A MITEL
PRODUCT
GUIDE

Unify OpenScape Xpressions

Multi Tenancy

Administrator Documentation
11/2018

A31003-S2370-M104-8-76A9

Mitel

Notices

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

Trademarks

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

Contents

History of Changes

Date	Change	Reason
2011-09-28	Extension of the Caller Guide script for supporting the multi-tenant solution. See Section 2.5, “Separate Caller Guide Support for Tenants”, on page 67.	RQ00032467
2011-09-28	Added: New option for defining a multi-tenant administrator. See Section 2.4.2.7, “Tenant Administration”, on page 60.	RQ00027208
2012-09-03	Extended configuration to select the NCO locations for tenants and to configure the voicemail script used specifically for the single tenant. See Section 2.4.2.3, “Configuring Tenants”, on page 48.	FRN5259
2013-01-07	New note: The tenant-specific configuration introduced with V7R1 for the Voicemail script is only available for SIP connections. Configuring several Voicemail script entities via H.323 for ISDN connections is still supported. See Section 1.1, “Multi-Tenant Solution based on the XPR Server”, on page 7 und Section 2.1, “Multi-Tenant Solution – What is that?”, on page 13.	CQ00240176
2013-04-25	New feature: Configuration of an individual welcome greeting for each tenant. See Section 2.4.2.3, “Configuring Tenants”, on page 48.	FRN5984
2014-03-28	New description: How to create the “Tenant” database field and assign users to the single tenants via this database field.	CQ00281127
2015-12-16	Note about tenant features	UCBE-2077

1 Introduction and important Notes

This section provides information on the following topics:

1.1 Multi-Tenant Solution based on the XPR Server

This manual contains important information about planning and installing a multi-tenant environment.

A multi-tenant solution based on an XPR server provides users of different tenants with XPR services:

- Receiving/sending e-mails
- Receiving/sending fax messages
- Receiving/sending voicemails
- Receiving/sending SMS messages
- Using the Telephone User Interfaces (TUIs)

NOTE: Using the new, simplified voicemail configuration for the telephone user interface, which can be deployed with version V7R1, is only possible with the use of SIP connections. However, with ISDN connections, several voicemail entities can be configured to still enable using the current configuration with the H.323 protocol.

- Using the conferencing feature via *OpenScape Web Client*
- Incoming-message notification and message status
- MWI signaling (Message Waiting Indication) on the phone

The speciality here is that the tenants' user groups thus created work independent from each other though using the same XPR server: If a user of tenant A deploys an XPR server service, he/she does not realize that users of tenant B use the services of the same XPR server at the same time. The users of the single tenants can thus deploy the XPR server services fully autonomously.

1.2 Target Group of this Manual

This manual addresses system administrators who are in charge of planning and implementing a multi-tenant system based on an XPR server.

This manual contains important information about planning and installing a multi-tenant environment. Please follow these instructions precisely to avoid faulty setups and to profit from these applications as much as possible.

1.3 Working with this Manual

1.3.1 Structure of this Manual

The instructions on hand are divided into the following chapters:

Chapter 1, “Introduction and important Notes”

This chapter informs you about the structure and use of these operating instructions.

Chapter 2, “Multi-Tenant Solution”

In this chapter you receive information about how to realize a multi-tenant solution based on the XPR server in different application scenarios.

1.3.2 Reference Manuals

You find further administrative information about using the XPR server for enabling a multi-tenant solution in the following documentation:

- **Release Notes**
  Supplemental information that arrived past the editorial deadline of the manuals is available in the Release Notes on the OpenScape Xpressions server.
- ***Server Administration***
  This manual informs 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.
- ***Server Installation***
  This installation manual describes the linear XPR system setup as well as the retrospective 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.

- ***Release Notice***
  The Release Notice lists the features, setup requirements and operational restrictions of the OpenScape Xpressions server and its components.

1.3.3 Formats

In the manual on hand the following conventions apply:

Purpose	Display	Example
Special emphasis	Bold	**Name** must not be deleted.
User interface elements	Bold	Click **OK**.
Menu sequence	>	**File > Close**
Cross references, companies as well as product names	Italic	For further information please refer to the *Network* subject area. *Microsoft Outlook* *Web Assistant*
Output	Font with fix character spacing, e.g. Courier	`Command not found.`
Entry	Font with fix character spacing, e.g. Courier	Enter `LOCAL` as file name.
Variable	Italic in angle brackets	Enter the user name under *User Name*>.
Key combination	Bold	**[Ctrl]+[Alt]+[Esc]**
Steps and subordinate steps in instructional text	Numeric and alphabetic lists	1. Configure the RADSL telephony subscribers with the respective extensions. a) Click **Add**. b) Enter the name of the RADSL telephony subscriber in **RADSL telephony subscriber**.
Alternative steps in instructional text	Bulleted list	• If you would like to issue amounts, activate the check box **Issue amounts instead of units**. • If you would like to issue units, deactivate the check box **Issue amounts instead of units**.

1.3.4 Hints

Types of hints

In this manual we use the following types of hints:

NOTE: Indicates useful notes.

IMPORTANT: Indicates situations that may result in damage to property and/or loss of data.

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.

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

Employees of *Unify Software and Solutions GmbH & Co. KG* are bound to safeguard trade secrets and personal data under the terms of the company's work rules. In order to ensure that the statutory requirements during service – whether during "on-site service" or during "remote service" – are consistently met, you should always observe the following rules. You will not only maintain the interests of your and our customers, you will also avoid personal consequences.

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

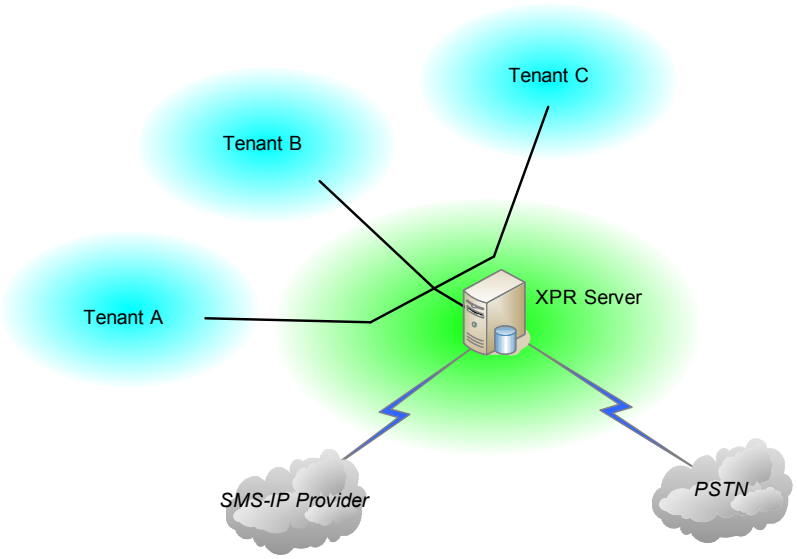
- Ensure that only authorized persons have access to customer data.
- Take full advantage of password assignment options; do not allow unauthorized persons to gain access to passwords by writing them down on a piece of paper or via other means.
- Ensure that no unauthorized person is able to process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

2 Multi-Tenant Solution

2.1 Multi-Tenant Solution – What is that?

Before we deliver detailed technical information, we will first contemplate the general concept of a multi-tenant solution based on the XPR server. The following figure shows the components and basic structure of a multi-tenant environment.



A multi-tenant solution based on an XPR server provides users of different tenants with XPR services.

The particularity here is that the users assigned to the tenants work independently though they deploy the same XPR server. For the example in the figure this means: when a user of tenant A uses an XPR server service, he/she will not know that users of tenant B use services of the same XPR server at the same time. The users assigned to the single tenants are thus able to deploy the XPR server autonomously.

The services that can be used via the XPR server are:

- Receiving/sending e-mails
- Receiving/sending fax messages
- Receiving/sending voicemails
- Receiving/sending SMS messages

- Using Telephone User Interfaces, TUIs

> ***NOTE:*** Using the new, simplified voicemail configuration for the telephone user interface, which can be deployed with version V7R1, is only possible with the use of SIP connections. However, with ISDN connections, several voicemail entities can be configured to still enable using the current configuration with the H.323 protocol.

- Using the conferencing feature via *OpenScape Web Client*
- Incoming-message notification and message status
- MWI signaling (Message Waiting Indication) on the phone

The multi-tenant solution is particularly suited for the following applications:

- If the XPR server services are to be hired via a service provider.
- If companies wish to share an XPR server in an appropriate IT infrastructure.

The XPR server administrator configures and administers the XPR components of a multi-tenant environment centrally via the *Web Assistant*.

> ***NOTE:*** Communications client does not support tenant features. WebAssistant is recommended to be used to work with Tenant.

Beyond that, one user per tenant, the so-called **contact person**, may be granted read access to the associated tenant settings.

This **contact person** has default user privileges and the following properties:

- He/she may view his/her own tenant configuration for the tenant he/she belongs to.

> ***NOTE:*** Only the OpenScape Xpressions administrator is entitled to modify the configuration, though.

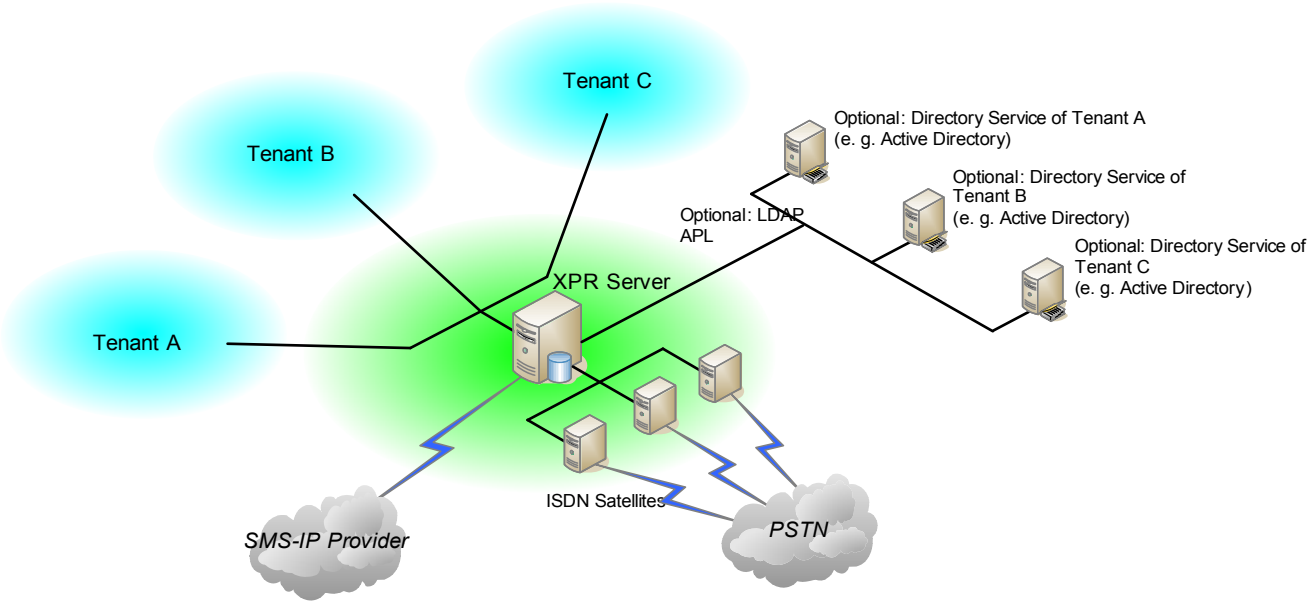
- He/she is recipient of notification e-mails if a user has reached the threshold for fax or SMS transmission.

2.2 Application Scenarios

The following application scenarios can be realized via a multi-tenant configuration:

- Unified Messaging Solution with ISDN Connection to the PSTN.
- Unified Messaging Solution with IP Connection.
- Unified Messaging Solution for Tenants that use Microsoft Exchange with the ISDN connection to the PSTN or IP connection to an *OpenScape Voice* PBX versions.

2.2.1 Unified Messaging Solution with ISDN Connection to the PSTN



In this scenario, the tenants of the multi-tenant environment are connected to the PSTN via ISDN satellites.

For a multi-tenant solution, a distributed XPR server with ISDN satellites is used. The number of satellite systems used depends on the following parameters:

- Number of S_{2M} lines to the PSTN
  In a multi-tenant solution with up to 2 S_{2M} lines, the lines are directly connected to the kernel computer. If more ISDN lines are required for a multi-tenant solution, ISDN satellites must be used. Each of these ISDN satellites can connect up to 2 S_{2M} lines.

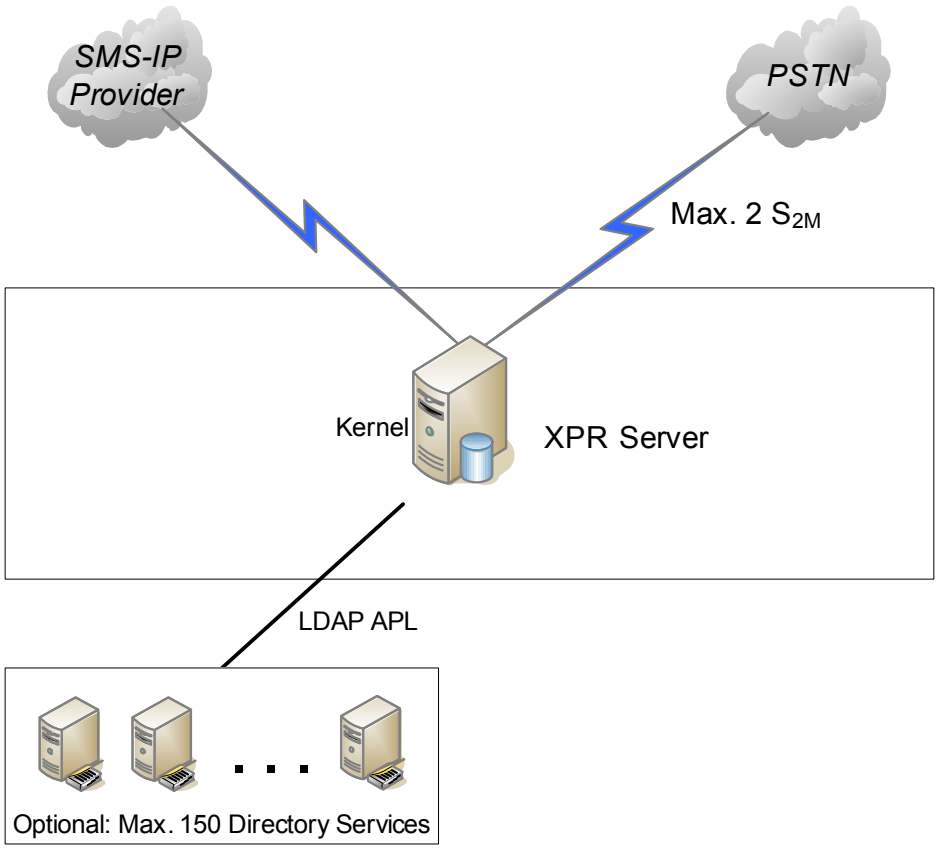
Users may be optionally administered via available directory services of the tenants.

The optional connection to an SMS-IP provider is always directly set up to the XPR kernel.

2.2.1.1 Expansion Stages of the XPR Server for the ISDN Connection to the PSTN

The XPR server may be used in this multi-tenant scenario in 5 expansion stages. The ideal design depends on the technical requirements to be met by the system.

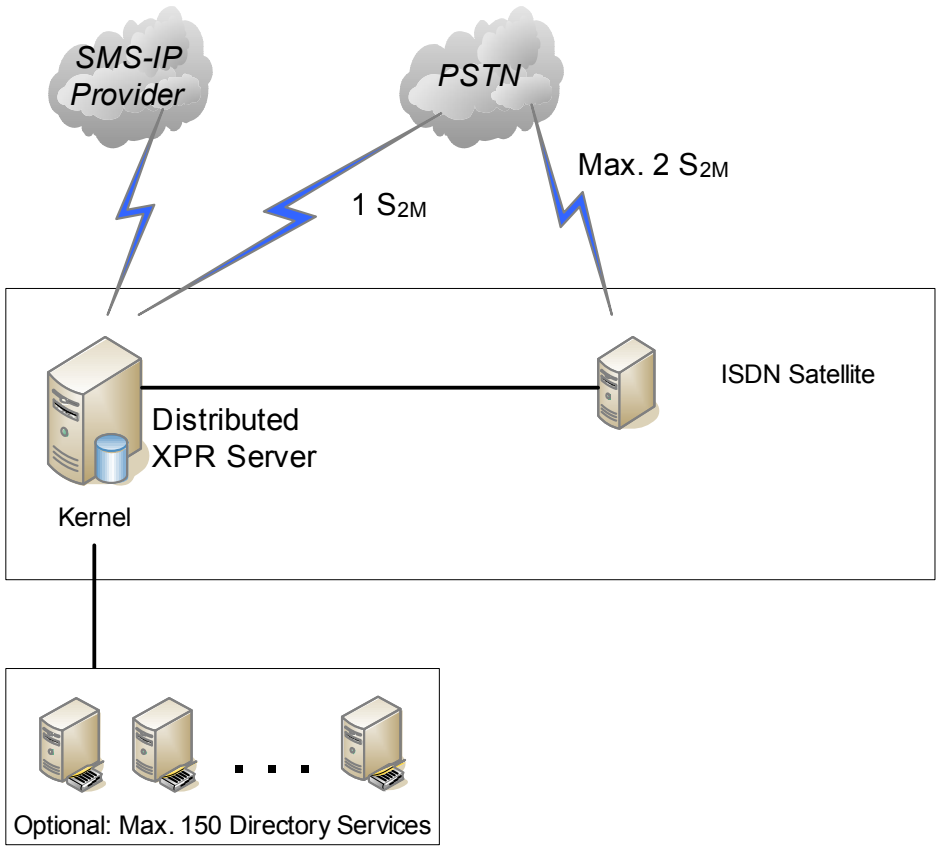
XPR server for up to 60 B-channels



Max. number of kernel B-channels	60
Number of ISDN satellites	–
Max. number of satellite B-channels	–
Max. number of connections to SMS IP providers	any*
Max. number of tenants	150
Max. number of users	25000

* The number of SMS IP providers that can be connected is defaulted by the resources of the computer system.

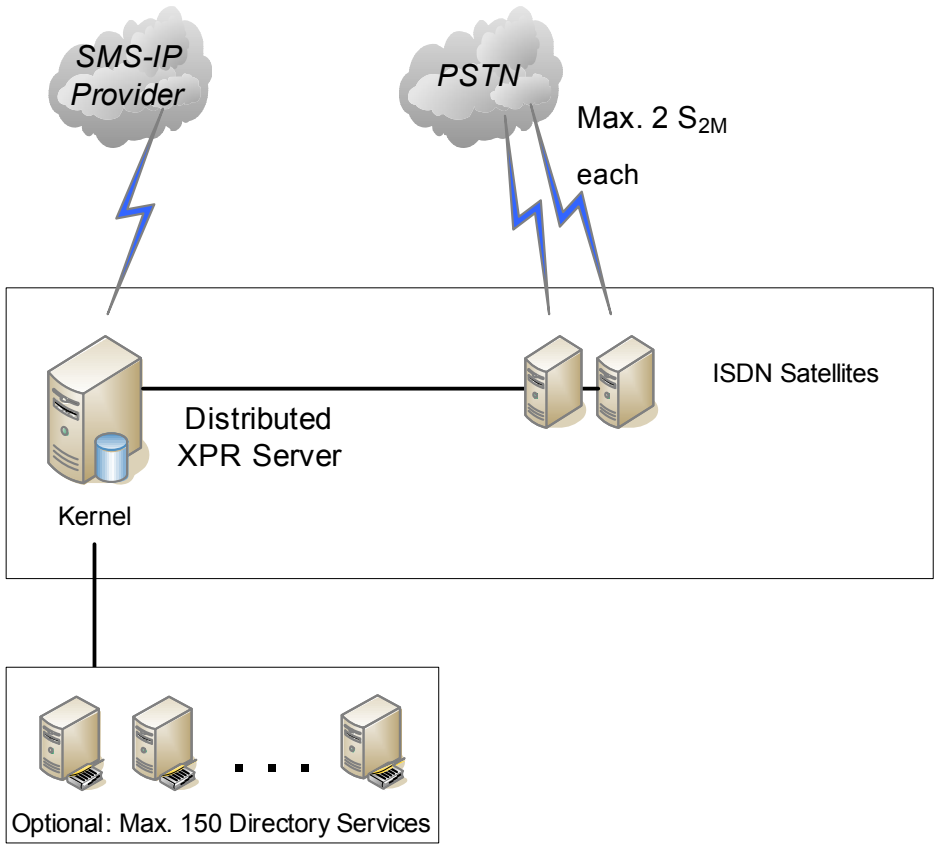
XPR server for up to 90 B-channels



Max. number of kernel B-channels	30
Number of ISDN satellites	1
Max. number of satellite B-channels	60
Max. number of connections to SMS IP providers	any*
Max. number of tenants	150
Max. number of users	25000

* The number of SMS IP providers that can be connected is defaulted by the resources of the computer system.

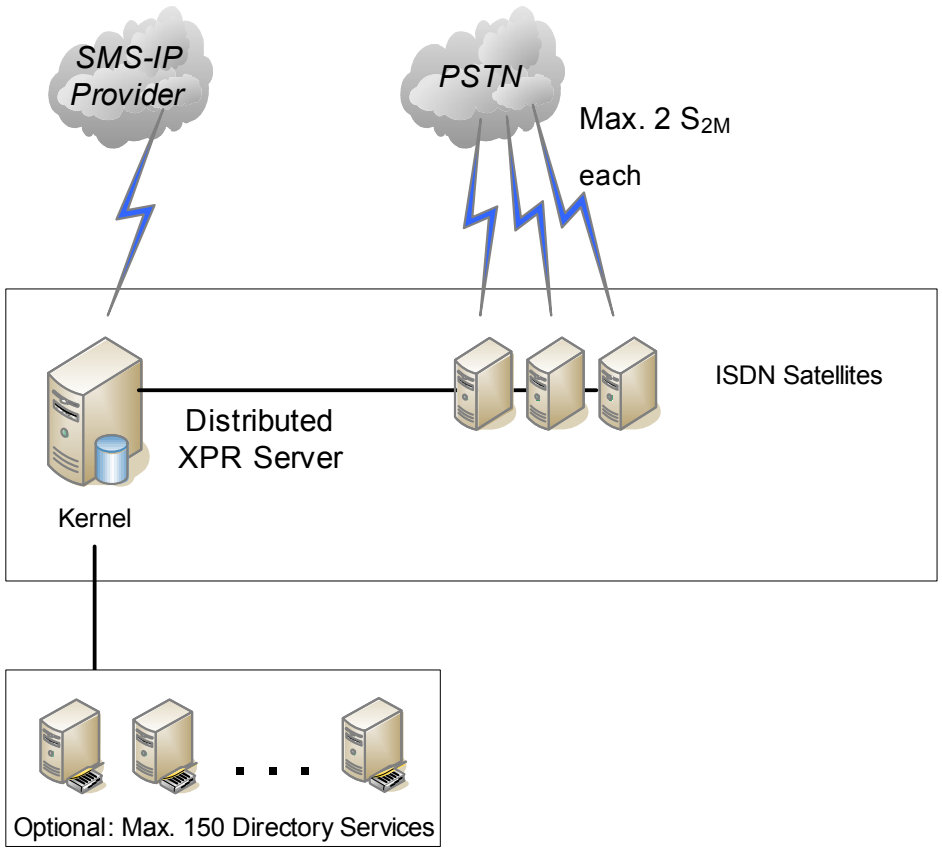
XPR server for up to 120 B-channels



Max. number of kernel B-channels	–
Number of ISDN satellites	2
Max. number of satellite B-channels	120
Max. number of connections to SMS IP providers	any*
Max. number of tenants	150
Max. number of users	25000

* The number of SMS IP providers that can be connected is defaulted by the resources of the computer system.

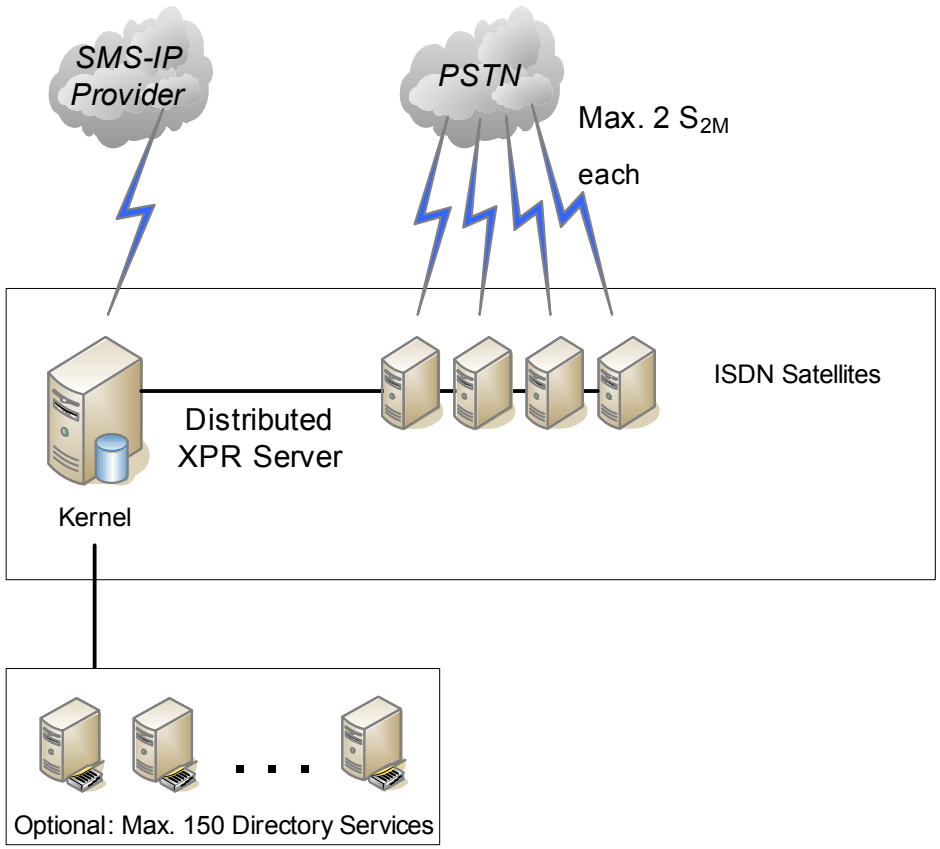
XPR server for up to 180 B-channels



Max. number of kernel B-channels	–
Number of ISDN satellites	3
Max. number of satellite B-channels	180
Max. number of connections to SMS IP providers	any*
Max. number of tenants	150
Max. number of users	25000

* The number of SMS IP providers that can be connected is defaulted by the resources of the computer system.

XPR server for up to 240 B-channels



Max. number of kernel B-channels	–
Number of ISDN satellites	4
Max. number of satellite B-channels	240
Max. number of connections to SMS IP providers	any*
Max. number of tenants	150
Max. number of users	25000

* The number of SMS IP providers that can be connected is defaulted by the resources of the computer system.

2.2.1.2 Connecting the XPR Server with ISDN to the PSTN

In a multi-tenant environment with ISDN connection to the PSTN, the XPR server is connected to the following components or networks:

- Public telephone network (PSTN) via ISDN
- Directory Services (optional)
- SMS IP provider (optional)

Let us take a close look at these connections in the following sections.

Connection to the PSTN

The XPR server is connected to the PSTN via ISDN APLs. Depending on the expansion stage, these APLs are installed on the kernel or on the ISDN satellites.

The service account of the kernel domain is used for the ISDN satellites as well (cf. Section 2.2.3.2, “Connection to the Exchange servers”, on page 35).

Connection to directory services (optional)

The connection to the Directory Services can be used to replicate user data from the directories to the XPR server user database. This requires the users of each tenant being administered in an individual Directory Service.

The Directory Services are connected via the XPR server LDAP APL. The LDAP APL is installed on the kernel. From there it can connect to the Directory Services used. So that the LDAP APL can access the Directory Services of the user groups, a corresponding service account must be implemented in the Windows domains of the single tenants.

The privileges that this service account must have depend on the requirements on the multi-tenant solution. If the Directory Service information is only to be read for replicating it to the server user database, read privileges for the service account are sufficient. In the event that also modifications are to be returned to the Directory Service, write privileges are required as well.

Connection to an SMS-IP provider (optional)

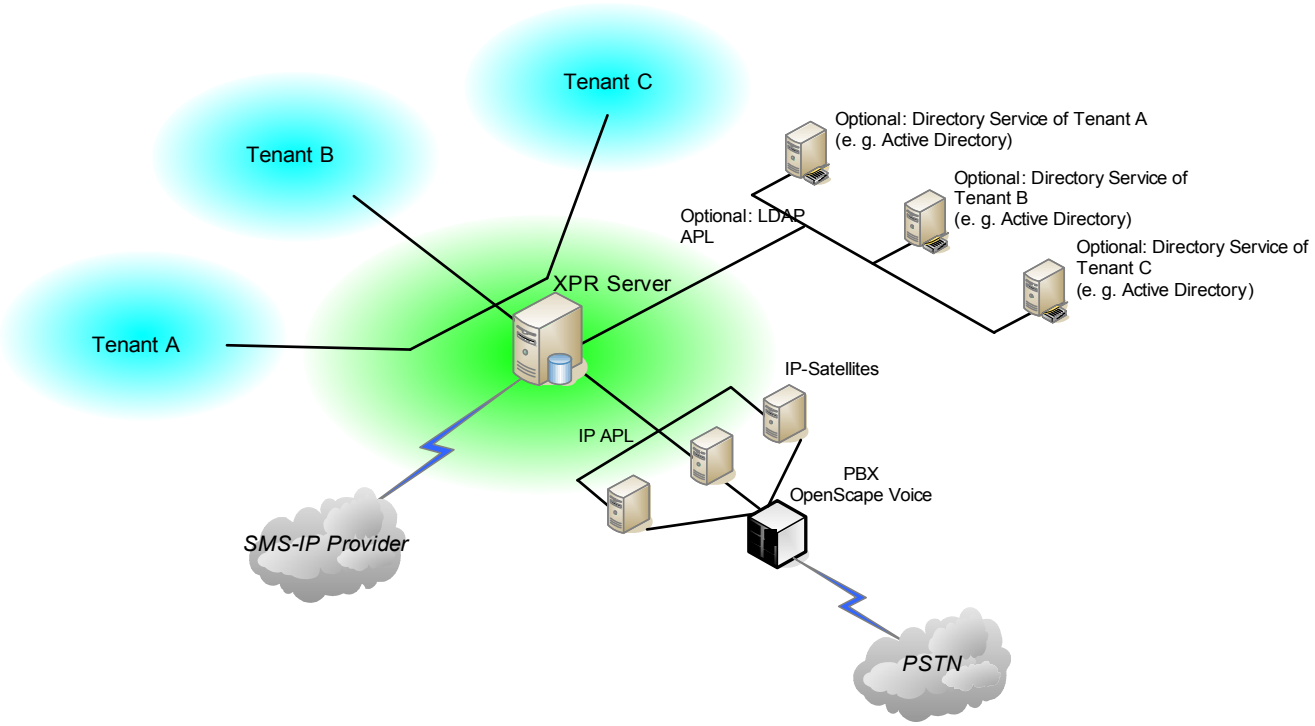
The XPR server can be connected to SMS IP providers via the SMSIP APL. The XPR server communicates with the provider via the TCP/IP protocols. The transfer of SMS messages can be made particularly secure by the XPR server connecting to the provider via a VPN tunnel. EMI/UCP is supported in version 4.6 as transmission protocol.

The SMSIP APL does not limit the number of configurable provider connections directly. Instead, the resources of the computer system used default the maximum number of SMS IP providers that can be connected to a multi-tenant solution.

2.2.1.3 Installation of the Multi-Tenant Environment

The installation is described in Section 2.3, “Installation of the Multi-Tenant Solution”, on page 37.

2.2.2 Unified Messaging Solution with IP Connection



In this scenario, the tenants of a multi-tenant environment are provided with a connection via IP to any systems that support this connection type. The figure shows an IP connection to an *OpenScape Voice* PBX, for example.

A distributed XPR server with IP satellites is used for a multi-tenant solution. The total number of channels to be used determines the number of required satellite systems.

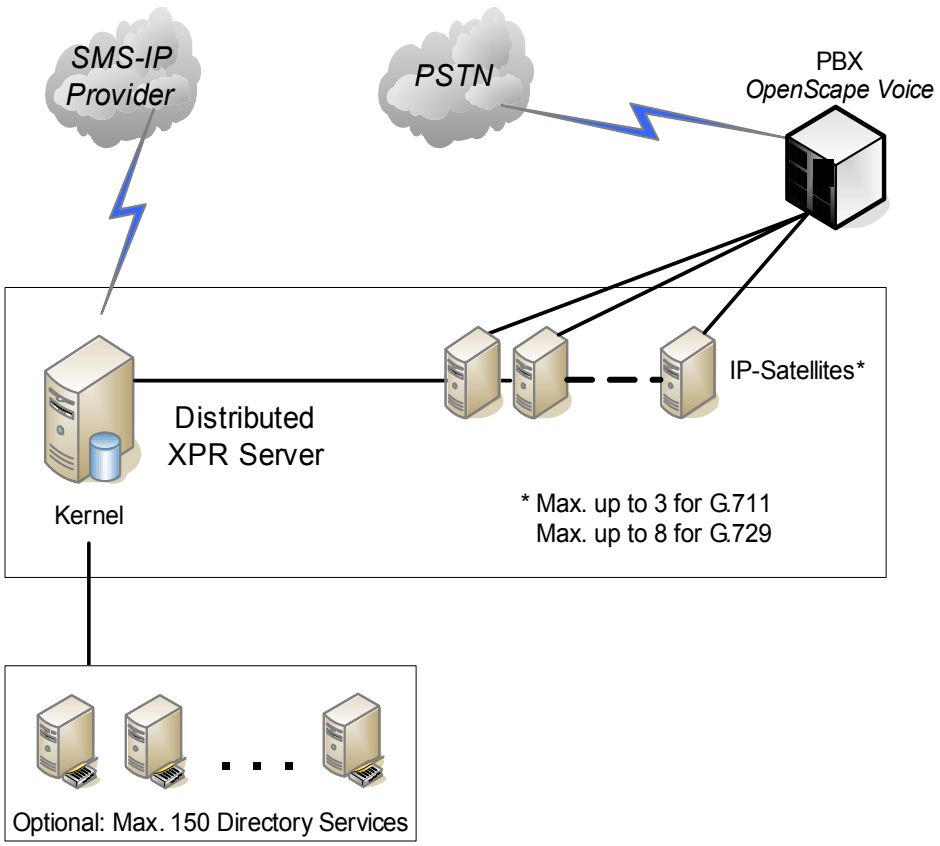
Users may be optionally administered via available directory services of the tenants.

The optional connection to an SMS-IP provider is always directly set up to the XPR kernel.

2.2.2.1 Expansion Stages of the XPR Server for the IP Connection to an OpenScape Voice

In this multi-tenant scenario, the XPR server may be used in various expansion stages. The optimized design depends on the technical system requirements, i. e., the total number of channels to be used.

2.2.2.2 XPR Server with Connection via IP Satellites



Number of IP satellites for G.711	Max. 3
Number of IP satellites for G.729	Max. 8
Max. number of connections to SMS IP providers	any*
Max. number of tenants	150
Max. number of users	25000

* The number of SMS IP providers that can be connected is defaulted by the resources of the computer system.

2.2.2.3 Connections to the XPR Server

In this multi-tenant environment the XPR server is connected to the following components or networks:

- The PBX *OpenScape Voice* via IP satellites
- Directory Services (optional)
- SMS IP provider (optional)

Let us take a close look at these connections in the following sections.

Connection to the PBX *OpenScape Voice*

The XPR server is connected to the PBX *OpenScape Voice* via the IP APL and IP satellites.

Connection to directory services (optional)

The connection to the Directory Services can be used to replicate user data from the directories to the XPR server user database. This requires the users of each tenant being administered in an individual Directory Service.

The Directory Services are connected via the XPR server LDAP APL. The LDAP APL is installed on the kernel. From there it can connect to the Directory Services used. So that the LDAP APL can access the Directory Services of the user groups, a corresponding service account must be implemented in the Windows domains of the single tenants.

The privileges that this service account must have depend on the requirements on the multi-tenant solution. If the Directory Service information is only to be read for replicating it to the server user database, read privileges for the service account are sufficient. In the event that also modifications are to be returned to the Directory Service, write privileges are required as well.

Connection to an SMS-IP provider (optional)

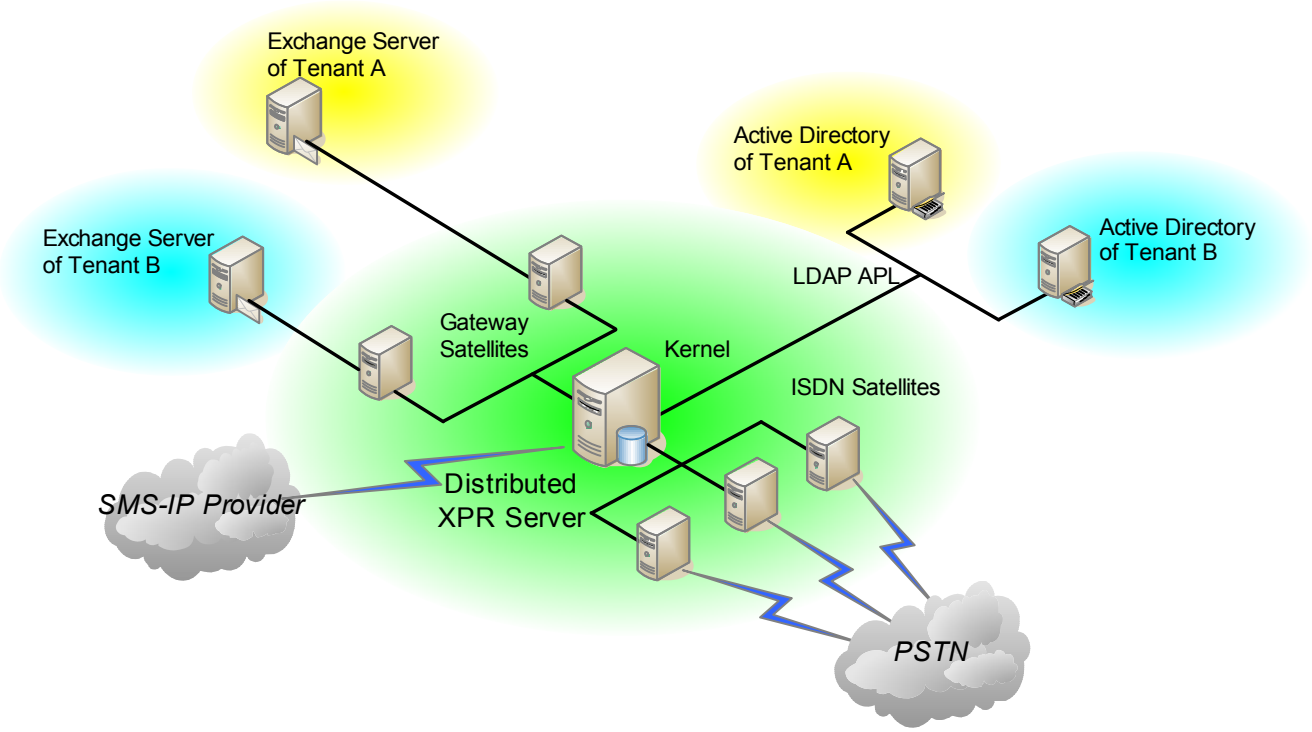
The XPR server can be connected to SMS IP providers via the SMSIP APL. The XPR server communicates with the provider via the TCP/IP protocols. The transfer of SMS messages can be made particularly secure by the XPR server connecting to the provider via a VPN tunnel. EMI/UCP is supported in version 4.6 as transmission protocol.

The SMSIP APL does not limit the number of configurable provider connections directly. Instead, the resources of the computer system used default the maximum number of SMS IP providers that can be connected to a multi-tenant solution.

2.2.2.4 Installation of the Multi-Tenant Environment

The installation is described in Section 2.3, “Installation of the Multi-Tenant Solution”, on page 37.

2.2.3 Unified Messaging Solution for Tenants that use Microsoft Exchange



An Active Directory is connected to the XPR server for each tenant of the multi-tenant environment with Exchange servers. Such a directory contains the data of all users of the relevant tenant. In the XPR server, users are assigned to a tenant while such user data is replicated from the Active Directories to the XPR server user database. In this process, the XPR server automatically assigns tenant A the user data administered in the Active Directory of tentant A.

By connecting the XPR server to the Exchange servers of the single tenants, it can access the mailboxes of all users.

For a multi-tenant solution, a distributed XPR server with ISDN and gateway satellites is used. The number of satellite systems used depends on the following parameters:

- Connected tenants
  For each tenant an Exchange server is connected to the XPR server via a gateway satellite. If required, such gateway satellites can be installed on the respective Exchange servers.

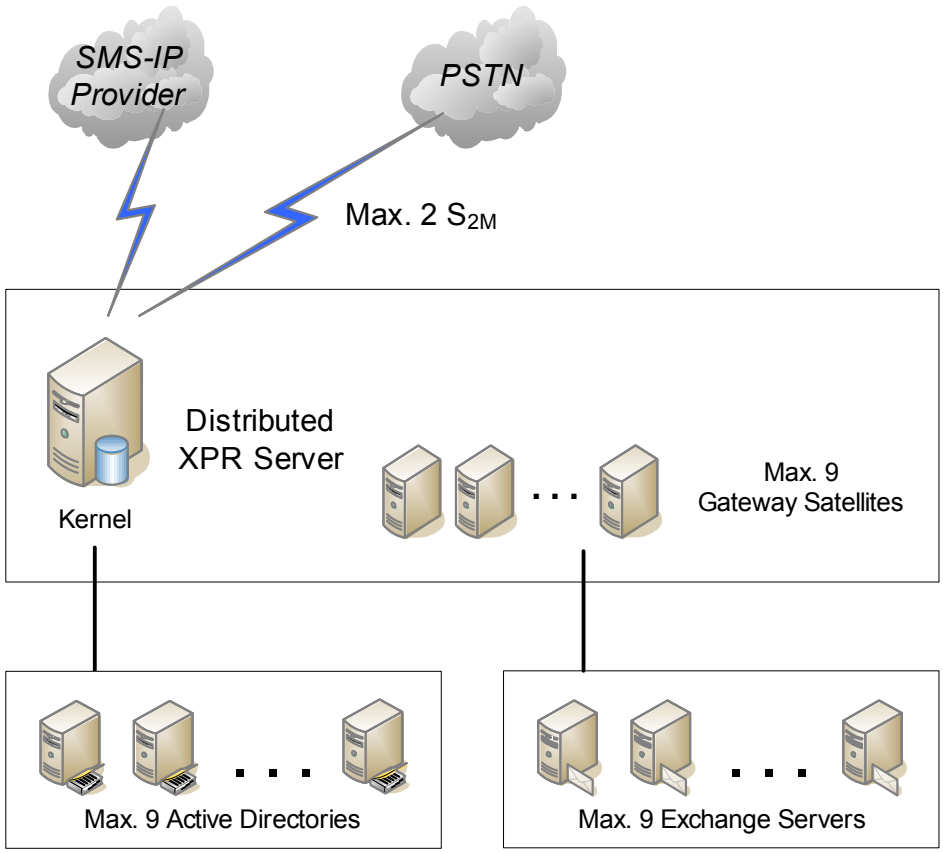
- Number of S_{2M} lines to the PSTN
  In a multi-tenant solution with up to 2 S_{2M} lines, the lines are directly connected to the kernel computer. If more ISDN lines are required for a multi-tenant solution, ISDN satellites must be used. Each of these ISDN satellites can connect up to 2 S_{2M} lines.

The Active Directory servers as well as the optional link to an SMS IP provider are always directly connected to the XPR kernel.

2.2.3.1 Expansion Stages of the XPR Server for a Multi-Tenant Solution with Exchange Servers

The XPR server may be used in this multi-tenant scenario in 5 expansion stages. The ideal design depends on the technical requirements to be met by the system.

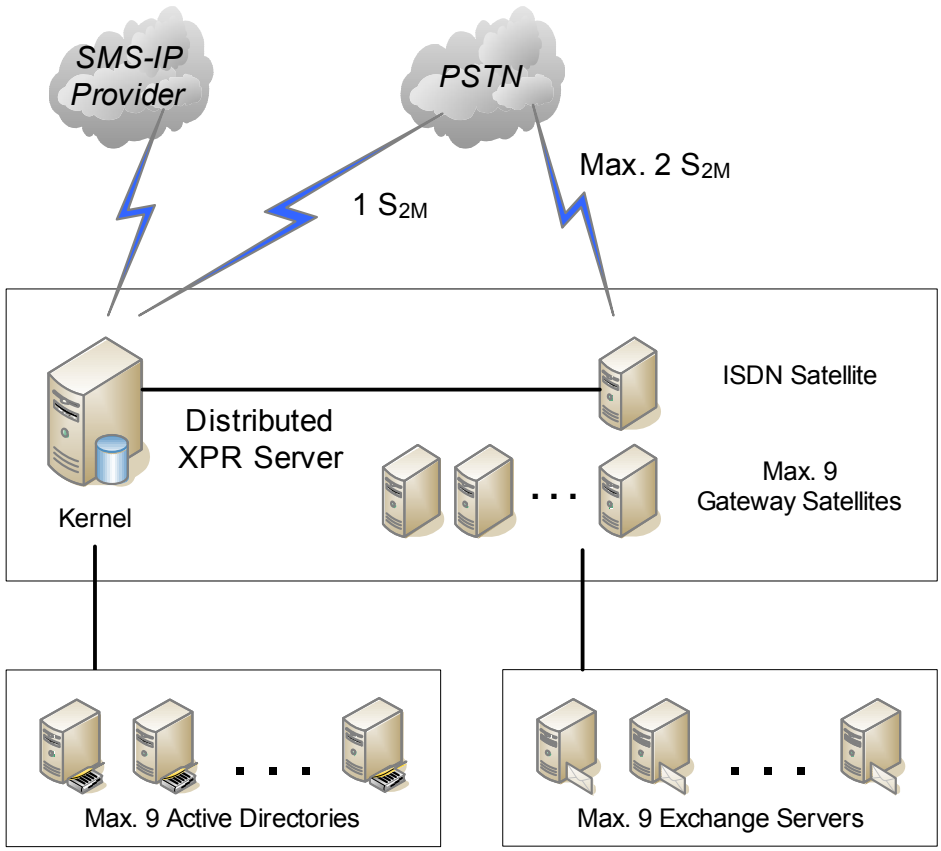
XPR server for up to 60 B-channels



Max. number of kernel B-channels	60
Number of gateway satellites	one per tenant
Number of ISDN satellites	–
Max. number of satellite B-channels	–
Max. number of connections to SMS IP providers	any*
Max. number of tenants	9
Max. number of users	25000

* The number of SMS IP providers that can be connected is defaulted by the resources of the computer system.

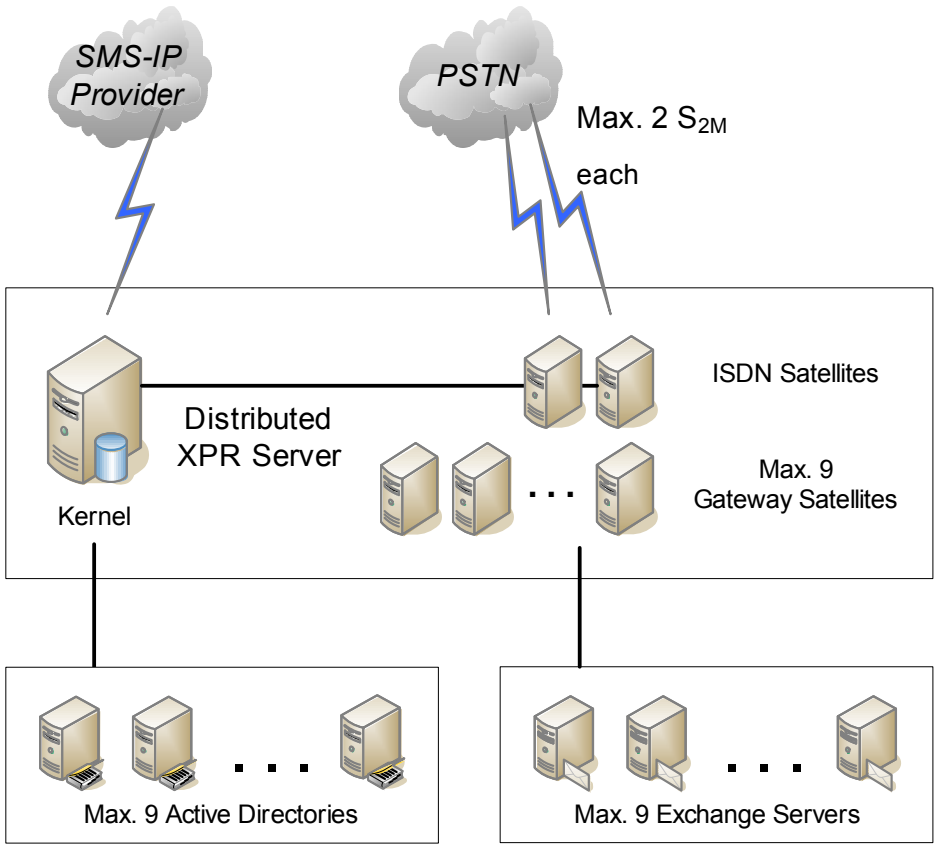
XPR server for up to 90 B-channels



Max. number of kernel B-channels	30
Number of gateway satellites	one per tenant
Number of ISDN satellites	1
Max. number of satellite B-channels	60
Max. number of connections to SMS IP providers	any*
Max. number of tenants	9
Max. number of users	25000

* The number of SMS IP providers that can be connected is defaulted by the resources of the computer system.

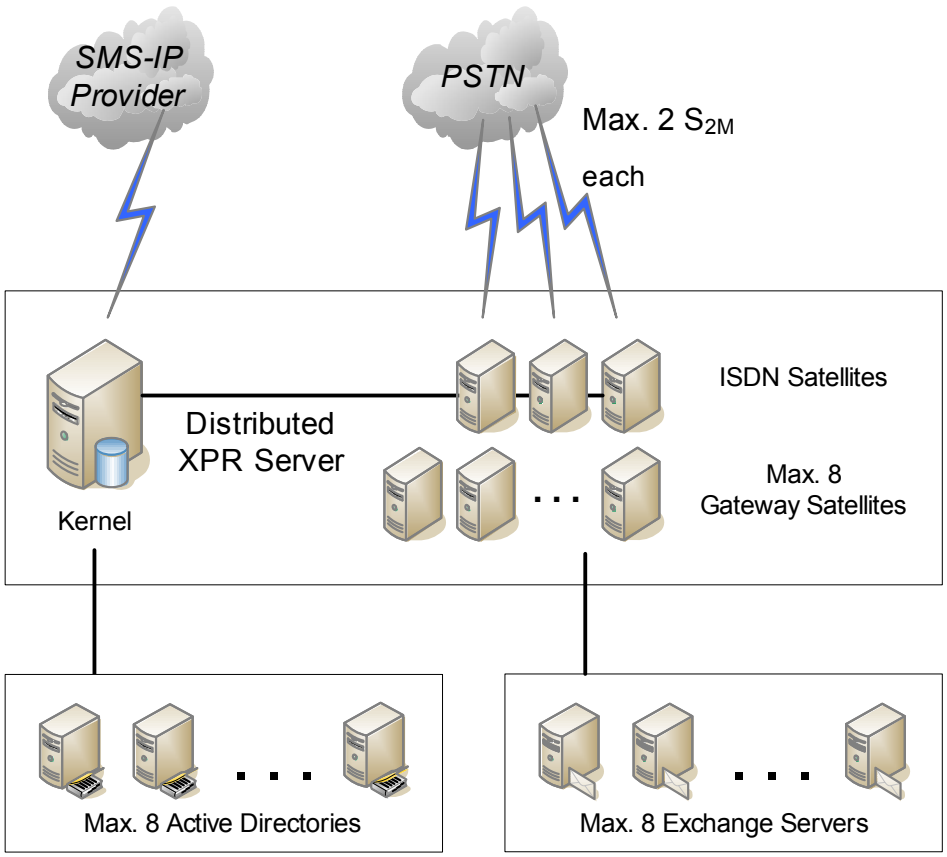
XPR server for up to 120 B-channels



Max. number of kernel B-channels	–
Number of gateway satellites	one per tenant
Number of ISDN satellites	2
Max. number of satellite B-channels	120
Max. number of connections to SMS IP providers	any*
Max. number of tenants	9
Max. number of users	25000

* The number of SMS IP providers that can be connected is defaulted by the resources of the computer system.

XPR server for up to 180 B-channels

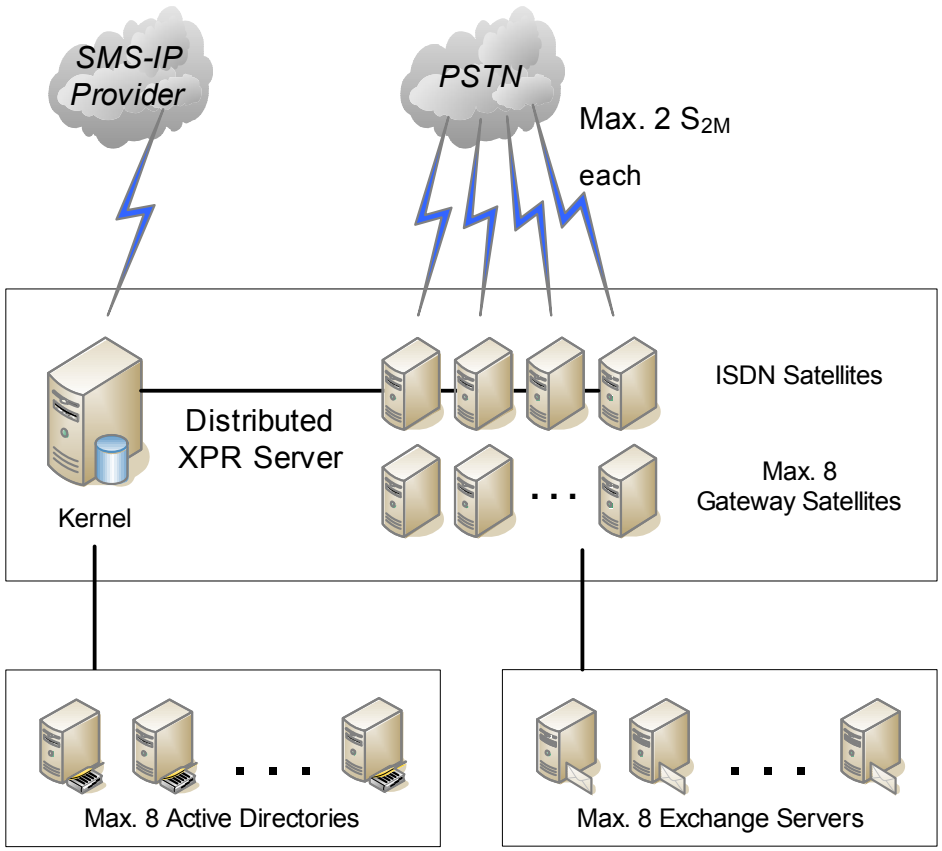


Max. number of kernel B-channels	–
Number of gateway satellites	one per tenant
Number of ISDN satellites	3
Max. number of satellite B-channels	180
Max. number of connections to SMS IP providers	any*
Max. number of tenants	8
Max. number of users	25000

* The number of SMS IP providers that can be connected is defaulted by the resources of the computer system.

IMPORTANT: In this expansion not more than eight tenants are supported.

XPR server for up to 240 B-channels



Max. number of kernel B-channels	–
Number of gateway satellites	one per tenant
Number of ISDN satellites	4
Max. number of satellite B-channels	240
Max. number of connections to SMS IP providers	any*
Max. number of tenants	8
Max. number of users	25000

* The number of SMS IP providers that can be connected is defaulted by the resources of the computer system.

IMPORTANT: In this expansion not more than eight tenants are supported.

2.2.3.2 Connections to the XPR Server

In a multi-tenant environment with Exchanger servers the XPR server is connected to the following components or networks:

- Exchange servers
- Public telephone network (PSTN) via ISDN
- Active directories
- SMS IP provider (optional)

Let us take a close look at these connections in the following sections.

Connection to active directories

The connection to the Active Directories is used to replicate user data from the directories to the XPR server user database. This occurs under the assumption that the users of each tenant are administered in an individual Active Directory. This requirement must be met since users are assigned to user groups on grounds of the affiliation to an Active Directory.

The Active Directories are connected via the XPR server LDAP APL. The LDAP APL is installed on the kernel. From there it can connect to the Active Directories. So that the LDAP APL can access the Active Directories of the user groups, a corresponding service account must be implemented in the Windows domains of the single tenants.

The privileges that this service account must have depend on the requirements on the multi-tenant solution. If the Active Directory information is only to be read for replicating it to the XPR server user database, read privileges for the service account are sufficient. In the event that also modifications are to be returned to the Active Directory, write privileges are required as well.

Connection to the Exchange servers

The XPR server accesses the users' mailboxes via the Exchange server connection. It also uses this connection to deliver fax messages and voicemails to the Exchange users' inboxes. Here again we assume that for each tenant an individual Exchange server is available.

The Exchange servers are connected to the XPR server via gateway satellites with an Exch APL each or with a combination of Exch and ExUM APL. If required, the gateway satellites can also be directly installed in the corresponding Exchange domains.

So that the Exchange APLs can access their associated Exchange servers, a corresponding service account must be configured in the kernel domain. This account is available overlapping the domains by positions of trust between the kernel domain and the tenant domains. The required privileges of this service account are comprehensively described in the *OpenScape Xpressions Microsoft Exchange Gateway* manual.

Connection to the PSTN

The XPR server is connected to the PSTN via ISDN APLs. Depending on the expansion stage, these APLs are installed on the kernel or on the ISDN satellites.

The service account of the kernel domain is used for the ISDN satellites as well (cf. Section 2.2.3.2, “Connection to the Exchange servers”, on page 35).

Connection to an SMS IP provider

The XPR server can be connected to SMS IP providers via the SMSIP APL. The XPR server communicates with the provider via the TCP/IP protocols. The transfer of SMS messages can be made particularly secure by the XPR server connecting to the provider via a VPN tunnel. EMI/UCP is supported in version 4.6 as transmission protocol.

The SMSIP APL does not limit the number of configurable provider connections directly. Instead, the resources of the computer system used default the maximum number of SMS IP providers that can be connected to a multi-tenant solution.

2.2.3.3 Installation of the Multi-Tenant Environment

The installation is described in Section 2.3, “Installation of the Multi-Tenant Solution”, on page 37.

2.3 Installation of the Multi-Tenant Solution

This chapter describes the installation of a multi-tenant environment.

2.3.1 General Installation Requirements

Before you can start with the setup in the next section, some requirements must be met. The following checklist itemizes these requirements. When all requirements are complied with, you can start the installation.

☐	If Directory Services are to be deployed for administering users, they must have been configured as operable. ***Note:*** Using the *Active Directory* Directory Service is mandatory for the Exchange server solution.
☐	In case of an Exchange server solution the Exchange servers of the single tenants must have been configured as operable. ***Attention:*** For the installation of the Exchange server solution we assume that the Exchange servers are in the tenants' Windows domains (tenants domains) separated from each other.
☐	In an Exchange server solution, several connections for message routing can be used on the Exchange servers. In this case, suitable transmission options must be configured under Exchange for the desired prioritization of the single connections.
☐	Between the kernel domain and the tenant domain, bidirectional positions of trust must be configured.
☐	The kernel and the required satellite systems of the distributed XPR server must be installed. The number of ISDN satellites results from the number of required S_{2M} lines into the PSTN. The number of IP satellites results from the number of required channels to the *OpenScape Voice* PBX. The number of gateway satellites results from the number of available Exchange domains, i. e. from the number of tenants. ***Attention:*** For the following installation we assume that the kernel, the ISDN satellite systems and the IP satellite systems are in the same domain (kernel domain). The following APLs must be installed particularly for the distributed XPR server: ☐ ISDN APL(s) Depending on the multi-tenant environment on the kernel (up to a maximum of 60 B-channels) or on the ISDN satellites (in case of more than 60 B-channels) ☐ Exch APLs For a tenant environment that uses Exchange servers. Configure one Exchange connection per Exchange tenant via a gateway satellite.
	☐ LDAP APL If Directory Services is deployed for user administration. The LADP APL required for this must be installed on the kernel. ☐ SMSIP APL (on the kernel) ***Note:*** Is only required if an SMS-IP provider is to be connected.

2.3.2 Technical Framework

The following chapter describes technical conditions for using the XPR server in a multi-tenant environment.

2.3.2.1 Requirements on the Computer System Hardware

The following table shows the minimum requirements to be met by the computer systems (kernel, satellites) in a multi-tenant solution.

- Processor — 3 x Intel Xeon 3,0 GHz
- Working memory — 8 GB RAM
- Hard disks — 4 x 72 GB SCSI RAID5, Hot-Plug
- Miscellaneous — At least two free PCI slots with full implementation size and PCI Rev 2.2

2.3.2.2 Requirements on the Network

The network connection between the kernel and the satellite of a distributed XPR server must comply with the following requirements:

- Bandwidth — 100 Mb/s
- Runtime — <1 ms

2.3.2.3 Functional Restrictions on PhoneMail and Ergo

The following functional restrictions apply for PhoneMail and Ergo:

- It is not possible to call back the originator of a voicemail
- It is not possible to reroute a caller to another subscriber (postmaster, deputy etc.)

2.3.2.4 Ports used on the Transport Layer

The kernel must be able to communicate with the components of its satellites. For this purpose, unhampered communication via the following ports must be ensured. This requirement is of particular importance if firewalls are used between the components of the multi-tenant environment.

Components	Port number	for the connection between	Remark
Exch APL, ExUm APL, NameLoc ISDNAPL IP APL	UDP 137	Kernel – Gateway satellite	Distributed XPR server via firewall
Exch APL, ExUm APL, NameLoc SDN APL IP APL	UDP 138	Kernel – Gateway satellite	Distributed XPR server via firewall
Exch APL, ExUm APL, NameLoc SDN APL IP APL	TCP 139	Kernel – Gateway satellite	Distributed XPR server via firewall
Exch APL, ExUm APL, NameLoc SDN APL IP APL	TCP/UDP 445	Kernel – Gateway satellite	Distributed XPR server via firewall (SMB via TCP/IP)
LDAP APL	TCP 389	Kernel – Active Directory controller	
Web APL	TCP 080	Kernel – PC client	HTTP server
Web APL	TCP 443	Kernel – PC client	Secure HTTP server
Rep APL	TCP/UDP 1433	Kernel – SQL server	ODBC-default port
SMSIP APL	Individual	Kernel – Internet	Requires adjustment to the SMS IP provider.

2.3.3 Performing the Installation

The installation of a multi-tenant environment can be divided into the following phases:

1. Resetting the XPR Server to Domain Service Account
2. Installing Gateway Satellites
3. Activating the Multi-Tenant Feature

The following sections guide you through these single installation phases.

2.3.3.1 Resetting the XPR Server to Domain Service Account

Via a position of trust the kernel components must later be able to access the gateway satellites configured in the tenant domains. For this, all XPR services must be executed under a service account that is specified in the kernel domain as domain user.

Perform the following steps to

- create a new service account in the kernel domain and
- switch the XPR server to this service account.

Requirement

- You are logged in at the system as domain administrator and you are authorized to define domain users.

Installation steps

1. Create a new service account in the kernel domain. For the installation steps to follow we select as example the account name *MTenant*.
2. Assign the following privileges to the new service account:
   - Domain User
   - Domain Admins
   - Enterprise Admins
   - Schema Admins
3. Configure all kernel services in a way that they can be executed under the new service account. In our example under *MTenant*.
4. If the multi-tenant environment contains ISDN satellites:
   Configure all services of these ISDN satellites in a way that they are executed under the new service account as well. In our example under *MTenant*.

5. If the multi-tenant environment contains IP satellites:
   Configure all services of these IP satellites in a way that they are executed under the new service account as well. In our example under *MTenant*.
6. Restart the thus adapted XPR services.
7. For checking purposes, log on to the kernel domain on the Exchange servers of the different tenants under the new service account. In our example under *MTenant*.

What can I do …

- *if I want to log on and the kernel domain is not available for selection?*
  - Check the configured position of trust between the kernel domain and the tenant domain of the relevant Exchange server.

2.3.3.2 Installing Gateway Satellites

NOTE: You find further information about the configuration of satellite systems in the *Server Installation* manual.

The Exchange APLs of the multi-tenant environment are installed on satellite systems that are administered in the different tenant domains. It is possible to install an Exch APL or a combination of Exch and ExUM APL on each satellite system. If required, the satellite systems may also be installed on the tenants' Exchange servers.

Execute the following steps to install the Exch APL or Exch and ExUM APL on a gateway satellite.

IMPORTANT: For the following satellite configuration the new service account (*MTenant*) must be used as start account for the Exchange APLs. If the gateway satellite was previously installed with another start account, the satellite installation must be performed again.

Installation steps

1. Install the gateway satellite under an administrator account of the relevant tenant domain. In the course of this installation specify that the new service account is used as start account for the Exchange APLs. In our example the service account *MTenant*.

2.3.3.3 Activating the Multi-Tenant Feature

After you have completed the setup of the multi-tenant environment and the license for deploying this feature is available, you can immediately use it.

2.4 Configuring a new Tenant

This chapter describes how to create a new tenant in a multi-tenant environment.

2.4.1 General Configuration Requirements

Before you can start configuring a new tenant, the following requirement must be met:

- ☐ You have the Web APL installed on the XPR server to be able to configure the XPR server with the *Web Assistant*.

2.4.2 Performing the Configuration

The configuration of a new tenant can be divided into the following phases:

1. Adding the “TENANT” database field in the user administration
2. Adding Tenants in the XPR Server
3. Configuring Tenants
4. Assigning users to the tenant
5. Connecting the Tenant's Directory Service
6. Assigning the active directory to the new tenant
7. Configuring Multiline for the Exchange Tenants

The following sections guide you through these single installation phases.

2.4.2.1 Adding the “TENANT” Database Field in the User Administration

In order to assign a user to a specific tenant, there must be a database field on the XPR server via which this assignment can be performed.

You must call this database field **TENANT** and add it manually via the *Web Assistant*.

NOTE: You find a detailed description of how to extend the database mask in the *Web Assistant* manual.

How to extend the XPR database by the **TENANT** field:

1. Start the *Web Assistant*.
2. Log on to the system with administrative privileges.
3. Expand the **Special server settings** link in the navigation area.
4. Switch with a click on the appropriate link in the navigation area to the **Mask editor** settings page.
5. Select mask **USER** from the combo box as the one to be edited.
6. Click on the **Edit** button.
   The user database definitions are displayed.
7. Paste the following entry anywhere in the list of database fields:

   ```
   TENANT        ##################################
   ```

   NOTE: The empty space between the database field name and the wildcards for the field's width must consist of blanks (no tab!).

   ---

8. Click on the **Check mask description** button.
   If this delivers an error, check your entry's syntax.
9. If the check did not produce an error message, click on **Save** at the bottom margin of the settings page. The database field is added.

The required **TENANT** database field is thus configured and available for assigning users to the corresponding tenants.

You can make sure on this by opening a user specification in the *Web Assistant* via **Server settings >** User administration. An additional database field called **TENANT** should now be available there.

2.4.2.2 Adding Tenants in the XPR Server

When you create a new tenant, assign a unique ID to this tenant. Within the XPR server this ID is mainly used for the following purposes:

- To uniquely identify the tenant.
- To hide the users of different tenants from one another.
- To manage tenant-related quotas for fax and SMS messages.

Perform the following steps to add a new tenant in the XPR server.

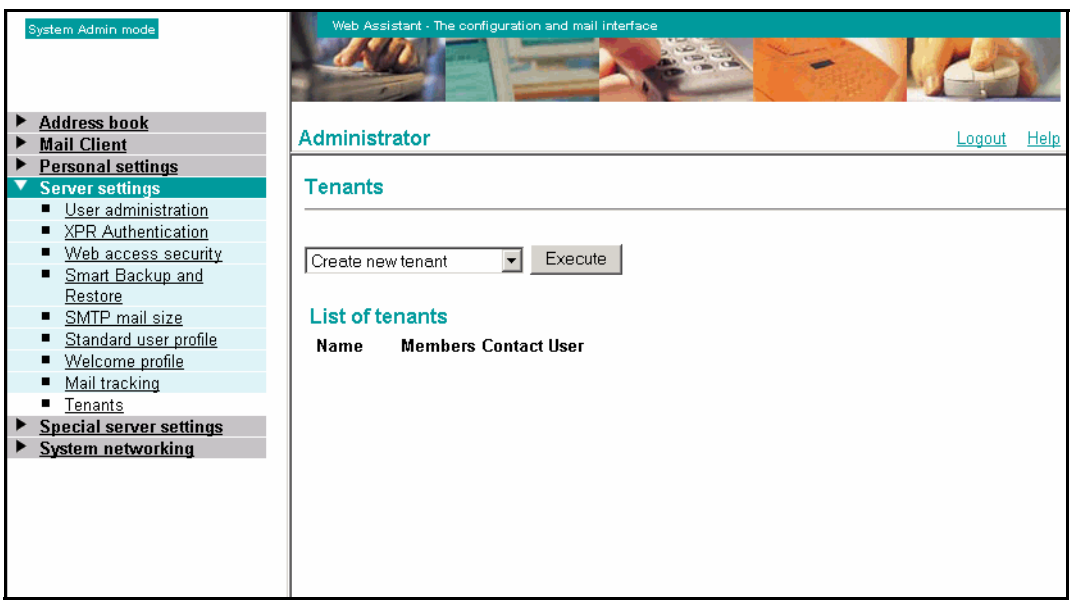
Requirement

- A *Web Assistant* gives you access to the XPR server.

Installation steps

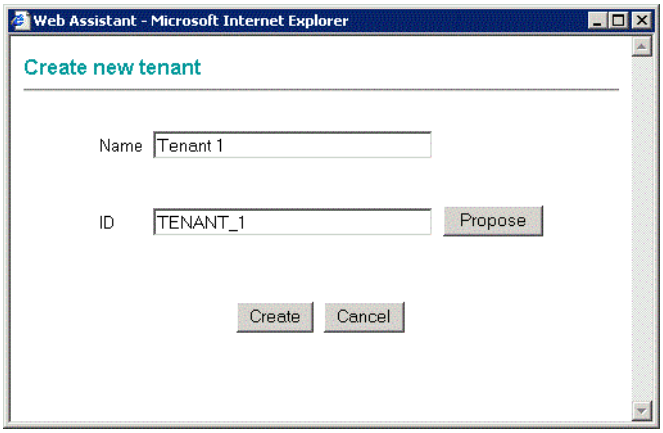
1. Start the *Web Assistant*.
2. Log on under an XPR server user account that has administrative privileges.
3. Open the menu option **Server settings > Tenants**.

   The following page is displayed:



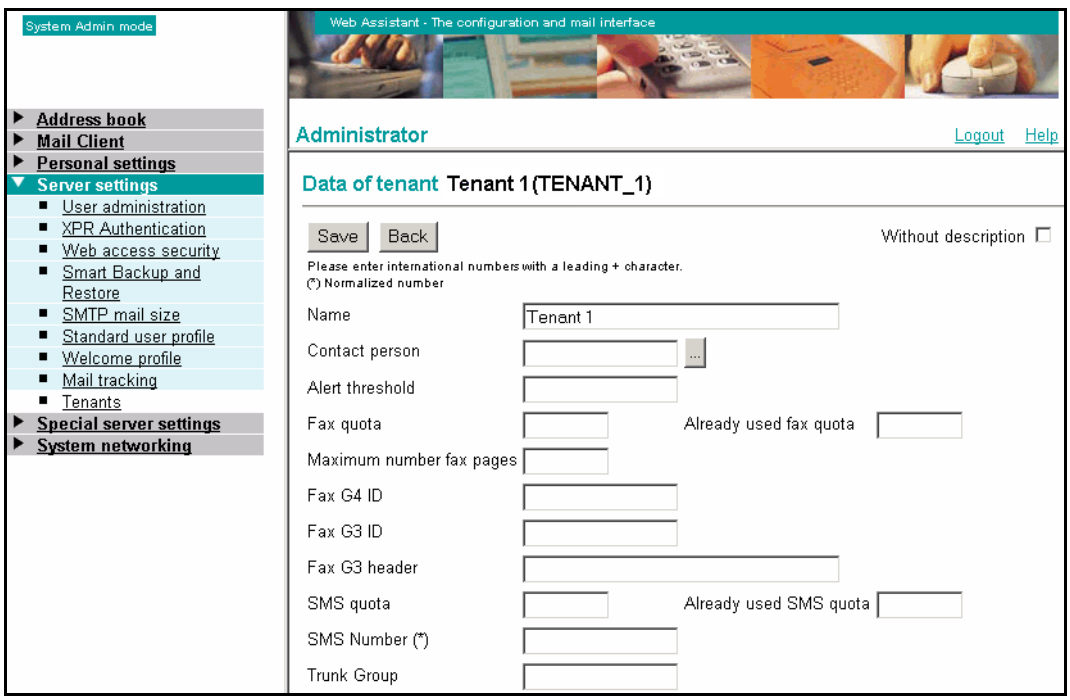
4. In the selection field choose the **Create new tenant** option and confirm the selection with **Execute**.

   The following page is displayed:



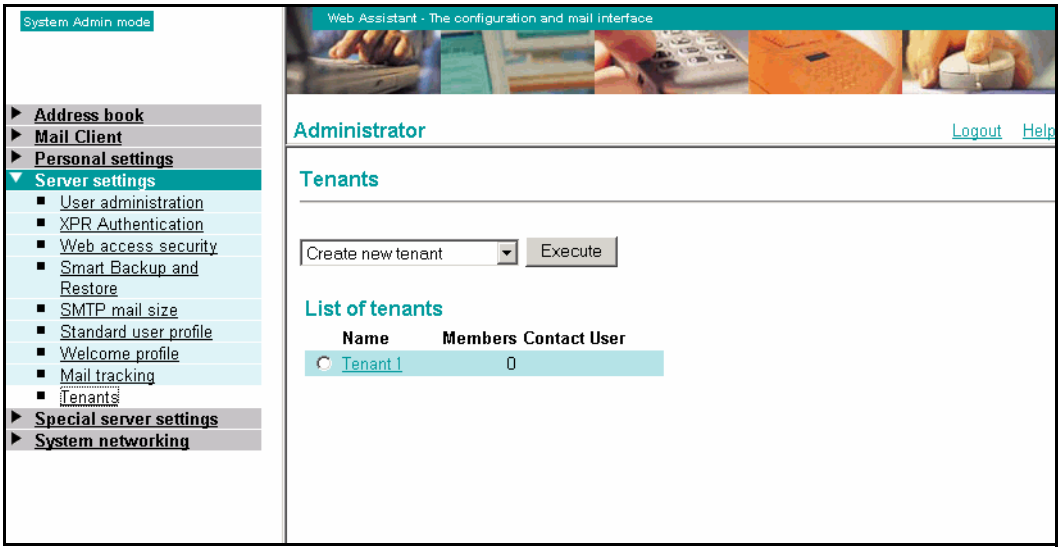
5. Enter a name for the new tenant in the **Name** field. Assign a "speaking" name here to improve clarity. As example we choose the name *Tenant 1*. While you enter the name, a unique tenant ID is created in the **Id** field.
   Confirm your entry with **Create**.

   The following page is displayed:



6. Copy the newly created tenant with **Save**.
7. Open the menu option **Server settings > Tenants**.

   The following page is displayed:



8. Verify that the newly created tenant is displayed in the tenant list.

What can I do …

- *if the newly created tenant is not displayed in the tenant list....?*
  - Create the tenant once more.
- *if the error message* “Tenant <*tenant*> already exists” *is displayed....?*
  - Open the menu option **Server settings > Tenants** and check whether the tenant list already contains a tenant with the desired name.
  - If the tenant list already contains a tenant with the desired name, create the new tenant under another name.
  - If the tenant list does not contain a tenant with the desired name, remove the incorrectly saved tenant with the desired name from the XPR user database. You find it there under the class name *Tenant*.

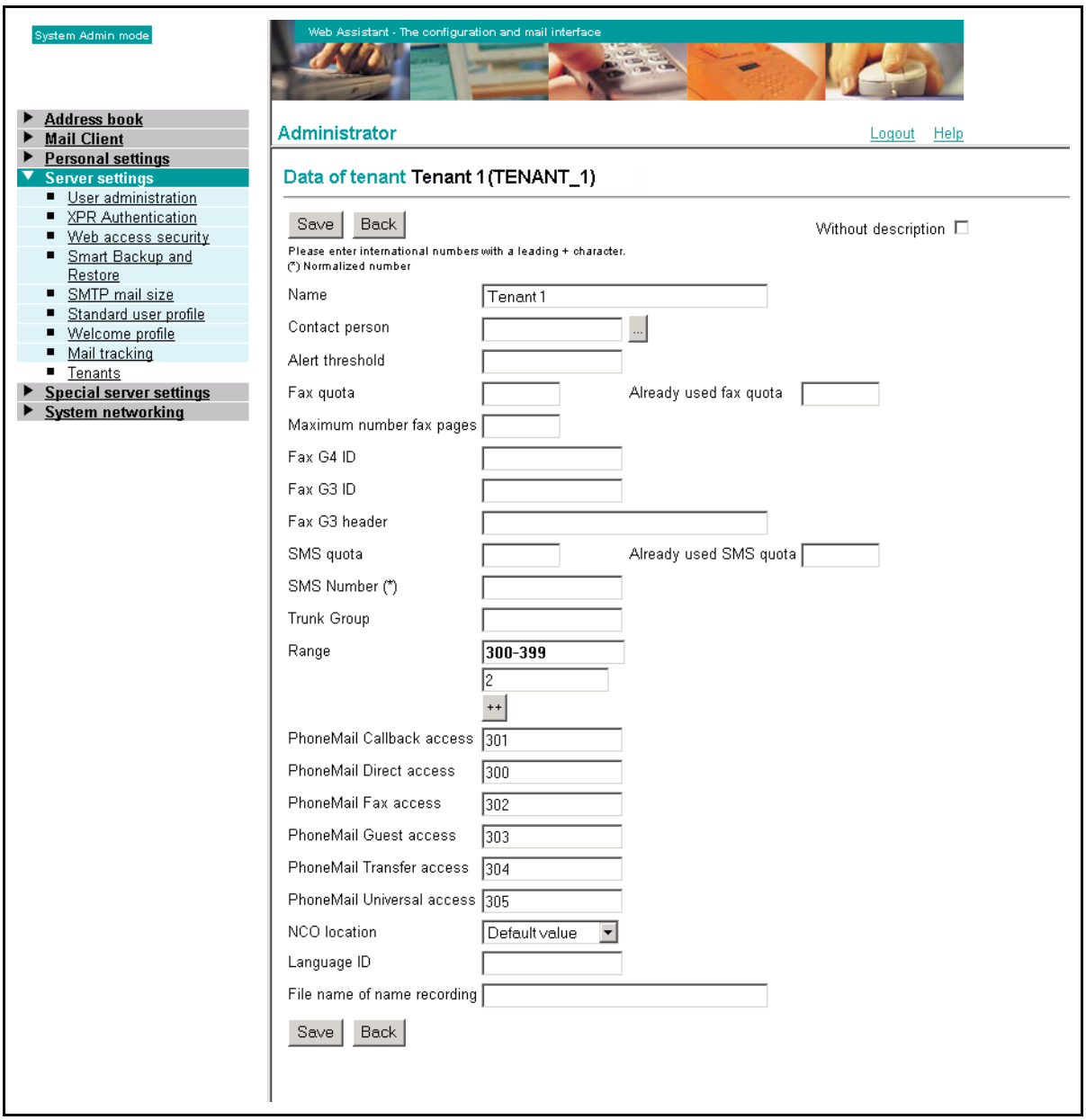
2.4.2.3 Configuring Tenants

You need to configure the message quotas and the voicemail script used for the single tenants. These quotas restrict the amount of messages that the XPR server routes for the users of the relevant tenant. The voicemail script configuration assigns the service access to a voicemail script to the users of a tenant.

Execute the following steps to configure a new tenant:

1. Open the menu option **Server settings > Tenants**.
2. Select the newly created tenant from the tenant list. In our case *Tenant1.*

   The following page is displayed:



3. Make the corresponding entries in the tenant data fields.

   - **Name**
     This field features the name you have already assigned to this tenant. The input line lets you change the tenant name if required.

- **Contact person**
  Enter here the ID of the XPR user to have access to the data of this tenant. Thus to the setting page displayed here.

  IMPORTANT: The defined user must belong to the relevant tenant.

  This **contact person** has default user privileges and the following properties:

  – He/she may view his/her own tenant configuration for the tenant he/she belongs to.

  NOTE: Only the OpenScape Xpressions administrator is entitled to modify the configuration, though.

  – He/she is recipient of notification e-mails if a user has reached the threshold for fax or SMS transmission.

- **Alert threshold**
  Enter here a value in percent, which is used in combination with the **Fax quota** and **SMS quota** fields.
  If the ratio of the sent fax or SMS messages and the associated threshold reaches this percentage, the XPR user defined under **Contact person** is informed accordingly.

- **Fax quota**
  Enter here the total number of fax messages that the XPR server is to rout for the users of this tenant.
  When the total number of sent fax messages reaches this threshold, the XPR user defined under **Contact person** is informed accordingly. You can set the precise number of messages that triggers this information via the defaulted value under **Alert threshold**.
  Once this quota has been reached, the XPR server does not send any further fax messages for this tenant. In this case, a sending party receives an error message with a corresponding information.

- **Maximum number fax pages**
  Enter here the number of pages that each fax message to be sent must not exceed. The XPR server will not send fax messages with more pages.

- **Fax G3 ID**
  Enter here the fax number for fax G3 that is to appear on this tenant's fax messages to be sent.

- **Fax G4 ID**
  Enter here the fax number for fax G4 that is to appear on this tenant's fax messages to be sent.

- **Fax G3 header**
  If you wish to specify a header for the fax message, specify it here.

- **SMS quoata**
  Enter here the total number of SMS messages that the XPR server is to rout for the users of this tenant.
  When the total number of sent SMS messages reaches this threshold, the XPR user defined under **Contact person** is informed accordingly. You can set the precise number of messages that triggers this information via the defaulted value under **Alert threshold**.
  Once this quota has been reached, the XPR server does not send any further SMS messages for this tenant. In this case, a sending party receives an error message with a corresponding information.

- **SMS Number (*)**
  Specify here the mobile phone number to be used as originator address for the SMS message.

- **Trunk group**
  You can reserve an ISDN trunk group for a tenant's communication. For this purpose, enter here the class name for the relevant trunk group. The class name is a portion of an NVS address and arises in the following way: `NVS:NODE.CLASS/USER`

- **Range**
  This input field allows specifying the phone number range for the service access numbers of the voicemail scripts used. You can make the Entry in the format <*number*>-<*number*> as phone number range or as single phone number. If further fields need to be created for entering single phone numbers, click on ++. Three more fields are then added for making phone number entries. The following conventions apply for entering the phone number range:

  – The phone number ranges for tentants of the same site must not overlap.

  – Both values that form a phone number range must consist of the same number of digits and be specified in ascending order.

  If you make a mistake while specifying the phone number range, an error message will inform you when you attempt to save the data.

  Phone number definition for the voicemail script *PhoneMail*:

NOTE: Using these new, simplified voicemail configuration for the telephone user interface, which can be deployed with version V7R1, is only possible with the use of SIP connections.

In the following input fields you can specify the service access numbers for the single access types to use the voicemail script PhoneMail:

- PhoneMail Callback access
- PhoneMail Direct access
- PhoneMail Fax access
- PhoneMail Guest access
- PhoneMail Transfer access
- PhoneMail Universal access
- **NCO location**
  Selecting the NCO location for this tenant. You can select the location via the combo box from the specified NCO locations. If you do not make a specification here, the ***Default value*** pre-setting is used.
- **Language ID**
  Specify there the language ID (for example: 1031 for Germany, 1033 for the USA, etc.) to set the language to be used in the voicemail script.
- **File name of name recording**
  Specify here the name of the announcement file (example: *CompanyNo1.pcm*) to be played as welcome greeting for this tenant.

NOTE: This file must first have been created by the administrator and stored in the following directory:
`<drive>...\xpr\Userdata\vmdata`
When specifying the file name ensure correct spelling as the existance of this file will not be checked.

What can I do …

- *if the configured quotas do not show any effect in live operation?*
  - Activate the **Privilege check** option in the Exch APL of the relevant tenant.

2.4.2.4 Assigning Users to a Tenant

The users must now be assigned to the single tenants. The properties of the tenant definition are thus transferred to those users.

How to assign users to the single tenants via the **TENANT** database field:

1. Start the *Web Assistant*.
2. Log on to the system with administrative privileges.
3. Expand the **Server settings** link in the navigation area.
4. Switch with a click on the appropriate link in the navigation area to the **User administration** settings page.
5. Click in the **List of users** on the name of the user you wish to assign to a tenant.
   The user data mask is displayed.
6. Scroll to the **TENANT** entry.
7. Select the corresponding tenant from the combo box that associates this data field.
8. Click on **Save** at the bottom margin of the dialog.

Assigning a user to a selected tenant is thus complete.

2.4.2.5 Connecting the Tenant's Directory Service

A Directory Service can be connected to the XPR server via the LDAP APL for each tenant. From this directory all user data are replicated to the XPR user database.

NOTE: You find a detailed description of the LDAP APL settings in the LDAP chapter of the *Server Administration* manual.

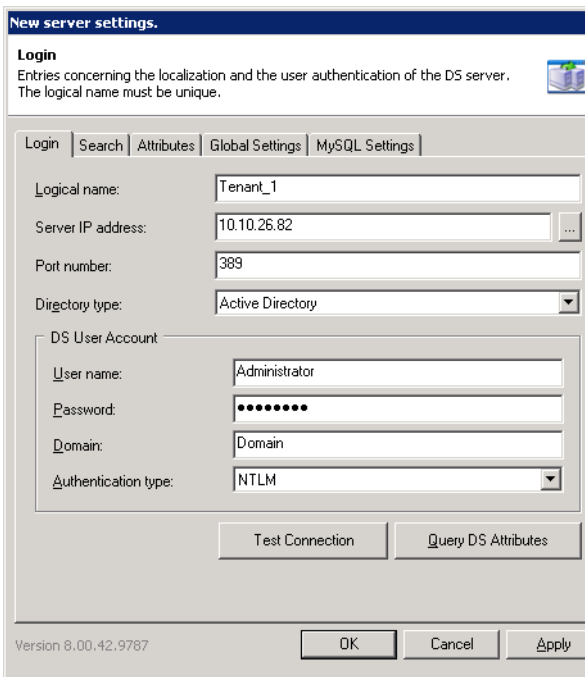
This is mandatory for configuring a multi-tenant solution with Exchange servers since the Exchange user data are maintained in the Active Directory. For the other multi-tenant solutions, using Directory Services is optional.

Connecting the tenant to the XPR server

Perform the following steps to connect the Active Directory of the new tenant to the XPR server:

1. In the XPR monitor open the LDAP APL settings via the menu option **Settings > LDAP APL > Set Options**. Select **Import** to connect a new Active Directory to the XPR server.
2. Select for the import the LDAP configuration file `ExRepl.lcf`, which you find in the `<XPR Install>\xpr\res\ldap` directory.

   The following dialog appears:



3. On the **Login** tab, enter values in the following fields.

   - **Logical name**
     Assign here a unique ID for connecting the new Active Directory. To improve clarity, we suggest using the ID of the associated tenant.
   - **Server IP address**
     Enter here the IP address of the server on which the Active Directory is found.
   - **Directory type**
     Select here the **Active Directory** option.
   - **User name**
     Enter here the name of the user ID to be used for accessing the Active Directory to be connected.
   - **Password**
     Enter here the password that associates the above user ID.
   - **Domain**
     Enter here the name of the domain in which the Active Directory to be connected is found.
   - **Authentication type**
     Enter here the type of authentication you want to use for accessing the Active Directory.

4. Select **Test Connection** to test the directory connection.

What can I do …

- *if the connection test fails?*
  - Check the network connection between kernel and LDAP server.
  - Verify that the data for accessing the Active Directory are correct.

Adjusting the LDAP synchronization setting

A basis script `ExRepl.Icf` is used for replicating the user data from the Active Directory of a tenant domain. In this basis script the attributes required for configuring users in a default Exchange environment are defined. In a tenant scenario, the basis script replicates the **GROUP** attribute along with the user data, which poses a security problem.

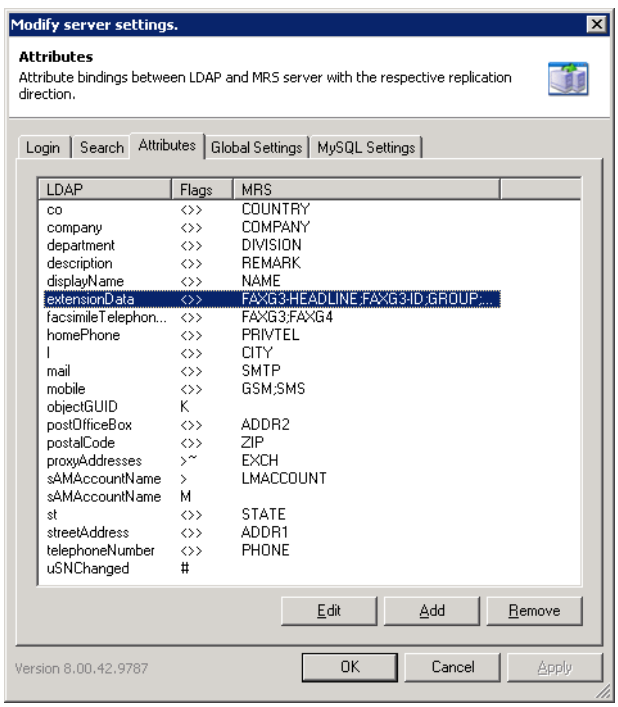
Replication of the LDAP attribute **GROUP** must therefore be undone. Otherwise, every user who may administer the Active Directory(ies) can change the **GROUP** attribute. For example, assigning the ***SUPERVISOR*** privilege to the **GROUP** attribute would allow all group members to take control of the XPR server.

NOTE: In special cases, the XPR administrator can still configure the **GROUP** attributes via the *Web Assistant*.

Replication of the LDAP attribute **GROUP** must therefore be undone. How to proceed:

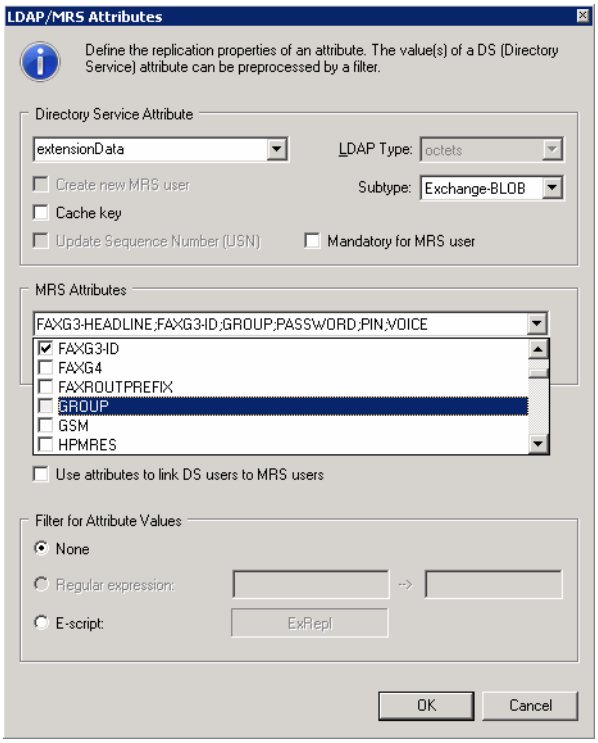
1. Switch to the **Attributes** tab in the **Change server settings** dialog.

   The following dialog appears:



2. Select the **extensionData** entry in the list of LDAP attributes (see figure above).

3. Click on the **Edit** button.
   The **LDAP/ MRS Attributes** dialog opens.



You can now see all attributes of the directory attribute **extensionData** in the **MRS Attributes** combo box.

4. Move to the **GROUP** data field in the window for **MRS Attributes**.
5. Untick the **GROUP** entry.

NOTE: In the above figure the tick has already been removed.

---

6. Click on **OK** to apply the setting. You return to the **Attributes** tab.

Assigning the active directory to the new tenant

After you have connected the Active Directory of the new tenant to the kernel, it must be assigned to the corresponding tenant.

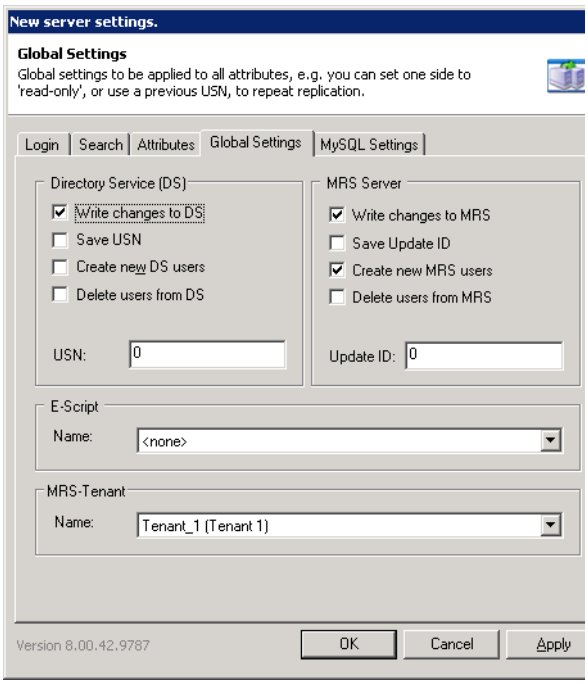
Perform the following steps to connect the newly configured Active Directory to the new tenant:

NOTE: You find a detailed description of the LDAP APL settings in the LDAP chapter of the *Server Administration* manual.

---

1. In the **New server settings** dialog switch to the **Global Settings** tab.

   The following dialog appears:



2. In the **MRS-Tenant: Name** field select the newly created tenant. In our example *Tenant 1*.

What can I do …

- *if the* **MRS-Tenant: Name** *field is shaded gray?*
  - Check whether the license for using this feature is available. Section 2.3.3.3, “Activating the Multi-Tenant Feature”, on page 42.

- *if the* **MRS-Tenant: Name** *field does not display the desired tenant?*
  - Create the desired tenant. Cf. Section 2.4.2.2, “Adding Tenants in the XPR Server”, on page 45.

3. Click on **OK** to activate your LDAP settings. You return to the **LDAP Server** dialog.
4. In there click on **OK** to complete the LDAP configuration.

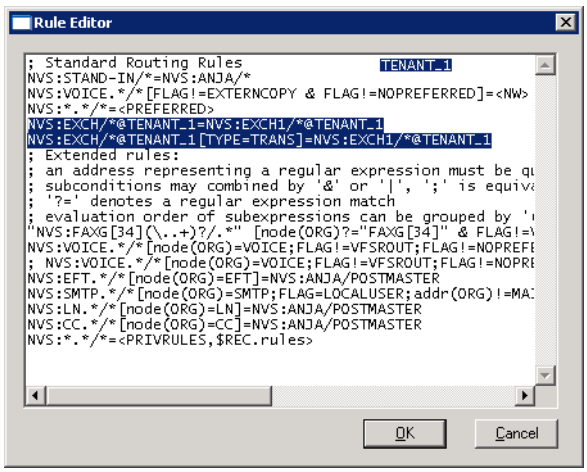
2.4.2.6 Configuring Multiline for the Exchange Tenants

So that you can use a multi-tenant solution in an Exchange environment, the **Multiline** feature must be activated on the gateway satellite.

How to activate **Multiline** is described in detail in the *XPR Microsoft Exchange Gateway* manual, chapter *Multiline Configuration for independent Exchange Servers*.

Verify that the routing rule entries for the Exch Apl as well as for the ExUM Apl are correct.

Example:



2.4.2.7 Tenant Administration

You can configure at least one special user per tenant. This user can perform some important administrative tasks for this tenant.

To this, the following requirements must be complied with:

- The user must be member of the corresponding tenant.
- The user must be member of the **TENANTSUPER** user group.

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

The additional privileges of the **TENANTSUPER** user group have the following meaning:

- Tenant Supervisor Privilege (SYS_TENANTSUPER)

  This privilege allows the user:

  – to see and edit all database fields flagged with **PSERV**.

  – to access the configuration pages **Server settings > User administration** in the *Web Assistant*.
  Having this privilege, the user can click on **Execute** for accessing the actions of the user administration and create new users or change user data.

  > ***NOTE:*** The **Create new user group** feature is not available to this user.

- Global Distribution List Editor (SYS_REDIT)

  This privilege allows the user:

  – to create, change or delete global broadcast groups (global groups).

  > ***NOTE:*** Via the *Web Assistant* on the configuration page **Personal settings > Groups**.

- Global Alias Editor (SYS_SEDIT)

  This privilege allows the user:

– to create, change or delete global contact information.

NOTE: Via the *Web Assistant* on the configuration page **Address book > Public**.

Creating an administrative tenant user

How to create a new user with administrative privileges for managing tenants:

1. Start the *Web Assistant*.
2. Log on under an XPR server user account that has administrative privileges.
3. Open the configuration page **Server settings > User administration**.
4. Create the new user in the *Web Assistant*.
   Action to select: **Create new user > Execute**.
5. In the **Create new user** dialog, enter the **User ID** and the **Voice mailbox number**.
6. Save these entries with a click on the Create button.
   The new user is created and the data record of this user opens, so that you can make further specifications.
7. Add this user to the **TENANTSUPER** user group via the user data mask.
8. Assign this user to the desired tenant via the **Tenant** database field on the user data mask.
9. After you have accomplished editing the user data record, save the settings with the **Save** button. An indication dialog appears to confirm the storing.

NOTE: The **Back** button takes you to the start page of the user administration. The specified user data is then dismissed.

10. Click on **Continue**. The new user data record is displayed in the List of users.

Creating a tenant-specific user who has administrative privileges is now complete.

2.4.3 Public Address Books for Tenants

The OpenScape Xpressions administrator can configure public address books separately for each tenant. Such address books are exclusively available for the users of the single tenants. The public address books of tenant A can thus only be seen and used for addressing by tenant A users.

NOTE: A user who belongs to the TENANTSUPER group can also create and administer address books. See Section 2.4.2.7, “Tenant Administration”, on page 60.

The public address books are defined with configuring groups, which are then assigned to the corresponding tenants.

2.4.3.1 Configuring the public Address Books

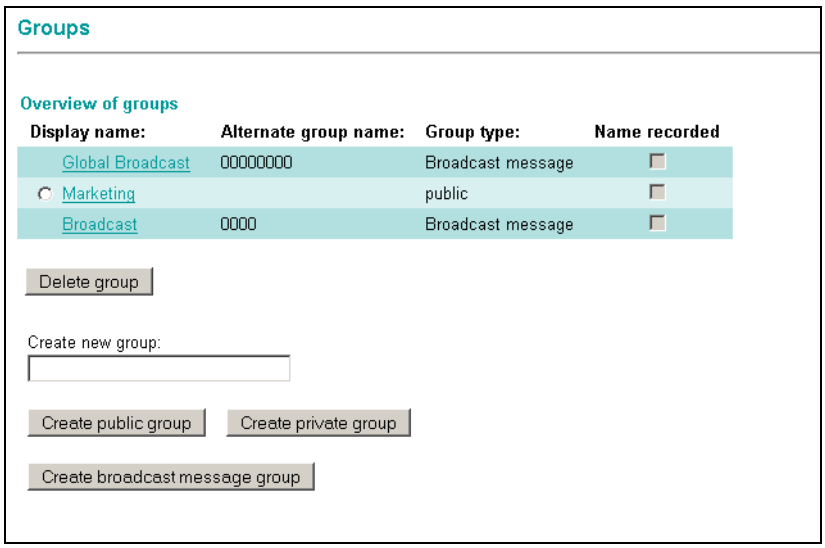
Public and private address books are realized by group definition. The OpenScape Xpressions administrator creates and administers such groups with the *Web Assistant*.

NOTE: Public groups are available to all users of the XPR system if they are not assigned to a tenant.

How to configure public address books:

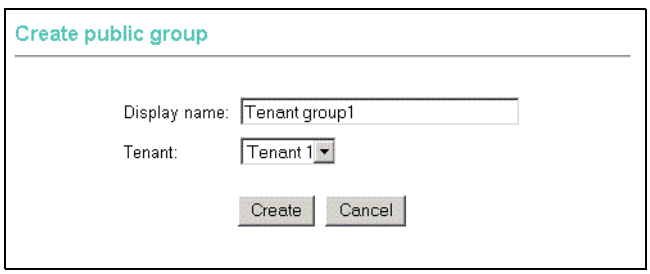
1. Start the *Web Assistant* and log on to the XPR server under a user account that has administrative privileges.
2. Open the menu option **Personal settings > Groups**.

   The following page is displayed:



Creating a group

1. Enter the desired group name in the **Create new group** field.
2. Click on the **Create public group** button to create a global group. The **Create public group** dialog opens.



3. You can perform the following settings in this dialog:

   Display name
   In this input field you can edit the displayed group name.

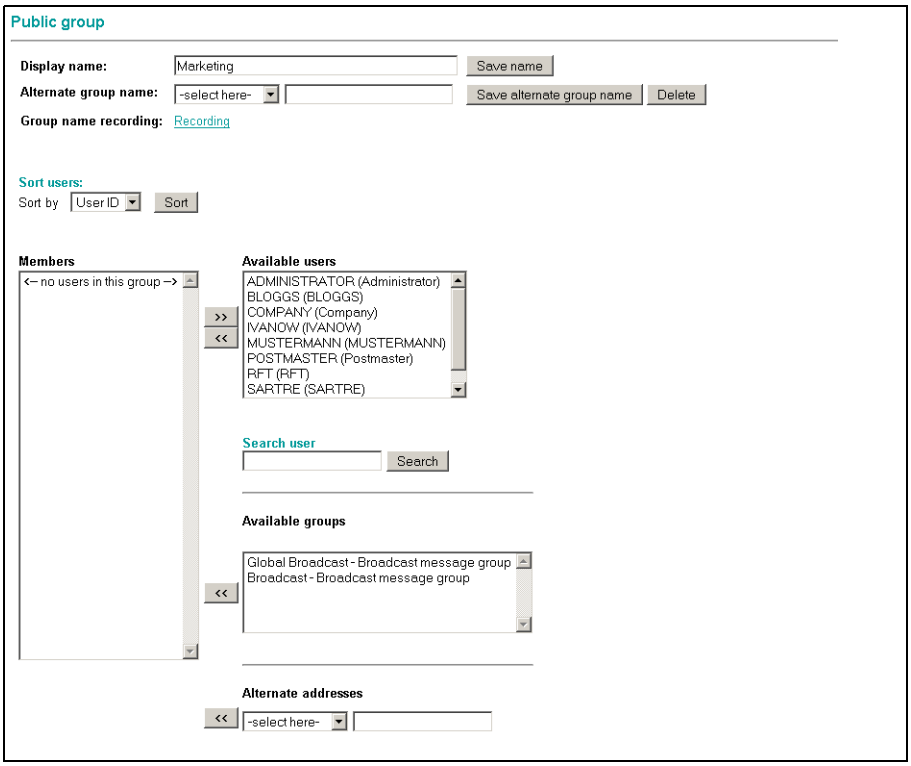
   Tenant
   In case of a tenant solution this input field lets you assign the created group to a specific tenant. Only the users of this tenant can see the group then.

   Click on the Create button to complete the process. The group type (public) is displayed in the **Group type** column.

4. The newly created group is still empty. You can now create more, not precisely defined groups or edit the new group, i. e. define group members and further details.

Editing a group

1. Click on the **Display name** of the group the definition of which you want to edit. A new page opens.



2. Enter a name for the group in the **Display name** field if required. You can use special characters. Then click on the **Save name** button.

3. Select a message type from the **list field** under **Alternate group name** and enter a group address.

   At this point you can decide whether you want an internet mail address (e.g. distributionlist@company.com) or a so-called NVS address (e.g. `NVS:VOICE/12345`) as **group address**. An NVS address is always composed of the prefix *NVS:* followed by the service to be used (VOICE, FAXG3, etc.) and a phone number or address. For example, if you wish to enable message transmission to the group via the telephone user interface (TUI), you need to enter the address `NVS:VOICE/<phone number>`. Then click on the **Save alternate group name** button.

4. Next to **Group name recording** you find the **Recording** link for recording a name greeting for the selected group.

Integrating users in the group

The **Available users** list shows all users registered in the system. The **Available groups** list shows all groups already created.

You can select single persons as well as groups already defined as members for a group. If a person is integrated in the member list several times, he/she is considered still only once when messages are distributed.

The lists offer a maximum of 50 entries for selection at the same time.

1. If required, select a different list sorting in the **Sort by** combo box and click on the **Sort** button to update the sorting.

   NOTE: The set sorting criterion (**User ID** or **Name**) affect searching for users in step 4. If you set the **User ID** sorting criterion but look for a user name in step 4, no entries will be found.

2. Click on the **Show next users** button to display further list entries.
3. Click on the **Back to beginning** to reload the first 50 entries.
4. If you look for a specific user name or user ID, enter the name/ID in the **Search user** field and click on the **Search** button. In doing so please note the sorting criterion set in step 1.

   NOTE: When looking for user names please heed case sensitivity.

5. Click in the **Available users** list on a user to select him/her for the group.
6. Click on the **<<** button to integrate the selected user in the group.
7. Integrate further users or groups in the same way.
8. If required, select under **Alternate addresses** further external addresses for the group (e.g. e-mail addresses) and click on the **<<** button to integrate them in the group.
9. Click on the **Back button** to return to the **Groups** page.

Removing users from the group

You can remove users from the group anytime.

1. Click on an entry in the **Members** list.
2. Keep the **[Ctrl]** key pressed for selecting several entries.
3. Click on the **>>** button to remove the selected entries from the list.

Deleting groups

You can delete a group anytime.

1. Click on the **radio button** that precedes the desired group.
2. Click on the **Delete group** button. A security prompt is displayed.

3. Confirm the **security prompt**. The selected group is deleted.

2.5 Separate Caller Guide Support for Tenants

The Caller Guide is a routing wizard preferably operated by voice input. Using the Caller Guide you can search the XPR database for contacts and have a phone connection immediately set up to the found XPR user.

You can use the Caller Guide in a multi-tenant solution specific to a tenant. In other words, if a user assigned to a specific tenant invokes the Caller Guide as voice-controlled routing wizard, only users of his/her own tenant are announced to him/her as search hits.

If you wish to use the Caller Guide in a multi-tenant solution, please note the following requirements:

- A Caller Guide entity with its own access number must be configured for each tenant on the XPR server. That means, an individual Caller Guide script must be made available to each tenant.
- Each Caller Guide entity must be assigned to a tenant.

2.5.1 Installing and Configuring the Caller Guide Entities

How to install the Caller Guide:

1. Install the Caller Guide with the ASR machine of your choice (ASR = Automatic Speech Recognition)
2. Add the Caller Guide script to the list of installed protocols.
3. Give the protocol an expressive name.
4. Repeat the installation for as many scripts as you need for assignment to the tenants.

NOTE: You find detailed information about setting up and configuring the Caller Guide on the XPR server in chapter "*Protocols of the XPR Server*" of the "*OpenScape Xpressions Server Administration*" manual.

2.5.2 Assigning Caller Guide Entities to Tenants

The Caller Guide script operates as protocol in the context of a Telematic APL. Consequently, you reach the Caller Guide configuration dialogs only via the settings dialog of the Telematic APL used in the XPR monitor.

How to assign a Caller Guide entity to a tenant:

1. Start the XPR monitor and open in the components window the settings pages of the telematic APL used.
2. Select the Caller Guide script and click on the **Script parameter** icon in the toolbar to open the configuration pages of the Caller Guide script. The configuration of the Caller Guide script is divided in the tabs *General*, *Options*, *Name Dialing* and *Customer*.
3. Switch to the *Customer* tab. On this tab you can perform special settings using a command-line utility.
4. Enter the following command in the input field:
   tenant=<*tenant ID of the first tenant*>
5. Click on **OK** to complete the configuration for this Caller Guide script. Assigning this Caller Guide script to the selected tenant in now complete.
6. Repeat this process for the Caller Guide scripts you wish to assign to the other tenants.

Index

R

T

U

W

X