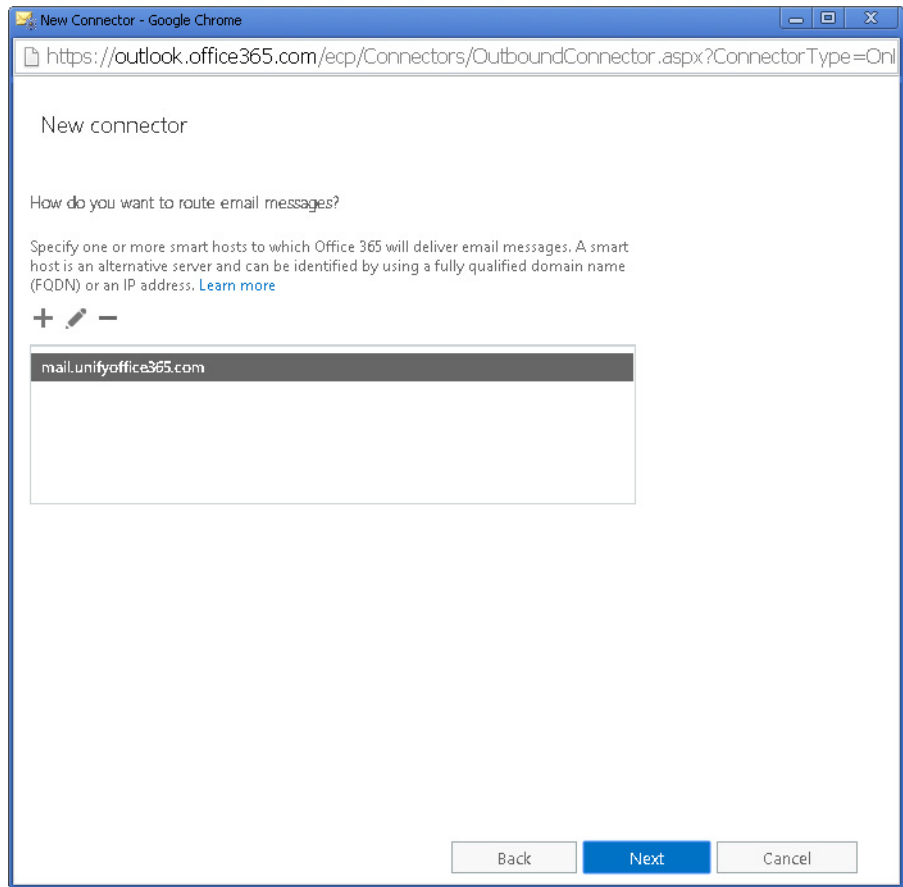
☐ Only when I have a transport rule set up that redirects messages to this connector
☐ For email messages sent to all accepted domains in your organization
☒ Only when email messages are sent to these domains

+ ✎ -

fax.unifyoffice365.com

Back Next Cancel

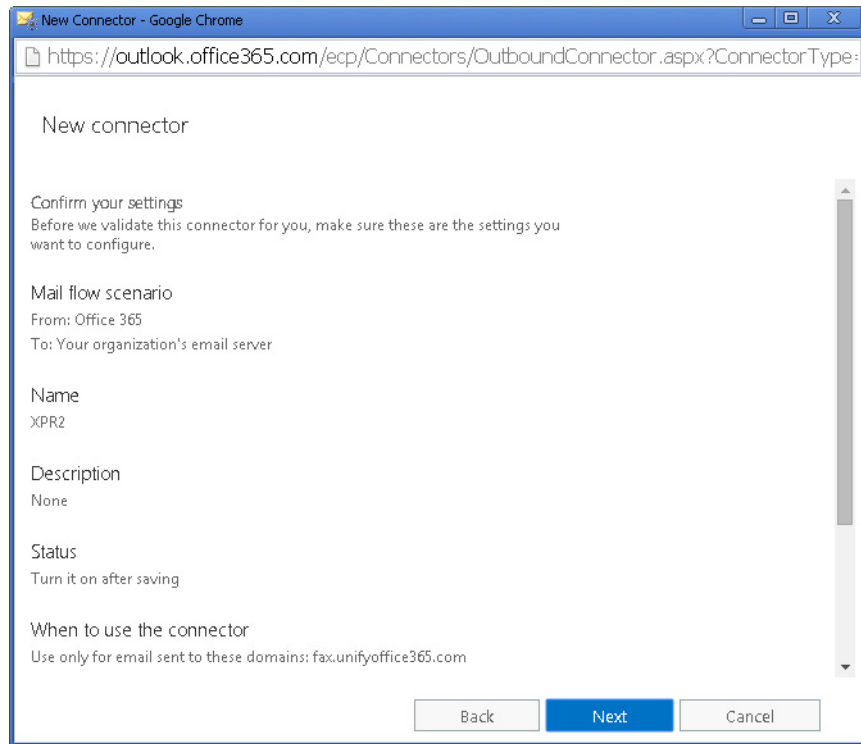
4. Configure the valid internet address for the Xpressions' SmtplApl:



5. Configure the TLS settings as suits to the environment to be used.

The screenshot shows a web browser window titled "New Connector - Google Chrome" with the address bar displaying <https://outlook.office365.com/ecp/Connectors/OutboundConnector.aspx?ConnectorType=Onl>. The main content area is titled "New connector" and contains the question "How should Office 365 connect to your email server?". Below this, there are three radio button options: "Always use Transport Layer Security (TLS) to secure the connection (recommended)" (which is selected), "Any digital certificate, including self-signed certificates", and "Issued by a trusted certificate authority (CA)". There is also an unchecked checkbox labeled "And the subject name or subject alternative name (SAN) matches this domain name:". Below the checkbox is a text input field with the placeholder text "Example: contoso.com or *.contoso.com". At the bottom right of the form are three buttons: "Back", "Next", and "Cancel".

6. Configure the Office 365 side.



10.2.2 Using Exchange on-premises as relay on a hybrid deployment

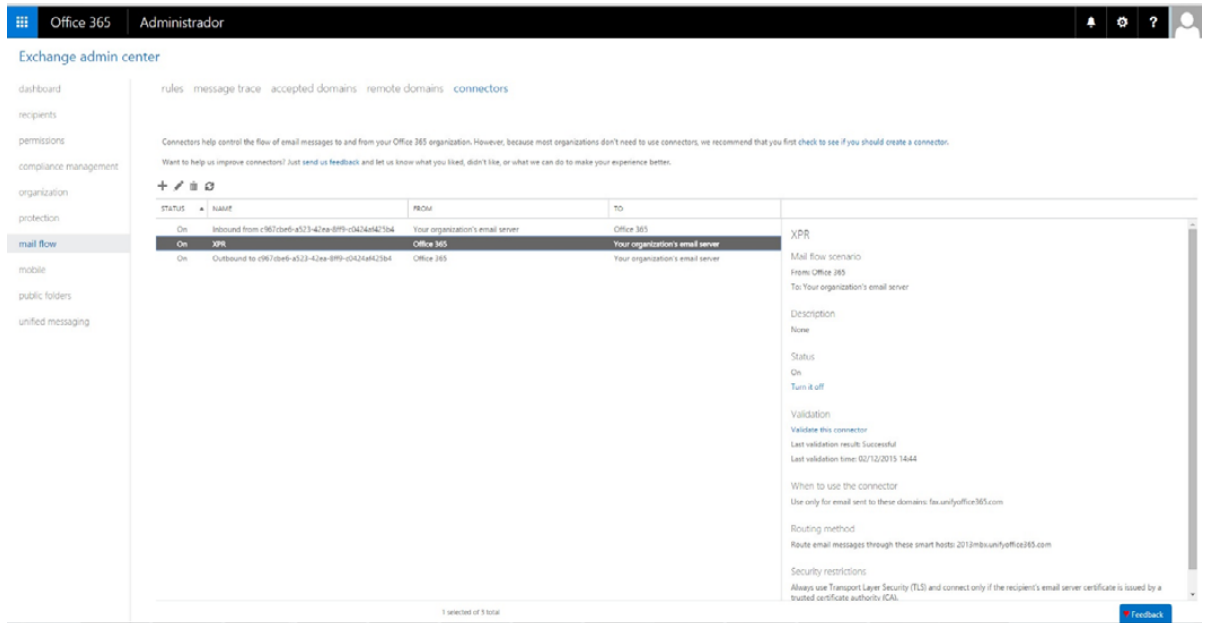
Sending fax messages from Exchange Online to Xpressions passing through an Exchange on-premises as a SMTP relay demands two connectors:

- One configured on Exchange online side, sending messages sent to a fax domain to the Exchange on-premises;
- And another configured on Exchange on-premises side, sending those messages to the Xpressions system.
- Also, the fax domain must be added to the "Local Domains" on Xpressions Smtpl configuration.

Below you can see a step by step examples of this configuration. On this particular example the connector was named "XPR".

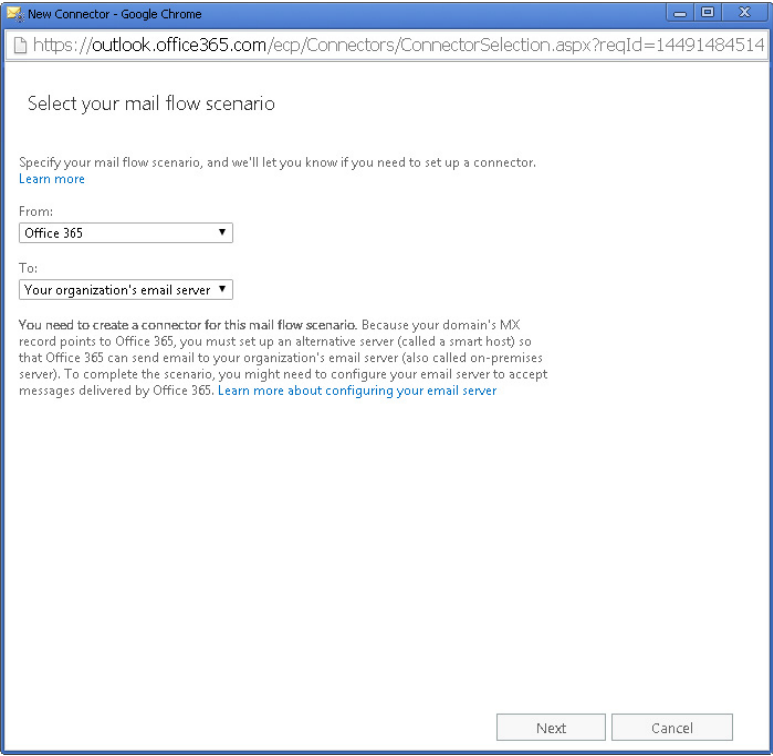
10.2.2.1 Example of creating a connector on the Exchange Online side

1. Create a connector on Exchange online:



2. On the first screen on the connector creation wizard, choose to send message from "Office 365" to "Your organization's email server":

Sending Faxes from Exchange to Xpressions
Exchange Online (Office 365)



3. On the next screen, name the connector:

Sending Faxes from Exchange to Xpressions

Exchange Online (Office 365)

The screenshot shows a web browser window titled "New Connector - Google Chrome". The address bar displays the URL: <https://outlook.office365.com/ecp/Connectors/OutboundConnector.aspx?ConnectorType=Onl>. The page content is titled "New connector" and includes the following elements:

- A descriptive sentence: "This connector lets Office 365 deliver messages to your organization's email server."
- A label "*Name:" followed by a text input field containing the text "XPR2".
- A label "Description:" followed by a large, empty text area.
- A section titled "What do you want to do after connector is saved?" with two checked options:
 - ☒ Turn it on
 - ☒ Retain internal Exchange email headers (recommended)
- At the bottom right, there are two buttons: "Next" and "Cancel".

Sending Faxes from Exchange to Xpressions

Exchange Online (Office 365)

4. Next, choose the option "Only when email messages are sent to these domains". Also, configure the domain name the users will add to the fax number to send it to Xpressions:

New Connector - Google Chrome

https://outlook.office365.com/ecp/Connectors/OutboundConnector.aspx?ConnectorType=Onl

New connector

When do you want to use this connector?

☐ Only when I have a transport rule set up that redirects messages to this connector

☐ For email messages sent to all accepted domains in your organization

☒ Only when email messages are sent to these domains

+ ✎ -

faxunifyoffice365.com

Back Next Cancel

5. Configure the valid domain name of the on-premises Exchange server which will route these messages to Xpressions:

New Connector - Google Chrome

https://outlook.office365.com/ecp/Connectors/OutboundConnector.aspx?ConnectorType=Onl

New connector

How do you want to route email messages?

Specify one or more smart hosts to which Office 365 will deliver email messages. A smart host is an alternative server and can be identified by using a fully qualified domain name (FQDN) or an IP address. [Learn more](#)

+ ✎ -

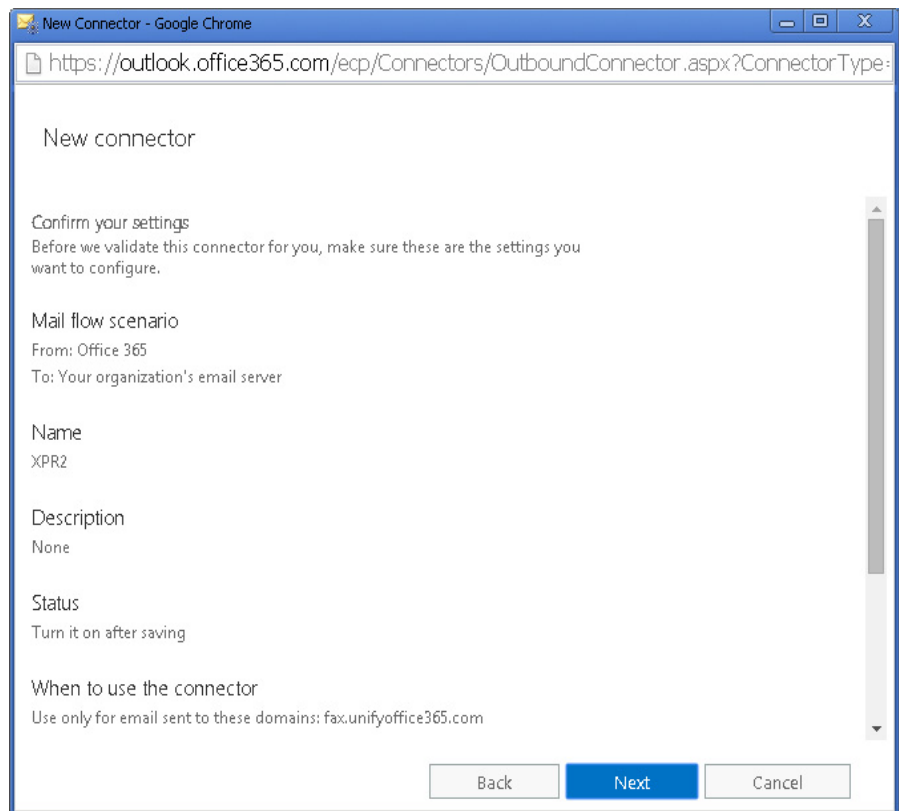
mail.unifyoffice365.com

Back Next Cancel

6. Configure the TLS settings as it suits to the environment to be used:

The screenshot shows a web browser window titled "New Connector - Google Chrome". The address bar displays the URL: `https://outlook.office365.com/ecp/Connectors/OutboundConnector.aspx?ConnectorType=Onl`. The main content area is titled "New connector". Below this, it asks "How should Office 365 connect to your email server?". There are two main options:
1. ☒ "Always use Transport Layer Security (TLS) to secure the connection (recommended)".
2. ☐ "Connect only if the recipient's email server certificate matches this criteria".
Under the second option, there are two sub-options:
- ☐ "Any digital certificate, including self-signed certificates"
- ☒ "Issued by a trusted certificate authority (CA)"
Below these, there is a checkbox ☐ "And the subject name or subject alternative name (SAN) matches this domain name:". If this checkbox is selected, a text input field is shown with the example: "Example: contoso.com or *.contoso.com". At the bottom right, there are three buttons: "Back", "Next", and "Cancel".

7. The final screen of the Office 365 side should be similar to the one below:



The screenshot shows a web browser window titled 'New Connector - Google Chrome'. The address bar displays the URL: <https://outlook.office365.com/ecp/Connectors/OutboundConnector.aspx?ConnectorType=>. The main content area is titled 'New connector' and contains the following sections:

- Confirm your settings**
Before we validate this connector for you, make sure these are the settings you want to configure.
- Mail flow scenario**
From: Office 365
To: Your organization's email server
- Name**
XPR2
- Description**
None
- Status**
Turn it on after saving
- When to use the connector**
Use only for email sent to these domains: fax.unifyoffice365.com

At the bottom right, there are three buttons: 'Back', 'Next' (highlighted in blue), and 'Cancel'.

10.2.2.2 Example of creating a connector on the Exchange on-premises side

1. On the on-premises Exchange server, create a new "Send Connector".
2. Name the connector and choose Type: "Custom"

The screenshot shows a web browser window titled "Send Connector - Google Chrome". The address bar displays the URL: <https://10.10.110.17/ecp/ConnectorMgmt/NewSendConnector.aspx?pwmcid=2&ReturnObjectT>. The page content includes a title "new send connector" with a "Help" link. Below this is a descriptive text: "A send connector can route mail directly through DNS or redirect it to a smart host. [Learn more...](#)". Under the heading "*Network settings:", it says "Specify how to send mail with this connector." and provides two radio button options: "MX record associated with recipient domain" (which is selected) and "Route mail through smart hosts". Below these options are three icons: a plus sign, a pencil, and a minus sign. A table with the header "SMART HOST" contains one entry, "10.10.158.10", which is highlighted. At the bottom of the form is a checkbox labeled "Use the external DNS lookup settings on servers with transport roles". At the very bottom of the page are three buttons: "back", "next", and "cancel".

3. Configure the domain that will be routed to the XPR server:

new send connector

A Send connector routes mail to a specified list of domains. These domains can be an SMTP address space or a custom type. [Learn more...](#)

*Address space:
Specify the address space or spaces to which this connector will route mail.

+ -

TYPE	DOMAIN	COST
SMTP	fax.unifyoffice365.com	1

☐ Scoped send connector

back next cancel

4. Choose the on-premises Exchange servers that will route those messages:

new send connector

A send connector sends mail from a list of servers with transport roles or Edge Subscriptions. [Learn more...](#)

*Source server:
Associate this connector with the following servers containing transport roles. You can also add Edge Subscriptions to this list.

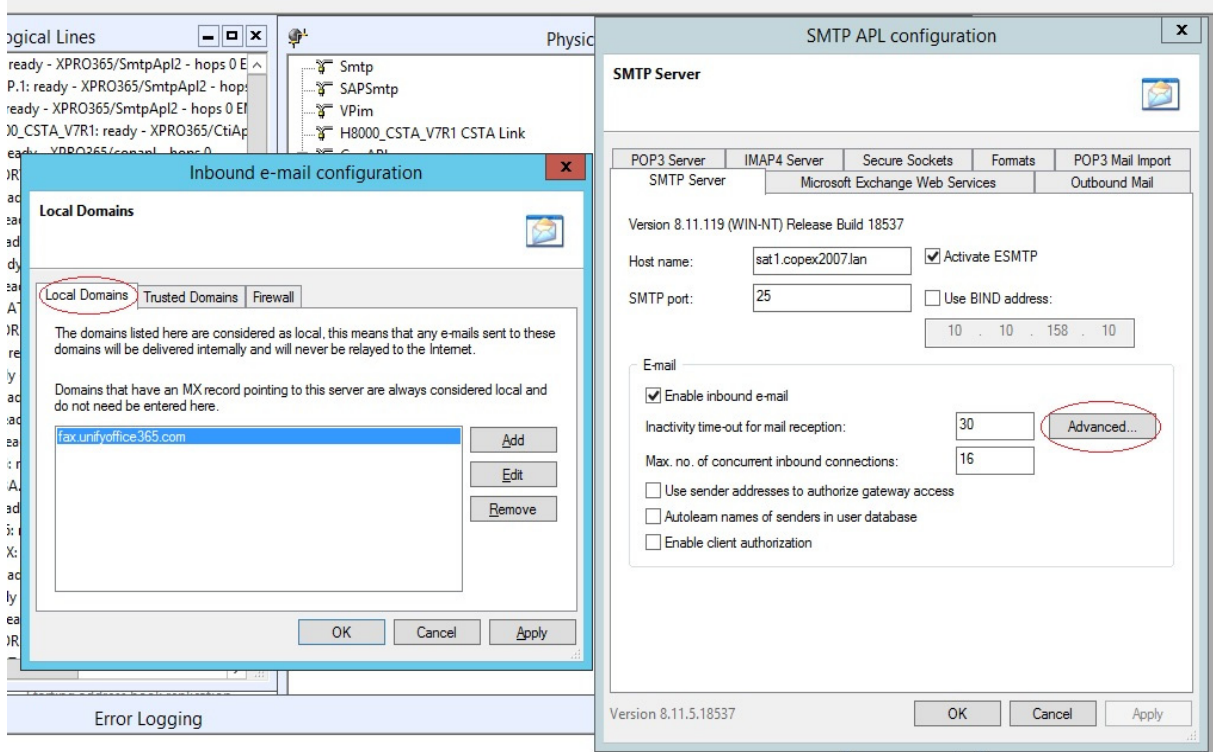
+ -

SERVER	SITE	ROLE

back finish cancel

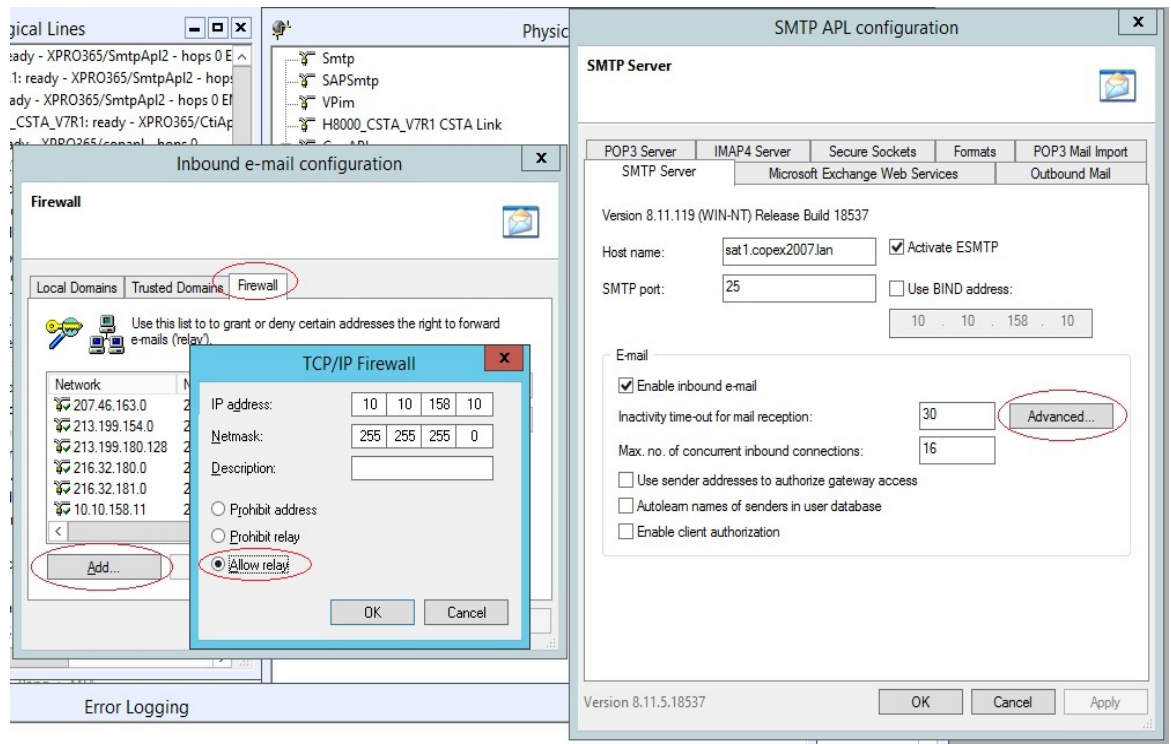
10.2.3 Smtpl2 configuration

On the Smtpl2 configuration, navigate to **Smtpl2 Server > Advanced... > Local Domains** and add the created fax domain:



Next, navigation to **Smtpl2 Server > Advance... > Firewall > Add...** and add all the IP addresses of the SMTP relay servers with "Allow relay" option selected:

Sending Faxes from Exchange to Xpressions Exchange Online (Office 365)



Sending Faxes from Exchange to Xpressions

Exchange Online (Office 365)

11 Troubleshooting

11.1 ExchAplConfigurator

To collect traces of the installation process, verify the temporary folder of the user that is installing the Apl.

Installation Traces:

%TEMP%\MrsExch.log

11.2 EWSApl service

<Unified Log Tool path>\EWSNotification.log

Web Services HTTPS requests/responses

<XPR Installation
Folder>\Log\EWSTraces\<DATE_HOUR_MILLISECOND> log folder.

IMPORTANT: The Web Services HTTPS requests/responses must only be enabled for advanced troubleshooting purposes due to the amount of files created.

To enable the Web Services HTTPS requests/responses, see the EWS Registry key sections.

11.3 EWSApl - Persistent delay in message synchronization and MWI

In case of persistent delays between connection of Xpressions and Office 365, it is recommended to:

- Increase the number subscriptions per thread
- Disable Junk Folder monitoring (MonitorJunkFolder)
- Disable Mailbox Rules verification (DisableMailboxRules)

11.4 EWSApl - OAuth authentication

Use the EWSEditor, available at:

<https://github.com/dseph/EwsEditor/releases>

1. In the EWSEditor main interface, navigate to **File > New Exchange Service...**
2. Select **Service URL** and click on the **365 Default** button to fill this field with default settings.
3. Then select '**Use OAuth (Registration must have been completed first)**' and fill with the information necessary.
4. Set the Redirected URI with the following content:

`urn:ietf:wg:oauth:2.0:oob`

Note: The value of the field Client App ID need to be provided by the Azure Administrator.

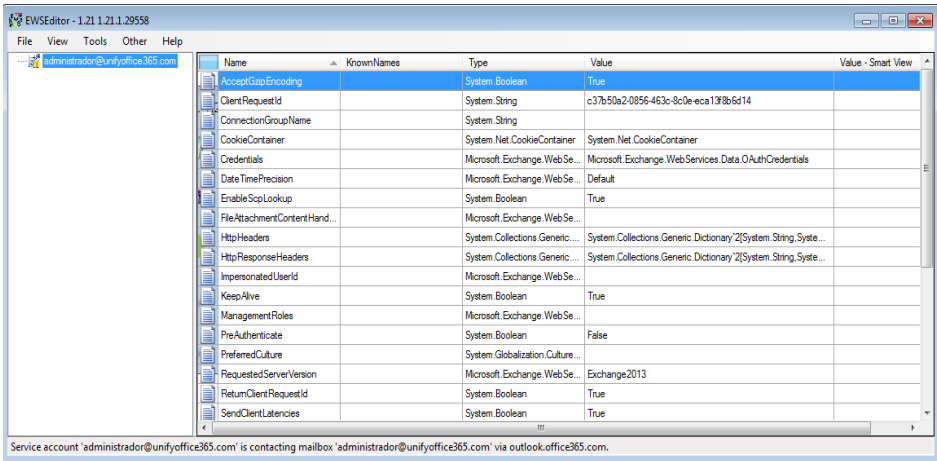
5. Click **Ok**.

Note: Depending on your browser security settings you may face some warnings when the sign in window is loaded, like the following:

6. Add this URL to the trusted sites list.

If a JavaScript error message appears, select **Yes** to allow running Scripts on this page: If those warnings appear, an error message log will then be shown. Close this window and try again.
7. In the Microsoft login window, enter your username and password as requested.:

If the authentication is successful, a prompt window will appear asking you to confirm if you want to automatically add the mailbox roo to the tree viewer. Select **Yes** and the following window should appear:



Message submission rate for this client has exceeded the configured limit" issue on SmtplApi

11.5 Message submission rate for this client has exceeded the configured limit" issue on SmtplApi

If the messages sent to Exchange On-Premises via SMTPApi are not delivered and the message "421 4.4.2 Message submission rate for this client has exceeded the configured limit" is logged in the SMTPApi traces or in the Exchange On-Premises SMTP protocol log, it is necessary to increase the Message Rate limit of the Receive connector in the Exchange On-Premises/Online.

SMTPApi logs:

09.14:49:54.785 SmtplApi Send 4 [118.4] <- 421 4.4.2 Message submission rate for this client has exceeded the configured limit

09.14:49:54.785 SmtplApi Send D [118.4] host returned '421 4.4.2 Message submission rate for this client has exceeded the configured limit'

Exchange logs:

*2016-12-13T13:29:54.088Z,2016EXCH\Default Frontend
2016EXCH,08D3FD072DBDF301,6,10.10.102.51:25,10.10.102.52:62221,>,421 4.4.2
Message submission rate for this client has exceeded the configured limit,*

Cause

The message rate limit is set to a value that allows less messages to be sent concurrently than the connector needs.

Resolution

To avoid such behavior, it is necessary to increase the message submission rate of the Receive connector in the Exchange On-Premises. Refer the Microsoft forum Exchange 2016/2019 SMTP limits.

To see which the current message rate limit is, use the following command;

```
Get-ReceiveConnector | ft Name, MessageRateLimit
```

To check the logs of the Receive connectors see the section "Structure of the protocol log files" in the Protocol logging of the Microsoft documentation.

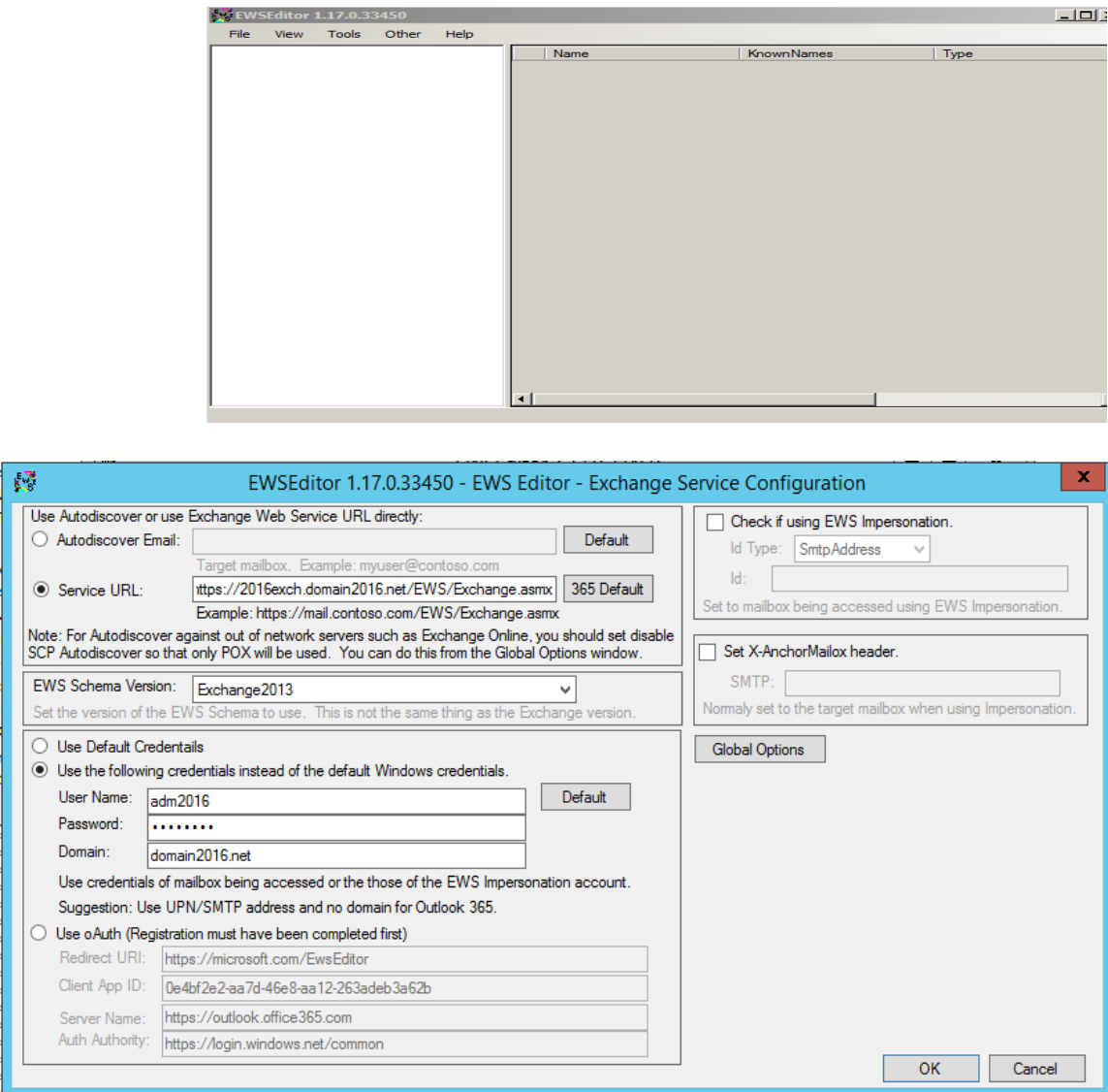
11.6 Microsoft Tools

For Office 365/Exchange 2016/2019 troubleshooting purposes is possible to use the Microsoft tool:

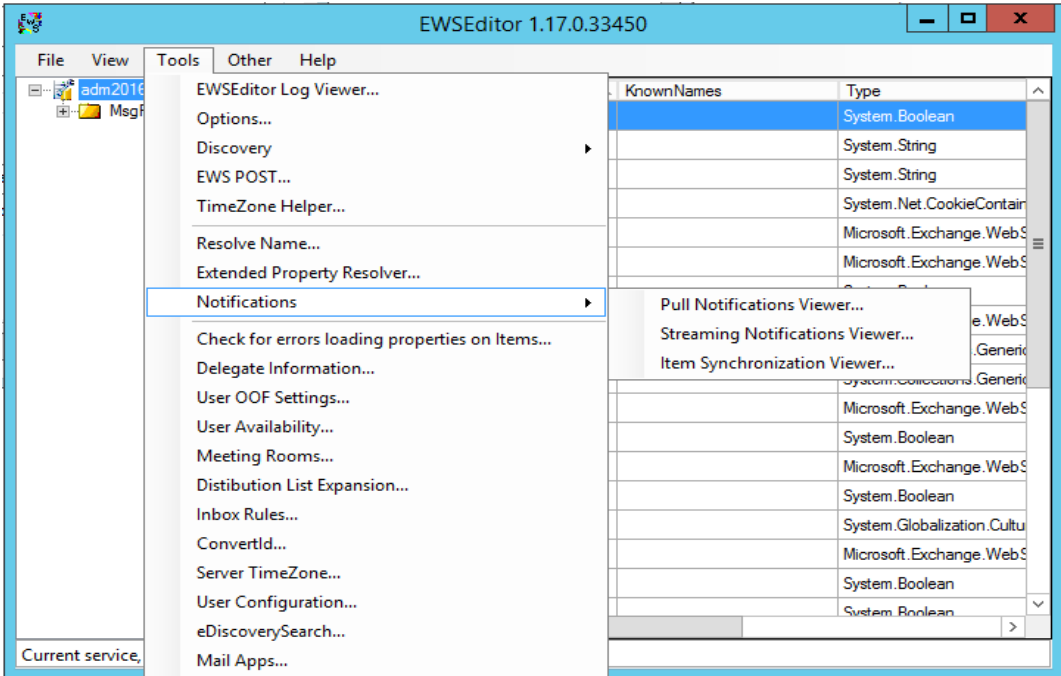
11.6.1 Exchange Web Services Editor

<https://ewseditor.codeplex.com/>

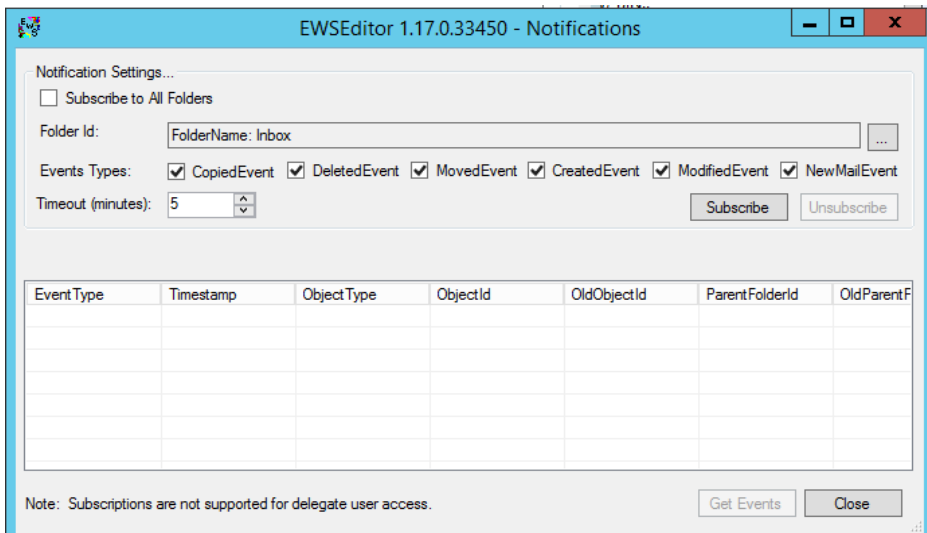
The EWSEditor is a open source tool that allow to perform tests using the Exchange Web Services functionality. Allow to perform connection tests and operations that are done similarly by the EWSApl. Is a recommended tool for troubleshooting issues with Exchange On-Premises solution.



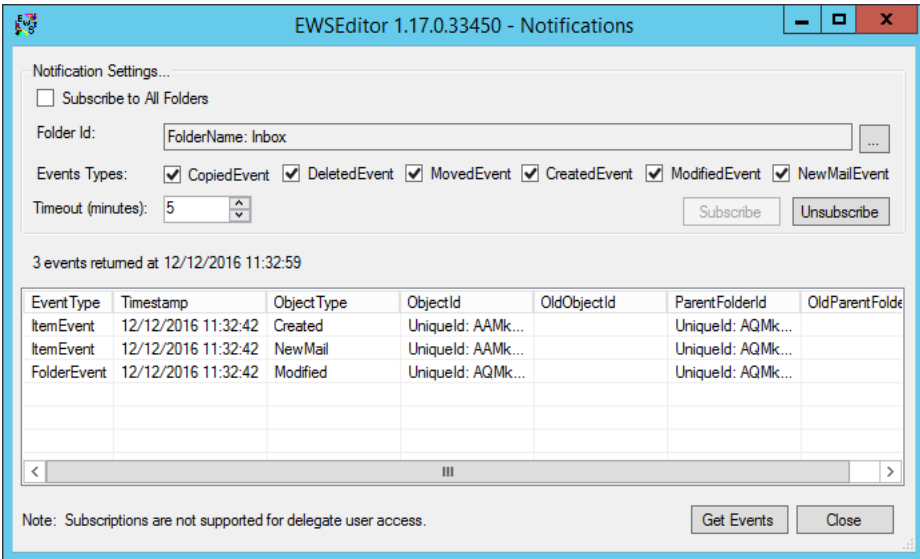
Tools > Notifications > Pull Notifications Viewer ...



Select **Inbox** folder > **Subscribe**



Get events



Click **Unsubscribe**

Click **Close Exchange Service**.

11.6.2 Remote Connectivity Analyzer

<https://testconnectivity.microsoft.com/>

Use the "Exchange Server" tab. The tool simulates the same procedure used by the EWSApl connection.

In the test below first use the existing service account to verify it can be opened via the "TestConnectivity". Then continue to test a configured mailbox to test the impersonation.

If during the test configuration you receive the following "Connectivity Test Failed message" it might be a configuration issue.

The screen below is a test sample method for "TestConnectivity.microsoft.com".

Enter the test user in the "Target mailbox email address" and "Impersonate user" dialog boxes.

Service Account Access (Developers)

Target mailbox email address:

Service Account User Name (Domain\User Name or UPN)

Service account password:

Confirm password:

☐ Use Autodiscover to detect server settings

☒ Specify Exchange Web Services URL

☒ Test predefined folder

☐ Specify folder ID

☒ Use Exchange Impersonation

Impersonated user:

Impersonated user identifier:

☒ Ignore Trust for SSL

☒ I understand that I must use the credentials of a working account from my Exchange domain

12 Outlook/Exchange Extensions

12.1 Outlook Extensions Features

The Outlook/Exchange Extensions are very handy, additional features to everybody using *MS Outlook* as client:

- Icon forms
 - Representation of specific message icons in the *MS Outlook* inbox journal for different message types (icon forms).
- Message forms
 - A simplified addressing method when fax messages are sent or polled.
 - Convenient SMS message transmission.
 - Forwarding of inbound messages independent from service (fax, e-mail or voicemails) to one or several addresses. The message can previously be extended with a text and/or voice comment. The voice annotation can be recorded via telephone or via a microphone connected to the sound card.
 - Answering incoming messages. Depending on the service, different answering options are available. The message is then immediately furnished with the originator address, if it is contained in the system. The message can previously be extended with a text and/or voice comment. The voice annotation can be recorded via telephone or via a microphone connected to the sound card.

NOTE: If the message is addressed to several recipients (for example as Carbon Copy, Cc), the reply can be simultaneously sent to all original recipients.

- Transmission of new voicemails.
- Reading or listening to incoming fax and voicemails in the preview window.

NOTE: Fax and voicemails cannot be edited in the preview window with *Outlook XP*.

When you open such messages with a double-click, a convenient fax editing function is available so that you can add text or graphic elements to incoming fax messages before they are forwarded. Voicemails can be played back either via sound card or the individual telephone and extended with a voice annotation before they are forwarded.

So that fax and voicemails can be represented or put out in offline operation (for example at laptop computers), the **Synchronize forms** checkbox must be set.

- In *Outlook XP* you reach the corresponding settings dialog either via key combination [Ctrl] + [Alt] + S or call the **Tools > Send/Receive > Send/Receive Settings > Define Send/Receive Groups...** menu. In the dialog now open select the **All Accounts** entry and press the **Edit...** button. In the next dialog, **Send/Receive Settings - All Accounts**, you find the **Synchronize forms** checkbox to the right of the directory tree.
 - In *Outlook 2003* the following path leads to this option: **Tools > Send/Receive Settings > Define Send/Receive Groups....** In there select the **All accounts** entry and enable the **Edit...** button. In the **Send/Receive Settings - All Accounts** dialog which follows you find in the **Account Options** section the **Synchronize forms** checkbox.
- Representing additional information in the **From** and **Subject** columns of the Outlook journal. You perform the configuration on the **Display Formats** tab.
 - See for Exchange 2007 **Display Formats** [Section 4.3.5.5, “Display Formats Tab”](#), on page 127 with the connector settings.
 - See for Exchange 2010 **Display Formats** [Section 5.3.5.5, “Display Formats Tab”](#), on page 245 with the connector settings.
 - With Unify OpenScape Xpressions V7 optiClient 130 you can use the full range of the XPR server CTI features from Outlook. Precondition is that the required CTI components are installed on the XPR server.

12.2 XPR Icon and Message Forms

12.2.1 Icon Forms

All messages transmitted from the XPR server to Exchange (fax, SMS or voicemails) are indicated in the *MS Outlook* inbox journal with the e-mail standard icon (envelop).

The additional messages icons help the user to quickly see which types of messages are in the inbox. The message type or status is immediately graphically displayed. These icons are not only available for standard messages but also for CTI status displays and for an administrator report. Refer to the following table for the additional icons and the message classes and states they indicate:

CTI Message Classes:		
Icon	Displayed for:	Name Entry in the Form Manager
	Incoming call has not reached the user	IPM.Note.MRS.CTI.Inbound.Failed
	Incoming call has not reached the user, rescheduled	IPM.Note.MRS.CTI.Inbound.Failed.Rescheduled
	Incoming call has reached the user	IPM.Note.MRS.CTI.Inbound.Success
	Incoming call has reached the user, rescheduled	IPM.Note.MRS.CTI.Inbound.Success.Rescheduled
	Outgoing call has not reached the user	IPM.Note.MRS.CTI.Outbound.Failed
	Outgoing call has not reached the user, rescheduled	IPM.Note.MRS.CTI.Outbound.Failed.Rescheduled
	Outgoing call has reached the user	IPM.Note.MRS.CTI.Outbound.Success
	Outgoing call has reached the user, rescheduled	IPM.Note.MRS.CTI.Outbound.Success.Rescheduled

Table 35 CTI Icons and their Message Classes

Outlook/Exchange Extensions

XPR Icon and Message Forms

Data Message Classes		
Icon	Displayed for:	Name Entry in the Form Manager
	Received fax message, supports fax messages of the Outlook Extensions	IPM.NOTE.FAX
	Received fax message, standard	IPM.Note.MRS.Fax
	Received fax on demand	IPM.Note.MRS.form_rev
	Sent fax message	IPM.Note.MRS.form_fax
	Fax message, transmission OK	IPM.Note.MRS.Fax.DR
	Fax message, transmission faulty	IPM.Note.MRS.Fax.NDR
	Sent SMS	IPM.Note.MRS.form_sms
	Voicemail, standard	IPM.Note.MRS.Voice
	Voicemail, supports voicemails of the Outlook Extensions	IPM.Note.Voice
	Voicemail, supports voicemails of Xpressions 470	IPM.Note.Voice.Unity
	Voice comment attached to received message	IPM.Note.MRS.Annotation

Table 36 Message Icons and their Message Classes

Administration Message Classes:		
Icon	Displayed for:	Name Entry in the Form Manager
	Administration report; e.g. to display errors during the address-book replication	IPM.Note.MRS.AdminReport

Table 37 Icon for the Administration Report and its Message Class

12.2.2 Message Forms

NOTE: Since the message forms are integrated as Visual Basic Script, the Office component *Visual Basic Scripting Support* must be installed on each client computer. Without this component the form code cannot be executed and the forms do not work. This component is an element of the Microsoft Office standard installation, but can be excluded from a customized installation.

Message forms provide two basic types of usage:

- **Edit Forms:** these forms are integrated as ActiveX components in Outlook. They enable editing incoming fax and voicemails in the preview window or in a separate dialog.
There is one restriction: In *Outlook XP* it is currently not possible to edit messages in the preview window for technical reasons. It is well possible, though, to edit an incoming fax or voicemail by opening the message via double-click or context menu. Subsequently, the messages can be edited with the associated tools.

NOTE: When using the context menu (rightclick on a fax or voicemail in the journal), Outlook generates a localization error. The German menu option **Öffnen** appears in English (**Open**). Please heed this particularity.

Both message types are also available as file attachment (fax messages in .TIF format, voice messages in .WAV format). These formats can also be read or listened to with a suitable viewing or playback program after locally saving them.

- **Send forms:** As preparative measure, message forms are stored on the Exchange server to make them available to all desired subscribers with an extended functional range. The only requirement for this purpose is the additional start of the "Unattended Setup" with each client that is to use the functions. For this purpose, the setup can be made accessible via a share or simply be distributed as file attachment to the corresponding users by e-mail. The only entry you need to make during this setup is the URL to start the *Web Assistant*.

The message forms feature range comprises:

- Reading, editing, forwarding and answering fax messages.
- Voicemails playback either via soundcard or the individual telephone and attachment of a voice annotation before the message is forwarded.
- Furnishing any messages, independent from the service (fax, e-mail or voicemail), with a text and/or voice comment. Such messages can then be forwarded to one or several addresses or returned as reply to the

originator. If the received message is addressed to several recipients (for example as Carbon Copy, Cc), the reply can be transmitted to all original recipients. The voice annotation can be recorded via telephone or via a microphone connected to the sound card.

- Simplified addressing with sending fax messages.

NOTE: You can send fax messages via the appropriate send form only if no image files are enclosed in fax stationery possibly used or in the Outlook signature. This restriction does not apply if the fax message is sent directly via the Outlook default form (via the address: `MRS : FAXG3 / +49 . . .`).

- A fax-polling feature
- Convenient SMS message sending

NOTE: When sending SMS messages via the appropriate send form, a prefix or suffix possibly provided by server configuration is usually not included in the transmission. The message body is sent only. This restriction does not apply if you set registry value [SMS_AL-LOW_DIGEST \[REG_DWORD\]](#) to 1 under `HKLM\SOFTWARE\Wow6432Node\PP-COM\MRS\ExchAp` or sent the SMS message directly via the Outlook default form (address: `MRS : SMS / +49 . . .`).

- Creating and sending voicemails

12.2.3 General Information about Installing the Forms

You install the server components via the Microsoft Outlook client. You can currently use the following MS Outlook versions:

Microsoft Office 2007, 2010 (32-bit and 64-bit version) and 2013 (32-bit and 64-bit version).

Please consult the *OpenScape Xpressions, Release Notice* manual for information about current Microsoft Outlook version/operating system use options.

NOTE: In case of Windows Vista operating systems, the installation can be blocked by the Windows firewall. Unblock the firewall in the information dialog to continue the installation.

12.2.3.1 General Information about Installing the Forms in Outlook 2007

The forms extensions for *MS Outlook* are installed in two steps in Outlook 2007:

- Installation of the server components (`ServerBasedForms`) for general use of the icon and message forms.
In this process, the icon and message forms are centrally stored as organization form on the Exchange server in one installation step.

NOTE: The server component is installed independently from the Exchange server version.

- Installation of the client component (`ServerBasedFormsClientComponents`) on each Outlook client to use the forms.

12.2.3.2 General Information about Installing the Forms in Outlook 2010 and further versions

IMPORTANT: The forms extensions for MS Outlook 2010 and 2013 are now installed only using Outlook Forms (VSTO) on each Outlook client .

If you have Forms installed on Exchange for Outlook 2007, it can work together with Outlook 2010 / 2013.

Outlook/Exchange Extensions

XPR Icon and Message Forms

In case of Outlook 2010/2013 you must remove the previous client installation from Local Forms before install the new client components, even if Server Based Forms are available on Exchange they will not be used in Outlook Client 2010/2013.

Since the new and old forms are deployed by different setup packages, the update can not be performed directly on machines which already have the old forms installed.

Therefore, the old forms will have to be removed prior to the installation of the new ones.

For the new Outlook forms (for Outlook 2010 and 2013), the installation of Server Based Forms is no longer necessary, once all elements needed by the OL Forms are installed on the Client side.

For Windows 8 machines “.NET Framework 3” is required.

For Windows 7 machines “.NET Framework 4” is required.

12.2.4 Installation of the Server Components

12.2.4.1 Requirements for Installing the Icon and Message Forms

NOTE: This chapter only applies if Outlook 2007 is used as a client, no matter which Exchange version is being used.

- The setup for the server component of the icon and message forms can be started from any computer on which an *MS Outlook* client of the Exchange organization is installed. The installing user must be logged in at this system with administrative privileges. For the installation, select the Outlook profile of the user who has been granted the owner privilege for the forms library. See [Section 12.2.5, “Requirements for Installing the Icon and Message Forms”, on page 531](#).
- The Collaboration Data Object (CDO.DLL) must be available on the computer from which the installation is to be performed.

For MS Office versions **before** Office 2007:

In case of an *MS Office* default installation (typical mode), the CDO is not automatically installed. It must then be subsequently installed from the Office CD.

For MS Office 2007:

As of Microsoft Office 2007 the Microsoft Collaboration Data Object (CDO) is no longer an Office package component. Installing the server-based forms requires the CDO, though. Therefore, the CDO must be manually installed on the client from which the setup is to be performed. You can download the **ExchangeCdo.MSI** installation file provided by Microsoft for this purpose from the website:

<http://www.microsoft.com/downloads/details.aspx?FamilyID=2714320d-c997-4de1-986f-24f081725d36&displaylang=en>

IMPORTANT: *MS Outlook* must not be installed on the XPR and Exchange server. The CDO.DLL coming with the *MS Outlook* installation would override and disable the CDO.DLL required by other components and already installed by the system manager.

For MS Office 2010/2013:

There is no special Microsoft Collaboration Data Object (CDO) for Office 2010/2013 either. However, if you heed the following setup sequence you can use the CDO that you could install for Microsoft Office 2007 for Microsoft Office 2010/2013 also:

1. Install Microsoft Outlook 2007 first.
2. Install then the Microsoft Collaboration Data Object (CDO) for Outlook 2007.
3. Perform now the update installation on Microsoft Outlook 2010/2013 (2-bit and 64-bit version).

NOTE: You find more information about using the Microsoft Collaboration Data Object (CDO) for Outlook 2007 with Outlook 2010/2013 on the support pages of Microsoft under:

<http://support.microsoft.com/kb/2028411/en-us>

- If you have defined several user profiles in Outlook: make sure that in Outlook, under **Tools > Options...**, the **Prompt for a profile to be used** option is selected on the **Mail Services** tab. This enables you to log on as user who has the forms library owner privileges. Otherwise the error message might appear that the required user privilege for the organization folder does not exist.
- The installing user must have a mailbox on the Exchange server.
- In profile settings of the installing user the **Use Cached Exchange Mode** option must be deactivated. You reach this option via **Start > Control Panel > Mail > E-mail Accounts...** There select under **E-Mail** the **View or change existing e-mail accounts**. Click on **Next**. In the following dialog select the corresponding e-mail account and click **Change....** Deactivate the **Use Cached Exchange Mode** if it has been set.
- The installing user needs to have the owner privilege for the **Exchange Forms Library**.

12.2.5 Requirements for Installing the Icon and Message Forms

All forms of message classes must be installed in a global library so that they can later be made available to all connected Outlook clients.

Before the setup start for the icon and message forms a directory must first be created for the forms in the global library

NOTE: This chapter only applies if Outlook 2007 is used as a client, no matter which Exchange version is being used.

12.2.5.1 Creating the Forms Directory in Exchange Server 2007/2010

You may create and configure the forms directory via the Exchange management console->toolbox->Public Folder Management Console.

Alternatively you can use the Exchange management shell instead.

The assignment of the LOCALE_ID has changed. This ID is important for language selection so that the Outlook clients can access the right forms folder. The assignment occurs via the Exchange management shell or the Exchange maintenance utility of the XPR server.

How to prepare *Exchange Server 2007/2010* for installation of the XPR Outlook forms:

Creating the forms directory and assignment of the required privileges on the Exchange Server 2007/2010:

NOTE: If there is no global forms library (database for public folders) in your *Exchange Server 2007/2010* environment, create it in the desired storage group using the *Exchange management console* .

1. Start the *Exchange management shell*.
2. Create the organization directory with the command:

```
New-PublicFolder -path "\NON_IPM_SUBTREE\EFORMS  
REGISTRY" -name "<directory name>"
```

NOTE: For the *<directory name>* variable you can use, for example, the description **organization forms**.

3. Set the properties of the newly created directory with the command:

```
Set-PublicFolder -identity "\NON_IPM_SUBTREE\EFORMS  
REGISTRY\<directory name>" -HiddenFromAddressLists  
Enabled $true -UseDatabaseQuotaDefaults $false
```

4. Assign the required privileges to the newly created directory with the following three commands:

```
Add-PublicFolderAdministrativePermission -identity  
"\NON_IPM_SUBTREE\EFORMS REGISTRY\<directory name>" -  
AccessRights AllExtendedRights -User <administrator>
```

```
Add-PublicFolderAdministrativePermission -identity  
"\NON_IPM_SUBTREE\EFORMS REGISTRY\<directory name>" -  
AccessRights AllStoreRights -User <administrator>
```

```
Add-PublicFolderClientPermission -identity  
"\NON_IPM_SUBTREE\EFORMS REGISTRY\<directory name>" -  
AccessRights  
CreateItems,ReadItems,CreateSubfolders,FolderOwner,Folde  
rContact,FolderVisible,EditOwnedItems,EditAllItems,Delet  
eOwnedItems,DeleteAllItems -User <administrator>
```

Assigning the LOCAL_ID via the XPR server

The **PR_EFORMS_LOCALE_ID** property of the forms directory may be assigned via the Exchange management shell

```
Get-PublicFolder -Identity "\NON_IPM_SUBTREE\EFORMS  
REGISTRY\<directory name>" | Set-PublicFolder -  
EformsLocaleID [<CultureInfo>]"
```

for example: `Get-PublicFolder -Identity`

```
"\NON_IPM_SUBTREE\EFORMS REGISTRY\MRS-EN | Set-PublicFolder  
-EformsLocaleID EN-US".
```

For more information about [*<CultureInfo>*] please visit:

<http://go.microsoft.com/fwlink/?LinkId=184859>

Alternatively this can be done via the Exchange maintenance utility of the XPR server.

This requires the following steps:

1. Open the application start-up panel via **Start > Run**.
2. In the **Run** dialog enter the **cmd** command and confirm with **OK**. The DOS window opens.
3. Switch to the directory path:
`<Drive>\XPR setup directory\xpr\bin`
4. Enter at the cursor position the following command:
`exch2kmaint /mode=setlocale /exchangeserver=<Exchange
server name> /folder=<directory name> /localeid=<id> /
interactive=1`

The variables must be replaced with the following values:

<Exchange server name>: Name of the Exchange Server 2007 if the Exchange environment is of monolithic structure. In case of a modular *Exchange Server 2007* structure the name of the server that hosts the public folders.

<Directory name>: Name of the created forms directory.

<id>: Country code (decimal) for language setting (for example 1031 for Germany and 1033 for US English).

NOTE: You find further country codes for language setting in the Internet under the address:

<http://msdn2.microsoft.com/en-us/library/aa579489.aspx>

12.2.5.2 Starting the Installation Routine for the Server Component

Now that the preparations are complete, the server component is installed next.

NOTE: The setup for the server component of the icon and message forms can be started from any computer on which an *MS Outlook* client of the Exchange organization is installed. The installing user must be logged in at this system with administrative privileges. For the installation, select the Outlook profile of the user who has been granted the owner privilege for the forms library. See [Section 12.2.5, “Requirements for Installing the Icon and Message Forms”, on page 531](#).

The installation consists of two integrated processes:

- a) Copying all required files.
- b) Automatic start of the `Formregister.exe` program that writes the required forms in the organization folder.

How to perform the installation:

1. Start the `Setup.exe` setup program. You find the setup program on the product carrier in the directory

`\Add-On\Client\Exchange\Forms\ServerBasedForms\`

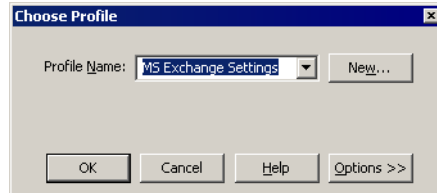
After the setup program start, a welcome dialog appears first.

2. Confirm the welcome dialog with **Next**.

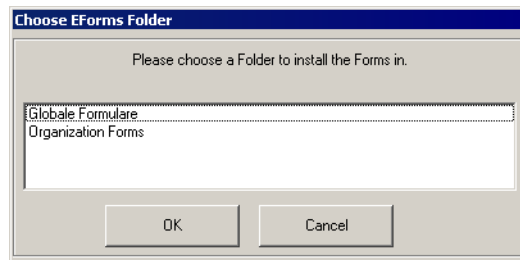
The dialog for starting the installation opens.

3. Click on **Install** in this dialog.

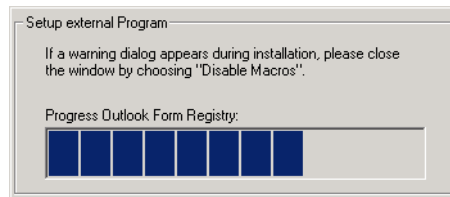
4. The next dialog shows the file copying via a progress display.
5. Select the appropriate profile to authenticate yourself as installing user.
For this purpose, select the Outlook profile of the user who has been granted the owner privilege for the forms library. See [Section 12.2.5, “Requirements for Installing the Icon and Message Forms”](#), on page 531.



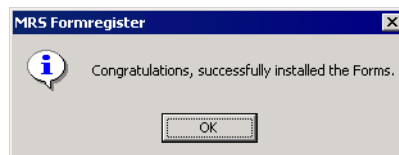
6. Confirm your selection with **OK**.
7. Specify the forms folder in which the forms are to be registered. There's one Folder per language available.
Therefore you can choose the folder with the language you want to use. In multi-language environments you can rerun the setup against the used language folders.



Select the desired forms folder and click on **OK**.
A progress indicator displays the form registration process.



Finally, the message appears that the entire process has been successfully completed.



Confirm this message with **OK**.

8. Click on **Finish** to complete the installation.

The installation of the server component for the icon and message forms is thus performed.

Checking the Installation

To check the successful installation you can look up the entered message icons in Outlook:

1. Start Outlook
2. Select **Tools** and then the **Options...** function in the Outlook menu.
3. Switch to the **Other** tab.
4. In the **General** section push the **Advanced Options...** button.
5. In the advanced options dialog click **Custom Forms...**
Another option window opens.
6. Enable the **Manage Forms** button here.
The forms manager is subsequently displayed. The left hand side of this dialog should now list all message and icon forms under the name specified for the forms folder.

12.2.5.3 Subsequent Message and Icon Forms Registration

NOTE: `FormRegister.exe` x must be started on the computer on which the corresponding forms files were stored. This means that the subsequent registration is only possible from the client computer on which the initial installation was performed.

In the course of Setup, the forms are registered in the forms folder that you have selected in Setup. After the installation you can register the forms additionally in another organization folder.

This requires the `FormRegister.exe` program. After the installation of the server component you find this program in the program directory of the computer from which you have performed the installation. The precise path reads:

```
%ProgramFiles%\Common Files\Siemens\ServerBasedForms
```

How to perform a belated registration:

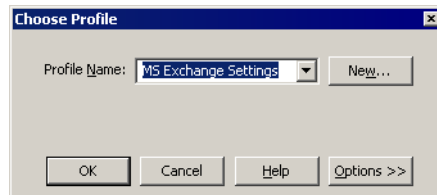
1. Start the command line interpreter via **Start > Run > cmd**
2. Switch to the directory in which the files of the `ServerBasedForms` are stored.

3. Execute the `FormRegister.exe` program with the `x` parameter.

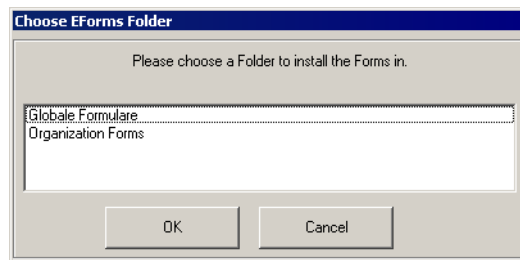
Program invocation: `Formregister.exe x`

The executing user requires a valid Outlook profile on the computer from where the operation is started and the owner privilege for the **Exchange Form Library**.

4. Select the Outlook profile of the user who has been granted the owner privilege for the forms library. See [Section 12.2.5.1, "Creating the Forms Directory in Exchange Server 2007/2010"](#), on page 531.

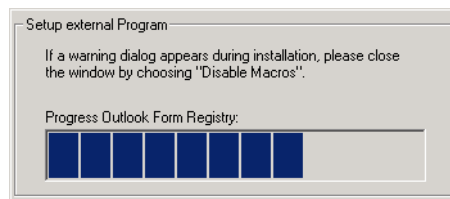


5. Confirm your selection with **OK**.
6. Specify the forms folder in which the forms are to be registered.

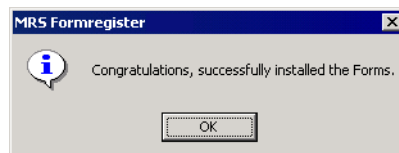


7. Confirm your selection with **OK**.

A progress indicator displays the form registration process.



Finally, the message appears that the entire process has been successfully completed.



8. Confirm this message with **OK**.

Registering the server component for the icon and message forms in another forms folder is thus complete.

Removing forms from the organization folder is done analog to the previously described procedure. The `DeInstallBtn.exe` program serves this purpose. It is also called from the `ServerBasedForms` directory with the `x` parameter to log off the message and icon forms.

12.2.5.4 Uninstalling Message and Icon Forms

Message and icon forms should always be removed as customary under Windows. Proceed as follows:

NOTE: In case of Windows Vista operating systems, the uninstallation can be blocked by the Windows firewall. Unblock the firewall in the information dialog to continue the uninstallation.

1. Start the control panel via **Start > Settings > Control Panel** and call the **Add/Remove Software** function.
In this way the list of application programs already installed is displayed.
2. In this list select the **Exchange Forms Server** entry.
3. Click the **Change/Remove** button to start the uninstallation program.
4. Then follow the instructions given in the corresponding windows to remove the forms from the system.

12.2.6 Security Settings for the ActiveX Control Elements

The security settings of the zone selected in Outlook (**Internet** or **Restricted sites**) can be changed from a more general type of activation (**Enable**) to a more restricted, safer one (**Administrator approved**) for the ActiveX controls. In this way, only the ActiveX control elements installed with the XPR Outlook Extensions are released for usage.

NOTE: This adaption requires domain-administrator privileges.

12.2.6.1 Local Configuration on a Workstation

If executing the ActiveX controls shall be allowed on specific workstations only, you can use the Registry patch `faxocx.reg`.

You find the file for adjusting the local registry on the product data carrier in the directory:

AddOn\Client\Exchange\Forms\ServerBasedForms\GroupPolicy\W
2K3

These actions require the following steps:

1. Copy the `faxocx.reg` file to the workstation on which executing the ActiveX controls shall be allowed.
2. Execute the Registry patch with a doubleclick.

NOTE: Alternatively, you can install the Registry patch from any shared directory in which the `faxocx.reg` file is stored.

12.2.6.2 Configuration for Microsoft Server 2008

In Microsoft Server 2008 environments you adjust the group policy used in the Active Directory.

In a first step you extend the group policy and in a second step this extension is activated.

You extend the group policy using the files `faxocx.admx` and `faxocx.adml`.

- You adjust the group policy via file `faxocx.admx`.
- Depending on the required language version you configure the text strings via file `faxocx.adml`.

You find both files on the product carrier in the directory:

- `faxocx.admx`
`\AddOn\Client\Exchange\Forms\ServerBasedForms\GroupPolicy\W2K8`
- `faxocx.adml` (for the English version)
`\AddOn\Client\Exchange\Forms\ServerBasedForms\GroupPolicy\W2K8\en-US`
- `faxocx.adml` (for the German version)
`\AddOn\Client\Exchange\Forms\ServerBasedForms\GroupPolicy\W2K8\de-DE`

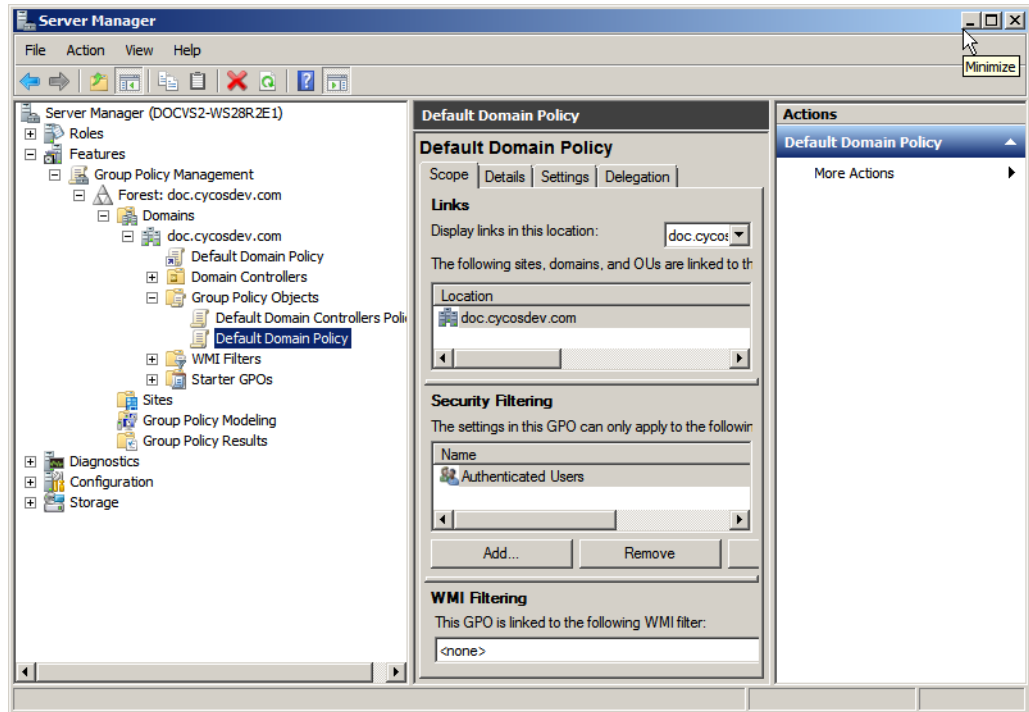
How to adjust the group policy:

1. Copy file `faxocx.admx` to the `%WINDIR%\PolicyDefinitions\` directory of the relevant Windows server 2008.
2. Depending on the desired language copy the string file `faxocx.adml` to the `%WINDIR%\PolicyDefinitions\en-US` or `%WINDIR%\PolicyDefinitions\en-DE` directory of the relevant Windows server 2008.
3. Open the system program **Server Manager**.
4. Open there the **Features** container and expand the view **Group Policy Management > Forest:<server name> > Domains > <server name> > Group Policy Objects > Default Domain Policy**.

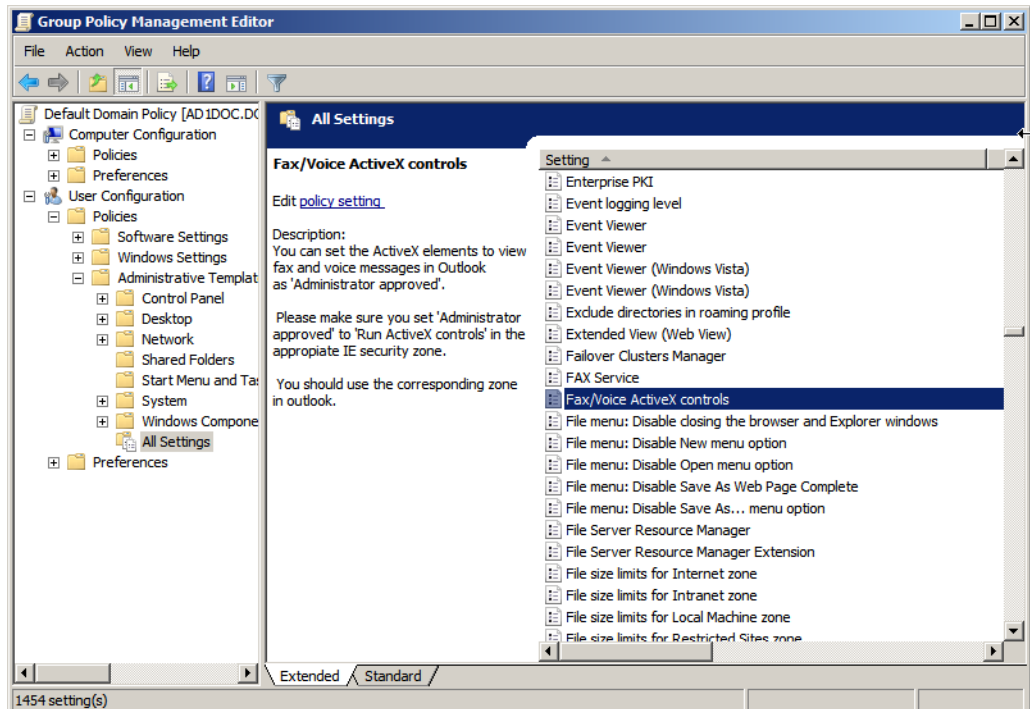
NOTE: If you cannot yet see the **Group Policy Management** under **Features**, you can configure the **Group Policy Management** via the **Add Features** function.

Outlook/Exchange Extensions

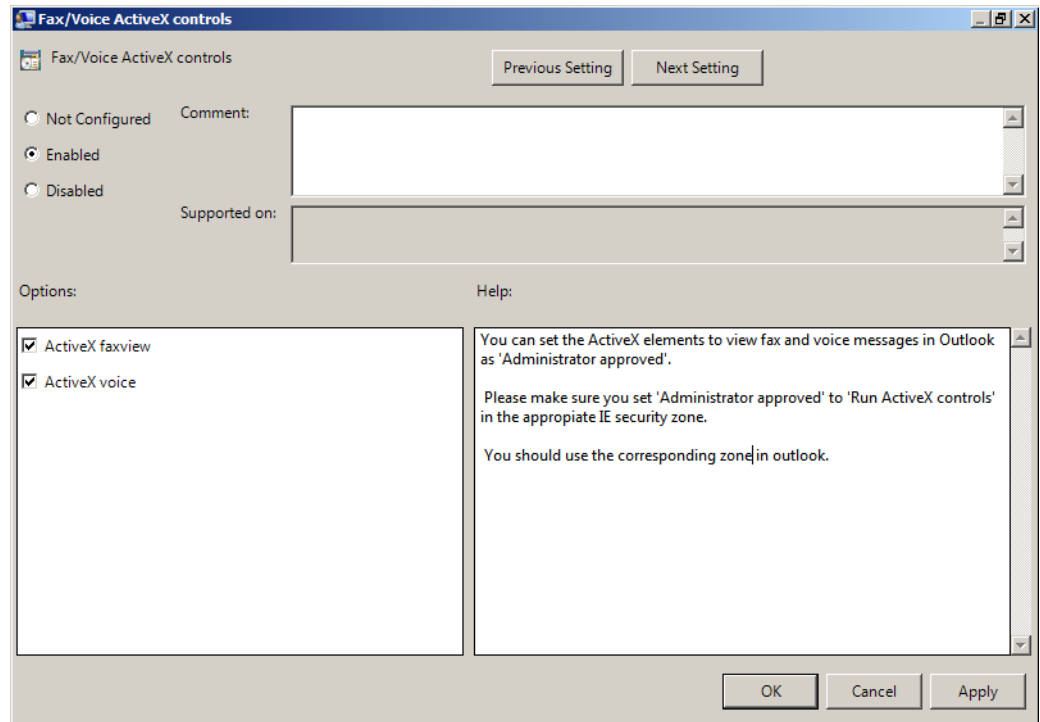
XPR Icon and Message Forms



5. Open the context menu with a rightclick on **Default Domain Policy**.
6. Select **Edit** in the context menu. The **Group Policy Management Editor** dialog opens.



7. Open the **User Configuration** container and expand the view **Policies > Administrative Templates > All Settings**. The list of available settings is displayed.
8. Open the **Fax/Voice ActiveX controls** setting with a doubleclick. The dialog **Fax/Voice ActiveX controls** for activating the policy opens.



9. Select the **Enabled** function here first.
10. Then select the components to be activated via radio button. You can optionally activate the ActiveX control for fax messages, the ActiveX control for voicemails or for both.
11. Click on **OK** to save the setting. The **Fax/Voice ActiveX controls** dialog closes.

The new group policy for the ActiveX control is thus configured.

12.3 Installation of Client Components

You find information about installing further client components in the *Unify OpenScape Xpressions V7 Server Installation* manual.

IMPORTANT: Due to the adaption of the client setup programs to Windows Installer (Msi), a direct update installation of the clients is not possible. The old clients must be completely uninstalled beforehand.

12.3.1 Configuration Overview

The following tables provide an overview of the configurations in which extensions can be installed.

12.3.1.1 Windows Client Operating Systems

You can integrate the client components in the Outlook versions of the Microsoft Office versions 2007 2013 (32-bit and 64-bit version) and 2013 (32-bit and 64-bit version).

The following operating systems have been approved for these Office versions:

	Windows XP Professional SP2 or SP3	Windows Server 2003 SP1	Windows Vista Business Enterprise	Windows Vista Professional Ultimate Enterprise	Windows 8 Pro Edition	Microsoft 2000/2003 Terminal Server	Citrix MetaFrame XP
optiClient 130	Yes	Yes	Yes	Yes	Yes	Yes*	Yes*
Message forms	Yes	Yes	Yes	Yes	Yes	Yes	Yes

* Supporting optiClient 130 in Microsoft terminal server respectively Citrix MetaFrame environments is restricted to the use of CTI features. Usage as IP client is not possible here.

Please consult the *OpenScape Xpressions, Release Notice* manual for information about current Microsoft Outlook version/operating system use options.

12.3.2 User-defined Installation of the Message Forms on the Clients

The message forms features can be determined for the users by adjustments in the installation file.

With XPR 5.0, setting up the clients has been adjusted to Microsoft MSI packets (Windows Installer). This means, the installation management via an `.INI` file used with the previous program versions is no longer available.

You can edit the parameters described in the following:

12.3.2.1 Tables: “Property” for Outlook Forms for Outlook 2007

Address for the *Web Assistant*

The administrator can enter the *Web Assistant* address in the “Property” table to permanently default it before the installation. If this value is left unchanged, the user can enter the URL for the *Web Assistant* during the installation.

Property	PWEBADMINLNK
VALUE	<URL Web Assistant> Example: https://<Server address>/cgi_bin/webassistant/start
Default Value	http://webAssistant/

Installation for all users

By default the forms are so installed that they are available to each user logged in at the respective computer (admin installation).

By changing the property value `ADDINFORALL=0`, Setup can be executed in a way that only the user currently logged in and performing Setup can use the forms.

Property	ADDINFORALL
VALUE	0: The forms are only available to the installing user.
Default Value	1: The forms are available to all users.

Upgrading

In case of an upgrade, all registry values are usually correctly set already. Via the public property `NOOVERWRITE=1` you can instruct the MSI installer not to override any entries in the registry. The disadvantage is that newly accrued registry values are then not written either. Therefore, it may be more useful to override the registry values modified according to [Section 12.3.2.2, “Tables: “Registry” for Outlook Forms for Outlook 2007”, on page 544](#) in the registry after the installation.

Property	NoOverwrite
VALUE	1: Registry values are not to be overridden in case of an upgrade.
Default Value	0: Registry values are overridden in case of an upgrade.

12.3.2.2 Tables: “Registry” for Outlook Forms for Outlook 2007

In this section you can, for example, configure the program for specific operation environments or restrict the available functional range.

Automatic number filtering

Key	Software\Wow6432Node\Cycos AG\ExchForms Client
Name	NoNumberOnlyResolution
Default Value	0
Description	All numeric values entered in the e-mail address field are automatically interpreted as fax G3 address (0). This behavior can be switched off since it may lead to addressing errors, if your address entries in the global or personal address book are not only updated according to names but partly also to code numbers (1).

Restricting the functional range

The entire functional range is usually installed. However, you can exclude every single form from the installation. For this purpose, set the corresponding entry to 1.

Key	Software\Wow6432Node\Cycos AG\ExchForms Client
Name	NoFaxBtn
Default Value	0
Description	“1” deactivates the fax icon and form.

Key	Software\Wow6432Node\Cycos AG\ExchForms Client
Name	NoFaxViewForm
Default Value	0
Description	“1” deactivates the Active X object for fax messages.

Key	Software\Wow6432Node\Cycos AG\ExchForms Client
Name	NoFODBtn
Default Value	0
Description	“1” deactivates the fax polling icon and form.

Key	Software\Wow6432Node\Cycos AG\ExchForms Client
Name	NoSMSBtn

Default Value 0

Description "1" deactivates the SMS icon and form.

Key Software\Wow6432Node\Cycos AG\ExchForms Client

Name NoVMBtn

Default Value 0

Description "1" deactivates the voice mail icon and form.

Key Software\Wow6432Node\Cycos AG\ExchForms Client

Name NoVoiceViewForm

Default Value 0

Description "1" deactivates the Active X object for voicemails.

Key Software\Wow6432Node\Cycos AG\ExchForms Client

Name NoWebAssistantBtn

Default Value 0

Description Enter a "1" here if the icon for starting the *Web Assistant* is not to be displayed in the toolbar.

Changing the Telephone Number

Key Software\Wow6432Node\Cycos AG\ExchForms Client

Name ChangePhoneNo

Default Value 1

Description Via this option you can disallow the Microsoft Outlook client user to change the individual phone number. Therefore set the value to 0.

Keep area code "0"

Key	Software\Wow6432Node\Cycos AG\ExchForms Client
Name	NoZeroCut
Default Value	0
Description	With "1" you can enforce that for outgoing fax and SMS messages the leading area code "0" is not omitted when an address is selected from the address book. Example: In case of an Outlook-conformable phone number such as +49 (02404) 901100, the 0 of (02404) is not cut.

Replacing the +-prefix with an arbitrary string

Key	Software\Wow6432Node\Cycos AG\ExchForms Client
Name	SubstituteForPlus
Default Value	-
Description	Is used to automatically replace the leading + character by any digit combination. For this purpose, write the desired digit combination in the value field.

Opening Outlook .msg files

Key	Software\Wow6432Node\Cycos AG\ExchForms Client
Name	MsgFile
Default Value	0
Description	To enable opening Outlook .msg files as fax or voice mails, set "1" instead of "0".

Exchange operation

Key	Software\Wow6432Node\Cycos AG\ExchForms Client
Name	IMAPMode
Default Value	0
Description	For operation at Exchange the default setting ("0") is to be maintained.

Suppress warning

Key	Software\Wow6432Node\Cycos AG\ExchForms Client
Name	MsgShowNoNumber
Default Value	0
Description	If you want to suppress the warning that for the selected address book entry no corresponding fax or SMS number is available, enter a "1" here. Note: the user can otherwise configure this function by setting the "Don't show this dialog again" checkbox placed on the warning message himself/herself.

Notifications

Key	Software\Wow6432Node\Cycos AG\ExchForms Client\FAX
Name	DeliveryReceipt
Default Value	1
Description	Changing this value to "0" suppresses a requested delivery receipt for fax messages.
Key	Software\Wow6432Node\Cycos AG\ExchForms Client\FAX
Name	ReadReceipt
Default Value	1
Description	Changing this value to "0" suppresses a requested read receipt for fax messages.
Key	Software\Wow6432Node\Cycos AG\ExchForms Client\SMS
Name	DeliveryReceipt
Default Value	0
Description	Changing this value to "0" suppresses a requested delivery receipt for SMS messages.
Key	Software\Wow6432Node\Cycos AG\ExchForms Client\SMS
Name	ReadReceipt
Default Value	0
Description	Changing this value to "0" suppresses a requested read receipt for SMS messages.
Key	Software\Wow6432Node\Cycos AG\ExchForms Client\SMS
Name	TextLength
Default Value	612
Description	This instruction is used for restricting the number of characters in an SMS message. This may be required if you have defined, for example, for SMS messages a prefix (or a suffix) on the XPR server. The number of characters of this SMS code automatically enclosed in each message must then be deduced from the maximum number of possible characters.

12.3.3 Installation of the Xpressions Outlook Forms for Outlook 2010 and further versions (VSTO Forms)

Some Outlook Forms features can be determined for the users by adjustments on the installation process. The installation management may be done via .INI file and via registry. In case of mass roll-out installations it is possible to set the installation properties as parameters to the msi file.

NOTE: Detailed install information can be found in the document *OpenScape Xpressions V7, Client Installations, Installation Guide*, in chapter *Installing the Outlook Forms for Microsoft Outlook 2010 and further versions*.

12.3.4 Outlook Forms in Metaframe or Terminal Server Environments

Outlook forms require the support of Visual Basic Script (VBScript) so that the implemented features can be executed.

NOTE: The ActiveX components for fax and voice do not run under the standard settings for Outlook 2007, since executing VBScript features in shared folders is deactivated by default. To change this behavior, select the Allow script in shared folders option. You reach this option from the Outlook menu under **Tools > Trust Center > E-Mail Security**. There, in the **Script in Folders** section, select the option **Allow script in shared folders**.

If Outlook 2007 is executed on a terminal server computer, the following proceedings are required to activate the VBScript support for Outlook forms:

1. Install Outlook 2007.
2. Determine the GUID (Globally Unique Identifier) for the Outlook 2007 version just installed.
 - If you have installed Outlook 2007 as independent application, use the corresponding product GUID of this version.

- If you have installed Outlook 2007 as component of an Office Enterprise 2007, use the corresponding product GUID of this version.

NOTE: The Microsoft Knowledge Base article 928516 (<http://support.microsoft.com/kb/928516>) describes under the title “Description of the numbering scheme for product code GUIDs in 2007 Office suites and programs” how to determine the GUID of the installed product.

3. After you have determined the product GUID, execute the following command via the command line:

```
msiexec /i <product code GUID of [SKUName]WW.msi>  
ADDLOCAL=OutlookVBScript /qb
```

NOTE: In this command the variable stands for your product GUID.

<Product code GUID of [SKUName]WW.msi>

In case of an Office Enterprise 2007 installation your product ID reads e.g. as follows:

{90120000-0030-0000-0000-00000000FF1CE}

Therefore, the complete command line for the above GUID must appear as follows:

```
msiexec /i {90120000-0030-0000-0000-00000000FF1CE}  
ADDLOCAL=OutlookVBScript /qb
```

4. Another step may be required if step 3 is not sufficient. In this case the following additional key must be created in the registry:

```
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\  
Installer\UserData\S-1-5-18\Components\  
D5F662842F9AB9B43AC8199855FE5B0C
```

the REG_SZ

0000210903000000000000000000F01FEC

with the content

C:\Program Files\Microsoft Office\Office12\OUTLVBS.DLL

NOTE: Value 0000210903000000000000000000F01FEC originates from Microsoft Office Enterprise 2007. This ID may be different for another version.

NOTE: The Outlvbs.dll file is a component of the Microsoft product *MS Office* and must therefore not be passed on by the Unify Software and Solutions GmbH & Co. KG.

Outlook/Exchange Extensions

Installation of Client Components

You find further information on this topic under:

<http://support.microsoft.com/kb/302003>

12.3.5 Uninstalling the Local Outlook 2007 Forms Components

If you want to remove message icons or message forms from a client, do so in the manner common under Windows.

Proceed as follows:

1. Start the control panel via **Start > Settings > Control Panel** and call the **Programs > Programs and Features** function.
In this way the list of application programs already installed is displayed.
2. In this list, select the entry **Local Client Components for Outlook**.
3. Click the **Uninstall** button to start the uninstallation program.

Then follow the instructions given in the corresponding windows to remove the forms from the system.

12.3.6 Uninstalling the Server Based Forms for Outlook 2007

If you want to remove message icons or message forms from a client, do so in the manner common under Windows.

Proceed as follows:

1. Start the control panel via **Start > Settings > Control Panel** and call the **Programs > Programs and Features** function.
In this way the list of application programs already installed is displayed.
2. In this list, select the entry **Outlook Client Components**.
3. Click the **Uninstall** button to start the uninstallation program.

Then follow the instructions given in the corresponding windows to remove the forms from the system.

12.3.7 Uninstalling the Outlook Forms for Outlook 2010 and further versions

If you want to remove message icons or message forms from a client, do so in the manner common under Windows.

Proceed as follows:

1. Start the control panel via **Start > Settings > Control Panel** and call the **Programs > Programs and Features** function.
In this way the list of application programs already installed is displayed.
2. In this list, select the entry **Openscape Xpressions Outlook Forms**.
3. Click the **Uninstall** button to start the uninstallation program.

Then follow the instructions given in the corresponding windows to remove the forms from the system.

A Appendix

A.1 Service Provider (MSP)

This provider serves as global substructure for all client applications using XPR server services. While several client applications can run on a computer simultaneously, only one entity of the XPR Service Provider is available.

The following services are provided:

- Local database (cache)
It is not necessary for every client application to keep an individual database up to date. If required, the service provider synchronizes its local database with the database of the XPR server. Thereby the contents of the local database is made available to all client applications so that fast access is enabled any time.
- Store & Forward interface
Client applications can send documents to or receive them from an XPR server. This refers to classic communication by fax, e-mail etc. The XPR server CTI journal also operates via this interface
- Transaction interface
Through this service, client applications can communicate with components of the XPR server that support transactions. This enables in particular the use of CTI features for the corresponding client applications.

According to requirements the MSP is automatically implemented upon the installation of an XPR client component. When the installation is completed you will find the file `MSP.INSTALL.LOG` in the `TEMP` directory of the installing user, helping to detect errors if problems should occur.

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

For further information on the service provider and on profile definition refer to the *Server Administration* manual.

A.2 Connector Installation on Microsoft Small Business Server

In case of a standard Small Business Server 2003 (SBS 2003) installation the Microsoft Exchange MTA Stacks service and its functions are deactivated.

The XPR-Exchange connector requires this service so that the Exch Apl can duly run.

A.2.1 Activating the Exchange MTA Stacks in SBS 2003

MTA is activated in several steps. Modifications must be performed in the registry and at the start type of a service.

IMPORTANT: Before you start with the modifications, please save the current system state first.

Proceed as follows to receive the full functionality:

- Removing Registry Keys
- Modifying the Start Type of Microsoft Exchange MTA Stacks
- Restarting Services
- Installing the Exchange connector if required

A.2.1.1 Removing Registry Keys

1. Open `Regedit.exe`.
2. Move to the following registry key:

`HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\MSExchangeIS\<Server name>\Private`

3. Remove the following two entries:

- "Gateway In Threads"
- "Gateway Out Threads"

4. Move to the following registry key:

`HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\MSExchangeIS\<Server name>\Public`

5. Remove the following two entries:

- “Gateway In Threads”
- “Gateway Out Threads”

6. Close `Regedit.exe`.

A.2.1.2 Modifying the Start Type of Microsoft Exchange MTA Stacks

1. Open the services management console (**All Programs > Administrative Tools > Services**) or select Run and enter “Services.msc”. Confirm the command with **OK**.
2. Doubleclick the “Microsoft Exchange MTA Stacks” entry to open the **Properties** dialog.
3. In the **General** tab set the start type from “Disabled” to “Automatic”.
4. Click **Apply** and start this service.
5. Close the **Properties** dialog.

NOTE: Do not close the services management console yet!

A.2.1.3 Restarting Services

1. Select the “Microsoft Exchange System Attendant” service and restart it. This restarts all depending services as well.

NOTE: If the XPR-Exchange connector has already been installed, restart the “XPR ExchangeApl” service.

2. Close the services management console.

A.2.1.4 Installing the XPR Exchange Connector

Install the XPR-Exchange connector if this has not been done yet.

A.3 “Xpressions” Folder with *PhoneMail* in Case of Inbox Replication

Using *Phonemail* you can employ a special Outlook folder for message output via telephone. To configure this function, some preparative steps must be taken by the user (at the Outlook client) as well as by the administrator (at the XPR server) in the **sequence** described here.

IMPORTANT: If you do not stick to this succession, the messages will be lost due to internal Exchange server synchronization mechanisms.

We strongly recommend to save the contents of the “Xpressions” folder and of the inbox before activating this feature.

NOTE: **XpressionsFolder** registry key should be set to 1 in order to enable the access to PhoneMail Xpressions folder from WebClient.

For further information refer to chapter “*Entries of the Con APL*” of *OpenScape Xpressions V7 Server Administration, Administrator Documentation*.

1. The corresponding user must first define the “Xpressions” folder in Outlook with the following defaults:
 - The folder may only be called “Xpressions”.
 - The folder must be defined in the same level as the inbox folder.
2. The user must then share the use of this folder via the *Web Assistant* on the page **Voice mail system -> Edit personal filter**.

Using the “Xpressions” folder via the *PhoneMail* script is now configured.

If the “Xpressions” folder is to be immediately available to the user, the administrator must be notified so that he/she can perform an Exchange APL reboot.

IMPORTANT: The Exchange APL must be rebooted before messages are moved or transmitted to the “Xpressions” folder. Otherwise all this mail will be lost with rebooting the APL.

After the APL reboot the administrator must inform the user that messages can now be moved or, by routing rules, delivered to the “Xpressions” folder.

The “Xpressions” folder will otherwise be activated after the configuration reload (this occurs in 24-hour intervals overnight). In other words, it will not be available until the next day.

A.4 Automatic Client Software Distribution

A.4.1 Client Log-in via Windows User Account

To simplify client software distribution, the Windows user account can be assigned to an XPR user account instead of a user profile with XPR user ID and password.

In a scenario with an Exchange connection the administrator thus need not maintain individual XPR user profiles on the respective client computer anymore, but for the required login (e.g. for using the Outlook forms) the Windows user account already specified is used. Logging in via the Windows user account is performed via the **LMACCOUNT** data field.

NOTE: Using **LMACCOUNT** requires the XPR sever and the respective users to be in a Windows domain.

Before this feature can be used, the Windows domain and user account of each user must be present in the **LMACCOUNT** database field. Example: for user **TESTUSER** in the **TEST** domain the entry would be: **TEST\TESTUSER**. Thus logging in under Windows NT/2000/XP/2003 and Vista occurs automatically via a corresponding validation at the domain server. In case of an error (for example, when the **LMACCOUNT** field among the user data has not been filled in), a user profile must still be created via the service provider before the first log-in.

A prerequisite for this log-in version is that no XPR user has a backslash [\] in their **USER** database field.

The **LMACCOUNT** user database field is available per default. You find it under the name **Windows Account** among the XPR user data on the **Advanced** tab. Here you can also check whether a correct entry has been made for a user via LDAP replication. Another LDAP APL configuration is not required since the corresponding settings are performed via the LDAP configuration file (**ExRepl.Icf**). So that the **LMACCOUNT** user database field is automatically filled in with the domain and the user name, the **LMACCOUNT** XPR attribute is assigned to the **sAMAccountName** Active Directory attribute.

This assignment can be checked in the **Attributes** tab of the LDAP configuration dialog. In the attributes list the **LMACCOUNT** XPR attribute is entered next to the **sAMAccount** Active Directory attribute.

You find more detailed information about configuring **LMACCOUNT** in the *Server Administration* manual.

A.5 Registry Entry Directory

A.5.1 General Considerations

All system-relevant values are normally configured via Setup and subsequently via the Exchange Admin. These settings are partly stored in the Registry. In most cases the Registry need not be edited.

IMPORTANT: We strongly recommend only to perform modifications here when you are absolutely sure about the ensuing consequences. In an extreme case wrong entries may lead to the complete system stopping its service with all consequential damages!

Registry entries have the format: **Value Name:Data Type:Value**. The **Value** entries depend on the data type. The following data types are used here:

- String: **REG_SZ**.
- Data: **REG_DWORD**, with either binary -, decimal- or hexadecimal based entries.
- Multipart strings: **REG_MULTI_SZ**.

A.5.2 Registry Entries for *Exchange Server 2007*

A.5.2.1 HKLM\SOFTWARE\Wow6432Node\PP-COM\MRS\ExchApl

The ExchApl values are stored in the following key:

HKKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\PP-COM\MRS\ExchApl

AcceptedDomain [REG_SZ]

Default:	-
Possible values:	<Domain name>

Memory location for the name of the domain accepted by the Exchange Hub Transport Server for sending status notifications. So that all status messages can be correctly routed back from Exchange to the XPR server, the XPR server as originator must use the Exchange 2007 “Standard Accepted Domain”. This value is directly written by the E2k7 Apl. The E2k7 Apl uses the Windows domain as originator by default. If the Windows domain is not identical with the mail domain, an adjustment must be performed via this registry key.

Access [REG_SZ]

Default:	-
Possible values:	<Password>

Password of the installing Exchange account. The password is entered here encoded.

Account [REG_SZ]

Default:	-
Possible values:	<Exchange account name>

Service account under which the ExUMApl runs. The service account must have administrator authority under Microsoft Exchange.

Addr_Lookup_Mode [REG_DWORD]

Default:	1
Possible values:	0 or 1
Remark:	Except in the case of extremely limited harddisk storage space, generation of the table should not be terminated since otherwise the performance is dramatically reduced.

A fax look-up table is created in which all mailboxes with fax numbers are integrated (1). This is the default setting. Since this table can be very large, it is possible to prevent its use with this parameter (0), so that required dialing numbers can be sequentially queried.

Address_Mode [REG_DWORD]

Default:	0
Possible values:	0 or 1

Determines if a dialing number is to be searched for in the global address list (0) or in the site container (1).

Address_Restrict_Mode [REG_DWORD]

Default:	1
Possible values:	0 or 1
Remark:	A restrict error occurs with containers that include more than 16,000 users. In this case Restrict should not be applied and the value should be set to "1".

Decides whether a MAPI restrict with fax numbers is to be executed on containers (0), or if the Connector goes through all entries individually and integrates only those mailboxes in the lookup table that have a fax number (1).

Admingroup_RDN [REG_SZ]

Default:	-
Possible values:	<Name entry>

Display name of the routing group (under "Administrative Groups") in which the connector is installed.

ADsDomainPath [REG_SZ]

Default:	-
Possible values:	<path specification>
Remark:	Example: DC=docutest, DC=alsdorf, DC=cycos, DC=com

Domain LDAP path (root path to the Active Directory).

Attrib [REG_MULTI_SZ]

Default:	<i>SF, IN, OUT, RCIT</i>
Possible values:	<i>SF, IN, OUT, RCIT, PRIV</i>
Remark:	<i>SF</i> : This logical line allows store-and-forward of documents. <i>IN</i> : This logical line allows inbound traffic with reference to the server. <i>OUT</i> : This logical line allows outbound traffic with reference to the server. <i>RCIT</i> : If a read report is received on this line, the corresponding CIT signal is deactivated. <i>PRIV</i> : To activate the privilege check for Exchange 2007 this value is written in the Attrib key. The initiating entity will then be checked as to whether it is entitled to execute send jobs that require a privilege.

A list of protocol attributes. With the APL installation they are reasonably preset so that in most cases no modifications have to be and should not be performed. In particular, some attributes are, depending on the type of line, unsuitable and even prevent the regular or intended operation via this line if they are added.

APL_SLOWDOWN [REG_DWORD]

Default:	<i>0</i>
Possible values:	<i><1000 ms, <value in milliseconds></i>
Remark:	The maximum value should not exceed 1000 ms.

Is used to default set a break between the transmission of single fax messages. This gives the MTA sufficient time to handle single send jobs with e.g. bulk mailing.

CLASSFAX_DR [REG_SZ]

Default:	<i>-</i>
Possible values:	<i><message classes></i>
Remark:	Example: IPM.NOTE

The user-defined *message class* entered here is used as form for a fax message delivery report (DR).

CLASSFAX_MSG [REG_SZ]

Default:	<i>-</i>
Possible values:	<i><message classes></i>
Remark:	Example: IPM.NOTE

The user-defined *message class* entered here is used as form for standard fax messages (MSG).

CLASSFAX_NDR [REG_SZ]

Default:	-
Possible values:	<message classes>
Remark:	Example: IPM.NOTE

The user-defined *message class* entered here is used as form for a fax message non-delivery report (NDR).

CLASSSMS_DR [REG_SZ]

Default:	-
Possible values:	<message classes>
Remark:	Example: IPM.NOTE

The user-defined *message class* entered here is used as form for a short-message delivery report (DR).

CLASSSMS_MSG [REG_SZ]

Default:	-
Possible values:	<message classes>
Remark:	Example: IPM.NOTE

The user-defined *message class* entered here is used as form for standard short messages (MSG).

CLASSSMS_NDR [REG_SZ]

Default:	-
Possible values:	<message classes>
Remark:	Example: IPM.NOTE

The user-defined *message class* entered here is used as form for a short message non-delivery report (NDR).

CLASSVOICE_DR [REG_SZ]

Default:	-
Possible values:	<message classes>
Remark:	Example: IPM.NOTE

The user-defined *message class* entered here is used as form for a voicemail delivery report (DR).

CLASSVOICE_MSG [REG_SZ]

Default:	-
Possible values:	<message classes>
Remark:	Example: IPM.NOTE

The user-defined *message class* entered here is used as form for standard voicemails (MSG).

CLASSVOICE_NDR [REG_SZ]

Default:	-
Possible values:	<message classes>
Remark:	Example: IPM.NOTE

The user-defined *message class* entered here is used as form for a voicemail non-delivery report (NDR).

Contacts [REG_MULTI_SZ]

Default:	-
Possible values:	<Entries>
Remark:	Example: <i>ExternalContacts;Business;CycosBusinessTelephoneNumber;Home;CycosHomeTelephoneNumber;Mobile;CycosMobileTelephoneNumber; etc.</i>

Via entries in this registry key, mapping of the data fields for calling number normalization of public folders is performed, when the Exch APL is to take over the normalization for CTI (see also [SupportContactScan Section A.5.4.1](#), “[SupportContactScan \[REG_DWORD\]](#)”, on page 632). For each database field available in the Outlook entry forms a corresponding database field can be assigned, via which the normalization is executed. These fields have the format:

```
public folder name;from1;to1;...fromN;toN
```

CreateDefaultMessageClasses [REG_DWORD]

Default:	0
Possible values:	0 or 1

When this registry value is set to 0 and no message classes are defined, no special forms are used to represent XPR documents. Thus the value 0 leads to the registry being read (as before) to use the message classes defined there. See registry keys CLASSxxx_MSG on this. This setting is normally used when the ServerBasedForms are not installed. In this case you can use the setting of the **Delivery_Reports** and **Suppress_Reports** registry keys to control which mechanism is to be used for sending the reports (Exchange Reports or XPR Reports).

Changing the default value from 0 to 1 results in the use of default message classes for voice and fax messages. In this way compatibility to existing installations and maximum flexibility is ensured.

CreateJournalBodyInformation [REG_DWORD]

Default:	0
Possible values:	0 or 1

If a fax message, passed on to Exchange via the XPR server, cannot be delivered, it is automatically routed to the inbox of the user defined under Postmaster. From there it can be forwarded to the actual recipient. For reasons of data security such messages do not have a body (message text). Setting this registry key to 1 generates a message text that provides details about the message recipient.

CTI_Lookup_Counter [REG_DWORD]

Default:	32
Remark:	For internal use only!

Number of CTI messages in the Drop Directory queue of the Connector. These messages are searched for and subsequently processed before other e-mail jobs are processed. Used to accelerate the processing of e-mail generated CTI jobs.

CTI_Monitor [REG_DWORD]

Default:	1
Possible values:	0 or 1

Determines whether (1) or not (0) the Connector Journal function is to be used with an available CTI license.

DeleteOutOfOfficeReply [REG_DWORD]

Default:	0
Possible values:	0 or 1

To rule out the rare case of a message loop occurring under unfavorable circumstances, this registry value can be set to 1.

The following scenario can be ruled out via this registry key: subscriber A sends a message to subscriber B. Subscriber B has activated his/her absence assistant. Therefore, after a certain period, an absence message is sent to A. In the meantime, A has activated his/her absence assistant as well, now replying to this message with an out-of-office message. In other words, an infinite exchange of absence messages would here be generated, only to be ended with one of the two subscribers logging on to Outlook again.

DeleteOutOfOfficeReplyTemplate [REG_DWORD]

Default:	0
Possible values:	0 or 1

This key prevents the message loop if an Outlook message template is used for the out-of-office message. Function see **DeleteOutOfOfficeReply**.

Delivery_Report [REG_DWORD]

Default:	0
Possible values:	0 or 1

If the standard Exchange Reports are to be used, set this value to 1. In the **Suppress_Reports** registry key the value must be set to 0 in addition.

NOTE: When set to 1, a report is definitely sent to the Exchange client, even if this option is disabled in the client.

Distrib_Count [REG_DWORD]

Default:	0
Possible values:	<Entry>

Maximum number of processed users in an Exchange distribution list in one run. No restrictions when set to 0.

DL_DelayStep [REG_DWORD]

Default:	0
Possible values:	0 or 1

Setting value 1 enables the delayed delivery of messages sent via a recipient list. A waiting period then separates the single send jobs. This waiting period between the messages is specified in the **DL_DelayTime** key.

Using the **DL_DelayStep** and **DL_DelayTime** key avoids the SMI_QUEUE overflow problem.

DL_DelayTime [REG_DWORD]

Default:	500
Possible values:	<Value in milliseconds>

In combination with the **DL_DelayStep** registry key, the delay time between processing the single send jobs of a recipient list is defaulted here.

Domain [REG_SZ]

Default:	-
Possible values:	<Domain name>

Name of the domain in which the Exchange server is installed.

DO_NOT_AUTO_RESTART [REG_DWORD]

Default:	0
Possible values:	0 or 1

Using this registry key the administrator can disable the watchdog feature for the E2k7Apl without changing the watchdog setting. This allows stopping/starting the E2k7Apl manually. If the value is set to 0, the watchdog attempts to restart the E2k7Apl automatically according to the defaulted watchdog setting. If the value is set to 1, a restart attempt via the watchdog will not be carried out and the administrator must restart the E2k7Apl manually.

DropDirectory [REG_SZ]

Default:	-
Possible values:	<UNC path name>

Storage for the network path to the storage directory.

EnableResolveCallerNumber [REG_DWORD]

Default:	1
Possible values:	0 or 1

Whether 1 or not 0 the display name for an incoming calling number shall be automatically determined is stored in this registry key.

EVERSION [REG_DWORD]

Default:	-
Possible values:	12 for connecting an <i>Exchange Server 2007</i> or later 14 for connecting an <i>Exchange Server 2010</i> .

This registry key holds the version of the Exchange server connected to the XPR server.

EXADDRESSTYPE [REG_SZ]

Default:	-
Possible values:	<address space name>
Example:	MRSn, with n = 1, 2, 3, ...

If several XPR servers and consequently several Exchange connectors are connected to an Exchange environment, this registry key is required for differentiating the Exchange foreign connectors. Assigning special address space names then optimizes message transmission. The foreign connectors are labeled by consecutive numbering.

ExchangeServer [REG_SZ]

Default:	-
Possible values:	<Name>

This registry value is the storage location for the name of the Exchange server that the Exch Apl connects. If the connection to a clustered Exchange environment is set up, the registry value is the storage location for the Windows cluster name.

ExtensionBuildNumbers [REG_DWORD]

Default:	-
Possible values:	<Build number>
Remark:	For internal use only!

Here the extension build number is automatically entered with the installation.

FaxLegacySenderAddress [REG_SZ]

Default:	-
Possible values:	<MRS:proxy address@MRS>
Remark:	See Section 4.11, "Fax Foreign-Systems Support", on page 171.

Users that are also Exchange users can use the fax legacy support by default. Via entry of the proxy address of a defined Exchange user, standard XPR users can also send fax messages to the Exchange server and thus via the special fax server.

FaxLegacySupport [REG_DWORD]

Default:	1
Possible values:	0 or 1
Remark:	See Section 4.11, "Fax Foreign-Systems Support", on page 171.

Value 1 activates the fax legacy support, 0 deactivates it.

FaxLegacySupportNumberLocalize [REG_DWORD]

Default:	1
Possible values:	0 or 1
Remark:	See Section 4.11, “Fax Foreign-Systems Support”, on page 171.

Value 1 activates calling number normalization. If this is not desired, deactivate the normalization (0) so that the address entry calling number is used.

Format [REG_MULTI_SZ]

Default:	PMF, ASC, TXT, WAV, AS7, BMP, BMP-COL, BIN, TG3, TG4
Possible values:	PMF, ASC, TXT, WAV, AS7, BMP, BMP-COL, BIN, TG3, TG4
Remark	For internal use only!

Presettings for the formats into which documents and file attachments are converted for Exchange.

FORMAT_TIFF4_Only [REG_DWORD]

Default:	-
Possible values:	Any value except 0
Remark:	This key must only be defined when FaxG3 documents arrive via a AVM Fritz ISDN card or should be displayed with the Kodak (Wang) fax viewer. 0 disables this feature.

The configuration of this registry key makes sure that the FaxG3 format invalid for the AVM Fritz ISDN card is intercepted and converted into a TIFFG4 format, which can then be read with the Kodak (Wang) fax viewer.

FromFieldFormatFax [REG_SZ]

Default:	-
Possible values:	originator, callername, callernumber, size, orgnumber, service with additional text.
Remark:	See Advanced Settings > Display Formats in Section 4.5.3.1, “Display Formats tab”, on page 145.

In this registry key the configuration data for representing additional information merely on **fax messages** are stored in the **From (Fax)** Outlook column.

FromFieldFormatVoice [REG_SZ]

Default:	-
Possible values:	<i>originator, callername, callernumber, size, orgnumber, service</i> with additional text.
Remark:	See Advanced Settings > Display Formats in Section 4.5.3.1, "Display Formats tab" , on page 145.

In this registry key the configuration data for representing additional information on **voice messages** is stored in the **From (Voice Message)** Outlook column.

GC_RECONNECT [REG_DWORD]

Default:	0
Possible values:	0 or 1

When set to 1, ExchApl will not use the local cache to search for the Exchange Server Global Catalog Server.

GUID [REG_SZ]

Default:	-
Possible values:	<CLSID>

Storage location for the automatically assigned CLSID of the connector.

HUBTRANSPORTSERVER [REG_SZ]

Default:	-
Possible values:	<server name>

Storage for the name of the Exchange Hub Transport server that is specified during the connector installation.

HUBTRANSPORTSERVER1 [REG_SZ]

Default:	-
Possible values:	<server name>
Remark:	In case of multiple hub transport server support this key must be manually created for the second Exchange Hub Transport server.

Storage for the name of the second Exchange Hub Transport server.

HUBTRANSPORTSERVER2 [REG_SZ]

Default:	-
Possible values:	<server name>
Remark:	In case of multiple hub transport server support this key must be manually created for the third Exchange Hub Transport server.

Storage for the name of the third Exchange Hub Transport server.

HUBTRANSPORTSERVER3 [REG_SZ]

Default:	-
Possible values:	<server name>
Remark:	In case of multiple hub transport server support this key must be manually created for the fourth Exchange Hub Transport server.

Storage for the name of the fourth Exchange Hub Transport server.

HUBTRANSPORTSERVER4 [REG_SZ]

Default:	-
Possible values:	<server name>
Remark:	In case of multiple hub transport server support this key must be manually created for the fifth Exchange Hub Transport server.

Storage for the name of the fifth Exchange Hub Transport server.

HUBTRANSPORTSERVER5 [REG_SZ]

Default:	-
Possible values:	<server name>
Remark:	In case of multiple hub transport server support this key must be manually created for the sixth Exchange Hub Transport server.

Storage for the name of the sixth Exchange Hub Transport server.

InformPostmasterWhenMailBoxFull [REG_DWORD]

Default:	1
Possible values:	0 or 1

1: All generated notifications are sent to the postmaster. You find details on this in [Section 4.9, “Waiting Loop Configuration for repeated Delivery”](#), on [page 161](#).

0: Only the final notification is sent to the postmaster.

InstallAddressTemplates [REG_DWORD]

Default:	0
Possible values:	<Value>
Remark:	For internal use only!

Storage for the installed address templates.

InstallPath [REG_SZ]

Default:	-
Possible values:	<path specification>

Path to the application file of the Exchange connector.

MailBoxFullRepeatCount [REG_DWORD]

Default:	5
Possible values:	0, 1, 2, ... <number of repetition attempts>
Remark	Entering the value 0 deactivates the function.

This defines how many delivery attempts are to take place. You find details on this in [Section 4.9, “Waiting Loop Configuration for repeated Delivery”](#), on page 161.

MailBoxFullRepeatIntervalInSeconds [REG_DWORD]

Default:	3600 (one hour)
Possible values:	<Any value in seconds>

This value determines in which time intervals the delivery attempts are to take place. You find details on this in [Section 4.9, “Waiting Loop Configuration for repeated Delivery”](#), on page 161.

MailboxStore [REG_SZ]

Default:	-
Possible values:	<Path to the mailbox store>

Path to the mailbox store in which the connector mailbox lies.

Multiline_Support [REG_DWORD]

Default:	0
Possible values:	0 or 1

Activates (1) the so-called multiline mode for several Exchange connectors. This is required when from a single XPR server Exchange connectors to several Exchange servers are to be installed.

NumberDisplayPresentation [REG_MULTI_SZ]

Default:	-
Possible values:	<Normalization rule(s)>
Remark:	See Section 4.5.3.1, "Normalization tab", on page 147.

In this registry key all rules are entered according to which the conversion of incoming calling numbers is to occur.

Organization_RDN [REG_SZ]

Default:	-
Possible values:	<Name entry>

Store for the display name of the organization.

PostmasterDisplay [REG_SZ]

Default:	-
Possible values:	<Name>
Remark:	Example: <i>Postmaster</i>

Name of the set postmaster address (in this example ***Postmaster***). This is where undeliverable messages are automatically routed to.

PostmasterDN [REG_SZ]

Default:	-
Possible values:	<Entry>
Remark:	Example: \o=<Organization>\ou=<Site>\cn=<Recipient Container> \cn=<Recipient>

Entry of the Postmaster Account's Distinguished Name (DN).

Read_Report [REG_DWORD]

Default:	1
Possible values:	0 or 1

When set to 1 a read report will be requested for a newly delivered e-mail message by Exchange Server. For large organizations this can be suppressed here (0).

This is required for new or modified dialing numbers.

ReplayDirectory [REG_SZ]

Default:	-
Possible values:	<UNC path name>

Memory location for the network path to the replay directory for the first Hub Transport server.

ReplayDirectory1 [REG_SZ]

Default:	-
Possible values:	<UNC path name>
Remark:	Configuration in case of multiple hub transport server operation.

Memory location for the network path to the replay directory for the second Hub Transport server in case of multiple hub transport server operation.

ReplayDirectory2 [REG_SZ]

Default:	-
Possible values:	<UNC path name>
Remark:	Configuration in case of multiple hub transport server operation.

Memory location for the network path to the replay directory for the third Hub Transport server in case of multiple hub transport server operation.

ReplayDirectory3 [REG_SZ]

Default:	-
Possible values:	<UNC path name>
Remark:	Configuration in case of multiple hub transport server operation.

Memory location for the network path to the replay directory for the fourth Hub Transport server in case of multiple hub transport server operation.

ReplayDirectory4 [REG_SZ]

Default:	-
Possible values:	<UNC path name>
Remark:	Configuration in case of multiple hub transport server operation.

Memory location for the network path to the replay directory for the fifth Hub Transport server in case of multiple hub transport server operation.

ReplayDirectory5 [REG_SZ]

Default:	-
Possible values:	<UNC path name>
Remark:	Configuration in case of multiple hub transport server operation.

Memory location for the network path to the replay directory for the sixth Hub Transport server in case of multiple hub transport server operation.

RouteTableMinRebuildTime [REG_DWORD]

Default:	3600
Possible values:	<Any value in seconds>

Time in seconds after which the Fax Look-up table is to be reinstalled. This is required for new or modified dialing numbers.

Routinggroup [REG_SZ]

Default:	-
Possible values:	<Routing group name>

Store for the name of the routing group found first.

SentRepresenting [REG_DWORD]

Default:	0
Possible values:	0 or 1

Via this key you can configure which address information an e-mail is to contain that is replicated from Exchange to XPR.

0: The delegate's address is included.

1: The address of the user on whose behalf the message has been sent is included.

SendRTFBody [REG_DWORD]

Default:	1
Possible values:	0 or 1

E-mail messages will be transmitted inclusive the RTF body part to the XPR server (1). The RTF representation can be excluded with a value of 0.

Server [REG_SZ]

Default:	-
Possible values:	<server name>
Remark:	Example: XPR server

Windows name of the server on which the connector has been installed.

Site [REG_SZ]

Default:	-
Possible values:	<Site name>
Remark:	Example: /o=Sample AG /ou=AURELIUS

Name of the site under which the connector has been installed. This is done in X.500 notation as used with the Distinguished Names of Microsoft Exchange Server.

SMS_ALLOW_DIGEST [REG_DWORD]

Default:	0
Possible values:	0 or 1

When forwarding messages as short messages to a cell phone, a digest algorithm can be applied to the message. This algorithm, configurable on the XPR server, sees to an intelligent message shortening so that the maximum permissible number of characters for SMS messages is not exceeded. If a digest algorithm is defined and shall be used, too, set this registry value to 1.

Standard_Cti_Settings [REG_SZ]

Default:	-
Possible values:	0 or 1, for each of the four parameters <u,v,w,x>
Remark:	u, v, w, x = 0 or 1, 0 deactivated, 1 activated Example: If for the parameters u, v, w, x the values 0, 1, 0, 1 are set, only journal entries for failed calls are generated. Successful calls are not logged.

Via this registry key you can set the default behavior for call logging. You can define which journal entries are generated for all users that can employ CTI functions. Each of the four parameters (u, v, w and x) represents a notification option:

u: Successful inbound message (IN)
v: Unsuccessful inbound message (IN)
w: Successful outbound message (OUT)
x: Unsuccessful outbound message (OUT)

StorageGroup [REG_SZ]

Default:	-
Possible values:	<Path to the first storage group>

Storage for the path to the first storage group.

SubjectFieldFormat [REG_SZ]

Default:	-
Possible values:	originator, callername, callernumber, size, orgnumber, service with additional text.
Remark:	See Advanced Settings > Display Formats in Section 4.5.3.1, "Display Formats tab" , on page 145.

In this registry key the configuration data for representing additional information on fax and voice messages are stored in the **From** Outlook column.

SubjectFieldFormatFax [REG_SZ]

Default:	-
Possible values:	<i>originator, callername, callernumber, size, orgnumber, service</i> with additional text.
Remark:	See Advanced Settings > Display Formats in Section 4.5.3.1, "Display Formats tab" , on page 145.

In this registry key the configuration data for representing additional information on fax messages are stored in the **Subject (Fax)** Outlook column.

SubjectFieldFormatVoice [REG_SZ]

Default:	-
Possible values:	<i>originator, callername, callernumber, size, orgnumber, service</i> with additional text.
Remark:	See Advanced Settings > Display Formats in Section 4.5.3.1, "Display Formats tab" , on page 145.

In this registry key the configuration data for representing additional information on fax and voice messages are stored in the **From (Voice Message)** Outlook column.

SupportContactScan [REG_DWORD]

Default:	0
Possible values:	0 or 1

Phone number normalization of contacts in public folders can be activated (1) or deactivated (0) via the Exch APL. See also [Section A.5.2.1, "Contacts \[REG_MULTI_SZ\]"](#), on page 563.

Suppress_MID_Reports [REG_DWORD]

Default:	1
Possible values:	0 or 1

In reports the MID character string (message ID) is removed from the subject line (0). If the MID is required, a value of 1 should be used.

SuppressMIDinSubject [REG_DWORD]

Default:	0
Possible values:	0 or 1

If you do not want the MID (Message ID) to be displayed in a message's subject line, enter 1 here to avoid it. If 0 is set, the MID is indicated in the subject line as well.

Suppress_Reports [REG_DWORD]

Default:	0
Possible values:	0 or 1

If the Exchange Reports are used for sending and error confirmations (**Delivery_Report = 1**), the value must be set to 0.

If the XPR Report Forms are to be used (**Delivery_Report = 0**), this value is set to 1.

UnknownSenderName [REG_SZ]

Default:	<Unknown>
Possible values:	<Arbitrary entry for indicating an unknown originator>

Here you can deposit a text string used as originator information for all users when a message from an unknown originator arrives.

USEDSSERVER [REG_DWORD]

Default:	0
Possible values:	0 or 1

When set to 1, ExchApl will use the Global Catalog Server specified on <HKEY_CURRENT_USER\Software\Microsoft\Exchange\Exchange Provider\Provider\DS Server> when creating the MAPI profile for the Exchange Server connection.

WorkAroundAreaCodeProblem [REG_DWORD]

Default:	0
Possible values:	0 or 1

Addressing from within Outlook can cause problems when telephone or fax numbers in the format "+xxx(yyyy)zzzz" are stored in the contact information. Upon calling and handing over one of these addresses, the expression in brackets is replaced by its ASCII character and consequently the message cannot be sent. In the event that problems arise here, change the default value from (0) to 1 to avoid wrong addressing.

A.5.2.2 HKLM\SOFTWARE\Wow6432Node\PP-COM\MRS\ExUMApI

The values for the True Unified Messaging connector (ExUMApI) are stored in the following key:

HKKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\PP-COM\MRS\ExUMApI

Access [REG_SZ]

Default:	-
Possible values:	<Password>

Password of the installing Exchange account. The password is entered here encoded.

Account [REG_SZ]

Default:	-
Possible values:	<Exchange account name>

Service account under which the ExUMApI runs. The service account must have administrator authority under Microsoft Exchange.

AVOIDMAPIRELEASE [REG_DWORD]

Default:	0
Possible values:	0 or 1

In some Exchange environments the ExUMApI occasionally terminates its service unscheduled when the MAPI interface is shut down. If this behavior occurs you can stop the ExUMApI from terminating with help of this registry key. To this effect, set the value in this registry key from "0" to "1".

CPU_POLLING_INTERVAL [REG_DWORD]

Default:	0
Possible values:	any value in seconds

The registry key CPU_POLLING_INTERVAL allows to controls the interval (in seconds) of each check for the CPU consumption for the ExUmApI. Values less than 10 seconds, will be adjusted to 10.

CPU_LIMIT [REG_DWORD]

Default:	95
Possible values:	1 - 100

The registry key CPU_LIMIT specifies the limit acceptable for the CPU usage (percentage). If the ExUmApl exceeds the CPU_LIMIT three times (each CPU_POLLING_INTERVAL) the Apl will be restarted.
The default value is 95 if this registry key is not set but CPU_POLLING_INTERVAL is.

Domain [REG_SZ]

Default:	-
Possible values:	<Name>

The domain in which the Exchange server is installed.

EVERSION [REG_DWORD]

Default:	-
Possible values:	12 for connecting an <i>Exchange Server 2007</i> or later 14 for connecting an <i>Exchange Server 2010</i> .

This registry key holds the version of the Exchange server connected to the XPR server.

EXADDRESSTYPE [REG_SZ]

Default:	-
Possible values:	<address space name>
Example:	MRSn, with n = 1, 2, 3, ...

If several XPR servers and consequently several Exchange TUM connectors are connected to an Exchange environment, this registry key is required for differentiating the Exchange TUM connectors. Assigning special address space names then optimizes message transmission. The TUM connectors are labeled by consecutive numbering.

ExchangeClusterName [REG_SZ]

Default:	-
Possible values:	<Name>

Storage location for the Exchange cluster name, if the ExUM Apl is installed in a clustered Exchange environment.

ExchSCCPollTimer [REG_DWORD]

Default:	60
Possible values:	<Value in seconds>
Remark:	You can use this key only in the Single Copy Cluster (SCC) scenario in an Exchange Server 2007 environment. It must be added manually if required.

After the period given here the cluster status in the cluster installation is checked for changes.
Cluster status: Unchanged (active and no node switch because of an error) or changed (node switch because of an error)
If a node switch is detected, the ExUM Apl is shut down. Subsequently, it is rebooted with watchdog support.

ExchangeServer [REG_SZ]

Default:	-
Possible values:	<Name>

This registry value is the storage location for the name of the Exchange server that the ExUM Apl connects. If the connection to a clustered Exchange environment is set up, the registry value is the storage location for the Windows cluster name.

GUID [REG_SZ]

Default:	-
Possible values:	<CLSID>

Automatically assigned Connector CLSID.

HangedTimeout [REG_DWORD]

Default:	100
Possible values:	15, 16, 17, ...<value in seconds>
Remark:	If network errors are reported with the setting you have selected, the chosen value is too low; increase it in this case.

Settings parameter for the internal watchdog of the ExUM Apl.
Period after which a triggered ExUM APL thread is considered a “pending process”. Each detected “pending process” initiates a session cleanup. This terminates the process. Depending on the success or failure of the cleanup, a corresponding counter is counted up each.
Further setting parameters for the internal watchdog:

MaxFailedSessionCleanUps
MaxSessionCleanUps
ResetCountersPeriod
StopAplIfSessionsAreHanging
TerminateHanged

InstallPath [REG_SZ]

Default:	-
Possible values:	<path specification>
Remark:	Example: \\tsclient\Y\mrs7.01\2007-0~1\<product data carrier>\server

Path via which the ExUM APL was installed.

LINE_PROXY_PATTERN [REG_SZ]

Default:	-
Possible values:	<Regular expression>

In multiline environments a filter rule can be specified here that enables the control of user distribution among the single TUM connectors.

MaxFailedSessionCleanUps [REG_DWORD]

Default:	15
Possible values:	0, 1, 2, 3, ...
Remark:	If you enter value 0, the action is triggered with the first cleanup. The value should not be very high or too low altogether. A value too high may delay the error detection, and if it is too low, the ExUM Apl might be stopped too often.

Settings parameter for the internal watchdog of the ExUM Apl.

If the session cleanup counter reaches the value set here for failed cleanups, the action defined in key **StopAplIfSessionsAreHanging** is triggered.

Further setting parameters for the internal watchdog:

HangedTimeout
MaxSessionCleanUps
ResetCountersPeriod
StopAplIfSessionsAreHanging
TerminateHanged

MaxSessionCleanUps [REG_DWORD]

Default:	15
Possible values:	0, 1, 2, 3, ...
Remark:	If you enter value 0, the action is triggered with the first cleanup. The value should not be very high or too low altogether. A value too high may delay the error detection, and if it is too low, the ExUM Apl might be stopped too often.

Settings parameter for the internal watchdog of the ExUM Apl.

When the session cleanup counter reaches the value set here for successful cleanups, the action defined in key **StopAplIfSessionsAreHanging** is triggered.

Further setting parameters for the internal watchdog:

HangedTimeout
MaxFailedSessionCleanUps
ResetCountersPeriod
StopAplIfSessionsAreHanging
TerminateHanged

MULTILINE_SUPPORT [REG_DWORD]

Default:	0
Possible values:	0 or 1

To activate the multiline support, set this value to 1.

POLLING_INTERVAL [REG_DWORD]

Default:	0 (polling disabled)
Possible values:	0, 60 or higher (value in seconds)

Interval in seconds in which the ExUMApI checks whether the connection to the Exchange server is still up. You can determine the behavior triggered with an interrupted connection via the registry key **STOPONFAILURE** (see [Section A.5.2.2, “POLLING_INTERVAL \[REG_DWORD\]”, on page 582](#)

ResetCountersPeriod [REG_DWORD]

Default:	1
Possible values:	0, 1, 2, 3, ...<value in days>
Remark:	If you enter value 0, the session cleanup counters are not reset.

Settings parameter for the internal watchdog of the ExUM Apl.

Period in days in which the session cleanup counters are reset.

Further setting parameters for the internal watchdog:

HangedTimeout
MaxFailedSessionCleanUps
MaxSessionCleanUps
StopAplIfSessionsAreHanging
TerminateHanged

Server [REG_SZ]

Default:	-
Possible values:	<server name>
Remark:	

Windows name of the server on which the ExUM connector was installed.

Site [REG_SZ]

Default:	-
Possible values:	<Site name>
Remark:	Example: /o=<Organization>/ou=<Exchange mailbox store>

Name of the site under which the connector has been installed. This is done in X.500 notation as used with the Distinguished Names of Microsoft Exchange Server.

SKIPCALENDARONFAILURE[REG_DWORD]

Default:	0
Possible values:	0 or 1

If the login procedure is to carry on even if an error occurs when opening the calendar folder, you can configure that via this registry key. To this effect, set the value in this registry key from "0" to "1".

StopAplIfSessionsAreHanging [REG_DWORD]

Default:	0
Possible values:	0 or 1

Settings parameter for the internal watchdog of the ExUM Apl.

If an event is triggered via reaching the maximum value for **MaxSessionCleanUps** or **MaxFailedSessionCleanUps**, the corresponding action is selected here.

0 : A warning is issued in the log.

1 : The ExUM Apl is stopped. The XPR server watchdog detects this and an ExUM Apl restart is initiated.

Further setting parameters for the internal watchdog:

Appendix

Registry Entry Directory

HangedTimeout
MaxFailedSessionCleanUps
MaxSessionCleanUps
ResetCountersPeriod
TerminateHanged

STOPONFAILURE [REG_DWORD]

Default:	0
Possible values:	0 or 1

If activating **POLLING_INTERVAL** detects an interrupted connection to the Exchange server, you can specify the ExUMApI's behavior for this case via this registry key.

0: No action; the ExUMApI will not be rebooted.

1: The ExUMApI will be rebooted. This reboot is triggered by initiating the kernel watchdog.

TerminateHanged [REG_DWORD]

Default:	0
Possible values:	0 or 1

Settings parameter for the internal watchdog of the ExUM Apl.

Via this setting the session cleanup feature can be activated.

0: Function is deactivated

1: Function is active

Further setting parameters for the internal watchdog:

HangedTimeout

MaxFailedSessionCleanUps

MaxSessionCleanUps

ResetCountersPeriod

StopAplIfSessionsAreHanging

WaitExit [REG_WORD]

Default:	0
Possible values:	0 to 60

Settings parameter for the time (in seconds) to wait for the APL to finish the shutdown steps. It is used to ensure the Apl will not be locked during the shutdown procedure.

If it times out the APL exits abruptly.

A.5.3 Registry Entries for *Exchange Server 2010*

A.5.3.1 HKLM\SOFTWARE\Wow6432Node\PP-COM\MRS\ExchApl

The ExchApl values are stored in the following key:

HKKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\PP-COM\MRS\ExchApl

AcceptedDomain [REG_SZ]

Default:	-
Possible values:	<Domain name>

Memory location for the name of the domain accepted by the Exchange Hub Transport Server for sending status notifications. So that all status messages can be correctly routed back from Exchange to the XPR server, the XPR server as originator must use the Exchange 2007 “Standard Accepted Domain”. This value is directly written by the E2k7 Apl. The E2k7 Apl uses the Windows domain as originator by default. If the Windows domain is not identical with the mail domain, an adjustment must be performed via this registry key.

Access [REG_SZ]

Default:	-
Possible values:	<Password>

Password of the installing Exchange account. The password is entered here encoded.

Account [REG_SZ]

Default:	-
Possible values:	<Exchange account name>

Service account under which the E2k7Apl runs. The service account must have administrator authority under Microsoft Exchange.

Addr_Lookup_Mode [REG_DWORD]

Default:	1
Possible values:	0 or 1
Remark:	Except in the case of extremely limited harddisk storage space, generation of the table should not be terminated since otherwise the performance is dramatically reduced.

A fax look-up table is created in which all mailboxes with fax numbers are integrated (1). This is the default setting. Since this table can be very large, it is possible to prevent its use with this parameter (0), so that required dialing numbers can be sequentially queried.

Address_Mode [REG_DWORD]

Default:	0
Possible values:	0 or 1

Determines if a dialing number is to be searched for in the global address list (0) or in the site container (1).

Address_Restrict_Mode [REG_DWORD]

Default:	1
Possible values:	0 or 1
Remark:	A restrict error occurs with containers that include more than 16,000 users. In this case Restrict should not be applied and the value should be set to "1".

Decides whether a MAPI restrict with fax numbers is to be executed on containers (0), or if the Connector goes through all entries individually and integrates only those mailboxes in the lookup table that have a fax number (1).

Admingroup_RDN [REG_DW]

Default:	-
Possible values:	<Name entry>

Display name of the routing group (under "Administrative Groups") in which the connector is installed.

ADsDomainPath [REG_SZ]

Default:	-
Possible values:	<path specification>
Remark:	Example: DC=docutest, DC=alsdorf, DC=cycos, DC=com

Domain LDAP path (root path to the Active Directory).

Attrib [REG_MULTI_SZ]

Default:	<i>SF, IN, OUT, RCIT</i>
Possible values:	<i>SF, IN, OUT, RCIT, PRIV</i>
Remark:	<i>SF</i>: This logical line allows store-and-forward of documents. <i>IN</i>: This logical line allows inbound traffic with reference to the server. <i>OUT</i>: This logical line allows outbound traffic with reference to the server. <i>RCIT</i> : If a read report is received on this line, the corresponding CIT signal is deactivated. <i>PRIV</i>: To activate the privilege check for Exchange 2007 this value is written in the Attrib key. The initiating entity will then be checked as to whether it is entitled to execute send jobs that require a privilege.

A list of protocol attributes. With the APL installation they are reasonably preset so that in most cases no modifications have to be and should not be performed. In particular, some attributes are, depending on the type of line, unsuitable and even prevent the regular or intended operation via this line if they are added.

APL_SLOWDOWN [REG_DWORD]

Default:	<i>0</i>
Possible values:	<i><1000 ms, <value in milliseconds></i>
Remark:	The maximum value should not exceed 1000 ms.

Is used to default set a break between the transmission of single fax messages. This gives the MTA sufficient time to handle single send jobs with e.g. bulk mailing.

BYPASS_MBX_FOR_DAG [REG_DWORD]

Default:	<i>0</i>
Possible values:	<i>0 or 1</i>

Switching the connection to the DAG server that also connects the E2k7Apl to another DAG server stops the E2kApl. If the DAC server is to be switched, setting the registry key value from "0" to "1" prevents a fresh start of the E2KApl in this case.

CLASSFAX_DR [REG_SZ]

Default:	<i>-</i>
Possible values:	<i><message classes></i>
Remark:	Example: IPM.NOTE

The user-defined *message class* entered here is used as form for a fax message delivery report (DR).

CLASSFAX_MSG [REG_SZ]

Default:	-
Possible values:	<message classes>
Remark:	Example: IPM.NOTE

The user-defined *message class* entered here is used as form for standard fax messages (MSG).

CLASSFAX_NDR [REG_SZ]

Default:	-
Possible values:	<message classes>
Remark:	Example: IPM.NOTE

The user-defined *message class* entered here is used as form for a fax message non-delivery report (NDR).

CLASSSMS_DR [REG_SZ]

Default:	-
Possible values:	<message classes>
Remark:	Example: IPM.NOTE

The user-defined *message class* entered here is used as form for a short-message delivery report (DR).

CLASSSMS_MSG [REG_SZ]

Default:	-
Possible values:	<message classes>
Remark:	Example: IPM.NOTE

The user-defined *message class* entered here is used as form for standard short messages (MSG).

CLASSSMS_NDR [REG_SZ]

Default:	-
Possible values:	<message classes>
Remark:	Example: IPM.NOTE

The user-defined *message class* entered here is used as form for a short message non-delivery report (NDR).

CLASSVOICE_DR [REG_SZ]

Default:	-
Possible values:	< <i>message classes</i> >
Remark:	Example: IPM.NOTE

The user-defined *message class* entered here is used as form for a voicemail delivery report (DR).

CLASSVOICE_MSG [REG_SZ]

Default:	-
Possible values:	< <i>message classes</i> >
Remark:	Example: IPM.NOTE

The user-defined *message class* entered here is used as form for standard voicemails (MSG).

CLASSVOICE_NDR [REG_SZ]

Default:	-
Possible values:	< <i>message classes</i> >
Remark:	Example: IPM.NOTE

The user-defined *message class* entered here is used as form for a voicemail non-delivery report (NDR).

Contacts [REG_MULTI_SZ]

Default:	-
Possible values:	<Entries>
Remark:	Example: <i>ExternalContacts;Business;CycosBusinessTelephoneNumber;Home;CycosHomeTelephoneNumber;Mobile;CycosMobileTelephoneNumber; etc.</i>

Via entries in this registry key, mapping of the data fields for calling number normalization of public folders is performed, when the Exch APL is to take over the normalization for CTI (see also [SupportContactScan Section A.5.2.1, "SupportContactScan \[REG_DWORD\]", on page 576](#)). For each database field available in the Outlook entry forms a corresponding database field can be assigned, via which the normalization is executed. These fields have the format:

```
public folder name;from1;to1;...fromN;toN
```

CreateDefaultMessageClasses [REG_DWORD]

Default:	0
Possible values:	0 or 1

When this registry value is set to 0 and no message classes are defined, no special forms are used to represent XPR documents. Thus the value 0 leads to the registry being read (as before) to use the message classes defined there. See registry keys CLASSxxx_MSG on this. This setting is normally used when the ServerBasedForms are not installed. In this case you can use the setting of the **Delivery_Reports** and **Suppress_Reports** registry keys to control which mechanism is to be used for sending the reports (Exchange Reports or XPR Reports).

Changing the default value from 0 to 1 results in the use of default message classes for voice and fax messages. In this way compatibility to existing installations and maximum flexibility is ensured.

CreateJournalBodyInformation [REG_DWORD]

Default:	0
Possible values:	0 or 1

If a fax message, passed on to Exchange via the XPR server, cannot be delivered, it is automatically routed to the inbox of the user defined under Postmaster. From there it can be forwarded to the actual recipient. For reasons of data security such messages do not have a body (message text). Setting this registry key to 1 generates a message text that provides details about the message recipient.

CTI_Lookup_Counter [REG_DWORD]

Default:	32
Remark:	For internal use only!

Number of CTI messages in the Drop Directory queue of the Connector. These messages are searched for and subsequently processed before other e-mail jobs are processed. Used to accelerate the processing of e-mail generated CTI jobs.

CTI_Monitor [REG_DWORD]

Default:	1
Possible values:	0 or 1

Determines whether (1) or not (0) the Connector Journal function is to be used with an available CTI license.

DAGNODES [REG_MULTI_SZ]

Default:	-
Possible values:	NODE1, NODE2, ..., NODEn

In this key, NODE1, NODE2, ..., NODEn are the name entries of the servers that form the Database Availability Group.

DATABASE [REG_SZ]

Default:	-
Possible values:	<Database name>

This registry key holds the database name of the Exchange server selected during the setup.

DeleteOutOfOfficeReply [REG_DWORD]

Default:	0
Possible values:	0 or 1

To rule out the rare case of a message loop occurring under unfavorable circumstances, this registry value can be set to 1.

The following scenario can be ruled out via this registry key: subscriber A sends a message to subscriber B. Subscriber B has activated his/her absence assistant. Therefore, after a certain period, an absence message is sent to A. In the meantime, A has activated his/her absence assistant as well, now replying to this message with an out-of-office message. In other words, an infinite exchange of absence messages would here be generated, only to be ended with one of the two subscribers logging on to Outlook again.

DeleteOutOfOfficeReplyTemplate [REG_DWORD]

Default:	0
Possible values:	0 or 1

This key prevents the message loop if an Outlook message template is used for the out-of-office message. Function see **DeleteOutOfOfficeReply**.

Delivery_Report [REG_DWORD]

Default:	0
Possible values:	0 or 1

If the standard Exchange Reports are to be used, set this value to 1. In the **Suppress_Reports** registry key the value must be set to 0 in addition.

NOTE: When set to 1, a report is definitely sent to the Exchange client, even if this option is disabled in the client.

Distrib_Count [REG_DWORD]

Default:	0
Possible values:	<Entry>

Maximum number of processed users in an Exchange distribution list in one run. No restrictions when set to 0.

DL_DelayStep [REG_DWORD]

Default:	0
Possible values:	0 or 1

Setting value 1 enables the delayed delivery of messages sent via a recipient list. A waiting period then separates the single send jobs. This waiting period between the messages is specified in the **DL_DelayTime** key.

Using the **DL_DelayStep** and **DL_DelayTime** key avoids the SMI_QUEUE overflow problem.

DL_DelayTime [REG_DWORD]

Default:	500
Possible values:	<Value in milliseconds>

In combination with the **DL_DelayStep** registry key, the delay time between processing the single send jobs of a recipient list is defaulted here.

Domain [REG_SZ]

Default:	-
Possible values:	<Domain name>

Name of the domain in which the Exchange server is installed.

DO_NOT_AUTO_RESTART [REG_DWORD]

Default:	0
Possible values:	0 or 1

Using this registry key the administrator can disable the watchdog feature for the E2k7Apl without changing the watchdog setting. This allows stopping/starting the E2k7Apl manually. If the value is set to 0, the watchdog attempts to restart the E2k7Apl automatically according to the defaulted watchdog setting. If the value is set to 1, a restart attempt via the watchdog will not be carried out and the administrator must restart the E2k7Apl manually.

DropDirectory [REG_SZ]

Default:	-
Possible values:	<UNC path name>

Storage for the network path to the storage directory.

EnableResolveCallerNumber [REG_DWORD]

Default:	1
Possible values:	0 or 1

Whether (1) or not (0) the display name for an incoming calling number is to be automatically determined is stored in this registry key.

EVERSION [REG_DWORD]

Default:	-
Possible values:	12 for connecting an <i>Exchange Server 2007</i> or later 14 for connecting an <i>Exchange Server 2010</i> .

This registry key holds the version of the Exchange server connected to the XPR server.

EXADDRESSTYPE [REG_SZ]

Default:	-
Possible values:	<address space name>
Example:	MRSn, with n = 1, 2, 3, ...

If several XPR servers and consequently several Exchange connectors are connected to an Exchange environment, this registry key is required for differentiating the Exchange foreign connectors. Assigning special address space names then optimizes message transmission. The foreign connectors are labeled by consecutive numbering.

ExchangeServer [REG_SZ]

Default:	-
Possible values:	<Name>

This registry value is the storage location for the name of the Exchange server that the Exch Apl connects. If the connection to a clustered Exchange environment is set up, the registry value is the storage location for the Windows cluster name.

ExtensionBuildNumbers [REG_DWORD]

Default:	-
Possible values:	<Build number>
Remark:	For internal use only!

Here the extension build number is automatically entered with the installation.

FaxLegacySenderAddress [REG_SZ]

Default:	-
Possible values:	<MRS:proxy address@MRS>
Remark:	See Section 4.11, "Fax Foreign-Systems Support", on page 171.

Users that are also Exchange users can use the fax legacy support by default. Via entry of the proxy address of a defined Exchange user, standard XPR users can also send fax messages to the Exchange server and thus via the special fax server.

FaxLegacySupport [REG_DWORD]

Default:	1
Possible values:	0 or 1
Remark:	See Section 4.11, "Fax Foreign-Systems Support", on page 171.

Value 1 activates the fax legacy support, 0 deactivates it.

FaxLegacySupportNumberLocalize [REG_DWORD]

Default:	1
Possible values:	0 or 1
Remark:	See Section 4.11, "Fax Foreign-Systems Support", on page 171.

Value 1 activates calling number normalization. If this is not desired, deactivate the normalization (0) so that the address entry calling number is used.

Format [REG_MULTI_SZ]

Default:	PMF, ASC, TXT, WAV, AS7, BMP, BMP-COL, BIN, TG3, TG4
Possible values:	PMF, ASC, TXT, WAV, AS7, BMP, BMP-COL, BIN, TG3, TG4
Remark	For internal use only!

Presettings for the formats into which documents and file attachments are converted for Exchange.

FORMAT_TIFF4_Only [REG_DWORD]

Default:	-
Possible values:	Any value except 0
Remark:	This key must only be defined when FaxG3 documents arrive via a AVM Fritz ISDN card or should be displayed with the Kodak (Wang) fax viewer. 0 disables this feature.

The configuration of this registry key makes sure that the FaxG3 format invalid for the AVM Fritz ISDN card is intercepted and converted into a TIFFG4 format, which can then be read with the Kodak (Wang) fax viewer.

FromFieldFormatFax [REG_SZ]

Default:	-
Possible values:	originator, callername, callernumber, size, orgnumber, service with additional text.
Remark:	See Advanced Settings > Display Formats in Section 4.5.3.1, "Display Formats tab", on page 145.

In this registry key the configuration data for representing additional information merely on **fax messages** are stored in the **From (Fax)** Outlook column.

FromFieldFormatVoice [REG_SZ]

Default:	-
Possible values:	<i>originator, callername, callernumber, size, orgnumber, service</i> with additional text.
Remark:	See Advanced Settings > Display Formats in Section 4.5.3.1, "Display Formats tab" , on page 145.

In this registry key the configuration data for representing additional information on **voice messages** is stored in the **From (Voice Message)** Outlook column.

GC_RECONNECT [REG_DWORD]

Default:	0
Possible values:	0 or 1

When set to 1, ExchApl will not use the local cache to search for the Exchange Server Global Catalog Server.

GUID [REG_SZ]

Default:	-
Possible values:	<CLSID>

Storage location for the automatically assigned CLSID of the connector.

HUBTRANSPORTSERVER [REG_SZ]

Default:	-
Possible values:	<server name>

Storage for the name of the Exchange Hub Transport server that is specified during the connector installation.

HUBTRANSPORTSERVER1 [REG_SZ]

Default:	-
Possible values:	<server name>
Remark:	In case of multiple hub transport server support this key must be manually created for the second Exchange Hub Transport server.

Storage for the name of the second Exchange Hub Transport server.

HUBTRANSPORTSERVER2 [REG_SZ]

Default:	-
Possible values:	<server name>
Remark:	In case of multiple hub transport server support this key must be manually created for the third Exchange Hub Transport server.

Storage for the name of the third Exchange Hub Transport server.

HUBTRANSPORTSERVER3 [REG_SZ]

Default:	-
Possible values:	<server name>
Remark:	In case of multiple hub transport server support this key must be manually created for the fourth Exchange Hub Transport server.

Storage for the name of the fourth Exchange Hub Transport server.

HUBTRANSPORTSERVER4 [REG_SZ]

Default:	-
Possible values:	<server name>
Remark:	In case of multiple hub transport server support this key must be manually created for the fifth Exchange Hub Transport server.

Storage for the name of the fifth Exchange Hub Transport server.

HUBTRANSPORTSERVER5 [REG_SZ]

Default:	-
Possible values:	<server name>
Remark:	In case of multiple hub transport server support this key must be manually created for the sixth Exchange Hub Transport server.

Storage for the name of the sixth Exchange Hub Transport server.

InformPostmasterWhenMailBoxFull [REG_DWORD]

Default:	1
Possible values:	0 or 1

1: All generated notifications are sent to the postmaster. You find details on this in [Section 4.9, “Waiting Loop Configuration for repeated Delivery”](#), on page 161.

0: Only the final notification is sent to the postmaster.

InstallAddressTemplates [REG_DWORD]

Default:	0
Possible values:	<Value>
Remark:	For internal use only!

Storage for the installed address templates.

InstallPath [REG_SZ]

Default:	-
Possible values:	<path specification>

Path to the application file of the Exchange connector.

MailBoxFullRepeatCount [REG_DWORD]

Default:	5
Possible values:	0, 1, 2, ... <number of repetition attempts>
Remark	Entering the value 0 deactivates the function.

This defines how many delivery attempts are to take place. You find details on this in [Section 4.9, “Waiting Loop Configuration for repeated Delivery”](#), on page 161.

MailBoxFullRepeatIntervalInSeconds [REG_DWORD]

Default:	3600 (one hour)
Possible values:	<Any value in seconds>

This value determines in which time intervals the delivery attempts are to take place. You find details on this in [Section 4.9, “Waiting Loop Configuration for repeated Delivery”](#), on page 161.

Multiline_Support [REG_DWORD]

Default:	0
Possible values:	0 or 1

Activates (1) the so-called multiline mode for several Exchange connectors. This is required when from a single XPR server Exchange connectors to several Exchange servers are to be installed.

NumberDisplayPresentation [REG_MULTI_SZ]

Default:	-
Possible values:	<Normalization rule(s)>
Remark:	See Section 4.5.3.1, “Normalization tab” , on page 147.

In this registry key all rules are entered according to which the conversion of incoming calling numbers is to occur.

Organization_RDN [REG_SZ]

Default:	-
Possible values:	<Name entry>

Store for the display name of the organization.

PostmasterDisplay [REG_SZ]

Default:	-
Possible values:	<Name>
Remark:	Example: <i>Postmaster</i>

Name of the set postmaster address (in this example ***Postmaster***). This is where undeliverable messages are automatically routed to.

PostmasterDN [REG_SZ]

Default:	-
Possible values:	<Entry>
Remark:	Example: lo=<Organization>\ou=<Site>\cn=<Recipient Container> \cn=<Recipient>

Entry of the Postmaster Account's Distinguished Name (DN).

Read_Report [REG_DWORD]

Default:	1
Possible values:	0 or 1

When set to 1 a read report will be requested for a newly delivered e-mail message by Exchange Server. For large organizations this can be suppressed here (0).

This is required for new or modified dialing numbers.

ReplayDirectory [REG_SZ]

Default:	-
Possible values:	<UNC path name>

Memory location for the network path to the replay directory for the first Hub Transport server.

ReplayDirectory1 [REG_SZ]

Default:	-
Possible values:	<UNC path name>
Remark:	Configuration in case of multiple hub transport server operation.

Memory location for the network path to the replay directory for the second Hub Transport server in case of multiple hub transport server operation.

ReplayDirectory2 [REG_SZ]

Default:	-
Possible values:	<UNC path name>
Remark:	Configuration in case of multiple hub transport server operation.

Memory location for the network path to the replay directory for the third Hub Transport server in case of multiple hub transport server operation.

ReplayDirectory3 [REG_SZ]

Default:	-
Possible values:	<UNC path name>
Remark:	Configuration in case of multiple hub transport server operation.

Memory location for the network path to the replay directory for the fourth Hub Transport server in case of multiple hub transport server operation.

ReplayDirectory4 [REG_SZ]

Default:	-
Possible values:	<UNC path name>
Remark:	Configuration in case of multiple hub transport server operation.

Memory location for the network path to the replay directory for the fifth Hub Transport server in case of multiple hub transport server operation.

ReplayDirectory5 [REG_SZ]

Default:	-
Possible values:	<UNC path name>
Remark:	Configuration in case of multiple hub transport server operation.

Memory location for the network path to the replay directory for the sixth Hub Transport server in case of multiple hub transport server operation.

RouteTableMinRebuildTime [REG_DWORD]

Default:	3600
Possible values:	<Any value in seconds>

Time in seconds after which the Fax Look-up table is to be reinstalled. This is required for new or modified dialing numbers.

Routinggroup [REG_SZ]

Default:	-
Possible values:	<Routing group name>

Store for the name of the routing group found first.

SentRepresenting [REG_DWORD]

Default:	0
Possible values:	0 or 1

Via this key you can configure which address information an e-mail is to contain that is replicated from Exchange to XPR.

0: The delegate's address is included.
1: The address of the user on whose behalf the message has been sent is included.

SendRTFBody [REG_DWORD]

Default:	1
Possible values:	0 or 1

E-mail messages will be transmitted inclusive the RTF body part to the XPR server (1). The RTF representation can be excluded with a value of 0.

Server [REG_SZ]

Default:	-
Possible values:	<server name>
Remark:	Example: <i>XPR server</i>

Windows name of the server on which the connector has been installed.

Site [REG_SZ]

Default:	-
Possible values:	<Site name>
Remark:	Example: /o=Sample AG /ou=AURELIUS

Name of the site under which the connector has been installed. This is done in X.500 notation as used with the Distinguished Names of Microsoft Exchange Server.

SMS_ALLOW_DIGEST [REG_DWORD]

Default:	0
Possible values:	0 or 1

When forwarding messages as short messages to a cell phone, a digest algorithm can be applied to the message. This algorithm, configurable on the XPR server, sees to an intelligent message shortening so that the maximum permissible number of characters for SMS messages is not exceeded. If a digest algorithm is defined and shall be used, too, set this registry value to 1.

Standard_Cti_Settings [REG_SZ]

Default:	-
Possible values:	0 or 1, for each of the four parameters <u,v,w,x>
Remark:	u, v, w, x = 0 or 1, 0 deactivated, 1 activated Example: If for the parameters u, v, w, x the values 0, 1, 0, 1 are set, only journal entries for failed calls are generated. Successful calls are not logged.

Via this registry key you can set the default behavior for call logging. You can define which journal entries are generated for all users that can employ CTI functions. Each of the four parameters (u, v, w and x) represents a notification option:

- u: Successful inbound message (IN)
- v: Unsuccessful inbound message (IN)
- w: Successful outbound message (OUT)
- x: Unsuccessful outbound message (OUT)

SubjectFieldFormat [REG_SZ]

Default:	-
Possible values:	<i>originator, callername, callernumber, size, orgnumber, service</i> with additional text.
Remark:	See Advanced Settings > Display Formats in Section 4.5.3.1, "Display Formats tab" , on page 145.

In this registry key the configuration data for representing additional information on fax and voice messages are stored in the **From** Outlook column.

SubjectFieldFormatFax [REG_SZ]

Default:	-
Possible values:	<i>originator, callername, callernumber, size, orgnumber, service</i> with additional text.
Remark:	See Advanced Settings > Display Formats in Section 4.5.3.1, "Display Formats tab" , on page 145.

In this registry key the configuration data for representing additional information on fax messages are stored in the **Subject (Fax)** Outlook column.

SubjectFieldFormatVoice [REG_SZ]

Default:	-
Possible values:	<i>originator, callername, callernumber, size, orgnumber, service</i> with additional text.
Remark:	See Advanced Settings > Display Formats in Section 4.5.3.1, "Display Formats tab" , on page 145.

In this registry key the configuration data for representing additional information on fax and voice messages are stored in the **From (Voice Message)** Outlook column.

SupportContactScan [REG_DWORD]

Default:	0
Possible values:	0 or 1

Phone number normalization of contacts in public folders can be activated (1) or deactivated (0) via the Exch APL. See also [Section A.5.2.1, "Contacts \[REG_MULTI_SZ\]"](#), on page 563.

Suppress_MID_Reports [REG_DWORD]

Default:	1
Possible values:	0 or 1

In reports the MID character string (message ID) is removed from the subject line (0). If the MID is required, a value of 1 should be used.

SuppressMIDinSubject [REG_DWORD]

Default:	0
Possible values:	0 or 1

If you do not want the MID (Message ID) to be displayed in a message's subject line, enter 1 here to avoid it. If 0 is set, the MID is indicated in the subject line as well.

Suppress_Reports [REG_DWORD]

Default:	0
Possible values:	0 or 1

If the Exchange Reports are used for sending and error confirmations (**Delivery_Report = 1**), the value must be set to 0.

If the XPR Report Forms are to be used (**Delivery_Report = 0**), this value is set to 1.

UnknownSenderName [REG_SZ]

Default:	<Unknown>
Possible values:	<Arbitrary entry for indicating an unknown originator>

Here you can deposit a text string used as originator information for all users when a message from an unknown originator arrives.

USEDSSERVER [REG_DWORD]

Default:	0
Possible values:	0 or 1

When set to 1, ExchApl will use the Global Catalog Server specified on <HKEY_CURRENT_USER\Software\Microsoft\Exchange\Exchange Provider\Provider\DS Server> when creating the MAPI profile for the Exchange Server connection.

WorkAroundAreaCodeProblem [REG_DWORD]

Default:	0
Possible values:	0 or 1

Addressing from within Outlook can cause problems when telephone or fax numbers in the format "+xxx(yyyy)zzzz" are stored in the contact information. Upon calling and handing over one of these addresses, the expression in brackets is replaced by its ASCII character and consequently the message cannot be sent. In the event that problems arise here, change the default value from (0) to 1 to avoid wrong addressing.

A.5.3.2 HKLM\SOFTWARE\Wow6432Node\PP-COM\MRS\ExUMAp1

The ExUMAp1 values are stored in the following key:

HKKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\PP-COM\MRS\ExUMAp1

Access [REG_SZ]

Default:	-
Possible values:	<Password>

Password of the installing Exchange account. The password is entered here encoded.

Account [REG_SZ]

Default:	-
Possible values:	<Exchange account name>

Service account under which the ExUMAp1 runs. The service account must have administrator authority under Microsoft Exchange.

ACCOUNTDN [REG_SZ]

Default:	-
Possible values:	<Data of the LegacyExchangeDN Active Directory Object for the TUM service account>

The LegacyExchangeDN Active Directory Object data is read into this registry key via an AD query. This object is used for localizing the XPR service account in the Active Directory to enable logging the XPR service account on to the Exchange server.

ACCOUNTDNFULL [REG_SZ]

Default:	-
Possible values:	<Entry of the LegacyExchangeDN object data>

If errors occur on reading in data of the LegacyExchangeDN object during the ExUMAp1 start, you can add this registry key manually. If the key is present and the entry specified, the data defaulted here for logging the XPR service account on to the Exchange server is automatically used. If the key is not available, the data provided in the registry key **ACCOUNTDN** via an AD query is used.

AVOIDMAPIRELEASE [REG_DWORD]

Default:	0
Possible values:	0 or 1

In some Exchange environments the ExUMApI occasionally terminates its service unscheduled when the MAPI interface is shut down. If this behavior occurs you can stop the ExUMApI from terminating with help of this registry key. To this effect, set the value in this registry key from “0” to “1”.

CASARRAY [REG_SZ]

Default:	-
Possible values:	0 or 1

Registry key for connecting the ExUM Apl to an organization with *Exchange Server 2010 CAS Array*. Adding this key and setting this value to 1 activates the support of the gateway solution.

CASARRAYNAME [REG_MULTI_SZ]

Default:	-
Possible values:	CASARRAY01-DNS CASARRAY02-DNS CASARRAYn-DNS <DNS-names of the respective Exchange Server CAS Arrays>

Name of the *Exchange Server 2010 CAS Arrays*. The DNS name of the respective CAS array must be used as value for **CASARRAYNAME**.

CHECKCASARRAY [REG_DWORD]

Default:	-
Possible value:	1

If no WNLB (Windows Network Load Balancing) is installed in the Exchange environment, the ExUmApl is connected to a single CAS server. In this case you must add this registry key manually. If you enter value “1” in this registry key, the ExUMApI adjusts the profile for this operating mode automatically.

CPU_POLLING_INTERVAL [REG_DWORD]

Default:	0
Possible values:	any value in seconds

The registry key CPU_POLLING_INTERVAL allows to controls the interval (in seconds) of each check for the CPU consumption for the ExUmApl. Values less than 10 seconds, will be adjusted to 10.

CPU_LIMIT [REG_DWORD]

Default:	95
Possible values:	1 - 100

The registry key CPU_LIMIT specifies the limit acceptable for the CPU usage (percentage). If the ExUmApl exceeds the CPU_LIMIT three times (each CPU_POLLING_INTERVAL) the Apl will be restarted.
The default value is 95 if this registry key is not set but CPU_POLLING_INTERVAL is.

Domain [REG_SZ]

Default:	-
Possible values:	<Name>

The domain in which the Exchange server is installed.

EVERSION [REG_DWORD]

Default:	-
Possible values:	12 for connecting an <i>Exchange Server 2007</i> or later 14 for connecting an <i>Exchange Server 2010</i> .

This registry key holds the version of the Exchange server connected to the XPR server.

EXADDRESSTYPE [REG_SZ]

Default:	-
Possible values:	<address space name>
Example:	MRSn, with n = 1, 2, 3, ...

If several XPR servers and consequently several Exchange TUM connectors are connected to an Exchange environment, this registry key is required for differentiating the Exchange TUM connectors. Assigning special address space names then optimizes message transmission. The TUM connectors are labeled by consecutive numbering.

ExchangeClusterName [REG_SZ]

Default:	-
Possible values:	<Name>

Storage location for the Exchange cluster name, if the ExUM Apl is installed in a clustered Exchange environment.

ExchangeServer [REG_SZ]

Default:	-
Possible values:	<Name>

This registry value is the storage location for the name of the Exchange server that the ExUM Apl connects. If the connection to a clustered Exchange environment is set up, the registry value is the storage location for the Windows cluster name.

GUID [REG_SZ]

Default:	-
Possible values:	<CLSID>

Automatically assigned Connector CLSID.

HangedTimeout [REG_DWORD]

Default:	100
Possible values:	15, 16, 17, ...<value in seconds>
Remark:	If network errors are reported with the setting you have selected, the chosen value is too low; increase it in this case.

Settings parameter for the internal watchdog of the ExUM Apl.

Period after which a triggered ExUM APL thread is considered a “pending process”. Each detected “pending process” initiates a session cleanup. This terminates the process. Depending on the success or failure of the cleanup, a corresponding counter is counted up each.

Further setting parameters for the internal watchdog:

MaxFailedSessionCleanUps
MaxSessionCleanUps
ResetCountersPeriod
StopAplIfSessionsAreHanging
TerminateHanged

InstallPath [REG_SZ]

Default:	-
Possible values:	<path specification>
Remark:	Example: \\tsclient\Y\mrs7.01\2007-0~1\<product data carrier>\server

Path via which the ExUM APL was installed.

LINE_PROXY_PATTERN [REG_SZ]

Default:	-
Possible values:	<Regular expression>

In multiline environments a filter rule can be specified here that enables the control of user distribution among the single TUM connectors.

MaxFailedSessionCleanUps [REG_DWORD]

Default:	15
Possible values:	0, 1, 2, 3, ...
Remark:	If you enter value 0, the action is triggered with the first cleanup. The value should not be very high or too low altogether. A value too high may delay the error detection, and if it is too low, the ExUM Apl might be stopped too often.

Settings parameter for the internal watchdog of the ExUM Apl.

If the session cleanup counter reaches the value set here for failed cleanups, the action defined in key **StopAplIfSessionsAreHanging** is triggered.

Further setting parameters for the internal watchdog:

- HangedTimeout
- MaxSessionCleanUps
- ResetCountersPeriod
- StopAplIfSessionsAreHanging
- TerminateHanged

MaxSessionCleanUps [REG_DWORD]

Default:	15
Possible values:	0, 1, 2, 3, ...
Remark:	If you enter value 0, the action is triggered with the first cleanup. The value should not be very high or too low altogether. A value too high may delay the error detection, and if it is too low, the ExUM Apl might be stopped too often.

Settings parameter for the internal watchdog of the ExUM Apl.

When the session cleanup counter reaches the value set here for successful cleanups, the action defined in key **StopAplIfSessionsAreHanging** is triggered.

Further setting parameters for the internal watchdog:

- HangedTimeout
- MaxFailedSessionCleanUps
- ResetCountersPeriod
- StopAplIfSessionsAreHanging
- TerminateHanged

MULTILINE_SUPPORT [REG_DWORD]

Default:	0
Possible values:	0 or 1

To activate the multiline support, set this value to 1.

POLLING_INTERVAL [REG_DWORD]

Default:	0 (polling disabled)
Possible values:	0, 60 or higher (value in seconds)

Interval in seconds in which the ExUMApI checks whether the connection to the Exchange server is still up. You can determine the behavior triggered with an interrupted connection via the registry key **STOPONFAILURE** (see [Section A.5.3.2, “STOPONFAILURE \[REG_DWORD\]”, on page 612](#)).

ResetCountersPeriod [REG_DWORD]

Default:	1
Possible values:	0, 1, 2, 3, ...<value in days>
Remark:	If you enter value 0, the session cleanup counters are not reset.

Settings parameter for the internal watchdog of the ExUM Apl.

Period in days in which the session cleanup counters are reset.

Further setting parameters for the internal watchdog:

HangedTimeout
MaxFailedSessionCleanUps
MaxSessionCleanUps
StopAplIfSessionsAreHanging
TerminateHanged

Server [REG_SZ]

Default:	-
Possible values:	<server name>
Remark:	

Windows name of the server on which the ExUM connector was installed.

Site [REG_SZ]

Default:	-
Possible values:	<Site name>
Remark:	Example: /o=<Organization>/ou=<Exchange mailbox store>

Name of the site under which the connector has been installed. This is done in X.500 notation as used with the Distinguished Names of Microsoft Exchange Server.

SKIPCALENDARONFAILURE[REG_DWORD]

Default:	0
Possible values:	0 or 1

If the login procedure is to carry on even if an error occurs when opening the calendar folder, you can configure that via this registry key. To this effect, set the value in this registry key from “0” to “1”.

StopApIfSessionsAreHanging [REG_DWORD]

Default:	0
Possible values:	0 or 1

Settings parameter for the internal watchdog of the ExUM Apl.

If an event is triggered via reaching the maximum value for **MaxSessionCleanUps** or **MaxFailedSessionCleanUps**, the corresponding action is selected here.

0 : A warning is issued in the log.

1 : The ExUM Apl is stopped. The XPR server watchdog detects this and an ExUM Apl restart is initiated.

Further setting parameters for the internal watchdog:

HangedTimeout
MaxFailedSessionCleanUps
MaxSessionCleanUps
ResetCountersPeriod
TerminateHanged

STOPONFAILURE [REG_DWORD]

Default:	0
Possible values:	0 or 1

If activating **POLLING_INTERVAL** detects an interrupted connection to the Exchange server, you can specify the ExUMApI's behavior for this case via this registry key.

0: No action; the ExUMApI will not be rebooted.

1: The ExUMApI will be rebooted. This reboot is triggered by initiating the kernel watchdog.

TerminateHanged [REG_DWORD]

Default:	0
Possible values:	0 or 1

Settings parameter for the internal watchdog of the ExUM Apl.

Via this setting the session cleanup feature can be activated.

0: Function is deactivated

1: Function is active

Further setting parameters for the internal watchdog:

HangedTimeout

MaxFailedSessionCleanUps

MaxSessionCleanUps

ResetCountersPeriod

StopAplIfSessionsAreHanging

WaitExit [REG_WORD]

Default:	0
Possible values:	0 to 60

Settings parameter for the time (in seconds) to wait for the APL to finish the shutdown steps. It is used to ensure the Apl will not be locked during the shutdown procedure.

If it times out the APL exits abruptly.

A.5.4 Registry Entries for *Exchange Server 2013*

A.5.4.1 HKLM\SOFTWARE\Wow6432Node\PP-COM\MRS\ExchApl

The ExchApl values are stored in the following key:

HKKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\PP-COM\MRS\ExchApl

AcceptedDomain [REG_SZ]

Default:	-
Possible values:	<Domain name>

Memory location for the name of the domain accepted by the Exchange Hub Transport Server for sending status notifications. So that all status messages can be correctly routed back from Exchange to the XPR server, the XPR server as originator must use the Exchange 2007 “Standard Accepted Domain”. This value is directly written by the E2k7 Apl. The E2k7 Apl uses the Windows domain as originator by default. If the Windows domain is not identical with the mail domain, an adjustment must be performed via this registry key.

Access [REG_SZ]

Default:	-
Possible values:	<Password>

Password of the installing Exchange account. The password is entered here encoded.

Account [REG_SZ]

Default:	-
Possible values:	<Exchange account name>

Service account under which the E2k7Apl runs. The service account must have administrator authority under Microsoft Exchange.

Addr_Lookup_Mode [REG_DWORD]

Default:	1
Possible values:	0 or 1
Remark:	Except in the case of extremely limited harddisk storage space, generation of the table should not be terminated since otherwise the performance is dramatically reduced.

A fax look-up table is created in which all mailboxes with fax numbers are integrated (1). This is the default setting. Since this table can be very large, it is possible to prevent its use with this parameter (0), so that required dialing numbers can be sequentially queried.

Address_Mode [REG_DWORD]

Default:	0
Possible values:	0 or 1

Determines if a dialing number is to be searched for in the global address list (0) or in the site container (1).

Address_Restrict_Mode [REG_DWORD]

Default:	1
Possible values:	0 or 1
Remark:	A restrict error occurs with containers that include more than 16,000 users. In this case Restrict should not be applied and the value should be set to "1".

Decides whether a MAPI restrict with fax numbers is to be executed on containers (0), or if the Connector goes through all entries individually and integrates only those mailboxes in the lookup table that have a fax number (1).

Admingroup_RDN [REG_DW]

Default:	-
Possible values:	<Name entry>

Display name of the routing group (under "Administrative Groups") in which the connector is installed.

ADsDomainPath [REG_SZ]

Default:	-
Possible values:	<path specification>
Remark:	Example: DC=docutest, DC=alsdorf, DC=cycos, DC=com

Domain LDAP path (root path to the Active Directory).

Attrib [REG_MULTI_SZ]

Default:	<i>SF, IN, OUT, RCIT</i>
Possible values:	<i>SF, IN, OUT, RCIT, PRIV</i>
Remark:	<i>SF</i>: This logical line allows store-and-forward of documents. <i>IN</i>: This logical line allows inbound traffic with reference to the server. <i>OUT</i>: This logical line allows outbound traffic with reference to the server. <i>RCIT</i> : If a read report is received on this line, the corresponding CIT signal is deactivated. <i>PRIV</i>: To activate the privilege check for Exchange 2007 this value is written in the Attrib key. The initiating entity will then be checked as to whether it is entitled to execute send jobs that require a privilege.

A list of protocol attributes. With the APL installation they are reasonably preset so that in most cases no modifications have to be and should not be performed. In particular, some attributes are, depending on the type of line, unsuitable and even prevent the regular or intended operation via this line if they are added.

APL_SLOWDOWN [REG_DWORD]

Default:	<i>0</i>
Possible values:	<i><1000 ms, <value in milliseconds></i>
Remark:	The maximum value should not exceed 1000 ms.

Is used to default set a break between the transmission of single fax messages. This gives the MTA sufficient time to handle single send jobs with e.g. bulk mailing.

BYPASS_MBX_FOR_DAG [REG_DWORD]

Default:	<i>0</i>
Possible values:	<i>0 or 1</i>

Switching the connection to the DAG server that also connects the E2k7Apl to another DAG server stops the E2kApl. If the DAG server is to be switched, setting the registry key value from "0" to "1" prevents a fresh start of the E2KApl in this case.

CLASSFAX_DR [REG_SZ]

Default:	<i>-</i>
Possible values:	<i><message classes></i>
Remark:	Example: IPM.NOTE

The user-defined *message class* entered here is used as form for a fax message delivery report (DR).

CLASSFAX_MSG [REG_SZ]

Default:	-
Possible values:	<message classes>
Remark:	Example: IPM.NOTE

The user-defined *message class* entered here is used as form for standard fax messages (MSG).

CLASSFAX_NDR [REG_SZ]

Default:	-
Possible values:	<message classes>
Remark:	Example: IPM.NOTE

The user-defined *message class* entered here is used as form for a fax message non-delivery report (NDR).

CLASSSMS_DR [REG_SZ]

Default:	-
Possible values:	<message classes>
Remark:	Example: IPM.NOTE

The user-defined *message class* entered here is used as form for a short-message delivery report (DR).

CLASSSMS_MSG [REG_SZ]

Default:	-
Possible values:	<message classes>
Remark:	Example: IPM.NOTE

The user-defined *message class* entered here is used as form for standard short messages (MSG).

CLASSSMS_NDR [REG_SZ]

Default:	-
Possible values:	<message classes>
Remark:	Example: IPM.NOTE

The user-defined *message class* entered here is used as form for a short message non-delivery report (NDR).

CLASSVOICE_DR [REG_SZ]

Default:	-
Possible values:	< <i>message classes</i> >
Remark:	Example: IPM.NOTE

The user-defined *message class* entered here is used as form for a voicemail delivery report (DR).

CLASSVOICE_MSG [REG_SZ]

Default:	-
Possible values:	< <i>message classes</i> >
Remark:	Example: IPM.NOTE

The user-defined *message class* entered here is used as form for standard voicemails (MSG).

CLASSVOICE_NDR [REG_SZ]

Default:	-
Possible values:	< <i>message classes</i> >
Remark:	Example: IPM.NOTE

The user-defined *message class* entered here is used as form for a voicemail non-delivery report (NDR).

Contacts [REG_MULTI_SZ]

Default:	-
Possible values:	<Entries>
Remark:	Example: <i>ExternalContacts;Business;CycosBusinessTelephoneNumber;Home;CycosHomeTelephoneNumber;Mobile;CycosMobileTelephoneNumber; etc.</i>

Via entries in this registry key, mapping of the data fields for calling number normalization of public folders is performed, when the Exch APL is to take over the normalization for CTI (see also [SupportContactScan Section A.5.2.1, "SupportContactScan \[REG_DWORD\]", on page 576](#)). For each database field available in the Outlook entry forms a corresponding database field can be assigned, via which the normalization is executed. These fields have the format:

```
public folder name;from1;to1;...fromN;toN
```

CPU_POLLING_INTERVAL [REG_DWORD]

Default:	0
Possible values:	<i>any value in seconds</i>

The registry key CPU_POLLING_INTERVAL allows to controls the interval (in seconds) of each check for the CPU consumption for the ExUmApl. Values less than 10 seconds, will be adjusted to 10.

CPU_LIMIT [REG_DWORD]

Default:	95
Possible values:	1 - 100

The registry key CPU_LIMIT specifies the limit acceptable for the CPU usage (percentage). If the ExUmApl exceeds the CPU_LIMIT three times (each CPU_POLLING_INTERVAL) the Apl will be restarted. The default value is 95 if this registry key is not set but CPU_POLLING_INTERVAL is.

CreateDefaultMessageClasses [REG_DWORD]

Default:	0
Possible values:	0 or 1

When this registry value is set to 0 and no message classes are defined, no special forms are used to represent XPR documents. Thus the value 0 leads to the registry being read (as before) to use the message classes defined there. See registry keys CLASSxxx_MSG on this. This setting is normally used when the ServerBasedForms are not installed. In this case you can use the setting of the **Delivery_Reports** and **Suppress_Reports** registry keys to control which mechanism is to be used for sending the reports (Exchange Reports or XPR Reports).

Changing the default value from 0 to 1 results in the use of default message classes for voice and fax messages. In this way compatibility to existing installations and maximum flexibility is ensured.

CreateJournalBodyInformation [REG_DWORD]

Default:	0
Possible values:	0 or 1

If a fax message, passed on to Exchange via the XPR server, cannot be delivered, it is automatically routed to the inbox of the user defined under Postmaster. From there it can be forwarded to the actual recipient. For reasons of data security such messages do not have a body (message text). Setting this registry key to 1 generates a message text that provides details about the message recipient.

CTI_Lookup_Counter [REG_DWORD]

Default:	32
Remark:	For internal use only!

Number of CTI messages in the Drop Directory queue of the Connector. These messages are searched for and subsequently processed before other e-mail jobs are processed. Used to accelerate the processing of e-mail generated CTI jobs.

CTI_Monitor [REG_DWORD]

Default:	1
Possible values:	0 or 1

Determines whether (1) or not (0) the Connector Journal function is to be used with an available CTI license.

DAGNODES [REG_MULTI_SZ]

Default:	-
Possible values:	NODE1, NODE2, ..., NODEn

In this key, NODE1, NODE2, ..., NODEn are the name entries of the servers that form the Database Availability Group.

DATABASE [REG_SZ]

Default:	-
Possible values:	<Database name>

This registry key holds the database name of the Exchange server selected during the setup.

DeleteOutOfOfficeReply [REG_DWORD]

Default:	0
Possible values:	0 or 1

To rule out the rare case of a message loop occurring under unfavorable circumstances, this registry value can be set to 1.

The following scenario can be ruled out via this registry key: subscriber A sends a message to subscriber B. Subscriber B has activated his/her absence assistant. Therefore, after a certain period, an absence message is sent to A. In the meantime, A has activated his/her absence assistant as well, now replying to this message with an out-of-office message. In other words, an infinite exchange of absence messages would here be generated, only to be ended with one of the two subscribers logging on to Outlook again.

DeleteOutOfOfficeReplyTemplate [REG_DWORD]

Default:	0
Possible values:	0 or 1

This key prevents the message loop if an Outlook message template is used for the out-of-office message. Function see **DeleteOutOfOfficeReply**.

Delivery_Report [REG_DWORD]

Default:	0
Possible values:	0 or 1

If the standard Exchange Reports are to be used, set this value to 1. In the **Suppress_Reports** registry key the value must be set to 0 in addition.

NOTE: When set to 1, a report is definitely sent to the Exchange client, even if this option is disabled in the client.

Distrib_Count [REG_DWORD]

Default:	0
Possible values:	<Entry>

Maximum number of processed users in an Exchange distribution list in one run.
No restrictions when set to 0.

DL_DelayStep [REG_DWORD]

Default:	0
Possible values:	0 or 1

Setting value 1 enables the delayed delivery of messages sent via a recipient list. A waiting period then separates the single send jobs. This waiting period between the messages is specified in the **DL_DelayTime** key.

Using the **DL_DelayStep** and **DL_DelayTime** key avoids the SMI_QUEUE overflow problem.

DL_DelayTime [REG_DWORD]

Default:	500
Possible values:	<Value in milliseconds>

In combination with the **DL_DelayStep** registry key, the delay time between processing the single send jobs of a recipient list is defaulted here.

Domain [REG_SZ]

Default:	-
Possible values:	<Domain name>

Name of the domain in which the Exchange server is installed.

DO_NOT_AUTO_RESTART [REG_DWORD]

Default:	0
Possible values:	0 or 1

Using this registry key the administrator can disable the watchdog feature for the E2k7Apl without changing the watchdog setting. This allows stopping/starting the E2k7Apl manually. If the value is set to 0, the watchdog attempts to restart the E2k7Apl automatically according to the defaulted watchdog setting. If the value is set to 1, a restart attempt via the watchdog will not be carried out and the administrator must restart the E2k7Apl manually.

DropDirectory [REG_SZ]

Default:	-
Possible values:	<UNC path name>

Storage for the network path to the storage directory.

EnableResolveCallerNumber [REG_DWORD]

Default:	1
Possible values:	0 or 1

Whether (1) or not (0) the display name for an incoming calling number is to be automatically determined is stored in this registry key.

EVERSION [REG_DWORD]

Default:	-
Possible values:	12 for connecting an <i>Exchange Server 2007</i> , 14 for connecting an <i>Exchange Server 2010</i> , 15 for connecting an <i>Exchange Server 2013</i> .

This registry key holds the version of the Exchange server connected to the XPR server.

EXADDRESSTYPE [REG_SZ]

Default:	-
Possible values:	<address space name>
Example:	MRSn, with n = 1, 2, 3, ...

If several XPR servers and consequently several Exchange connectors are connected to an Exchange environment, this registry key is required for differentiating the Exchange foreign connectors. Assigning special address space names then optimizes message transmission. The foreign connectors are labeled by consecutive numbering.

ExchangeServer [REG_SZ]

Default:	-
Possible values:	<Name>

This registry value is the storage location for the name of the Exchange server that the Exch Apl connects. If the connection to a clustered Exchange environment is set up, the registry value is the storage location for the Windows cluster name.

ExtensionBuildNumbers [REG_DWORD]

Default:	-
Possible values:	<Build number>
Remark:	For internal use only!

Here the extension build number is automatically entered with the installation.

FaxLegacySenderAddress [REG_SZ]

Default:	-
Possible values:	<MRS:proxy address@MRS>
Remark:	See Section 4.11, "Fax Foreign-Systems Support", on page 171.

Users that are also Exchange users can use the fax legacy support by default. Via entry of the proxy address of a defined Exchange user, standard XPR users can also send fax messages to the Exchange server and thus via the special fax server.

FaxLegacySupport [REG_DWORD]

Default:	1
Possible values:	0 or 1
Remark:	See Section 4.11, "Fax Foreign-Systems Support", on page 171.

Value 1 activates the fax legacy support, 0 deactivates it.

FaxLegacySupportNumberLocalize [REG_DWORD]

Default:	1
Possible values:	0 or 1
Remark:	See Section 4.11, "Fax Foreign-Systems Support", on page 171.

Value 1 activates calling number normalization. If this is not desired, deactivate the normalization (0) so that the address entry calling number is used.

Format [REG_MULTI_SZ]

Default:	PMF, ASC, TXT, WAV, AS7, BMP, BMP-COL, BIN, TG3, TG4
Possible values:	PMF, ASC, TXT, WAV, AS7, BMP, BMP-COL, BIN, TG3, TG4
Remark:	For internal use only!

Presettings for the formats into which documents and file attachments are converted for Exchange.

FORMAT_TIFF4_Only [REG_DWORD]

Default:	-
Possible values:	Any value except 0
Remark:	This key must only be defined when FaxG3 documents arrive via a AVM Fritz ISDN card or should be displayed with the Kodak (Wang) fax viewer. 0 disables this feature.

The configuration of this registry key makes sure that the FaxG3 format invalid for the AVM Fritz ISDN card is intercepted and converted into a TIFFG4 format, which can then be read with the Kodak (Wang) fax viewer.

FromFieldFormatFax [REG_SZ]

Default:	-
Possible values:	<i>originator, callername, callernumber, size, orgnumber, service</i> with additional text.
Remark:	See Advanced Settings > Display Formats in Section 4.5.3.1, “Display Formats tab” , on page 145.

In this registry key the configuration data for representing additional information merely on **fax messages** are stored in the **From (Fax)** Outlook column.

FromFieldFormatVoice [REG_SZ]

Default:	-
Possible values:	<i>originator, callername, callernumber, size, orgnumber, service</i> with additional text.
Remark:	See Advanced Settings > Display Formats in Section 4.5.3.1, “Display Formats tab” , on page 145.

In this registry key the configuration data for representing additional information on **voice messages** is stored in the **From (Voice Message)** Outlook column.

GC_RECONNECT [REG_DWORD]

Default:	0
Possible values:	0 or 1

When set to 1, ExchApl will not use the local cache to search for the Exchange Server Global Catalog Server.

GUID [REG_SZ]

Default:	-
Possible values:	<CLSID>

Storage location for the automatically assigned CLSID of the connector.

HUBTRANSPORTSERVER [REG_SZ]

Default:	-
Possible values:	<server name>

Storage for the name of the Exchange Hub Transport server that is specified during the connector installation.

HUBTRANSPORTSERVER1 [REG_SZ]

Default:	-
Possible values:	<server name>
Remark:	In case of multiple hub transport server support this key must be manually created for the second Exchange Hub Transport server.

Storage for the name of the second Exchange Hub Transport server.

HUBTRANSPORTSERVER2 [REG_SZ]

Default:	-
Possible values:	<server name>
Remark:	In case of multiple hub transport server support this key must be manually created for the third Exchange Hub Transport server.

Storage for the name of the third Exchange Hub Transport server.

HUBTRANSPORTSERVER3 [REG_SZ]

Default:	-
Possible values:	<server name>
Remark:	In case of multiple hub transport server support this key must be manually created for the fourth Exchange Hub Transport server.

Storage for the name of the fourth Exchange Hub Transport server.

HUBTRANSPORTSERVER4 [REG_SZ]

Default:	-
Possible values:	<server name>
Remark:	In case of multiple hub transport server support this key must be manually created for the fifth Exchange Hub Transport server.

Storage for the name of the fifth Exchange Hub Transport server.

HUBTRANSPORTSERVER5 [REG_SZ]

Default:	-
Possible values:	<server name>
Remark:	In case of multiple hub transport server support this key must be manually created for the sixth Exchange Hub Transport server.

Storage for the name of the sixth Exchange Hub Transport server.

InformPostmasterWhenMailBoxFull [REG_DWORD]

Default:	1
Possible values:	0 or 1

1: All generated notifications are sent to the postmaster. You find details on this in [Section 4.9, “Waiting Loop Configuration for repeated Delivery”](#), on page 161.

0: Only the final notification is sent to the postmaster.

InstallAddressTemplates [REG_DWORD]

Default:	0
Possible values:	<Value>
Remark:	For internal use only!

Storage for the installed address templates.

InstallPath [REG_SZ]

Default:	-
Possible values:	<path specification>

Path to the application file of the Exchange connector.

MailBoxFullRepeatCount [REG_DWORD]

Default:	5
Possible values:	0, 1, 2, ... <number of repetition attempts>
Remark	Entering the value 0 deactivates the function.

This defines how many delivery attempts are to take place. You find details on this in [Section 4.9, “Waiting Loop Configuration for repeated Delivery”](#), on page 161.

MailBoxFullRepeatIntervallInSeconds [REG_DWORD]

Default:	3600 (one hour)
Possible values:	<Any value in seconds>

This value determines in which time intervals the delivery attempts are to take place. You find details on this in [Section 4.9, “Waiting Loop Configuration for repeated Delivery”](#), on page 161.

Multiline_Support [REG_DWORD]

Default:	0
Possible values:	0 or 1

Activates (1) the so-called multiline mode for several Exchange connectors. This is required when from a single XPR server Exchange connectors to several Exchange servers are to be installed.

NumberDisplayPresentation [REG_MULTI_SZ]

Default:	-
Possible values:	<Normalization rule(s)>
Remark:	See Section 4.5.3.1, "Normalization tab", on page 147 .

In this registry key all rules are entered according to which the conversion of incoming calling numbers is to occur.

Organization_RDN [REG_SZ]

Default:	-
Possible values:	<Name entry>

Store for the display name of the organization.

PostmasterDisplay [REG_SZ]

Default:	-
Possible values:	<Name>
Remark:	Example: <i>Postmaster</i>

Name of the set postmaster address (in this example **Postmaster**). This is where undeliverable messages are automatically routed to.

PostmasterDN [REG_SZ]

Default:	-
Possible values:	<Entry>
Remark:	Example: \o=<Organization>\ou=<Site>\cn=<Recipient Container> \cn=<Recipient>

Entry of the Postmaster Account's Distinguished Name (DN).

Read_Report [REG_DWORD]

Default:	1
Possible values:	0 or 1

When set to 1 a read report will be requested for a newly delivered e-mail message by Exchange Server. For large organizations this can be suppressed here (0).

This is required for new or modified dialing numbers.

ReplayDirectory [REG_SZ]

Default:	-
Possible values:	<UNC path name>

Memory location for the network path to the replay directory for the first Hub Transport server.

ReplayDirectory1 [REG_SZ]

Default:	-
Possible values:	<UNC path name>
Remark:	Configuration in case of multiple hub transport server operation.

Memory location for the network path to the replay directory for the second Hub Transport server in case of multiple hub transport server operation.

ReplayDirectory2 [REG_SZ]

Default:	-
Possible values:	<UNC path name>
Remark:	Configuration in case of multiple hub transport server operation.

Memory location for the network path to the replay directory for the third Hub Transport server in case of multiple hub transport server operation.

ReplayDirectory3 [REG_SZ]

Default:	-
Possible values:	<UNC path name>
Remark:	Configuration in case of multiple hub transport server operation.

Memory location for the network path to the replay directory for the fourth Hub Transport server in case of multiple hub transport server operation.

ReplayDirectory4 [REG_SZ]

Default:	-
Possible values:	<UNC path name>
Remark:	Configuration in case of multiple hub transport server operation.

Memory location for the network path to the replay directory for the fifth Hub Transport server in case of multiple hub transport server operation.

ReplayDirectory5 [REG_SZ]

Default:	-
Possible values:	<UNC path name>
Remark:	Configuration in case of multiple hub transport server operation.

Memory location for the network path to the replay directory for the sixth Hub Transport server in case of multiple hub transport server operation.

RouteTableMinRebuildTime [REG_DWORD]

Default:	3600
Possible values:	<Any value in seconds>

Time in seconds after which the Fax Look-up table is to be reinstalled. This is required for new or modified dialing numbers.

Routinggroup [REG_SZ]

Default:	-
Possible values:	<Routing group name>

Store for the name of the routing group found first.

SentRepresenting [REG_DWORD]

Default:	0
Possible values:	0 or 1

Via this key you can configure which address information an e-mail is to contain that is replicated from Exchange to XPR.

0: The delegate's address is included.

1: The address of the user on whose behalf the message has been sent is included.

SendRTFBody [REG_DWORD]

Default:	1
Possible values:	0 or 1

E-mail messages will be transmitted inclusive the RTF body part to the XPR server (1). The RTF representation can be excluded with a value of 0.

Server [REG_SZ]

Default:	-
Possible values:	<server name>
Remark:	Example: XPR server

Windows name of the server on which the connector has been installed.

Site [REG_SZ]

Default:	-
Possible values:	<Site name>
Remark:	Example: /o=Sample AG /ou=AURELIUS

Name of the site under which the connector has been installed. This is done in X.500 notation as used with the Distinguished Names of Microsoft Exchange Server.

SMS_ALLOW_DIGEST [REG_DWORD]

Default:	0
Possible values:	0 or 1

When forwarding messages as short messages to a cell phone, a digest algorithm can be applied to the message. This algorithm, configurable on the XPR server, sees to an intelligent message shortening so that the maximum permissible number of characters for SMS messages is not exceeded. If a digest algorithm is defined and shall be used, too, set this registry value to 1.

Standard_Cti_Settings [REG_SZ]

Default:	-
Possible values:	0 or 1, for each of the four parameters <u,v,w,x>
Remark:	u, v, w, x = 0 or 1, 0 deactivated, 1 activated Example: If for the parameters u, v, w, x the values 0, 1, 0, 1 are set, only journal entries for failed calls are generated. Successful calls are not logged.

Via this registry key you can set the default behavior for call logging. You can define which journal entries are generated for all users that can employ CTI functions. Each of the four parameters (u, v, w and x) represents a notification option:

- u: Successful inbound message (IN)
- v: Unsuccessful inbound message (IN)
- w: Successful outbound message (OUT)
- x: Unsuccessful outbound message (OUT)

SubjectFieldFormat [REG_SZ]

Default:	-
Possible values:	originator, callername, callernumber, size, orgnumber, service with additional text.
Remark:	See Advanced Settings > Display Formats in Section 4.5.3.1, "Display Formats tab" , on page 145.

In this registry key the configuration data for representing additional information on fax and voice messages are stored in the **From** Outlook column.

SubjectFieldFormatFax [REG_SZ]

Default:	-
Possible values:	<i>originator, callername, callernumber, size, orgnumber, service</i> with additional text.
Remark:	See Advanced Settings > Display Formats in Section 4.5.3.1, "Display Formats tab" , on page 145.

In this registry key the configuration data for representing additional information on fax messages are stored in the **Subject (Fax)** Outlook column.

SubjectFieldFormatVoice [REG_SZ]

Default:	-
Possible values:	<i>originator, callername, callernumber, size, orgnumber, service</i> with additional text.
Remark:	See Advanced Settings > Display Formats in Section 4.5.3.1, "Display Formats tab" , on page 145.

In this registry key the configuration data for representing additional information on fax and voice messages are stored in the **From (Voice Message)** Outlook column.

SupportContactScan [REG_DWORD]

Default:	0
Possible values:	0 or 1

Phone number normalization of contacts in public folders can be activated (1) or deactivated (0) via the Exch APL. See also [Section A.5.2.1, "Contacts \[REG_MULTI_SZ\]"](#), on page 563.

Suppress_MID_Reports [REG_DWORD]

Default:	1
Possible values:	0 or 1

In reports the MID character string (message ID) is removed from the subject line (0). If the MID is required, a value of 1 should be used.

SuppressMIDinSubject [REG_DWORD]

Default:	0
Possible values:	0 or 1

If you do not want the MID (Message ID) to be displayed in a message's subject line, enter 1 here to avoid it. If 0 is set, the MID is indicated in the subject line as well.

Suppress_Reports [REG_DWORD]

Default:	0
Possible values:	0 or 1

If the Exchange Reports are used for sending and error confirmations (**Delivery_Report = 1**), the value must be set to 0.

If the XPR Report Forms are to be used (**Delivery_Report = 0**), this value is set to 1.

UnknownSenderName [REG_SZ]

Default:	<Unknown>
Possible values:	<Arbitrary entry for indicating an unknown originator>

Here you can deposit a text string used as originator information for all users when a message from an unknown originator arrives.

USEDSSERVER [REG_DWORD]

Default:	0
Possible values:	0 or 1

When set to 1, ExchApl will use the Global Catalog Server specified on <HKEY_CURRENT_USER\Software\Microsoft\Exchange\Exchange Provider\Provider\DS Server> when creating the MAPI profile for the Exchange Server connection.

WorkAroundAreaCodeProblem [REG_DWORD]

Default:	0
Possible values:	0 or 1

Addressing from within Outlook can cause problems when telephone or fax numbers in the format "+xxx(yyyy)zzzz" are stored in the contact information. Upon calling and handing over one of these addresses, the expression in brackets is replaced by its ASCII character and consequently the message cannot be sent. In the event that problems arise here, change the default value from (0) to 1 to avoid wrong addressing.

A.5.4.2 HKLM\SOFTWARE\Wow6432Node\PP-COM\MRS\ExUMAp1

The ExUMAp1 values are stored in the following key:

HKKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\PP-COM\MRS\ExUMAp1

Access [REG_SZ]

Default:	-
Possible values:	<Password>

Password of the installing Exchange account. The password is entered here encoded.

Account [REG_SZ]

Default:	-
Possible values:	<Exchange account name>

Service account under which the ExUMAp1 runs. The service account must have administrator authority under Microsoft Exchange.

ACCOUNTDN [REG_SZ]

Default:	-
Possible values:	<Data of the LegacyExchangeDN Active Directory Object for the TUM service account>

The LegacyExchangeDN Active Directory Object data is read into this registry key via an AD query. This object is used for localizing the XPR service account in the Active Directory to enable logging the XPR service account on to the Exchange server.

ACCOUNTDNFULL [REG_SZ]

Default:	-
Possible values:	<Entry of the LegacyExchangeDN object data>

If errors occur on reading in data of the LegacyExchangeDN object during the ExUMAp1 start, you can add this registry key manually. If the key is present and the entry specified, the data defaulted here for logging the XPR service account on to the Exchange server is automatically used. If the key is not available, the data provided in the registry key **ACCOUNTDN** via an AD query is used.

AVOIDMAPIRELEASE [REG_DWORD]

Default:	0
Possible values:	0 or 1

In some Exchange environments the ExUMApI occasionally terminates its service unscheduled when the MAPI interface is shut down. If this behavior occurs you can stop the ExUMApI from terminating with help of this registry key. To this effect, set the value in this registry key from “0” to “1”.

CASARRAY [REG_SZ]

Default:	-
Possible values:	0 or 1

Registry key for connecting the ExUM Apl to an organization with *Exchange Server 2010 CAS Array*. Adding this key and setting this value to 1 activates the support of the gateway solution.

CASARRAYNAME [REG_MULTI_SZ]

Default:	-
Possible values:	CASARRAY01-DNS CASARRAY02-DNS CASARRAYn-DNS <DNS-names of the respective Exchange Server CAS Arrays>

Name of the *Exchange Server 2010 CAS Arrays*. The DNS name of the respective CAS array must be used as value for **CASARRAYNAME**.

CHECKCASARRAY [REG_DWORD]

Default:	-
Possible value:	1

If no WNLB (Windows Network Load Balancing) is installed in the Exchange environment, the ExUMApI is connected to a single CAS server. In this case you must add this registry key manually. If you enter value “1” in this registry key, the ExUMApI adjusts the profile for this operating mode automatically.

Domain [REG_SZ]

Default:	-
Possible values:	<Name>

The domain in which the Exchange server is installed.

E2K13_DOMAIN [REG_SZ]

Default:	-
Possible values:	<Domain name>
Example:	company.com

Domain of the RPC/HTTP endpoint of the proxy server used by the MAPI clients.

E2K13_HOME_SERVER_DN [REG_SZ]

Default:	-
Possible values:	<Distinguished name of the home server>

Defined name of the home server. The name can be retrieved from the ServerLegacyDN and ExchangeGuid via a Get-Mailbox command.

Edit the character string as described in the following:

1. Replace the variable <Exchange 2013 Server> after the character string of the ServerLegacyDN
CN=SERVERS/CN=<EXCHANGE 2013 SERVER>
with value ExchangeGuid@<DOMAIN>.

Example:

```
/o=COMPANY ORG/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/  
cn=Configuration/cn=Servers/cn=fe5f84bf-36f9-42eb-ab2f-9e40e3413bf1@company.com
```

NOTE: The <DOMAIN> portion is replaced with the data from the E2K13_DOMAIN registry key.

E2K13_RPC_ALTERNATIVE_SERVERS [REG_MULTI_SZ]

Default:	-
Possible values:	<Exchange CAS server name>
Example:	ExchCAS_1,ExchCAS_2,ExchCAS_3...

This registry key serves for enabling an alternative failover. The registry key must contain the names (non-FQDN) of the Exchange CAS servers that the ExUm Apl attempts to reconnect in case of an error. In this process, the specified Exchange CAS servers are addressed in succession until a connectable one is found. See also [Section 7.10.4.5, “Making the ExUM Apl failsafe on the Exchange Server 2013”, on page 333.](#)

E2K13_RPC_PROXY_SERVER [REG_SZ]

Default:	-
Possible values:	< <i>server name</i> >
Example:	amb09-exch2k13.company.com

The FQDN of the RPC/HTTP endpoint of the proxy server used by the MAPI clients.

E2K13_SERVICEUSER_DN [REG_SZ]

Default:	-
Possible values:	< <i>Distinguished name of the <XPR service account></i> >

Defined name of the <XPR service account>. The name can be retrieved from the LegacyExchangeDN properties via a Get-Mailbox command.

Example:

```
/o=COMPANY ORG/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Recipients/  
cn=e092feee00504b1ebf88ba3afd6c059e-admin2k13
```

E2K13_UNRESOLVED_NAME [REG_SZ]

Default:	-
Possible values:	< <i>Mailbox alias for the <XPR service account></i> >
Example:	admin2k13

Mailbox alias name for the <XPR service account> on the Exchange Server 2013. Use the alias name you retrieved from the alias properties via a Get-Mailbox command.

E2K13_UNRESOLVED_SERVER [REG_SZ]

Default:	-
Possible values:	< <i>Personalized server ID</i> >
Example:	fe5f84bf-36f9-42eb-ab2f-9e40e3413bf1@company.com

Personalized server ID. Use the ID you retrieved from the ExchangeGuid properties via a Get-Mailbox command, followed by the domain name (format: <ExchangeGuid>@<Domain>).

The <DOMAIN> portion is replaced with the data from the E2K13_DOMAIN registry key.

EVERSION [REG_DWORD]

Default:	-
Possible values:	12 for connecting an Exchange Server 2007, 14 for connecting an Exchange Server 2010, 15 for connecting an Exchange Server 2013.

This registry key holds the version of the Exchange server connected to the XPR server.

EXADDRESSTYPE [REG_SZ]

Default:	-
Possible values:	<address space name>
Example:	MRSn, with n = 1, 2, 3, ...

If several XPR servers and consequently several Exchange TUM connectors are connected to an Exchange environment, this registry key is required for differentiating the Exchange TUM connectors. Assigning special address space names then optimizes message transmission. The TUM connectors are labeled by consecutive numbering.

ExchangeClusterName [REG_SZ]

Default:	-
Possible values:	<Name>

Storage location for the Exchange cluster name, if the ExUM Apl is installed in a clustered Exchange environment.

ExchangeServer [REG_SZ]

Default:	-
Possible values:	<Name>

This registry value is the storage location for the name of the Exchange server that the ExUM Apl connects. If the connection to a clustered Exchange environment is set up, the registry value is the storage location for the Windows cluster name.

GUID [REG_SZ]

Default:	-
Possible values:	<CLSID>

Automatically assigned Connector CLSID.

HangedTimeout [REG_DWORD]

Default:	100
Possible values:	15, 16, 17, ...<value in seconds>
Remark:	If network errors are reported with the setting you have selected, the chosen value is too low; increase it in this case.

Settings parameter for the internal watchdog of the ExUM Apl.

Period after which a triggered ExUM APL thread is considered a “pending process”. Each detected “pending process” initiates a session cleanup. This terminates the process. Depending on the success or failure of the cleanup, a corresponding counter is counted up each.

Further setting parameters for the internal watchdog:

MaxFailedSessionCleanUps
MaxSessionCleanUps
ResetCountersPeriod
StopAplIfSessionsAreHanging
TerminateHanged

InstallPath [REG_SZ]

Default:	-
Possible values:	<path specification>
Remark:	Example: \\tsclient\Y\mrs7.01\2007-0~1\<product data carrier>\server

Path via which the ExUM APL was installed.

LEGACYEXCHANGEDN [REG_SZ]

Default:	-
Possible values:	<Entry of the LegacyExchangeDN object data>
Note:	See the registry key ACCOUNTDNFULL

This key contains the data for the LegacyExchangeDN object. If no value has been entered here, the ExUM Apl will not work correctly. In this case, copy the value from the available registry key

ACCOUNTDNFULL [REG_SZ] as the registry value for this key.

LINE_PROXY_PATTERN [REG_SZ]

Default:	-
Possible values:	<Regular expression>

In multiline environments a filter rule can be specified here that enables the control of user distribution among the single TUM connectors.

MaxFailedSessionCleanUps [REG_DWORD]

Default:	15
Possible values:	0, 1, 2, 3, ...
Remark:	If you enter value 0, the action is triggered with the first cleanup. The value should not be very high or too low altogether. A value too high may delay the error detection, and if it is too low, the ExUM Apl might be stopped too often.

Settings parameter for the internal watchdog of the ExUM Apl.

If the session cleanup counter reaches the value set here for failed cleanups, the action defined in key **StopAplIfSessionsAreHanging** is triggered.

Further setting parameters for the internal watchdog:

HangedTimeout
MaxSessionCleanUps
ResetCountersPeriod
StopAplIfSessionsAreHanging
TerminateHanged

MaxSessionCleanUps [REG_DWORD]

Default:	15
Possible values:	0, 1, 2, 3, ...
Remark:	If you enter value 0, the action is triggered with the first cleanup. The value should not be very high or too low altogether. A value too high may delay the error detection, and if it is too low, the ExUM Apl might be stopped too often.

Settings parameter for the internal watchdog of the ExUM Apl.

When the session cleanup counter reaches the value set here for successful cleanups, the action defined in key **StopAplIfSessionsAreHanging** is triggered.

Further setting parameters for the internal watchdog:

HangedTimeout
MaxFailedSessionCleanUps
ResetCountersPeriod
StopAplIfSessionsAreHanging
TerminateHanged

MULTILINE_SUPPORT [REG_DWORD]

Default:	0
Possible values:	0 or 1

To activate the multiline support, set this value to 1.

POLLING_INTERVAL [REG_DWORD]

Default:	0 (polling disabled)
Possible values:	0, 60 or higher (value in seconds)

Interval in seconds in which the ExUMApI checks whether the connection to the Exchange server is still up. You can determine the behavior triggered with an interrupted connection via the registry key **STOPONFAILURE** (see [Section A.5.3.2, “STOPONFAILURE \[REG_DWORD\]”, on page 612](#).

ResetCountersPeriod [REG_DWORD]

Default:	1
Possible values:	0, 1, 2, 3, ...<value in days>
Remark:	If you enter value 0, the session cleanup counters are not reset.

Settings parameter for the internal watchdog of the ExUM Apl.
Period in days in which the session cleanup counters are reset.
Further setting parameters for the internal watchdog:

HangedTimeout
MaxFailedSessionCleanUps
MaxSessionCleanUps
StopApIfSessionsAreHanging
TerminateHanged

Server [REG_SZ]

Default:	-
Possible values:	<server name>
Remark:	

Windows name of the server on which the ExUM connector was installed.

Site [REG_SZ]

Default:	-
Possible values:	<Site name>
Remark:	Example: /o=<Organization>/ou=<Exchange mailbox store>

Name of the site under which the connector has been installed. This is done in X.500 notation as used with the Distinguished Names of Microsoft Exchange Server.

SKIPCALENDARONFAILURE[REG_DWORD]

Default:	0
Possible values:	0 or 1

If the login procedure is to carry on even if an error occurs when opening the calendar folder, you can configure that via this registry key. To this effect, set the value in this registry key from “0” to “1”.

StopAplIfSessionsAreHanging [REG_DWORD]

Default:	0
Possible values:	0 or 1

Settings parameter for the internal watchdog of the ExUM Apl.

If an event is triggered via reaching the maximum value for **MaxSessionCleanUps** or **MaxFailedSessionCleanUps**, the corresponding action is selected here.

0 : A warning is issued in the log.

1 : The ExUM Apl is stopped. The XPR server watchdog detects this and an ExUM Apl restart is initiated.

Further setting parameters for the internal watchdog:

HangedTimeout
MaxFailedSessionCleanUps
MaxSessionCleanUps
ResetCountersPeriod
TerminateHanged

STOPONFAILURE [REG_DWORD]

Default:	0
Possible values:	0 or 1

If activating **POLLING_INTERVAL** detects an interrupted connection to the Exchange server, you can specify the ExUMApI's behavior for this case via this registry key.

0: No action; the ExUMApI will not be rebooted.

1: The ExUMApI will be rebooted. This reboot is triggered by initiating the kernel watchdog.

TerminateHanged [REG_DWORD]

Default:	0
Possible values:	0 or 1

Settings parameter for the internal watchdog of the ExUM Apl.

Via this setting the session cleanup feature can be activated.

0: Function is deactivated

1: Function is active

Further setting parameters for the internal watchdog:

HangedTimeout

MaxFailedSessionCleanUps

MaxSessionCleanUps

ResetCountersPeriod

StopAplIfSessionsAreHanging

WaitExit [REG_WORD]

Default:	0
Possible values:	0 to 60

Settings parameter for the time (in seconds) to wait for the APL to finish the shutdown steps. It is used to ensure the Apl will not be locked during the shutdown procedure.

If it times out the APL exits abruptly.

A.5.4.3 HKCU\Software\Microsoft\WindowsNT\CurrentVersion\Windows Messaging Subsystem

IMPORTANT: Make sure that you are logged on with the account that is running the Exumapl.

PCHTTPProxyMap_EXUMAPL [REG_SZ]

Default:	-
Possible values:	<DOMAIN>=<ProxyServer><ProxyServerSettings>

With:

<Domain>

The domain name of the RPC/HTTP endpoint of the proxy server used by the MAPI clients, or * (asterisk icon).

<ProxyServer>

The <ProxyServer> parameter contains value <FrontEndPoolFQDN> and must be entered in the format `https://<FrontEndPoolFQDN>`. For example: `https://mail.company.com`

You can use the EMS for having value <FrontEndPoolFQDN> put out. Enter the following command in the command line there:

```
Get-OutlookAnywhere | fl server*, Interna*, identity
```

NOTE: Make sure that the value put out via `Get-OutlookAnywhere` is adopted in <FrontEndPoolFQDN> exactly.

<ProxyServerSettings>

The MAPI profile settings are stored in the <ProxyServerSettings> parameter. It comprises the following further parameters:

- <RpcHttpAuthenticationMethod>,
- <RpcAuthenticationMethod> and
- <IgnoreSslCert>

Inserting the parameter in the underlying abbreviated notation results in the complete value of the registry key:

```
<DOMAIN>=<ProxyServer>,<RpcHttpAuthenticationMethod>,<RpcAuthenticationMethod>,<IgnoreSslCert>
```

You can insert the following valid values for the single parameters:

for <RpcHttpAuthenticationMethod>

- Negotiate
- NTLM
- Basic

for <RpcAuthenticationMethod>

- Negotiate
- NTLM
- Anonymous
- None

for <IgnoreSslCert>

- True
- 1
- Y
- Yes

NOTE: Any other value inserted here is interpreted as `False`.

Examples:

```
unify.com=https://mail.unify.com,ntlm,ntlm,true  
*=https://mail.unify.com,ntlm,ntlm,true
```

You can obtain further information about this subject from the *Configuring the MAPI download for EXCHANGE 2013* instructions. You find these instructions in the Microsoft document `MAPI Download configuration guidance.docx` under:

<http://www.microsoft.com/en-us/download/details.aspx?id=39045>

A.5.5 Registry Entries for Exchange Server 2016

A.5.5.1 HKLM\SOFTWARE\Wow6432Node\PP-COM\MRS\EwsApl

The EWS Apl values are stored in the following key:

HKLM\SOFTWARE\Wow6432Node\PP-COM\MRS\EwsApl

EVersion [REG_DWORD]

Default:	<i>Exchange 2013 SP1</i>
Possible values:	<i>0 to 5</i>

Specify the exchange server version of the profile used to connect to the Exchange Server.

Possible Values:

- 1: Exchange 2010*
- 2: Exchange 2010 SP1*
- 3: Exchange 2010 SP2*
- 4: Exchange 2013*
- 5: Exchange 2013 SP1 / Exchange 2016*

A.5.6 HKLM\SOFTWARE\Wow6432Node\PP-COM\MRS\LdapApl

The global LDAP Apl values are stored in the following key:

HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\PP-COM\LdapApl

DlgSessions [REG_DWORD]

Default:	16
Remark:	Without function

For future dialog service expansions.

MRS-NonDeleteAtts [REG_MULTI_SZ]

Default:	PASSWORD GROUP PIN
Possible values:	<Attribute_1 Attribute_2 ...>

Here all XPR attributes can be listed that must not be deleted in case of an empty LDAP attribute. **Exception:** The user entry is completely deleted.

HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\PP-COM\MRS\LdapApl\Servers\Ex2003

The registry keys created here serve exclusively for storing the LDAP APL configuration data.

A.5.7 HKLM\SOFTWARE\Wow6432Node\Cycos AG \ExchForms Server

This key is written on the server on which the server components for the Outlook forms are installed.

InstallPath [REG_SZ]

Default:	-
Possible values:	<path specification>

Path to the Outlook extension application files.

SetupComplete [REG_DWORD]

Default:	-
Possible values:	0 or 1

Enter 1 after a completed setup.

A.5.8 HKLM\SOFTWARE\Wow6432Node\Cycos AG \ExchForms Client

In addition, the following keys are entered in the **ExchForms Client** folder on the client computers on which the Outlook forms are installed each:

NOTE: The values are written with the client component installation. They can be adjusted by editing the installation file. See [Section 12.3.2, “User-defined Installation of the Message Forms on the Clients”](#), on page 543.

AdmApprovedOcx [REG_SZ]

Default:	-
Possible values:	0 or 1

This key must be entered manually if the fax and voice OCX is to be executed on the “Administrator approved” security level in a network different from the Active Directory Network (for example Exchange 5.5 or Novell).

AutoNameResolution [REG_SZ]

Default:	0
Possible values:	0 or 1

By default, fax numbers in the Outlook fax forms are not automatically resolved because of problems that may otherwise occur in some system environments. If you wish names to be automatically resolved, set this registry value to 1.

ChangePhoneNo [REG_SZ]

Default:	1
Possible values:	0 or 1
Remark:	Registry key for using a specific Outlook forms feature. It may be adjusted for a user-defined installation of the forms in the MSI package.

If the default value 1 is set to 0, the corresponding client user cannot change his/her telephone number in the Outlook configuration dialog.

ExAddressType [REG_SZ]

Default:	-
Possible values:	<Exchange address type>
Remark:	Registry key for assigning different Exchange address types, so that users can be assigned to the single XPR servers. Remark: If this key is missing, the Outlook forms use the Exchange address type MRS available by default.

For scaling reasons you need to adjust the Exchange address types “Fax” and “Voice” for outgoing messages. This is, for example, the case when several XPR systems are operated at an Exchange environment. Using a customer-specific script, you can add this registry key during the rollout process to ensure that a special Exchange address type is assigned to the users of a specific XPR system. When using Outlook forms the address type stored here is read out and used instead of the value available by default.

Example: A fax shall be sent via the address **MRS_US:FAXG3/4711** instead of the default address **MRS:FAXG3/4711**. In this case the value is set to **MRS_US** via the key **ExAddressTyp**.

ExplorerInterval [REG_SZ]

Default:	100 <Value in milliseconds>
Possible values:	> 100
Remark:	The start delay deskews the many processes running at the same time when Outlook starts.

At the Outlook start, problems may be created by processes that run parallel to the loading of the Outlook Extensions. Depending on the system environment, Outlook may then sporadically crash. The Outlook Extensions are loaded with a delay of 100 ms by default.

The defaulted delay period may be overridden with the desired one by means of this registry entry.

IMAPMode [REG_SZ]

Default:	0
Possible values:	0 or 1
Remark:	Registry key for using a specific Outlook forms feature. It may be adjusted for a user-defined installation of the forms in the MSI package.

For operation at Exchange keep the default setting (0). If the forms are to be used at an SMTP server in IMAP mode, enter a “1”.

MsgFile [REG_SZ]

Default:	0
Possible values:	0 or 1
Remark:	Registry key for using a specific Outlook forms feature. It may be adjusted for a user-defined installation of the forms in the MSI package.

Specifies whether it is possible to open Outlook .msg files as fax or voice mails.

MsgShowNoNumber [REG_SZ]

Default:	0
Possible values:	0 or 1
Remark:	Registry key for using a specific Outlook forms feature. It may be adjusted for a user-defined installation of the forms in the MSI package.

If you want to suppress the warning that for the selected address book entry no corresponding fax or SMS number is available, enter a "1" here.

NoFaxBtn [REG_SZ]

Default:	0
Possible values:	0 or 1
Remark:	Registry key for using a specific Outlook forms feature. It may be adjusted for a user-defined installation of the forms in the MSI package.

Displays/hides the fax icon and the fax form in Outlook.

NoFaxViewForm [REG_SZ]

Default:	0
Possible values:	0 or 1
Remark:	Registry key for using a specific Outlook forms feature. It may be adjusted for a user-defined installation of the forms in the MSI package.

Displays/hides the fax view function in the Outlook preview window.

NoFODBtn [REG_SZ]

Default:	0
Possible values:	0 or 1
Remark:	Registry key for using a specific Outlook forms feature. It may be adjusted for a user-defined installation of the forms in the MSI package.

Displays/hides the fax-on-demand (FOD) form in Outlook.

NoNumberOnlyResolution [REG_SZ]

Default:	0
Possible values:	0 or 1
Remark:	Registry key for using a specific Outlook forms feature. It may be adjusted for a user-defined installation of the forms in the MSI package.

When set to 1, number entries in the address field are, contrary to the default behavior, no longer automatically considered a fax G3 address.

NoSMSBtn [REG_SZ]

Default:	0
Possible values:	0 or 1
Remark:	Registry key for using a specific Outlook forms feature. It may be adjusted for a user-defined installation of the forms in the MSI package.

Displays/hides the SMS icon and the SMS form in Outlook.

NoVMBtn [REG_SZ]

Default:	0
Possible values:	0 or 1
Remark:	Registry key for using a specific Outlook forms feature. It may be adjusted for a user-defined installation of the forms in the MSI package.

Displays/hides the “voicemail” icon and the forms in Outlook that serve to generate a voice annotation for different messages.

NoVoiceViewForm [REG_SZ]

Default:	0
Possible values:	0 or 1
Remark:	Registry key for using a specific Outlook forms feature. It may be adjusted for a user-defined installation of the forms in the MSI package.

Displays/hides the voicemail playback feature in the Outlook preview window.

NoWebAssistantBtn [REG_SZ]

Default:	0
Possible values:	0 or 1
Remark:	Registry key for using a specific Outlook forms feature. It may be adjusted for a user-defined installation of the forms in the MSI package.

Displays/hides the icon with which the *Web Assistant* is opened.

NoZeroCut [REG_DWORD]

Default:	0
Possible values:	0 or 1
Remark:	Registry key for using a specific Outlook forms feature. It may be adjusted for a user-defined installation of the forms in the MSI package.

With 1 you can enforce that for outgoing fax and SMS messages the leading 0 of the area code is **not** omitted when an address is selected from the Outlook address book. This is intended for countries in which a 0 must be dialed between the country code and the area code (for example in some regions of Italy).

SubstituteForPlus [REG_SZ]

Default:	-
Possible values:	<Any series of numbers>
Remark:	Registry key for using a specific Outlook forms feature. It may be adjusted for a user-defined installation of the forms in the MSI package.

Is used to automatically replace the leading + character by any digit combination.

TextLength [REG_SZ]

Default:	612
Possible values:	0 to 612
Remark:	Registry key for using a specific Outlook forms feature. It may be adjusted for a user-defined installation of the forms in the MSI package.

Is used for restricting the number of characters in an SMS message. This may be required if you have defined, for example, for SMS messages a prefix (or a suffix) on the XPR server. The number of characters of this SMS code automatically enclosed in each message must then be deduced from the maximum number of possible characters.

HKLM\SOFTWARE\Wow6432Node\Cycos AG \ExchForms Client\...

In the subdirectories under ... \ExchForms Client (\Fax, \FaxView, \FOD, \Shared, \SMS, \VoiceMail and \VoiceView) you merely find the text strings for different language versions. In addition, the following registry keys are found in the directories... \Fax and... \SMS each:

DeliveryReceipt [REG_SZ]

Default:	1
Possible values:	0 or 1
Remark:	Registry key for using a specific Outlook forms feature. It may be adjusted for a user-defined installation of the forms in the MSI package.

If the default value 1 is set to 0, the fax (SMS) form does not transmit a “sent notification”. This notification is considered useful for clients that rout such documents exclusively to a printer or a fax device.

ReadReceipt [REG_SZ]

Default:	1
Possible values:	0 or 1
Remark:	Registry key for using a specific Outlook forms feature. It may be adjusted for a user-defined installation of the forms in the MSI package.

If the default value 1 is set to 0, the fax (SMS) form does not transmit a “read notification”. This notification is considered useful for clients that rout such documents exclusively to a printer or a fax device.

Additionally in the directory ... \SMS:

TextLength [REG_SZ]

Default:	160
Possible values:	0 to 160
Remark:	Registry key for using a specific Outlook forms feature. It may be adjusted for a user-defined installation of the forms in the MSI package.

This key is used for restricting the number of characters in an SMS message. This may be required if you have defined, for example, for SMS messages a prefix (or a suffix) on the XPR server. The number of characters of this SMS code automatically enclosed in each message must then be deduced from the maximum number of possible characters.

A.5.9 HKLM\SOFTWARE\ or HKCU...

Additional values are created upon the installation of the Outlook-Com-Add-Ins.
Depending on the configuration you find those values in the HKLM or HKCU key.
This depends on whether the Add-Ins can only be used by the user who has installed it on the relevant computer (saving the values under CURRENT USER) or by any user who may log in at this computer (saving the values under LOCAL MACHINE) :

The values are found there in the subdirectory:

Software\Microsoft\Office\Outlook\Addins\Fax_SMS.UMSConnect

CommandLineSafe [REG_DWORD]

Default:	0

Description [REG_SZ]

Default:	<i>MRS Extensions for FAX and SMS</i>

FriendlyName: [REG_SZ]

Default:	<i>MRS Extensions</i>

LoadBehavior: 3 [REG_DWORD]

Default:	3

These keys are created with the installation and need not be edited.

A.5.10 HKCU\Software\Cycos AG\COM\...

The COM objects required for fax representation or voicemail editing and playback in Outlook generate the following registry keys:

For the fax editor

HKCU\Software\Wow6432Node\Cycos AG\COM\FaxViewer

FaxFillCol [REG_BINARY]

Default:	00 00 00 00 -> black
Possible values:	<Hex value according to the color setting>
Remark:	The color is stored hexadecimally coded according to the RGB model. 1st number pair -> value for red 2nd number pair -> value for green 3rd number pair -> value for blue 4th number pair -> without significance

Storage location for the object filling color selected last in the fax editor.

FaxGrid [REG_DWORD]

Default:	0
Possible values:	0 or 1
Remark:	1 -> Grid points displayed 0 -> Grid points hidden

Storage location for the **Grid Points** on/off option selected last in the fax editor.

FaxLineCol [REG_BINARY]

Default:	00 00 00 00 -> black
Possible values:	<Hex value according to the color setting>
Remark:	The color is stored hexadecimally coded according to the RGB model. 1st number pair -> value for red 2nd number pair -> value for green 3rd number pair -> value for blue 4th number pair -> without significance

Storage location for the line object color (for lines and object outlines) selected last in the fax editor.

FaxLogoFnt [REG_BINARY]

Default:	<i>f4 ff ff 00 00 00 00... Courier New ... 00 00</i>
Possible values:	<i><Hex value according to the font></i>
Remark:	The font is stored hexadecimally coded.

Storage location for the font used last in the fax editor for variable fields.

FaxPrintMode [REG_DWORD]

Default:	<i>1</i>
Possible values:	<i>0 or 1</i>
Remark:	<i>1 -> Optimum fit (attempt to optimally print out a fax message on DIN A4 sheets). 0 -> Fit fax to print page (the entire fax message is always put out on one print page).</i>

Storage location for fax-hardcopy representation settings.

FaxTxtFnt [REG_BINARY]

Default:	<i>f4 ff ff 00 00 00 00... Courier New ... 00 00</i>
Possible values:	<i><Hex value according to the font></i>
Remark:	The font is stored hexadecimally coded.

Storage location for the font used in the fax editor for text objects.

FaxTxtFntCol [REG_Binary]

Default:	<i>00 00 00 00 -> black</i>
Possible values:	<i><Hex value according to the color setting></i>
Remark:	The color is stored hexadecimally coded according to the RGB model. 1st number pair -> value for red 2nd number pair -> value for green 3rd number pair -> value for blue 4th number pair -> without significance

Storage location for the text object color selected last in the fax editor.

FaxZm [REG_DWORD]

Default:	<i>0</i>
Possible values:	<i><Hex value between 0 and 64></i>

Storage location for the currently set zoom factor. The value is specified as diminution value between 0 and 100%.

FaxZoom [REG_DWORD]

Default:	1
Possible values:	0, 1 or 2
Remark:	0 -> function is switched off, for example when another zoom factor (see FaxZm) has been selected. 1 -> Display entire fax in the window 2 -> Fit fax optimally to window width

Storage location for the set adjustment required for fax representation in the current window.

LastSavePath [REG_SZ]

Default:	-
Possible values:	<path specification>

Storage location for the path that was used with the last call of the **Save copy** feature.

LeftFaxMargin [REG_DWORD]

Default:	10
Possible values:	0...300, <value in millimeters>

Storage location for the width of the left margin of a fax hardcopy. The value is specified in millimeter from the left border.

RightFaxMargin [REG_DWORD]

Default:	0
Possible values:	0...300, <value in millimeters>
Remark:	This function is currently deactivated; thus changing the value does not affect the fax representation.

Storage location for the width of the right margin of a fax hardcopy.

For the voicemail editor

HKCU\Software\Cycos AG\COM\WavePlayer

AppendSource [REG_DWORD]

Default:	0
Possible values:	0 or 1
Remark:	0 -> New voice annotation. 1 -> Attach voice annotation to existing recording.

Storage location for the current switch setting of the button for re-recording or attaching a voice annotation.

LocalPhone [REG_SZ]

Default:	-
Possible values:	<Phone number>

Storage location for the number of the telephone that is temporarily used as voicemail output device.

MonitoringSucceededFromPhone [REG_DWORD]

Default:	-
Possible values:	0 or 1
Remark:	0 -> Not successful 1 -> Successful

Storage location for the message stating whether or not the monitoring access performed last has been successful.

PlayVoiceDeviceIndex [REG_DWORD]

Default:	-
Possible values:	0 or 1
Remark:	0 -> On the telephone defined as "local" 1 -> On the individual telephone

Storage location for the definition where voicemail are to be put out.

SeekSelection [REG_DWORD]

Default:	0
Possible values:	<0, 1, 2 or 3>
Remark:	0: Skip distance 1 second 1: Skip distance 2 seconds 2: Skip distance 4 seconds 3: Skip distance 8 seconds

Storage location for setting the skip distance when **Search** is pressed with voice mail playback.

VoiceMailFormat [REG_DWORD]

Default:	1
Possible values:	0 or 1
Remark:	0 -> μ -law 1 -> A-law

Storage location for the set voice format: A-law or μ -law.

A.5.11 HKLM\SYSTEM\...

After the successful Exchange service installation, the connectors have been integrated in the list of the Windows computer services. Consequently, the service keys exist as well:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\
Services\ExchApl $x$ 
```

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\
Services\ExchApl $x$ \Parameters
```

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\
Services\ExUmApl $x$ 
```

NOTE: x represents the consecutive number of the connector with distributed systems. In case of non-distributed systems, this value is omitted.

They contain the entries listed in the following.

IMPORTANT: These registry values are Windows-specific entries for the Exchange connector services and must not be modified.

DisplayName [REG_SZ]

Default:	-
Possible values:	<Connector name>
Remark:	Example: XPR-Exchange connector for i386 (AURELIO)

Displayed XPR connector name.

ErrorControl [REG_SZ]

Default:	-
Possible values:	<Value>
Remark:	Setting: 1

ImagePath [REG_EXPAND_SZ]

Default:	1
Possible values:	<Path>
Remark:	Example: C:\Company\XPR\bin\ExchApl.exe

ObjectName [REG_SZ]

Default:	-
Possible values:	<Account>
Remark:	Example: <Domain>\<User>

Displays the account under which the Exchange connector runs.

Start [REG_DWORD]

Default:	3
Possible values:	<2, 3 or 4>
Remark:	This setting is normally modified in Windows under Services. For this purpose, open the settings dialog for the XPR Exchange Connector for i386 service with a doubleclick. By enabling one of the available check boxes you can modify the default behavior there. The following starting mode options are available: • automatic (generates a 2 as registry value) • manual (generates a 3 as registry value) • deactivated (generates a 4 as registry value)

Start-up mode configuration.

Type <value> [REG_DWORD]

Default:	-
Possible values:	<Value>
Remark:	Setting: 16

under

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\
Services\ExchAplx\Parameters

HomeDSA <Name> [REG_SZ]

Default:	<i><Name of the server with the mailbox service role this Apl connects></i>
Possible values:	<i><Name of the server with the mailbox service role></i> <i><Name of the server with the client access service role></i>
Remark:	If the XPR server is active in an Exchange environment in which message delivery works only HomeDSA-delayed, you can change this value to the name of the <i>CAS server</i> in charge of address book resolution. This will accelerate message delivery because the server in charge is not yet to be determined then.

And under

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\
Services\XPRWebClient

Acronyms

This list contains the acronyms used in this manual.

Acronyms	Definition
APL	Access Protocol Layer, special XPR service for the protocol-controlled connection of foreign software to the XPR kernel.
CMC	Client Matter Code. The <i>Client Matter Code</i> corresponds to a project code. Via this project code calls can be assigned to specific accounts.
DV	Data processing
FOD	Fax-On-Demand
IM	Integrated Messaging
ISDN	Integrated Service Digital Network
IVR	Interactive Voice Response
LAN	Local Area Network
MMC	Microsoft Management Console
SMS	Short Message Service
TK	Private Branch Exchange
TUI	Telephone User Interface
TUM	True Unified Messaging
UM	Unified Messaging
VPIM	The VPIM protocol has been developed by the Internet Engineering Task Force (IETF) to exchange voicemails between voicemail systems of different manufacturers.

Index

64-bit system 49

A

Active directory
 concept, general 87
 general information 87
 interface (DSI) 88
 Active directory service (DS) 87
 Administration message classes 524
 Advanced Unified Messaging 21
 Assigning privileges, for Exchange Server 2007 55
 Assigning privileges, for Exchange Server 2010 162
 Assigning privileges, for Exchange Server 2013 297
 Attribute mapping 89

C

CAS array 160
 CDO with missing public folders 273, 421
 cluster, Exchange Server 2007 61
 cluster, Exchange Server 2010 172
 Configuration file 93, 359
 CPU_LIMIT 579, 608, 619
 CTI message classes 523

D

Data message classes 524
 Data protection and data security 18
 Database availability group 156, 160
 Database availability group, installation 181, 187, 336
 Definition address type "FAX" for Exchange 2007 139
 Definition address type "FAX" for Exchange 2010 257
 Definition address type "FAX" for Exchange 2013 405
 Directory access protocol, DAP 87, 353
 DS pattern 89
 DSI (active directory interface) 88

E

E2k10 message transport 156
 E2k7 message transport 51
 EXADDRESSTYPE for the Exch APL 138, 256, 404
 EXADDRESSTYPE for the ExUM APL 138, 256, 404
 Exchange 2007
 definition address type "FAX" 139
 E2k7Apl.exe 51
 Exchange 2007 ExchAPL

configuration
 display formats 127
 foreign connector 122
 global CTI settings 123
 message forms 124
 multi hub transport server 130
 version information 129
 XPR user data 118

Exchange 2010
 definition address type "FAX" 257
 E2k7Apl.exe 156

Exchange 2010 ExchAPL
 configuration
 display formats 245
 foreign connector 240
 global CTI settings 241
 message forms 242
 multi hub transport server 248
 version information 247
 XPR user data 236, 384

Exchange 2013
 definition address type "FAX" 405

Exchange 2013 ExchAPL
 configuration
 display formats 393
 foreign connector 388
 global CTI settings 389
 message forms 390
 version information 395

Exchange fail-safe wizard 31

Exchange management console 49

Exchange management shell 49

Exchange Server 2007
 installation
 Mapi and CDO 54

Exchange Server 2007 cluster 61

Exchange Server 2010
 installation
 Mapi and CDO 161

Exchange Server 2010 cluster 172

Exchange Server 2013
 installation
 Mapi and CDO 296

ExRep, E-script 111

F

Fail-safe wizard 31

Foreign Connector installation
Mapi and CDO 54, 161, 296

G

Global catalog 66, 177, 324

H

Hub transport server role 51, 156

I

IETF (Internet Engineering Task Force) 87
Installation of the Outlook message icons 529
Installation requirements for the connector installation with Exchange Server 2007 55
Installation requirements for the connector installation with Exchange Server 2010 163, 298
Installing 181, 187, 336
Integrated Messaging 21
Interactive voice response (IVR) 21
Internet standard RFC 1823 88

L

LDAP

configuration file 92
general information 87
installing the LDAP APL 90
LDAP APL settings 90
LDAP APL uninstallation 113
monitoring the LDAP APL 112
polling DS attributes 96, 214, 362
testing the connection 95, 213, 361

LDAP port 89

LDAP settings

editing attributes 102
global settings 110
login to DS server 94
MySQL settings 111, 229
search, definition of the replication directories 97

Lightweight directory access protocol, LDAP 87

LMACCOUNT 557

Local database (cache) 553

M

Mailbox server role 51, 156
Message classes 523
MMC files 77, 193, 342
Monitor 90, 285, 314
MSP (service provider) 553
Multiline configuration 423, 443

O

Object 87
Offline operating, Outlook 2003 522

Offline operation, Outlook XP 522
Outlook extensions 521, 542

P

Privilege check, activation with Exchange 2007 561
Privilege check, activation with Exchange 2010 588, 616
Privileges for the connector installation with Exchange Server 2007 55
Privileges for the connector installation with Exchange Server 2010 163
Privileges for the connector installation with Exchange Server 2013 298

R

Registry entries

Current_User\ExchForms Client

AdmApprovedOcx 650
AutoNameResolution 650
ChangePhoneNo 545
ChangePhonNumber 650
ExAddressType 651
ExplorerInterval 651
IMAPMode 546, 651
MsgFile 546, 652
MsgShowNoNumber 546, 652
NoFaxBtn 544, 652
NoFaxViewForm 544, 652
NoFODBtn 544, 652
NoNumberOnlyResolution 544, 653, 655
NoSMSBtn 545, 653
NoVMBtn 545, 653
NoVoiceViewForm 545, 653
NoWebAssistantBtn 545, 653
NoZeroCut 546, 654
SubstituteForPlus 546, 654

HKCU\Software\Cycos AG\COM\FaxViewer

AppendSource 659
FaxFillCol 657
FaxGrid 657
FaxLineCol 657
FaxLogoFnt 658
FaxPrintMode 658
FaxTxtFnt 658
FaxTxtFntCol 658
FaxZM 658
FaxZoom 659
LastSavePath 659
LeftFaxMargin 659
LocalPhone 660
MonitoringSucceededFromPhone 660
PlayVoiceDeviceIndex 660

- RightFaxMargin 659
- SeekSelection 660
- VoiceMailFormat 660
- HKLM + Current_User...\ExchForms Client\Fax
 - DeliveryReceipt 547, 655
 - ReadReceipt 547, 655
- HKLM + Current_User...\ExchForms Server
 - InstallPath 649
 - SetupComplete 649
- HKLM + HKCU...\ExchForms Client\SMS
 - DeliveryReceipt 547, 655
 - ReadReceipt 547, 655
 - TextLength 547, 655
- HKLM +
 - HKCU\Microsoft\Office\Outlook\Addins\Fax_SMS
 - .UMSConnect
 - CommandLineSafe 656
 - Description 656
 - FriendlyName 656
 - LoadBehavior 656
- HKLM...CurrentControlSet\Services\ExchApI
 - DisplayName 661
 - ErrorControl 662
 - ImagePath 662
 - ObjectName 662
 - Start 662
 - Type 662
- HKLM...CurrentControlSet\Services\ExchApI\Parameters
 - HomeDSA 663
- HKLM...Wow6432Node\PP-COM\MRS\LdapApI
 - DlgSessions 648
 - MRS-NonDeleteAtts 648
- Registry entries for Exchange 2007
 - HKLM...Wow6432Node\PP-COM\MRS\ExchApI
 - AcceptedDomain 559
 - Access 559
 - Account 559
 - Address_Mode 560
 - Address_Restrict_Mode 560
 - Addr_Lookup_Mode 560
 - Admingroup_RDN 560
 - ADsDomainPath 560
 - APL_SLOWDOWN 561
 - Attrib 561
 - CLASSFAX_DR 561
 - CLASSFAX_MSG 561
 - CLASSFAX_NDR 562
 - CLASSSMS_DR 562
 - CLASSSMS_MSG 562
 - CLASSSMS_NDR 562
 - CLASSVOICE_DR 562
 - CLASSVOICE_MSG 563
 - CLASSVOICE_NDR 563
 - contacts 563
 - CreateDefaultMessageClasses 563
 - CreateJournalBodyInformation 564
 - CTI_Lookup_Counter 564
 - CTI_Monitor 564
 - DeleteOutOfOfficeReply 564
 - DeleteOutOfOfficeReplyTemplate 565
 - Delivery_Report 565
 - Distrib_Count 565
 - DL_DelayStep 565
 - DL_DelayTime 565
 - DOMAIN 566
 - DO_NOT_AUTO_RESTART 566
 - DropDirectory 566
 - EnableResolveCallerNumber 566
 - EVERSION 566
 - EXADDRESSTYPE 567
 - ExchangeServer 567
 - ExtensionBuildNumbers 567
 - FaxLegacySenderAddress 567, 568
 - FaxLegacySupport 567
 - Format 568
 - FORMAT_TIFF4_Only 568
 - FromFieldFormatFax 568
 - FromFieldFormatVoice 569
 - GUID 569
 - HUBTRANSPORTSERVER 569
 - HUBTRANSPORTSERVER1 569
 - HUBTRANSPORTSERVER2 570
 - HUBTRANSPORTSERVER3 570
 - HUBTRANSPORTSERVER4 570
 - HUBTRANSPORTSERVER5 570
 - InformPostmasterWhenMailBoxFull 570
 - InstallAddressTemplates 571
 - InstallPath 571
 - MailBoxFullRepeatCount 571
 - MailBoxFullRepeatIntervallnSeconds 571
 - MailboxStore 571
 - Multiline_Support 571
 - NumberDisplayPresentation 572
 - Organization_RDN 572
 - PostmasterDisplay 572
 - PostmasterDN 572
 - Read_Report 572
 - ReplayDirectory 572
 - ReplayDirectory1 573
 - ReplayDirectory2 573
 - ReplayDirectory3 573
 - ReplayDirectory4 573
 - ReplayDirectory5 573

- RouteTableMinRebuildTime 574
- Routinggroup 574
- SendRTFBody 574
- SentRepresenting 574
- Server 574
- Site 574
- SMS_ALLOW_DIGEST 575
- Standard_Cti_Settings 575
- StorageGroup 575
- SubjectFieldFormat 575
- SubjectFieldFormatFax 576
- SubjectFieldFormatVoice 576
- SupportContactScan 576
- SuppressMIDinSubject 576
- Suppress_MID_Reports 576
- Suppress_Reports 577
- UnknownSenderName 577
- WorkAroundAreaCodeProblem 577
- HKLM...Wow6432Node\PP-COM\MRS\ExUMApi
 - Access 578
 - Account 578
 - AVOIDMAPIRELEASE 578
 - DOMAIN 579
 - EVERSION 579
 - EXADDRESSTYPE 579
 - ExchangeClusterName 579
 - ExchangeServer 580
 - ExchSCCPollTimer 580
 - GUID 580
 - HangedTimeout 580
 - InstallPath 581
 - LINE_PROXY_PATTERN 581
 - MaxFailedSessionCleanUps 581
 - MaxSessionCleanUps 582
 - Multiline_Support 582
 - POLLING_INTERVAL 582
 - ResetCountersPeriod 582
 - Server 583
 - Site 583
 - SKIPCALENDARONFAILURE 583
 - StopAplIfSessionsAreHanging 583
 - STOPONFAILURE 585
 - TerminateHanged 585
- Registry entries for Exchange 2010
 - HKLM...Wow6432Node\PP-COM\MRS\ExchApi
 - AcceptedDomain 586
 - Access 586
 - Account 586
 - Address_Mode 587
 - Address_Restrict_Mode 587
 - Addr_Lookup_Mode 587
 - Admingroup_RDN 587
 - ADsDomainPath 587
 - APL_SLOWDOWN 588
 - Attrib 588
 - BYPASS_MBX_FOR_DAG 588
 - CLASSFAX_DR 588
 - CLASSFAX_MSG 589
 - CLASSFAX_NDR 589
 - CLASSSMS_DR 589
 - CLASSSMS_MSG 589
 - CLASSSMS_NDR 589
 - CLASSVOICE_DR 590
 - CLASSVOICE_MSG 590
 - CLASSVOICE_NDR 590
 - contacts 591
 - CreateDefaultMessageClasses 591
 - CreateJournalBodyInformation 591
 - CTI_Lookup_Counter 592
 - CTI_Monitor 592
 - DAGNODES 592
 - DATABASE 592
 - DeleteOutOfOfficeReply 592
 - DeleteOutOfOfficeReplyTemplate 593
 - Delivery_Report 593
 - Distrib_Count 593
 - DL_DelayStep 593
 - DL_DelayTime 593
 - DOMAIN 594
 - DO_NOT_AUTO_RESTART 594
 - DropDirectory 594
 - EnableResolveCallerNumber 594
 - EVERSION 594
 - EXADDRESSTYPE 595
 - ExchangeServer 595
 - ExtensionBuildNumbers 595
 - FaxLegacySenderAddress 595, 596
 - FaxLegacySupport 595
 - Format 596
 - FORMAT_TIFF4_Only 596
 - FromFieldFormatFax 596
 - FromFieldFormatVoice 597
 - GUID 597
 - HUBTRANSPORTSERVER 597
 - HUBTRANSPORTSERVER1 597
 - HUBTRANSPORTSERVER2 598
 - HUBTRANSPORTSERVER3 598
 - HUBTRANSPORTSERVER4 598
 - HUBTRANSPORTSERVER5 598
 - InformPostmasterWhenMailBoxFull 598
 - InstallAddressTemplates 599
 - InstallPath 599
 - MailBoxFullRepeatCount 599
 - MailBoxFullRepeatIntervallInSeconds 599

- Multiline_Support 599
- NumberDisplayPresentation 599
- Organization_RDN 600
- PostmasterDisplay 600
- PostmasterDN 600
- Read_Report 600
- ReplayDirectory 600
- ReplayDirectory1 600
- ReplayDirectory2 601
- ReplayDirectory3 601
- ReplayDirectory4 601
- ReplayDirectory5 601
- RouteTableMinRebuildTime 601
- Routinggroup 601
- SendRTFBody 602
- SentRepresenting 602
- Server 602
- Site 602
- SMS_ALLOW_DIGEST 602
- Standard_Cti_Settings 603
- SubjectFieldFormat 603
- SubjectFieldFormatFax 603
- SubjectFieldFormatVoice 604
- SupportContactScan 604
- SuppressMIDinSubject 604
- Suppress_MID_Reports 604
- Suppress_Reports 604
- UnknownSenderName 605
- WorkAroundAreaCodeProblem 605
- HKLM...Wow6432Node\PP-COM\MRS\ExUMApi
 - Access 606
 - Account 606
 - ACCOUNTDN 606
 - ACCOUNTDNFULL 606
 - AVOIDMAPIRELEASE 607
 - CASARRAY 607
 - CASARRAYNAME 607
 - CHECKCASARRAY 607
 - DOMAIN 608
 - EVERSION 608
 - EXADDRESSTYPE 608
 - ExchangeClusterName 608
 - ExchangeServer 609
 - GUID 609
 - HangedTimeout 609
 - InstallPath 609
 - LINE_PROXY_PATTERN 610
 - MaxFailedSessionCleanUps 610
 - MaxSessionCleanUps 610
 - Multiline_Support 611
 - POLLING_INTERVAL 611
 - ResetCountersPeriod 611
 - Server 611
 - Site 611
 - SKIPCALENDARONFAILURE 612
 - StopApplIfSessionsAreHanging 612
 - STOPONFAILURE 612
 - TerminateHanged 613
- Registry entries for Exchange 2013
 - HKLM...Wow6432Node\PP-COM\MRS\ExchApi
 - AcceptedDomain 614
 - Access 614
 - Account 614
 - Address_Mode 615
 - Address_Restrict_Mode 615
 - Addr_Lookup_Mode 615
 - Admingroup_RDN 615
 - ADsDomainPath 615
 - APL_SLOWDOWN 616
 - Attrib 616
 - BYPASS_MBX_FOR_DAG 616
 - CLASSFAX_DR 616
 - CLASSFAX_MSG 617
 - CLASSFAX_NDR 617
 - CLASSSMS_DR 617
 - CLASSSMS_MSG 617
 - CLASSSMS_NDR 617
 - CLASSVOICE_DR 618
 - CLASSVOICE_MSG 618
 - CLASSVOICE_NDR 618
 - contacts 619
 - CreateDefaultMessageClasses 620
 - CreateJournalBodyInformation 620
 - CTI_Lookup_Counter 620
 - CTI_Monitor 620
 - DAGNODES 621
 - DATABASE 621
 - DeleteOutOfOfficeReply 621
 - DeleteOutOfOfficeReplyTemplate 621
 - Delivery_Report 621
 - Distrib_Count 622
 - DL_DelayStep 622
 - DL_DelayTime 622
 - DOMAIN 622
 - DO_NOT_AUTO_RESTART 622
 - DropDirectory 622
 - EnableResolveCallerNumber 623
 - EVERSION 623
 - EXADDRESSTYPE 623
 - ExchangeServer 623
 - ExtensionBuildNumbers 623
 - FaxLegacySenderAddress 624
 - FaxLegacySupport 624
 - Format 624

- FORMAT_TIFF4_Only 624
 - FromFieldFormatFax 625
 - FromFieldFormatVoice 625
 - GUID 625
 - HUBTRANSPORTSERVER 625
 - HUBTRANSPORTSERVER1 626
 - HUBTRANSPORTSERVER2 626
 - HUBTRANSPORTSERVER3 626
 - HUBTRANSPORTSERVER4 626
 - HUBTRANSPORTSERVER5 626
 - InformPostmasterWhenMailBoxFull 627
 - InstallAddressTemplates 627
 - InstallPath 627
 - MailBoxFullRepeatCount 627
 - MailBoxFullRepeatIntervallInSeconds 627
 - Multiline_Support 628
 - NumberDisplayPresentation 628
 - Organization_RDN 628
 - PostmasterDisplay 628
 - PostmasterDN 628
 - Read_Report 628
 - ReplayDirectory 629
 - ReplayDirectory1 629
 - ReplayDirectory2 629
 - ReplayDirectory3 629
 - ReplayDirectory4 629
 - ReplayDirectory5 630
 - RouteTableMinRebuildTime 630
 - Routinggroup 630
 - SendRTFBody 630
 - SentRepresenting 630
 - Server 630
 - Site 631
 - SMS_ALLOW_DIGEST 631
 - Standard_Cti_Settings 631
 - SubjectFieldFormat 631
 - SubjectFieldFormatFax 632
 - SubjectFieldFormatVoice 632
 - SupportContactScan 632
 - SuppressMIDinSubject 632
 - Suppress_MID_Reports 632
 - Suppress_Reports 633
 - UnknownSenderName 633
 - WorkAroundAreaCodeProblem 633
 - HKLM...Wow6432Node\PP-COM\MRS\ExUMApi
 - Access 634
 - Account 634
 - ACCOUNTDN 634
 - ACCOUNTDNFULL 634
 - AVOIDMAPIRELEASE 635
 - CASARRAY 635
 - CASARRAYNAME 635
 - CHECKCASARRAY 635
 - DOMAIN 635
 - E2K13_DOMAIN 292, 331, 636
 - E2K13_HOME_SERVER_DN 292, 331, 636
 - E2K13_RPC_PROXY_SERVER 292, 331, 637
 - E2K13_SERVICEUSER_DN 292, 332, 638
 - E2K13_UNRESOLVED_NAME 293, 332, 638
 - E2K13_UNRESOLVED_SERVER 293, 332, 638
 - EVERSION 638
 - EXADDRESSTYPE 639
 - ExchangeClusterName 639
 - ExchangeServer 639
 - GUID 639
 - HangedTimeout 640
 - InstallPath 640
 - LEGACYEXCHANGFEDN 293, 640
 - LINE_PROXY_PATTERN 640
 - MaxFailedSessionCleanUps 641
 - MaxSessionCleanUps 641
 - Multiline_Support 641
 - POLLING_INTERVAL 333, 642
 - ResetCountersPeriod 642
 - Server 642
 - Site 642
 - SKIPCALENDARONFAILURE 643
 - StopApIfSessionsAreHanging 643
 - STOPONFAILURE 333, 334, 636, 644
 - TerminateHanged 644
- S**
- Service Provider (MSP) 553
 - Stopping individual components 113, 231, 379
 - Store & forward interface 553
 - SupportContactScan 576
- T**
- Transaction interface 553
 - Transport directories 55, 162, 297
 - True Unified Messaging 21
- U**
- UID, update ID 110
 - Unified Messaging (UM) 21
 - Uninstalling individual components 113, 231, 379
 - Update ID (UID) 110
 - Update Sequence Number (USN) 110
 - User data 118, 236, 384
 - USN, update sequence number 110
- X**
- X.500 directory service 87
 - XPR message icons 523

