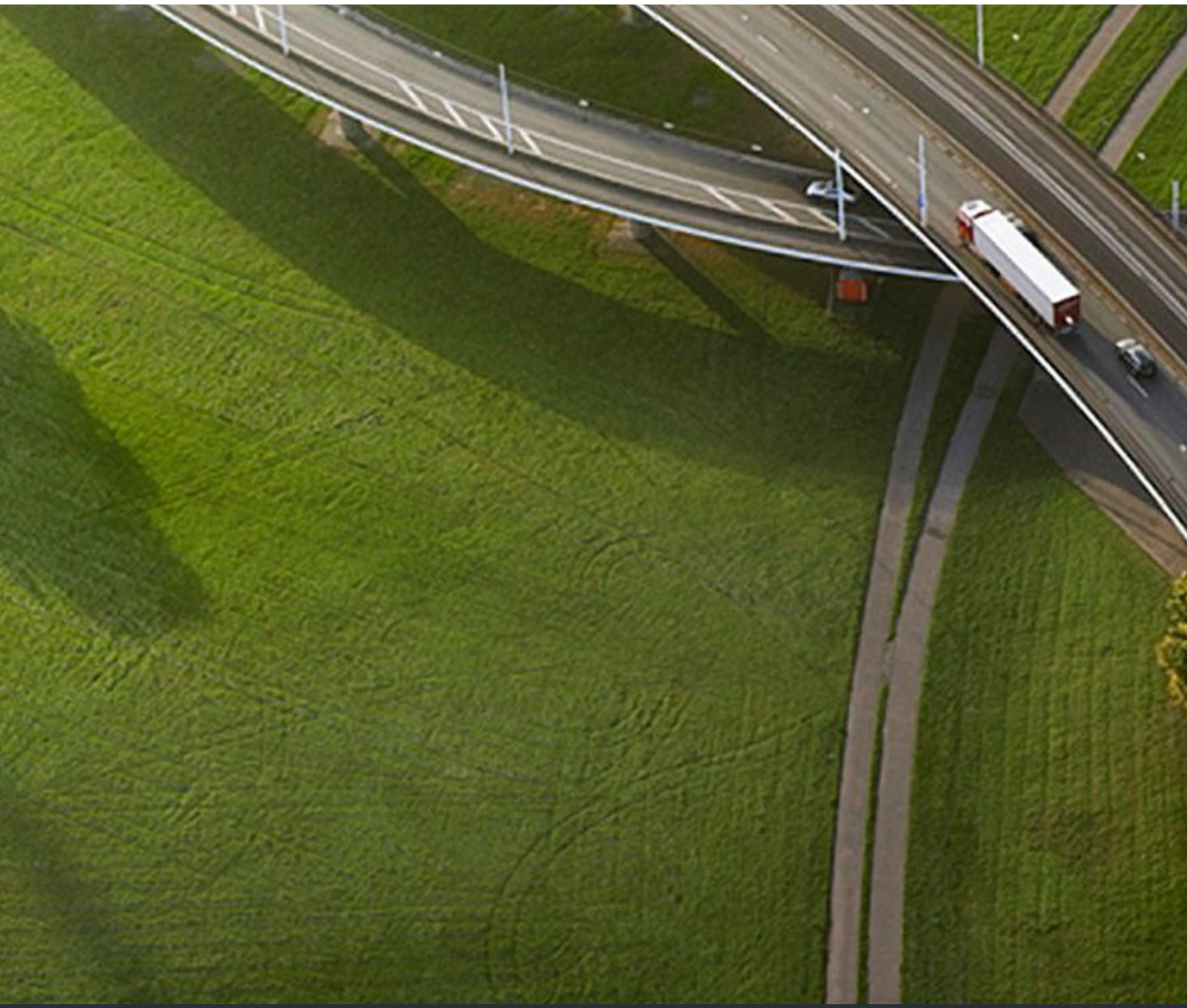
UNIFY Harmonize your enterprise



OpenScape Business V2

Feature Description

A31003-P3020-F100-07-7618

Provide feedback to further optimize this document to edoku@unify.com.

As reseller please address further presales related questions to the responsible presales organization at Unify or at your distributor. For specific technical inquiries you may use the support knowledgebase, raise - if a software support contract is in place - a ticket via our partner portal or contact your distributor.

Our Quality and Environmental Management Systems are implemented according to the requirements of the ISO9001 and ISO14001 standards and are certified by an external certification company.

Reference No.: A31003-P3020-F100-07-7618

unify.com

Contents

1 Introduction and Important Notes

This introduction provides you with an overview of the documentation structure. The introduction should assist you in finding information on selected topics faster.

1.1 About this Documentation

This documentation describes the features of the hardware platforms OpenScape Business X1, OpenScape Business X3, OpenScape Business X5 and OpenScape Business X8 as well as the Softswitch OpenScape Business S. The UC Suite functionality is provided through the optional UC Booster Card or the UC Booster Server. With OpenScape Business S, the UC Suite is integrated.

INFO: The hardware platforms OpenScape Business X1/X3/X5/X8 (or OpenScape Business X for short) and the Softswitch OpenScape Business S are referred to in this documentation as communication systems.

UC Suite designates the advanced unified communications functions, including the Multimedia Contact Center.

The information in this document contains general descriptions of the technical possibilities, which may not always be available in individual cases. The desired features must be contractually specified for each case.

If a function is not available as described here, this may be due to the following reasons:

- The communication system does not have this feature.
- The required license is not available or activated.

1.1.1 Documentation and Target Groups

The documentation for OpenScape Business is intended for various target groups.

Sales and Project Planning

The following documentation is intended for sales and project planning.

- Feature Description
  This documentation describes all the features. This document is an extract from the Administrator Documentation.

Installation and Service

The following documentation is intended for service technicians.

- OpenScape Business X1, Installation Guide
  This document describes the installation of the hardware and the initial installation of OpenScape Business X1.
- OpenScape Business X3/X5/X8, Installation Guide
  This document describes the installation of the hardware and the initial installation of OpenScape Business X3/X5/X8.
- OpenScape Business S, Installation Guide
  This documentation describes the initial installation of the OpenScape Business S softswitch.
- OpenScape Business X1, Service Documentation
  This documentation describes the hardware of OpenScape Business X1.
- OpenScape Business X3/X5/X8, Service Documentation
  This documentation describes the hardware of OpenScape Business X3/X5/X8.

Administration

The following documentation is intended for administrators.

- Administrator Documentation
  This documentation describes the configuration of features that are set up using the OpenScape Business Assistant (WBM). The Administrator documentation is available in the system as online help.
- Configuration for Customer Administrators, Administrator Documentation
  This documentation describes the configuration of features that can be set up using the OpenScape Business Assistant (WBM) with the **Basic** administrator profile.
- Manager E, Administrator Documentation
  This documentation describes the configuration of features that are set up using Manager E.

UC Clients / Telephone User Interfaces (TUI)

The following documentation is intended for UC users.

- myPortal Smart, User Guide
  This documentation describes the configuration and operation of the UC client myPortal Smart.
- myPortal for OpenStage, User Guide
  This documentation describes the configuration and operation of myPortal for OpenStage.
- myPortal for Desktop, User Guide
  This documentation describes the installation, configuration and operation of the UC client myPortal for Desktop.
- myPortal for Outlook, User Guide
  This documentation describes the installation, configuration and operation of the UC client myPortal for Outlook.
- Fax Printer, User Guide
  This documentation describes the installation, configuration and operation of Fax Printer.

- myPortal to go User Guide
  This documentation describes the configuration and operation of the mobile UC client myPortal to go for smartphones and tablet PCs.
- myAgent, User Guide
  This documentation describes the installation, configuration and operation of the Contact Center client myAgent.
- myReports, User Guide
  This documentation describes the installation, configuration and operation of the Contact Center client myReports.
- myAttendant, User Guide
  This documentation describes the installation, configuration and operation of the attendant console myAttendant.
- OpenScape Business Attendant, User Guide
  This documentation describes the installation, configuration and operation of the attendant console OpenScape Business Attendant.
- UC Smart Telephone User Interface (TUI), Quick Reference Guide
  This documentation describes the voicemail phone menu of the UC solution UC Smart.
- UC Suite Telephone User Interface (TUI), Quick Reference Guide
  This documentation describes the voicemail phone menu of the UC solution UC Suite.

1.1.2 Structure of the Feature Description Manual

This section shows you how the content of the Feature Description is structured. The hardware is described in the Service Documentation.

Section	Contents
Introduction and Important Notes	Overview of the structure of this documentation and important information/safety information to be observed during installation and operation
System overview	Overview of the communication system for a quick start
Administration Concept	Overview of administration programs and user roles in WBM
Licensing	Licensing procedures and licenses
Integration into the Data Network (LAN)	LAN/WAN interface, name resolution, data routing, DLI and DLS
Connecting to Service Providers	Internet access, IP telephony, trunk access
Station	Dial plan, IP stations, UP0 stations; DECT stations, ISDN and analog stations, virtual stations, users of UC clients, user profiles

Section	Contents
UC Smart	Clients and functions of the unified communications solution UC Smart, including Smart Voicemail. Presence status, directories and journal, conferences, team functions, voicemails
UC Suite	Clients and functions of the UC Suite unified communications solution: Presence status and CallMe, directories and journal, conferences and web collaboration, voice and fax messages, instant messaging
Functions at the Telephone	Make calls, call signaling, calling line ID, functions during the call, optimizing communication
Working in a Team (Groups)	Call pickup group, group call, hunt group, team/top, MULAP, UCD
Call Routing	Classes of service, toll restriction, tenant system, LCR, emergency calls
Attendants	AutoAttendants, OpenStage Attendant, PC-based attendants, intercept position
Multimedia Contact Center	Clients and functions of the Contact Center: agents, queues and schedules, VIP service, fallback, reports
Mobility	myPortal for Mobile, Mobility Entry, One Number Service, dual-mode telephony, IP mobility, Cordless/DECT
Security	Firewall, SPE, VPN, certificates, Samba share
Networking	Network plan, networking scenarios, central intercept position, survivability
Auxiliary Equipment	Announcement devices, fax devices and fax servers, entrance telephone and door opener, actuators and sensors, OpenStage Gate View
Application Connectivity	CSTA, TAPI, XMPP, Application Launcher
Accounting	Call detail recording, call charges and call duration, cost control
Maintenance	Backup and restore, update, restart, reload, shutdown, factory reset, inventory, actions, remote services
Configuration Limits and Capacities	Maximum values for the configuration limits and capacities of the different communication systems
Appendix	List of supported standards, the Euro-ISDN features and the IP protocols and port numbers used
Glossary	Brief descriptions of commonly used terms

1.1.3 Display Conventions

This documentation uses a variety of methods to present different types of information.

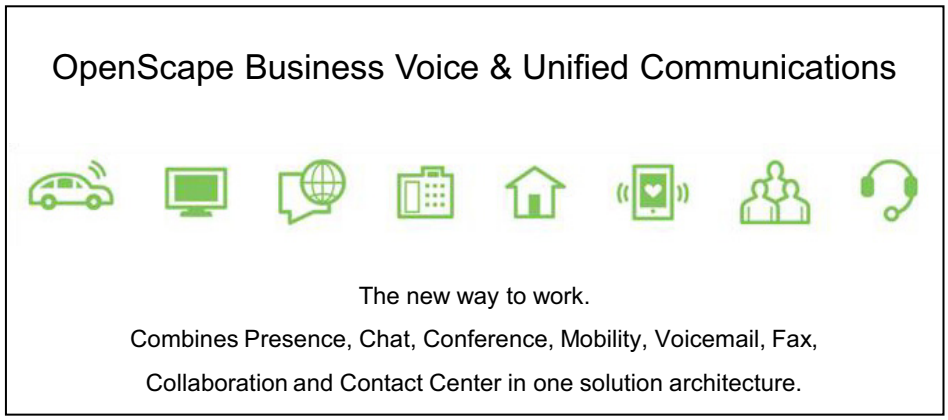
Type of information	Appearance	Example
User Interface Elements	Bold	Click on **OK**.
Menu sequence	>	**File > Exit**
Special emphasis	Bold	**Do not delete** Name.
Cross-reference text	Italics	You will find more information in the topic*Network*.
Output	Monospace font, e.g., Courier	`Command not found.`
Input	Monospace font, e.g., Courier	Enter `LOCAL` as the file name.
Key combination	Monospace font, e.g., Courier	`<Ctrl>+<Alt>+<Esc>`

2 System Overview

OpenScape Business offers small and medium-sized businesses the answer to their individual and diverse communication needs in a unified, flexible and scalable solution. The OpenScape Business solution architecture can be deployed independently of the existing telephony infrastructure, regardless of whether traditional telephony, IP or DECT is involved. From powerful telephony to a comprehensive Unified Communications (UC) solution, OpenScape Business always provides the right solution.

Flexible, scalable and powerful

OpenScape Business combines the best of HiPath 3000 and OpenScape Office in a new solution platform.



2.1 Highlights

OpenScape Business is the all-in-one solution for small and medium-sized enterprises and offers the following highlights.

Highlights

- Integrated voice services, presence management (presence status), drag and drop conferencing, visual voicemail (voicemail box), AutoAttendant, Multimedia Contact Center, IM (Instant Messaging), Mobility, directory access with database connection, fax, integration into business processes, and much more
- UC clients individually customized for the workplace and way of working
- Interface integration of OpenScape Web Collaboration
- The perfect solution for customers with one location or network-wide solution with multiple locations
- OpenScape Business offers a unified business solution architecture.
- Depending on the existing infrastructure, different OpenScape Business models are available for various configuration sizes. Alternatively, it is

possible to run the OpenScape Business software on a standard server (Softswitch) - also in fully virtualized environments, of course.

- The UC solution UC Smart is already provided on the mainboard. The additive UC solution UC Suite supports a larger number of UC users and offers an expanded scope of UC features. A UC Booster Card or a UC Booster Server is required for this.
- All communication interfaces are already available for diverse and heterogeneous requirements: IP, digital, analog and DECT, as well as all common trunk interfaces for voice communication

2.2 Unified Communications

Unified Communications (UC) is a technology that improves communication in enterprises by integrating various communication media in a unified application environment. Unified Communications simplify business processes in enterprises through an integrated presence management (e.g., calls are routed automatically to the mobile phone when the user is out of the office). Several other features such as dial-in conferencing, personal voicemail (voicemail box), personal fax box, Instant Messaging (IM), use of the mobile phone as an extension of the communication system, Contact Center, video and web collaboration, etc., are also combined in this unified solution.

With the flexible unified communications approach of OpenScape Business, a number of different UC solutions are offered, depending on the requirements at the workplace and the existing infrastructure. For the UC solution, you can choose between UC Smart and UC Suite (both cannot be used simultaneously).

The UC Smart solution already integrated in OpenScape Business can be migrated to the advanced UC Suite solution at any time via an upgrade license. Depending on the number of UC subscribers, OpenScape Business must then only be expanded with the internal board "UC Booster Card" or the external Linux server "UC Booster Server". As a pure softswitch, OpenScape Business S is available as a server solution with the optional UC Smart or UC Suite.

2.2.1 UC Features (Overview)

Depending on the selected UC solution (UC Smart or UC Suite) different UC functions are available to you.

The following tables are intended to help you choose the best UC solution for your requirements. Detailed functional constraints can be found in the relevant sections (UC Smart, UC Suite, Attendants) of the Feature Description and Administrator Documentation.

UC feature	UC Smart		UC Suite		Notes
	myPortal Smart	**myPortal to go**	**myPortal for Desktop/ Outlook**	**myPortal to go**	
Presence Status					
Presence status (presence management)	x	x	x	x	
Change presence status via the Client	x	x	x	x	
Change presence status via the TUI	-	-	x	-	
Status-based call forwarding	x	x	x	Via destinations defined in myPortal	With UC Smart, any number can be selected as the destination. With UC Suite, only a number from the preselection can be selected.
Status display in favorites	x	x	x	x	
Status display in directories	x	x	x	x	
Status display in the Journal	-	-	x	-	
Enable CallMe service	-	-	x	x	
Calendar integration (Outlook)	-	-	x	-	
Calendar integration (iCal) (only with myPortal for Desktop)	-	-	x	-	
Favorites					
Display call status	x	x	x	x	
Create groups	x	x	x	-	
Compact display of favorites	x	-	x	-	
Directories					
Personal directory	x	x	x	x	
Internal directory	x	x	x	x	
External directory	-	-	x	x	
Search in directories	x	x	x	x	In myPortal Smart, also a quick search
Access to speed-dial destinations defined in the system (SSD)	x	x	-	x	
Import / Manage personal contacts (CSV / XML)	x	-	x	-	
Access to Outlook Contacts	x	-	x	-	
Import of personal contacts (Mac OS) (myPortal for Desktop)	-	-	x	-	
Integration of external directory server via LDAP	-	-	x	-	

UC feature	UC Smart		UC Suite		Notes
	myPortal Smart	myPortal to go	myPortal for Desktop/ Outlook	myPortal to go	
Journal					
All calls	x	x	x	x	
Open calls	-	-	x	-	
Missed calls	x	x	x	x	
Answered calls	x	x	x	x	
Scheduled calls	-	-	x	-	
Voicemail	-	x	x	x	
Fax journal	-	-	x	-	
Calls					
Manual dialing	x	x	x	x	
Desktop dialer (click to call)	x	-	x	-	
Forwarding	x	x	x	x	
Place call on hold	x	x	x	x	
Record calls (voice recording)	-	-	x	-	
Send email	x	x	x	x	
Send SMS	-	x	-	x	
Start chat	x	-	x	-	
Popups	x	-	x	-	
Conferences					
AdHoc conference	x	x	x	x	
Scheduled conferences	-	-	x	-	
Permanent and open conferences (drag & drop conference)	x	-	x	-	
Web collaboration integration	x	-	x		
Voice and fax messages					
Voicemail box (visual voicemail)	x	x	x	x	Voicemail functionality for subscribers (IP, TDM)
Playback through phone	x	x	x	x	
Playback through PC sound card	-	-	x	-	
How to Send a Voice Message as an Email	x	x	x	-	
Fax	-	-	x	-	
Instant messaging					
Instant messaging (chat)	x	-	x	-	

1 myPortal to go also allows access to the local smartphone contacts.

Contact Center

UC feature	UC Smart	UC Suite		Notes
		myAgent	**myReports**	
Agents, queues and schedules	-	x	-	
Fax and email	-	x	-	
Predefined reports/report templates	-	x	x	
Scheduled creation of reports	-	-	x	

Optionally, the connection of OpenScape Contact Center is possible.

Attendants (Attendant Consoles)

UC feature	UC Smart	UC Suite	Notes
	Business Attendant	**myAttendant**	
Display of waiting calls with call type, name and phone	x	x	
Display connection status	x	x	
Fast switching of calls	x	x	
Speed-dialing via BLFs and user buttons. Individual configuration of the busy lamp fields and user buttons with call number or name	x	x	
View presence status of other subscribers	x	x	With OpenStage Business Attendant, presence requires the UC Booster Card/Server or Business S
Change presence status of other subscribers	x	x	
Personal directory	-	x	
Internal directory	x	x	
External directory	x	x	
Outlook Contacts	x	x	
LDAP access	x	x	
Journal	-	x	
AdHoc conference	x	x	
Scheduled, permanent and open conferences (drag & drop conference)	-	x	

UC feature	UC Smart	UC Suite	Notes
	Business Attendant	**myAttendant**	
Message Center	-	x	All voicemails, faxes, instant messages as well as SMS messages and emails are recorded and managed via the Message Center
Access to voicemail and fax messages of other subscribers	-	x	Must be released by each respective subscriber
Instant messaging (chat)	-	x	
Night service	x	x	

The recommended Attendant client for UC Suite is myAttendant. However, OpenScape Business Attendant can also be used with UC Suite.

Voicemail & Company AutoAttendant

UC feature	UC Smart	UC Suite	Note
Basic functionality of UC Smart Voicemail & Company AutoAttendant	x	-	
Basic functionality of UC Suite Voicemail & Company AutoAttendant	-	x	Requires UC Booster Card/ Server or Business S
UC Features			
Graphical operation of voicemail for subscribers (web interface or client interface)	x	x	
Voicemail prompts for presence function	x	x	Different announcements, depending on the set UC presence
Personal rules for greetings per mailbox	-	x	The subscriber defines detailed rules for the selection of his or her personal greetings
Voicemail to Email	x	x	Voicemail is attached to email as a wave file
AutoAttendant functions			
Attendant mailboxes (Basic AutoAttendants)	100	20	
Company AutoAttendant	x	x	Central attendant console and centralized voicemail with alternative greetings for each extension
Announcement prior to answer / Parallel signaling	x	x	Announcement to the caller while the subscriber is being called For UC Suite, this is only possible in conjunction with the Contact Center

UC feature	UC Smart	UC Suite	Note
Dial-in destinations for 4 day sections / Calendar for AutoAttendant	x	x	Variable automated Attendant for different times of the day Calendar function possibly with UC Smart via the automatic night service
Central calendar for mailbox	x	x	Announcements and call handling for company-wide events such as holidays, company holidays, etc.
Custom profiles for mailbox and personal AutoAttendant	-	x	Presence-based call handling that can be individually set per subscriber
Schedules	Day and Night service	Schedule with rules (Call Control Vector, CCV)	
Templates	1 AutoAttendant configured by default	5 customizable templates	
Graphical rule editor (CCV editor)	-	x	
Concatenation of mailboxes / Multi-step AutoAttendant	x	-	The call is forwarded from one concatenated mailbox to the next, and each time the respective announcement is played
Dial by Name	-	x	
Dial by Extension	x	x	
Voicemail features			
Personalized greetings per mailbox	4	10	Save and set various announcements
Forwarding of voice messages	-	x	Forward message to another subscriber/mailboxes
Callback from the voicemail box	x	x	Callback to the caller of the message can be activated
Notification call	-	x	When a message arrives, a call is made to an external destination, e.g., a mobile phone
Representative function	-	x	Forward caller to representative with personal announcement
Caller-based voicemail / CLI routing	-	x	Call number-based handling, e.g., a greeting in the language of the caller
Central group mailbox	x	x	With announcements for departments / groups

UC feature	UC Smart	UC Suite	Note
Live Recording	-	x	Recording of conversations with security functions
Save messages	-	x	Subscribers can save individual voicemail messages for themselves
Automatic deletion of messages	x	x	After a retention period, messages are deleted to free storage space
Switch voicemail box language on subscriber-specific basis	-	x	Selection of automatic announcements in individual language

2.2.2 User Access to UC Features (UC Clients)

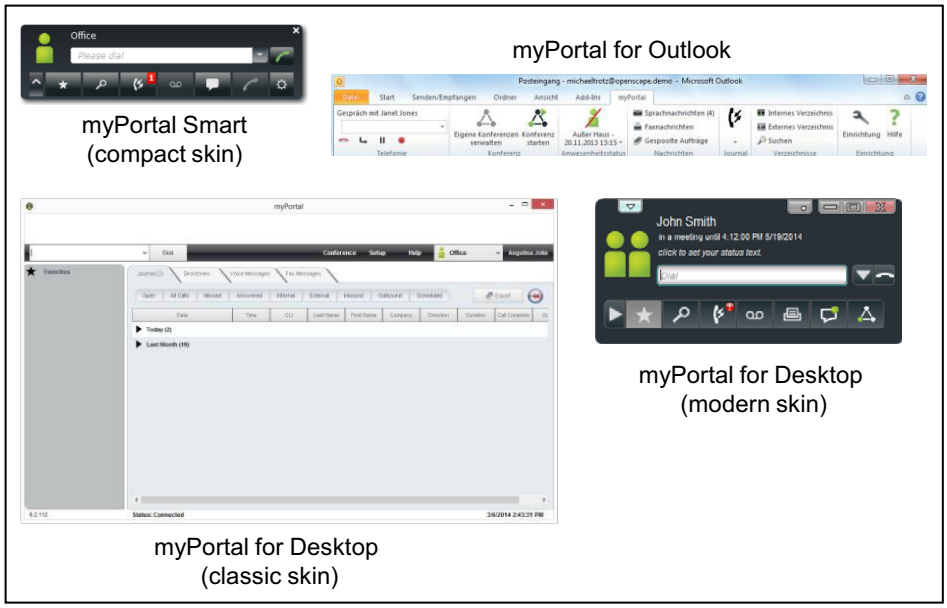
Access to the UC features occurs via UC clients. The presence status (UC Suite) and voicemail (UC Smart and UC Suite) can also be accessed through the telephone user interface (TUI).

UC clients are offered for the major operating systems. Please also note the requirements of the clients in the respective release notes.

Communication Clients (Desktop and Groupware Clients)

Client	Recommended for		Description
	UC Smart	UC Suite	
myPortal Smart	x	-	UC Desktop Client for Microsoft Windows and Apple Mac
myPortal for Desktop	-	x	Advanced UC Desktop Client for Microsoft Windows and Apple Mac
myPortal for Outlook	-	x	UC Groupware Client for Microsoft Outlook Integration
myPortal for OpenStage	x	x	Presence and voicemail control for UC Suite Presence control for UC Smart For OpenStage 60 HFA and OpenScape Desk Phone IP 55G HFA telephones
OpenScape Desk Phone CP 400/600 HFA(integrated Client to phone software)	x	x	Presence control and phonebook access for UC Suite and UC Smart

Figure: myPortal Smart, myPortal for Desktop and myPortal for Outlook



Mobility Clients

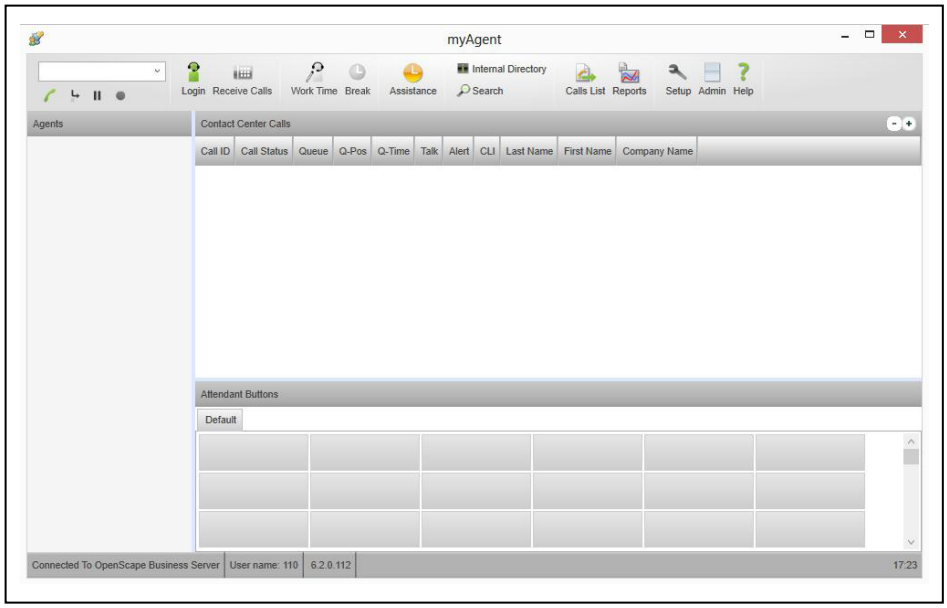
Client	Recommended for		Description
	UC Smart	UC Suite	
myPortal to go	x	x	Mobile app for smartphones and tablet PCs myPortal to go is available for UC Smart and UC Suite with slightly different features

Figure: myPortal to go

Contact Center Clients

Client	Recommended for		Description
	UC Smart	UC Suite	
myAgent	-	x	Contact Center Client
myReports	-	x	Reports/Reporting interface for Contact Center myReports can be also be used for system statistics independently of the Contact Center

Figure: myAgent

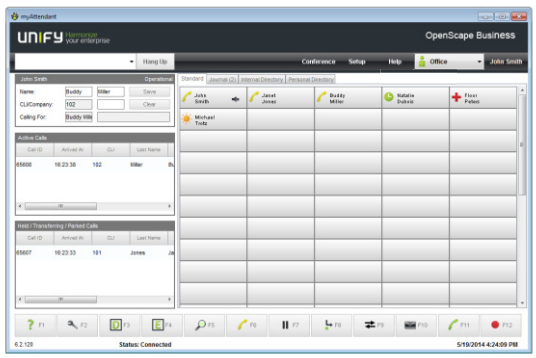


Attendants/Attendant Consoles

Client	Recommended for		Description
	UC Smart	UC Suite	
OpenScape Business Attendant	x	-	UC Attendant Console including presence
myAttendant	-	x	Advanced UC Attendant Console for UC Suite

Figure: myAttendant

Business Attendant



myAttendant

2.2.3 Integration in Business Applications

OpenScape Business can be integrated into existing IT infrastructures and business applications.

Applications

- Application Launcher for active interaction with CRM/ERP applications
- Accounting software for evaluating call charges

Integrated Services

- Directory services for information about callers and searching in internal and external directories
- Presence management and instant messaging (IM) to social media networks using XMPP
- Web services for interactions with web-based applications on mobile phones and tablet PCs, for example

CTI Middleware

- First and third-party TAPI Service Provider for call control from CTI and CRM/ERP applications

Interfaces and Protocols

- CSTA for monitoring and controlling different applications
- SIP for connecting to SIP trunking based applications
- LDAP for connecting to external directories or from external LDAP clients
- HTTP and HTTPS for accessing UC functions of the integrated web server
- TCP/IP as the basic protocol for all Ethernet connections
- SQL connector for connecting SQL databases (Microsoft SQL Server, PostgreSQL, Sybase SQL Server)
- LDAP connector for external LDAP servers such as Active Directory, for example

2.3 OpenScape Business Models

Different models are available for the use of telephony and UC functionality. You can choose between hardware models and pure software models that operate on standard servers or in a virtual environment with VMware vSphere.

The UC functionality for UC Smart is already integrated in OpenScape Business X. UC Suite additionally requires either the internally pluggable board "UC Booster Card" or the external Linux server "UC Booster Server". The OpenScape Business S softswitch optionally supports either UC Smart or UC Suite.

2.3.1 Expansion Levels Available through Sales

The OpenScape Business models have different expansion levels.

	X1	X3R/X3W	X5R/X5W	X8	S
Connection to Service Provider					
ITSP channels (SIP providers)	30	60	60	60	180
Max. number of active SIP providers	8	8	8	8	8
ISDN S_0 (BRI)	4	20	52	128	-
	via mainboard	X3R: 2* STLSX4R X3W: 2* STLSX4	X5R: 6* STLSX4R X5W: 6* STLSX4	SW limit, i.e., regardless of the number of STDM3 boards	
ISDN S_{2M} (PRI)	-	-	30	180	-
			1* TS2	3 * DIUT2	
Max. number of trunk channels (ITSP, SIP-Q, Native SIP, TDM trunks, MEB)	250	250	250	250	250
Stations					
ISDN	4	20	52	128	-
	via mainboard	X3R: 2* STLSX4R X3W: 2* STLSX4	X5R: 6* STLSX4R X5W: 6* STLSX4	8* STMD3	
Analog	4	20	52/68	384	-
	via mainboard	X3R: 2* SLAV8R X3W: 1* SLAV16	X5R: 6* SLAV8R X5W: 4* SLAV16	16* SLMA	
Digital ($U_{P0/E}$)	8	24	56	384	-
	via mainboard	2* SLU8(R)	6* SLU8(R)	16* SLMO2	
IP stations	20[1]	500	500	500	2000 (max. 500 SIP stations)
Cordless/DECT (CMI)	16	32	32/64	250	-
	1-7 base stations via Mainboard	1-7 base stations via mainboard + 8-15 via SLUN	X5R: 1-7 base stations via mainboard + 8-15 via SLUN X5W: 64 with 1* SLC16N	4* SLCN	
Max. number of stations	30[1]	500	500	500	2000
Unified Communications (UC Smart)					
UC Smart VoiceMail (Smart VM)	30	500/320[2]	500/320[2]	500/320[2]	1500

	X1	X3R/X3W	X5R/X5W	X8	S
Maximum number of simultaneously active UC Smart clients (Sum of myPortal Smart, myPortal to go, myPortal for OpenStage, Application Launcher, OpenScape Business Attendant, OpenScape Business BLF and 3rd Party WSI Clients)	30	250/50[2]	250/50[2]	250/50[2]	250
myPortal Smart	30	250/50[2]	250/50[2]	250/50[2]	250
OpenScape Business Attendant	8	8	8	8	8
OpenScape Business BLF	30	250	250	250	250
	Max 350 BLF keys	Max 350 BLF keys	Max 350 BLF keys	Max 350 BLF keys	Max 350 BLF keys
Max. number of the mobile stations	30	250/50[2]	250/50[2]	250/50[2]	250
Number of Mobility Entry User stations	30	150	150	150	250
myPortal to go	30	250/50[2]	250/50[2]	250/50[2]	250
Maximum number of channels for UC conferences	30	30	30	30	60
Unified Communications (UC Suite)					
UC Suite VoiceMail	-	500	500	500	1500
Maximum number of simultaneously active UC Suite clients (Sum of myPortal for Desktop, myPortal for Outlook, myAttendant, myAgent)	-	500/150[3]	500/150[3]	500/150[3]	1500
Max. number of other simultaneously active clients (Sum of myPortal to go, myPortal for OpenStage, Application Launcher, OpenScape Business Attendant, OpenScape Business BLF and 3rd Party WSI Clients)	-	-	-	-	500
myPortal for Desktop	-	500/150[3]	500/150[3]	500/150[3]	1500
myPortal for Outlook	-	500/150[3]	500/150[3]	500/150[3]	1500
myAttendant	-	20	20	20	20
OpenScape Business Attendant	8	8	8	8	8
OpenScape Business BLF	30	250	250	250	500
	Max 350 BLF keys	Max 350 BLF keys	Max 350 BLF keys	Max 350 BLF keys	Max 350 BLF keys

	X1	X3R/X3W	X5R/X5W	X8	S
myAgent	-	192 configurable / 64 active concurrently	192 configurable / 64 active concurrently	192 configurable / 64 active concurrently	192 configurable / 64 active concurrently
Max. number of the mobile stations	-	250/150[3]	250/150[3]	250/150[3]	250
Number of Mobility Entry User stations	-	150	150	150	250
myPortal to go	-	250/100[3]	250/100[3]	250/100[3]	250
myReports	-	1	1	1	1
Max. number of simultaneous fax channels	-	8	8	8	8
Maximum number of Fax Users	-	500/150[3]	500/150[3]	500/150[3]	1500
Maximum number of channels for UC conferences	-	20	20	20	60
Unified Communications (CRM, database connectivity)					
Application Launcher	30 configurable / 30 active concurrently	500 configurable / 50 active concurrently	500 configurable / 50 active concurrently	500 configurable / 50 active concurrently	500
TAPI 120/170 User (via CSTA, UC Booster Server / Card required)	-	500/150[3]	500/150[3]	500/150[3]	1500
TAPI 120 User (in UC Smart mode via the mainboard without CSTA)	30	30	30	30	-
Directory Services Connector (UC Booster Card/Server required)	-	4	4	4	4
Gate View					
Cameras	-	8/2[3]	8/2[3]	8/2[3]	8

1 Max. total number of IP and Deskshare Users = 20 (limited through configuration) - Max. total of IP, Deskshare, analog and digital stations = 30 (limited through licenses)
2 1st. value: maximum expansion with UC Booster Server / 2nd. value: maximum expansion with mainboard or UC Booster Card
3 1st. value: maximum expansion with UC Booster Server / 2nd. value: maximum expansion with UC Booster Card

For a detailed description of the expansion levels and capacity limits, see also *Configuration Limits and Capacities*.

OpenScape Business UC Networking

OpenScape Business offers extensive network connectivity options:

- Extensive voice and UC networking between the various OpenScape Business X (UC Booster Card/Server required for UC networking) and OpenScape Business S
- with multiple buildings on the company premises
- with distributed locations
- Central administration, including licenses (HiPath 5000 RSM is no longer required)

- Voice networking with OpenScape Enterprise in preparation

Voice networking supports networks with up to 32 nodes. UC networking supports networks with up to 8 nodes and up to 1000 stations (1500 stations with OpenScape Business S). In addition, project-specific releases are possible.

For a detailed description of the networking scenarios, see *Configuration Limits and Capacities*.

2.3.2 UC Hardware Models

The OpenScape Business X communication systems offer a high degree of flexibility in terms of functionality and design. Depending on the OpenScape Business X model, up to 500 stations are supported for IP, digital (ISDN), analog (a/b) and Cordless (DECT), and connections to the public network using ITSP (SIP), ISDN (BRI and PRI), CAS and analog and onboard IP (provisioned on the mainboard).

- OpenScape Business X1
  Communication system which comes in a wall housing and must be wall mounted.
- OpenScape Business X3W
  Communication system which comes in a wall housing and must be wall mounted.
- OpenScape Business X3R
  Communication system which comes in a 19-inch rack housing and can be installed in a 19-inch rack, as a standalone unit (desktop operation) or wall mounted.
- OpenScape Business X5 W
  Communication system which comes in a wall housing and must be wall mounted.
- OpenScape Business X5R
  Communication system which comes in a 19-inch rack housing and can be installed in a 19-inch rack, as a standalone unit (desktop operation) or wall mounted.
- OpenScape Business X8
  Modular communication system which can be used as a one-box system (base box) or two-box system (base box + expansion box). The communication system can be installed as a standalone unit or mounted in a 19-inch rack.

Figure: Hardware Platforms

2.3.3 UC Booster Hardware

UC Booster Hardware for OpenScape Business X.

- OpenScape Business UC Booster Card
  Board for OpenScape Business X if UC Suite is to be used as a UC solution with up to 150 UC users.
- OpenScape Business UC Booster Server
  External UC Booster Server (Linux) for OpenScape Business X if UC Suite is to be used as a UC solution with up to 500 UC users.
  SLES 11 SP4 64 Bit is used on the UC Booster Server. The UC Booster Server can also be run in a virtual environment with VMware vSphere.
  When using the UC Booster Server, the UC Booster Card is not required.
- OpenScape Business Voice Channel Booster Card
  Two optional modules for the extension of OpenScape Business X with additional DSP channels (e.g., for simultaneous voice connections with IP/TDM transitions).
  Eight DSP channels are provided on the mainboard. The Voice Channel Booster Card OCCB/1 provides a further 48 DSP channels, and the Voice Channel Booster Card OCCB/3 provides up to 128 DSP channels.

2.3.4 UC Software Models (Softswitch)

All-in-one server-based UC software solution that supports up to 1000 IP stations with connections to the public network using ITSP (SIP).

Independent of the platform used, OpenScape Business S can be installed on a Linux server. SLES 11 SP4 64 Bit is used as the operating system. OpenScape Business S can also be run in a virtual environment with VMware vSphere. If TDM interfaces are required for connection to TDM telephones or TDM trunks, OpenScape Business X systems can be used as a gateway.

2.3.5 Structure and Environmental Conditions

	X1	X3W	X3R	X5W	X5R	X8
Structure	Wall-mount system	Wall-mount system	Rack	Wall-mount system	Rack	Standard system (rack installation also possible)
Dimensions (HxBxT in mm)	470x370x80	450x460x130	89x440x380 (2U)	450x460x200	155x440x380 (3,5U)	490x440x430
Weight	about 2.8 kg	about 6 kg	about 6 kg	about 8 kg	about 8 kg	about 34 kg (fully loaded)
Housing color	White	White	Green / Dark Grey	White	Green / Dark Grey	Green / Dark Grey
Power supply	The models are equipped for connection to the power supply. • Rated input voltage (AC): 100 to 240 V • Nominal frequency: 50/60 Hz • Battery power (DC): -48 V					
Power consumption	Depending on the hardware platform and expansion					
Environmental Conditions	• Operating conditions: +5 to +40 °C (41 to 104 °F) • Humidity: 5 to 85%					

2.3.6 Supported Phones

OpenScape Business X enables telephony over IP/HFA (HiPath Feature Access), SIP, TDM, a/b, Cordless/DECT and WLAN. IP/HFA, SIP and wireless phones can be connected to OpenScape Business S.

OpenStage telephones (IP/ HFA, SIP and T)	• OpenStage 5/10/15/20/30/40/60/80
OpenScape Desk Phone (IP/ HFA, SIP)	• OpenScape Desk Phone IP 35G/55G • OpenScape Desk Phone IP 35G Eco • OpenScape Desk Phone CP 200/400/600 HFA and SIP
Key modules	• OpenStage Key Module, only for OpenStage 15/40/60 • OpenStage BLF 40 (Busy Lamp Field), only for OpenStage 40 and OpenStage 30 T • OpenScape Key Module 400/600, only for CP devices
OpenScape Business Cordless	• OpenStage S5/M3/SL4
PC clients (HFA, SIP)	• OpenScape Personal Edition (incl. video for SIP)
SIP phones (UC Suite) / AP adapter	• SIP phones with RFC 3725 support • Mediatrix 4102S (for connecting 2 analog phones or Fax devices)
WLAN Phones	• OpenStage WL3 professional
Analog and ISDN phones	• Analog (a/b) phones • Digital (S_0) ISDN phones

Older devices (such as optiPoint 410/420/500, Gigaset M2/SL3/S4 and optiPoint WL2 SIP) are supported. Optiset E devices cannot be operated.

Functions and Configuration of SIP Phones

OpenScape Business offers an extensive range of voice communication features for OpenStage HFA telephones. Many functions are also available for standard SIP phones.

An overview of the features supported with OpenStage SIP telephones and further information can be found in the Unify wiki at the following link

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

To control voice calls for SIP telephones using CTI (3PCC), a UC Booster Card or a UC Booster Server is required for OpenScape Business X3/X5/X8.

The control of voice calls for SIP telephones via UC Smart clients is supported for the OpenScape Business X3/X5 rack models with the Booster Card.

With the help of the DLI functions, the OpenScape Desk Phone (SIP) telephones can be centrally administered and supplied with software.

2.4 Further information

Further information can be found on the Internet and extranet. See also the release notes for limitations and recent changes.

2.4.1 Languages Supported

Several different language variants are available for the various software components (clients and WBM) and documentation/online help.

The following languages will be released as part of the country-specific introduction.

	de en	es fr it nl pt	da no sv	fi	ru	cs	pl	hr tr	hu	zh
UC Smart Clients										
myPortal Smart (Client)	X	X	X	X	X	X	X	X	X	–
myPortal Smart (User Guide)	X	X	–	–	–	–	–	–	–	–
myPortal to go (Client)	X	X	X	X	X	X	X	X	X	–
myPortal to go (User Guide/Online Help)	X	X	X	X	X	X	X	–	–	–
myPortal for OpenStage (Telephone)	X	X	X	X	X	X	X	X	X	–
myPortal for OpenStage (User Guide)	X	X	–	–	–	–	–	–	–	–
TUI (Telephone User Interface)	X	X	X	X	X	X	–	X	–	X
TUI (Quick Reference Guide)	X	X	–	–	–	–	–	–	–	–
OpenScape Business Attendant / BLF (Client)	X	X	–	–	–	X	–	–	–	–
OpenScape Business Attendant / BLF (User Guide)	X	X	–	–	–	X	–	–	–	–
UC Suite Clients										
myPortal for Desktop (Client)	X	X	X	X	X	X	X	X	X	X
myPortal for Desktop (User Guide/Online Help)	X	X	X	X	X	X	X	–	–	–
myPortal for Outlook (Client)	X	X	X	X	X	X	X	X	X	X
myPortal for Outlook (User Guide/Online Help)	X	X	X	X	X	X	X	–	–	–
myPortal to go (Client)	X	X	X	X	X	X	X	X	X	–
myPortal to go (User Guide/Online Help)	X	X	X	X	X	X	X	–	–	–
myPortal for OpenStage (Client)	X	X	X	X	X	X	X	X	X	–
myPortal for OpenStage (User Guide)	X	X	–	–	–	–	–	–	–	–
myAttendant (Client)	X	X	X	X	X	X	X	X	X	X
myAttendant (User Guide/Online Help)	X	X	X	X	X	X	X	–	–	–
myAgent (Client)	X	X	X	X	X	X	X	X	X	X
myAgent (User Guide/Online Help)	X	X	X	X	X	X	X	–	–	–
myReports (Client)	X	X	–	X	X	X	X	–	–	–
myReports (User Guide/Online Help)	X	X	–	X	X	X	X	–	–	–
TUI (Telephone User Interface)	X	X	X	X	X	X	X	X	X	X

	de en	es fr it nl pt	da no sv	fi	ru	cs	pl	hr tr	hu	zh
TUI (Quick Reference Guide)	X	X	–	–	–	–	–	–	–	–
Administration										
OpenScape Business Assistant (WBM)	X	X	–	–	–	–	–	–	–	–
OpenScape Business Assistant (Administrator Documentation/Online Help)	X	X (no nl)	–	–	–	–	–	–	–	–
Manager E	X	X	X	X	X	X	X	–	–	–
Manager E (Administrator Documentation/Online Help)	X	X	–	–	X	–	–	–	–	–

In addition, the UC Smart TUI is also offered in the languages Belgian (Flemish) and Slovenian.

INFO: A Russian or Chinese Windows operating system is required in order to use the Russian or Chinese user interface.

The following language codes (ISO 639-1) are used for the abbreviations in the table:

- de = German
- en = English
- cs = Czech
- da = Danish
- es = Spanish
- fi = Finnish
- fr = French
- hr = Croatian
- hu = Hungarian
- it = Italian
- nl = Dutch
- no = Norwegian
- pl = Polish
- pt = Portuguese
- ru = Russian
- sv = Swedish
- tr = Turkish
- zh = Chinese

2.4.2 Internet Links

More details and possibly more up-to-date information can be found on the Unify homepage, our expert wiki and the Unify portal for partners.

Internet Links

- Unify homepage:
  `http://www.unify.com`
- Expert wiki for telephones, communication systems and UC:
  `http://wiki.unify.com`
- Partner Portal (registration required):
  `https://www.unify.com/de/partners/partner-portal.aspx`
  or
  `https://www.unify.com/en/partners/partner-portal.aspx`

3 Administration Concept

The administration of the communication system is performed with the OpenScape Business Assistant.

3.1 OpenScape Business Assistant (WBM)

The OpenScape Business Assistant is web-based and is therefore also called Web-Based Management (WBM).

The scope of administrative tasks offered depends on the administrator profile being used.

An online help is available for each page of the WBM.

3.1.1 Requirements for the WBM

In order to use the WBM, the administration PC must have the appropriate software installed.

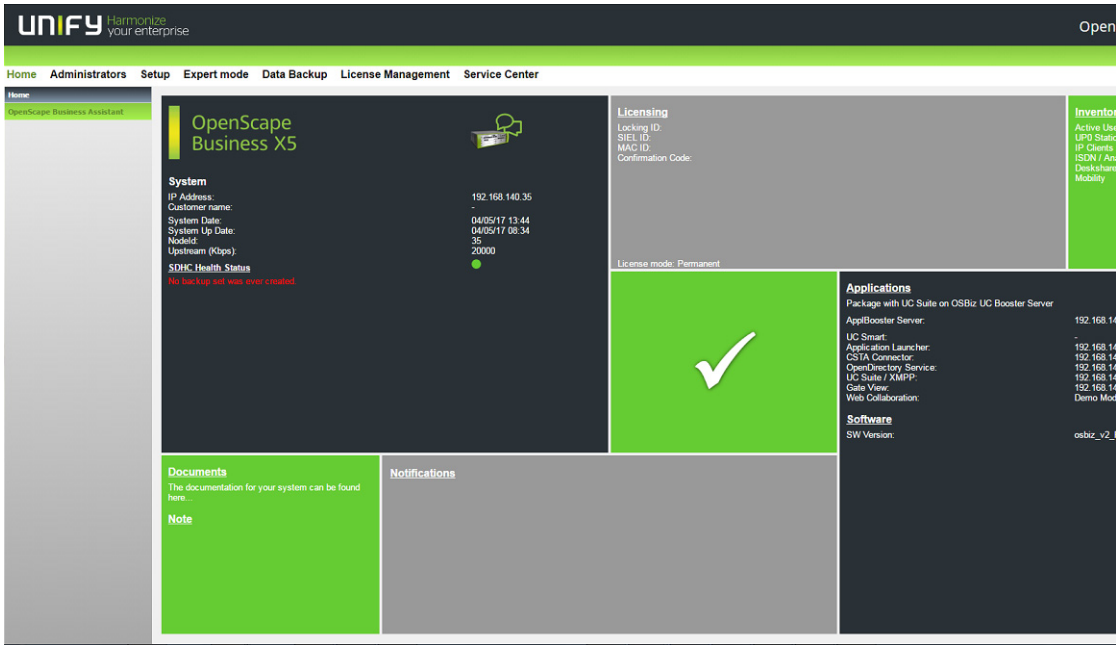
Supported Web browsers:

- Microsoft Internet Explorer 10 or later
- Mozilla Firefox 18 or later
- Google Chrome

3.1.2 Home Page of the WBM

The home page of WBM displays important system information, which is split into different areas (tiles). In addition, it includes notes and provides information on system errors, events and actions.

The presented system information depends on the administrator profile being used. The underlined headings in the individual areas are clickable and reference the related topic in the WBM.



The following information is displayed:

- Area: **Status** (Middle)
  - White check mark on green background: the communication system is fully functional - Messages highlighted in red in the other fields indicate actions that should be performed.
  - White check mark on red background: the communication system is not fully functional and requires the intervention of the administrator - Messages highlighted in red in the other fields indicate system errors or events that need to be resolved.
- Area: **System**
  - Brand
  - IP address of the communication system
  - Current date and time
  - Date and time of the last system restart
  - Notes when operating in an internetwork (system is master or slave, display of node ID)
  - Synchronization status
  - Bandwidth Upstream in kbps
  - SDHC Health Status
  - Notes on performing a backup and restore
  - Booster Card status
- Area: **Documents**
  - Link to the documentation
- Area: **Notifications**
  - Various notifications about the system
- Area: **Note**

  - Displays the latest information entered by an administrator. Clicking on the underlined title opens a text window in which all the information is displayed and further information can be entered.
- Area: **Licensing**
  - Locking ID for licensing
  - SIEL ID for licensing
  - Note on the licensing status, indicating if the system is in "Permanent" license mode or in "Pay As You Go" mode.
- Area: **Inventory**
  - Type and number of active stations
  - Number of activated ITSPs and a link to the ITSP status dialog in Service Center of active stations
- Area: **Applications** and Software
  Applications:
  - Used application package (UC Smart or UC Suite) and its components, including the IP addresses of the servers used.
  - Indicates whether a UC Booster Card is inserted.

  Software:
  - Version of the installed communication system software
  - Indicates whether a UC Booster Card is inserted. If the Booster Card is additionally accessible via an IP address, the version of the installed UC Booster Card software is displayed.
    The UC Booster Card and the communication system should always be on the same software version.
  - Expiration date of the 3-year software support.
    After the expiration date the message "Software Support licence has been expired, please update the Software Support licence" is displayed.
  - Note on the new software version

3.1.3 Introduction to the WBM

WBM is the web-based application for the administration of the system.

Language of the User Interface

You can select one of the following languages at login:

- German
- English
- French
- Italian
- Dutch (The online help is only available in English)
- Portuguese
- Spanish

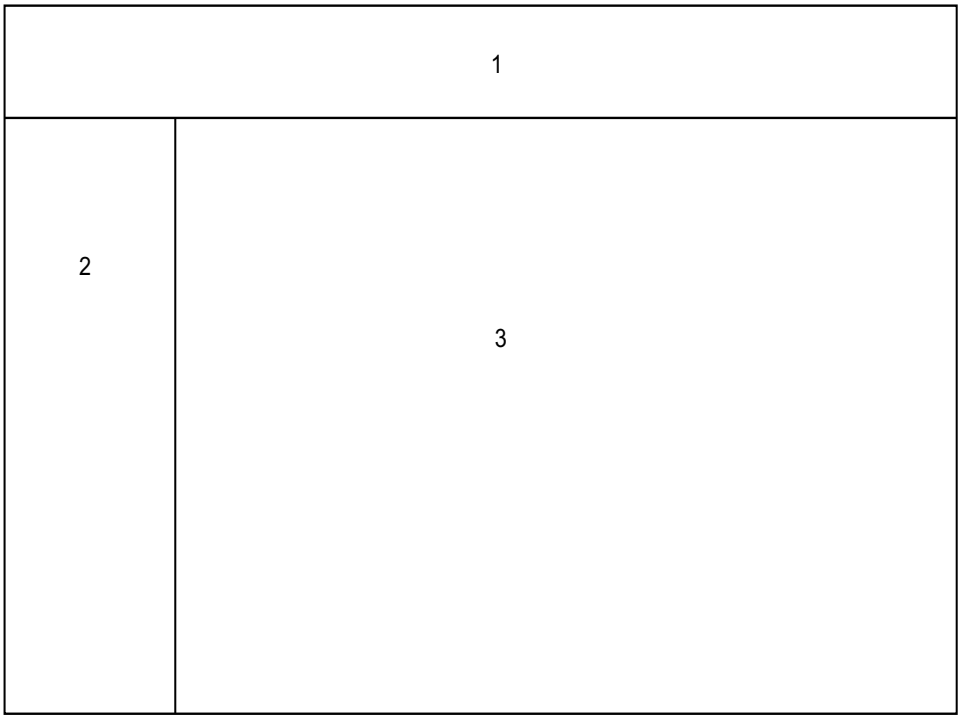
Ranking of the User Interfaces Described

Any tasks which can be performed in a wizard are described for the corresponding wizard only.

Any additional tasks which can be performed in Expert mode are described for the Expert mode only.

Any other remaining tasks are described for E Manager.

User Interface Elements



- Navigation bar (1)
  The navigation is the primary navigation aid and always shows the same links to main task centers, i.e., **Home**, **Administrators**, **Setup**, **Expert Mode**, **Data Backup**, **License Management**, **Service Center** as well as the current user name and the **Logout** link. When you click on one of these task centers, the associated navigation tree opens in the navigation area, and the home page of the task center appears in the workspace.
- Navigation area (2)
  The navigation area is the secondary aid and contains the navigation tree with the menu items of the selected task center. The name of the selected task center is displayed at the top of the navigation tree with expandable and collapsible menu groups and menu items below it. Different menu items are displayed in the menu groups, depending on the situation. Clicking on a menu item displays the associated page in the workspace.
- Workspace (3)
  The workspace is where administration tasks are performed. It is usually opened in a separate window. The number and selection of messages and

actions displayed depends on the menu item selected in the navigation tree. In Expert mode, the menu tree is displayed on the left in the workspace.

Navigating in the Menu Tree

The menu tree is used for navigation in the Expert mode of the WBM. The menu tree contains folders (e.g., **Maintenance**) with further elements (e.g., **Restart / Reload**).

You can navigate in the menu tree by clicking on a folder (which toggles its expanded or collapsed state).

Automatic Logout After Timeout

You are automatically logged off after 30 minutes of inactivity. You must log in again to continue working with the WBM. If you make some changes and then take a break, to be on the safe side, you should reload the page before making any further changes so that no changes are lost due the automatic logout.

3.1.4 WBM User Management

You can configure and manage up to 16 administrators for WBM (web-based management). Every administrator is assigned a profile that specifies the scope of his or her authorization. You can also change the password of a Manager E administrator.

The users of WBM are also referred to as administrators.

The default Administrator is `administrator@system` with the default password `administrator` and has the profile **Advanced**. This password must be changed on logging in for the first time. The password for an administrator must consist of at least 8 characters and a maximum of 128 characters, of which at least one character must be a digit. In addition, for a secure password, at least an uppercase letter, one lowercase letter and one special character should be included in the password.

Profiles

The WBM supports four profiles with different classes of service (authorizations) for administrators with different levels of technical expertise and tasks.

In order to prevent that no malicious user could login via ISDN and change the default password when logging in for the first time, it is compulsory for the user to change the password via Manager E as an installation step.

INFO: A password, which consists of 5 characters (*****), will not be accepted by the system for security reasons.

Table: Profile Classes of Service

Profile	Class of Service
Basic Basic knowledge of configuring the system	System information on the home page **Key Programming** wizard **Phone Book / Speed Dialing** wizard **Call Detail Recording** wizard **Music on Hold / Announcements** wizard **Station name and release** wizard Access to **Administrators** (only to change their own passwords) Access to **License Management > License Information** Access to **Service Center > Documents** Access to **Service Center > Software**
Enhanced Good knowledge of configuring the system	As for the **Basic** profile, plus: Access to all wizards (except the **Basic Installation**, **UC Suite** and **UC Smart** wizards) IMPORTANT: Access to all wizards is not supported in OpenScape Business S systems. Access to **Administrators** (only to change their own passwords) Access to **Backup And Restore** Access to **License Management** (excluding registration, license activation and settings) Access to **Service Center > Inventory** Access to **Service Center > Restart / Reload** (without reload) Access to **Service Center > Diagnostics > Status** Access to **Service Center > Diagnostics > Event Viewer**
Advanced Trained users	As for the **Enhanced** profile, plus: Access to all wizards Access to **Administrators** (only to change their own passwords) Access to the complete **License Management** Access to the complete **Service Center** Access to **Networking**
Expert Trained service technicians	As for the **Advanced** profile, plus: Access to **Administrators** (complete) Access to the **Expert mode**

Table: Profile Management

Profile	Maintenance
Basic Basic knowledge of configuring the system	Can change own password. Does not see any other configured administrators except himself or herself.
Enhanced Good knowledge of configuring the system	Can change own password. Does not see any other configured administrators except himself or herself.
Advanced Trained users	Can change own password. Does not see any other configured administrators except himself or herself.
Expert Trained service technicians	Can change own password and the user names and passwords of other administrators. Sees all configured administrators. Can add, edit and remove administrators.

INFO: As long as no administrator with the **Expert** profile exists, administrators with the **Advanced** profile can add, edit and remove further administrators. As soon as an administrator with the **Expert** profile exists, only administrators with the **Expert** profile can add, edit and remove further administrators.

Administrator Management in the Internetwork

The direct management of administrators is only possible in the WBM of the master node. The **Administrator** menu is not displayed on slave nodes. All administrator configurations are transmitted to the slave nodes. It is, however, possible to call up the WBM of the master node from within the WBM of the slave node via the Node View. The **Administrator** menu is displayed here, and administrators can then be managed.

Manager E Password Administration

An administrator can change (but not create a new user role) the password of the existing users which can access the embedded system through Manager E.

User will be prompted to change passwords only for the existing users and will not be able to change the user's Group and options like Created, Last Used are not viewable. This is a security feature and thus it does not provide the whole Manager E's administration screen.

3.1.5 Wizards

Wizards make it easy to install and configure the system. Only selected subset of the wizards are available to a customer administrator (with the **Basic** profile). A

trained service technician or an administrator with expertise (with the **Advanced** profile), by contrast, can access all the wizards.

The available wizards depend on the system configuration (UC Smart or UC Suite). Wizards can consist of several pages in succession. OK & Next saves changes and switches to the next page in the wizard. There is no undo function for changes committed with OK & Next. If no changes were saved, **Abort** closes the wizard. Clicking the **X** symbol in the upper right corner of the wizard window terminates the wizard and retains the changes previously saved with OK & Next.

3.1.5.1 Wizards – Basic Installation

The wizards under **Basic Installation** support the simple basic installation.

The following wizards are available under **Basic Installation**:

- **Initial installation**
  Single usage at initial setup. Country initialization, System IP address and DHCP server.
- **Basic Installation**
  Basic setup of system with station data, trunks, network parameters and Internet.
- **Licensing**
  Activating licenses online via the License Server.
- **Networking Configuration**
  Setup of system as part of a network.
- **Power Management**
  Setup and Activation of Power Management

3.1.5.2 Wizards – Network / Internet

The wizards under **Network / Internet** support the simple configuration of networks and the Internet access.

The following wizards are available under **Network / Internet**:

- **Network Configuration**
  Set up DHCP, IP Routing and DNS Server.
- **Internet Configuration**
  Access parameters of the Internet Provider data, e.g., User Account and Password.
- **VPN Configuration**
  Connection of workplaces via the Internet.

3.1.5.3 Wizards – Telephones / Subscribers

The wizards under **Telephones / Subscribers** support the simple configuration of phones and subscribers.

The following wizards are available under **Telephones / Subscribers**:

- **IP devices**
  Set up system-specific IP and SIP telephones, FAX call numbers as well as IP/analog adapters.
- **UP0 devices**
  Set up UP0 Telephones, FAX call numbers.
- **Portable parts (DECT devices)**
  Set up DECT phone, FAX call numbers.
- **ISDN devices**
  Unpowered ISDN ports for ISDN cards / modems and S0 stations.
- **Analog Terminals**
  Analog DTMF and CLIP-capable ports for Fax and Telephone.
- **Key programming**
  Name and function key programming for system-specific IP devices and UP0 devices.

3.1.5.4 Wizards – Central Telephony

The wizards under **Central Telephony** support the simple configuration of central telephony features.

The following wizards are available under **Central Telephony**:

- **CO Trunk ISDN / Analog / ITSP**
  Point-to-multipoint connections (MSN) and PABX number for ISDN connections, and assignment of analog and ITSP trunks.
- **Internet Telephony**
  Access parameters of the Internet Telephony Service Provider (ITSP), e.g., user account, password, SIP station number.
- **Directory / Speed Dialing**
  Set up central speed-dial destinations for the system's internal phone book.
- **Call Detail Recording**
  Set up call detail recording connection parameters for call detail applications.
- **Music on Hold / Announcements**
  Record new melodies and announcements for Music on Hold and announcement before answering.
- **Entrance Telephone (Door Opener)**
  Set up call allocation and access authorization for the entrance telephone at the analog station connection.
- **SmartVM**
  Setup of the UC Smart voicemail box (SmartVM).

3.1.5.5 Wizards – User Telephony

The wizards under **User Telephony** support the simple configuration of user telephony features.

The following wizards are available under **User Telephony**:

- **Class of Service**
  Set up classes of service with external call numbers that can be assigned to subscribers, e.g., emergency numbers, allowed numbers, denied numbers and assignment of class of service for night service.
- **Station Name and Release**
  Edit station and group names and reset lock code for individual stations.
- **Group call / Hunt group**
  Set up incoming calls for station groups (parallel, linear or cyclical call order).
- **Call Forwarding**
  Set up central system-wide station number assignments, and forwarding "after timeout" and "on busy".
- **Call pickup**
  Configure stations in a pickup group with the option of answering each other's calls.
- **Team Configuration**
  Setting up stations which are called concurrently with the main station for incoming calls and which can use its station number for outgoing calls.
- **Mobile Phone Integration**
  Set up a link between a mobile phone and an internal station with the goal of enabling incoming and outgoing availability under one station number (One Number Service).
- **Executive / Secretary**
  Set up a link between one or more Executive phones and one or more Secretary phones with the goal of enabling simplified call transfers and ring transfers.
- **UCD**
  Set up an automatic intelligent call distribution to a group with selected stations.
- **Attendant Console**
  Set up stations as attendant console numbers and station behavior for on busy, incorrect dialing and no answer.
- **Station Profiles**
  Assign stations to a profile and import/export profile data.

3.1.5.6 Wizards – Security

The wizards under **Security** support the simple configuration of the firewall.

The following wizards are available under **Security**:

- **Firewall**
  Configure port opening to restrict Internet traffic.

3.1.5.7 Wizards - UC Smart (only with UC Smart)

The setup of the UC solution UC Smart is supported by wizards under **UC Suite**.

The following wizards are available under **UC Smart** :

- **UC Smart**
  Basic Setup and User Configuration for UC Smart.

3.1.5.8 Wizards - UC Suite (only with UC Suite)

The setup of the UC solution UC Suite is supported by wizards under **UC Suite**.

The following wizards are available under **UC Suite**:

- **User Directory**
  Configuration of users.
- **Departments**
  Configuration of departments.
- **Groups**
  Configuration of voicemail and fax groups.
- **Templates**
  Configuration of SMS templates.
- **External Directory**
  Manual addition of individual contacts to the external directory.
- **External Providers Config**
  Input of access data for the Exchange or LDAP server.
- **Contact Center**
  Configuration of the Contact Center.
- **Schedules**
  Configuration of schedules.
- **File Upload**
  Uploading of audio files for announcements and music on hold.
- **Conferencing**
  Configuration of conference calls.
- **Profiles**
  Creation of user profiles.
- **Fax Headlines**
  Configuration of fax headers.
- **Skin Settings**
  Management of user interfaces.

3.1.6 Service Center

The **Service Center** of the WBM offers various maintenance functions, starts the software update and makes the documentation and software available.

3.1.6.1 Service Center – Documents

The **Documents** option provides documentation, CSV templates and links to related information. The documentation can be accessed in all the supported languages in PDF format.

Depending on the system configuration, the following contents are available:

Contents	UC Smart	UC Suite
Administrator Documentation (PDF)	-	x
User Guides (PDF)	-	x
Links to further information	x	x
CSV templates for importing data for • Stations • System Speed Dialing • External directory	x	x

3.1.6.2 Service Center – Software

The **Software** option provides the software for the UC clients, USB drivers and tools.

The following contents are available:

Contents	UC Smart	UC Suite
Installation files for the software of the UC clients	x	x
USB drivers	x	x
Tools	x	x
Links for direct access to the installation files	-	x

3.1.6.3 Service Center – Inventory

Inventory provides an overview of the basic configuration data of the system.

3.1.6.4 Service Center – Software Update

Software Update checks whether a software update is available on the web server and performs the update.

3.1.6.5 Service Center – E-mail Forwarding

E-mail Forwarding enables the sending of e-mails with system messages from the UC Suite to the administrator and e-mails with attached voicemail of fax messages to subscribers.

3.1.6.6 Service Center – Remote Access

Remote Access is used to configure access for the site-independent administration of the system.

3.1.6.7 Service Center – Restart / Reload

Restart / Reload enables a restart of the system, optionally resetting it back to factory settings.

3.1.6.8 Service Center – Diagnostics > Status

Status provides status information on the network, subscribers, call setup, ITSP and VPN.

See also *Inventory Management*.

3.1.6.9 Service Center – Diagnostics > Event Viewer

Event Viewer logs system events.

See also *Traces*.

3.1.6.10 Service Center – Diagnostics > Trace

Trace provides options for fault logging.

See also *Traces*.

3.1.6.11 Service Center – Diagnostics > Service log

Service log logs several system data in the form of HiPath 3000 Event.

It is necessary to be on WBM View mode, to refresh or download the file.

3.1.7 Expert Mode

The Expert mode provides trained service technicians (**Expert** profile) with several menus and functions to configure and maintain the system.

Detailed information can be found in the section on *Expert Mode*.

3.1.8 Online Help

The integrated online help describes key concepts and operating instructions. The online help is context-sensitive and opens the associated Help topic for each opened WBM page.

Navigation

The buttons in the online help provide the following functions:

- **Contents**
  provides you with an overview of the structure
- **Index**
  provides direct access to a topic using keywords
- **Search**
  allows you to do a full-text search and selectively find all relevant topics

3.2 Manager E

Manager E is a service tool with integrated help that runs under Windows and can be used for tasks which cannot be performed via the WBM.

Manager E can be used for OpenScape Business X1, OpenScape Business X3, OpenScape Business X5 and OpenScape Business X8. OpenScape Business S cannot be administered using Manager E.

Manager E is intended for trained service personnel and includes the following function blocks:

- Generation (including off-line generation)
- Copying and backing up customer data
- Service orders, such as restarting boards
- Resetting activated features
- Creation and printing of:
  - Key labels for optiPoint 500
  - Customer data printouts
  - Main distribution frame layout
- Separate user and password administration for after sales service.
- Database conversion routine for customer database (CDB).

System access via Manager requires a user name and a password. The Online mode can be used to perform changes quickly. The functionality of the Online mode corresponds to the Assistant T user interface.

The following features can no longer be administered using Manager E:

- Licensing
- Network
  - SNMP Partner
  - PSTN Peer
  - Routing
  - Mapping
  - Gatekeeper
  - Ext. H.323
  - IP Ports
- Maintenance
  - Error History
  - Event Log
  - Trace settings
  - Error Reaction Table
  - V.24 Status
  - DMA
- Traces

Working with the Customer Database (CDB)

The basic steps are as follows:

- Load the CDB from the system into Manager E
- Make any necessary changes in E Manager
- Use Manager E to store the CDB back on the system

4 Licensing

The flexible licensing concept of OpenScape Business allows customers to adapt the functional scope to their own requirements through licenses. All OpenScape Business X and OpenScape Business S communication systems are subject to this license concept. Phones, UC clients, UC functions and system-wide features can thus be unlocked according to individual customer needs. Uniform licenses are used for all OpenScape Business communication systems.

OpenScape Business can be expanded or equipped with additional features at a later date by purchasing additional licenses.

All licenses are always bound to the basic license of the communication system and enable the use of the purchased features for the associated version of OpenScape Business.

90-day evaluation licenses can be ordered to allow customers to test and evaluate special features.

Activation Period

The license activation must be completed within the activation period (duration of 30 days). The activation period begins when the current date is entered in the WBM. The expiration date of the activation period is stored in the process.

During the activation period, the product is fully functional, and the maximum number of licenses are available for use.

If the system loses the current date within the activation period (e.g., due to a discharged battery on the mainboard), the date must be updated in the WBM as soon as possible so that the system can continue to be used without restrictions during the activation period.

If the licensing is not completed before the activation period expires, the functionality of the communication system will be severely restricted. Internal communication between the individual stations is still possible, but only the first two active phones can make external calls (e.g., for emergency calls). Access to the communication system via Remote Access is still possible. The system also remains in this restricted state when the initial installation is carried out only with Manager E, since this does not start the activation period.

License Structure

The licenses for the communication system are structured as follows:

- A basic license permanently activates the software of the communication system. This basic license is also required for activating all other licenses.
- Station licenses activate the phones for external voice communications.
- User-oriented licenses to unlock specific user features.
- System licenses to unlock general system-wide features.

Migration

Existing HiPath 3000 V9 customers are being offered an upgrade license for license migration. License migration ensures investment protection for customers through continued use of telephones and voice features.

4.1 Licensing Procedure

Licensing is handled via the centralized OpenScape License Management procedure for the administration and activation of licenses. This ensures that a customer can use precisely the system configuration or features for which that customer has acquired the appropriate licenses (usage rights).

The licenses of the OpenScape Business communication systems are bound to the Locking ID or the Advanced Locking ID of the communication system (see *Locking ID and Advanced ID Locking*).

The customer orders the required features and receives a License Activation Code (LAC). After a successful initial installation of the communication system, the customer activates the acquired licenses via a license file. The license file provides the system with a license pool with all purchased licenses available for the subsequent allocation of licenses.

The WBM provides wizard-driven functions for the customer registration, license activation and the license assignments for standalone systems and systems in an OpenScape Business internetwork. Licensing with Manager E is not possible.

Steps for Successful Licensing

1. Configuration of the system within the activation period
2. Registration of customer data
3. License Activation
4. Assigning Licenses

Customer Registration

Within the framework of licensing, the input of the customer data of each respective system is mandatory for the registration of the customer. The customer data is used to retrieve information quickly in the case of security-related issues, especially in the context of product recalls. In addition, customers receive information on prevention of license misuse by third parties, e.g., via the new link to the license information.

License Activation

During the license activation, the purchased licenses are bound to the communication system using the license management of the WBM. Two methods are available for this:

- Online activation
  For online activation, after the LAC is entered via the Internet, a connection to the Central License Server (CLS) is set up, and the license file is automatically transferred to the integrated license agent (Customer License

Agent, CLA) in the communication system. The licenses are then automatically activated.

- Offline activation
  With offline activation, the communication system is not connected to the Central License Server (CLS). The license file is generated at the CLS by an authorized partner and must be transmitted manually during the license activation to the integrated license agent (Customer License Agent, CLA) in the communication system.

Assigning Licenses

All purchased licenses are permanently assigned to stations via the license management of the WBM.

To assign licenses to stations, the stations must be first set up with the WBM, e.g., during the initial installation. Each system configuration can be set independently of the existing licenses. However, the corresponding feature can only be used once the license have been assigned.

When assigning licenses, a distinction is made between the configuration and actual licensing. For station and user-oriented licenses, licence requests are first configured. If a license is available in the license pool for a license request, the corresponding feature is unlocked. If no license is available in the license pool, the configured license request is retained, but the corresponding feature is not unlocked. Missing licenses must be purchased if needed.

Licensing in an Internetwork

For an OpenScape Business internetwork, a network-wide license file (network license file) is generated by an authorized partner at the Central License Server (CLS). This network-wide license file is managed by the Central License Agent (CLA) of the master node and provides the licenses for the individual nodes. The assignment of the licenses occurs via the WBM of each individual node. Within an internetwork, the network licenses can be shifted freely by using the WBM.

Online activation is not possible when licensing an internetwork.

Pay As You Go

Apart from the traditional licensing scheme, OpenScape Business supports subscription licensing model (Pay As You Go). "Pay As You Go" gives the opportunity to invoice only for the used licenses on each billing period and use extra licenses without extending the license file. There is no need to decide the amount of the licenses beforehand

A permanent internet connection from OpenScape Business system to the Central License Server (CLS) is required. It can be activated either online with a a License Activation Code (LAC) or with file upload. After installing, configuring the solution according to the custom needs and activating "Pay As You Go" a periodically report of the used licenses are sent to the Central License Server (CLS) and is evaluated. Once a month, a final report is created on the Central License Server (CLS) product site and the content of used licenses of this final report is used for license accounting.

With subscription licensing a new time period is introduced, the qualifying period. The qualifying period starts with the system startup or if a "Pay As You Go" license file is activated. The period starts consecutively and during this period a license configuration done in WBM will not lead to license usage update. The maximum duration of the qualifuing period is 2 hours.

INFO: In order the firewall to have access to CLS the following actions are needed:

-) 7780 und 7790 Ports for incoming and outgoing IP traffic released

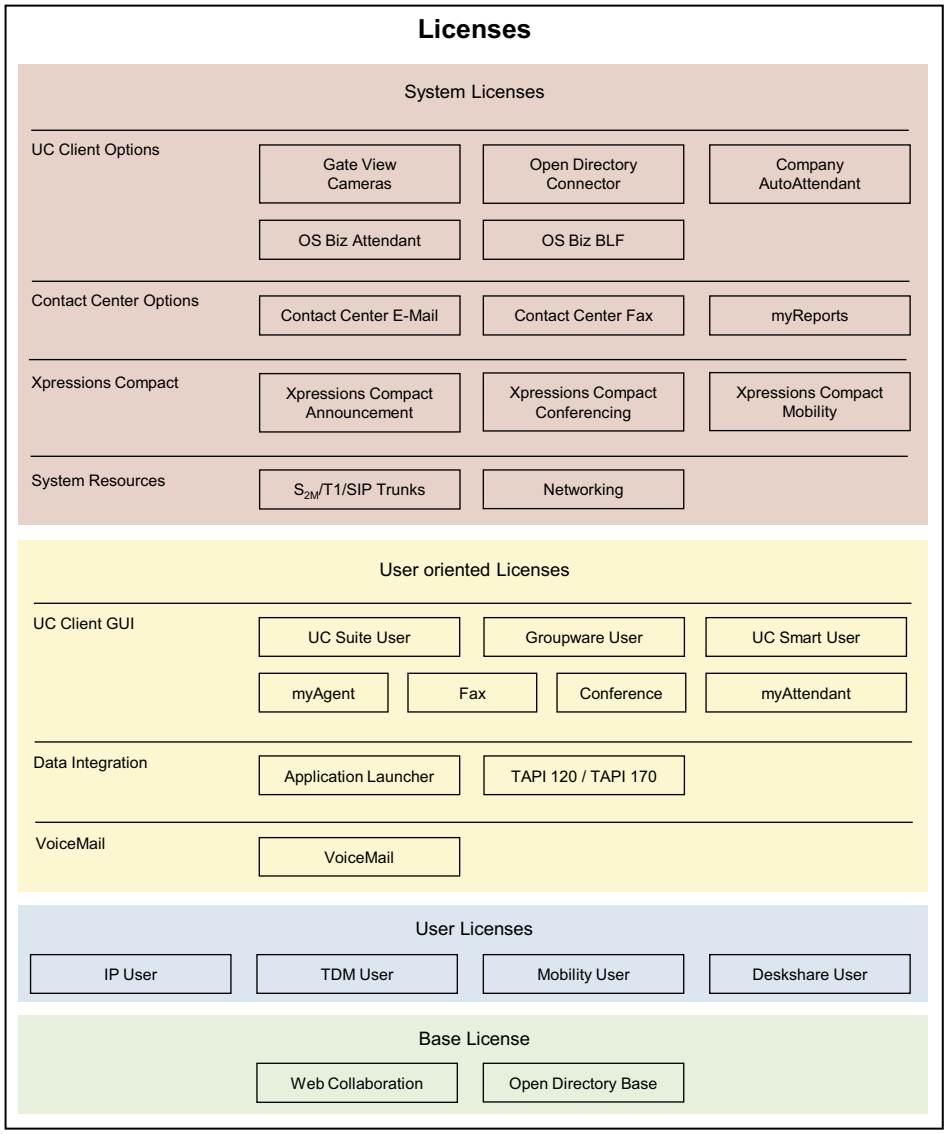
-) 188.64.16.4 released for incoming and outgoing IP traffic

4.2 Licenses

To use the features of the communication system, licenses must be purchased. The purchased licenses must be activated within a given period of time (activation period).

Licenses are categorized thematically into license groups. The following license groups are available:

- Basic Licenses
- Station Licenses
- User-oriented Licenses
- System licenses



The above licenses can be used for OpenScape Business X, OpenScape Business S and the OpenScape Business UC Booster Server. There is no basic license for the UC Booster Server. The licenses cover all features and can be combined in accordance with the wishes of the customer. The possible combinations of licenses are explained in greater detail in the "Assigning Licenses and License Profiles" section.

Station licenses and user-oriented licenses are permanently assigned to subscribers.

4.2.1 Basic License

A basic license permits the basic use of the communication system. It is also required for activating all other licenses.

Internet telephony and emergency operation is also possible without a basic license.

The following basic licenses are available:

- **OpenScape Business V2 X1 Base**
  for unlocking the V2 functionality of
  – OpenScape Business X1
  The basic license additionally includes the licenses OpenDirectory Base for using the Open Directory Service (ODS) and Web Collaboration for starting a web collaboration session. This makes it possible for the UC solution UC Smart to be connected to an external database.
- **OpenScape Business V2 Base**
  for unlocking the V2 functionality of
  – OpenScape Business X3/X5/X8 with or without UC Booster (UC Booster Card or UC Booster Server) or
  – OpenScape Business S
  The basic license additionally includes the license OpenDirectory Base for using the Open Directory Service (ODS) and Web Collaboration for starting a web collaboration session. This makes it possible to connect the UC solutions UC Suite or UC Smart to an external database.

4.2.2 Station Licenses

Every subscriber connected to the communication system requires a station license to make external calls. This license is permanently bound to the call number of the subscriber via the WBM.

Station licenses include the comprehensive voice functionality of OpenScape Business. Additional licenses are required to use the UC solutions UC Smart or UC Suite (see *User-oriented Licenses*).

The following station licenses are available:

- **IP User**
  For the use of IP system telephones (HFA) and SIP telephones.
- **TDM User**
  For the use of UP0 system phones, analog phones, analog fax devices, ISDN phones, ISDN fax and DECT phones.
- **Mobility User**
  For the use of GSM/mobile phones, smartphones and tablet PCs as an extension of the communication system. For the use of myPortal to go and Mobility Entry. The assignment of an additional desk phone is not required.
- **DeskShare User**
  For use of the DeskSharing feature. Only a phone number and no physical phone is permanently assigned to such users. DeskShare users can operate specific IP system phones using their permanently assigned phone number, and they can access their personal phone settings on these phones.

Flexible User Licensing

With the flexible user licensing, TDM, Mobility and Deskshare users can also be licensed with IP user licenses. If all the acquired TDM, DeskShare and Mobility user licenses have already been assigned to subscribers, and further TDM, DeskShare and Mobility users are required, then any remaining IP User licenses can be used to meet this demand.

The use of flexible user licensing requires the software version V1R3.3 and a newly generated license file at the CLS, which must be imported into the OpenScape Business and activated.

UC-Suite Flexible User Licensing

With the UC-Suite flexible user licensing, myPortal for Desktop users can also be licensed with myPortal for Outlook user licenses. If all the acquired myPortal for Desktop licenses have already been assigned, and further users are required, then the myPortal for Outlook User licenses can be used to meet this demand.

The use of flexible user licensing requires the software version V2 and a newly generated license file at the CLS, which must be imported into the OpenScape Business and activated.

Related Topics

- Assigning Licenses (Standalone)

4.2.3 User-oriented Licenses

User-oriented licenses are station-based and authorize the use of unified communications features and data integration applications. A user-oriented license also requires a station license and is permanently assigned to the phone number of the subscriber.

The following user-oriented licenses are available:

Voicemail

- **Voicemail**
  For the use of a personal voicemail box via the telephone (TUI) and via the user interface of the UC solutions UC Smart or UC Suite.

  INFO: If the UC solution UC Smart is expanded to UC Suite, the existing voicemail licenses and the assignments to the stations are retained.

UC Client User Interface

- **UC Smart User**
  For the use of UC Smart functions of the communication clients myPortal Smart, myPortal to go,myPortal for OpenStage and other Web Services clients.
- **UC Suite User**
  For the use of UC Suite functions of the communications clients myPortal for Desktop, myPortal to go, myPortal for OpenStage and other Web Services clients.
- **Groupware user**
  For the use of UC Suite functions of the communications clients myPortal for Outlook, myPortal to go, myPortal for OpenStage and other Web Services clients.
- **Fax**
  For use of a fax box within the UC Suite. As a prerequisite, one UC Suite User or Groupware User license is required additionally.
- **Conference**
  For the use of the UC Suite conference management features, such as managing and initiating permanent and recurring conferences. As a prerequisite, one UC Suite User license or Groupware User license is required additionally.
  No license is required for participating in conferences.
- **myAttendant**
  For use of the UC Suite Attendant features.
- **myAgent**
  For the use of Contact Center functions such as information about queues, pop-ups with customer information on incoming calls, and access to the call history.
- **Upgrade from myPortal Smart to myPortal for Desktop**
  For upgrading the UC Client myPortal Smart to the UC Client myPortal for Desktop in order to use the full UC functionality such as conferencing and fax, for example.

> ***INFO:*** For the mobile client myPortal to go, besides the Mobility User license, an additional UC Smart User license is required for the UC solution UC Smart, and an additional UC Suite User license or Groupware User license is required for the UC solution UC Suite.

Data Integration

- **Application Launcher**
  For call-related control of applications on a client PC during incoming and outgoing calls, e.g., launching an application or displaying caller information. Application Launcher can be operated with UC Smart or UC Suite and additionally requires a UC Smart User license (for UC Smart) or a UC Suite User / Groupware User license (for UC Suite). It can optionally use the Open Directory Service.

- **OpenScape Business TAPI**
  For the use of TAPI compliant applications and for PC-supported telephony with the customer's own applications from various software vendors. The UC Booster (UC Booster Card or UC Booster Server) is a prerequisite.

4.2.4 System Licenses

System licenses are not subscriber-specific and unlock the system-wide features. These features can be used by all subscribers of the communication system.

The following system licenses are available:

System Resources

- **S_{2M}/T1/SIP trunks**
  For the use of S_{2M}/T1 and ITSP channels. S_0 channels do not need to be licensed. This also includes connections to S_0 Fax servers in PP mode. For the primary multiplex connections S_{2M} or T1 (USA), the individual voice channels are licensed. For ITSP connections, the number of simultaneous connections to one or more ITSP providers (SIP providers) is licensed. The number of possible simultaneous connections depends on the bandwidth of the connection.
- **Networking**
  For IP networking via SIP-Q/native SIP and/or TDM networking via CorNet-NQ or QSIG. For networking the UC Suite applications. One license is required per node.

> ***INFO:*** The networking license unlocks the lines for voice networking and UC Suite networking for a node. No S 2_M/T1/SIP trunk licenses are required for network trunks.

Table: Overview of System Resource Licenses (S2M/ITSP)

Protocol	Licenses			
	No licence	**OSBiz Networking (1x per system)**	**OSBiz S2M / ITSP (1x per channel)**	**TDM User**
S0 internal				
Fax Server (DSS1/QSIG)	X			
Euro bus				per S0 station
S0 - CO trunks				
EURO CO PP	X			
Euro CO PMP	X			
S2M - CO trunks				
EURO CO PP			X	
ITSP - Provider				

Protocol	Licenses			
	No licence	OSBiz Networking (1x per system)	OSBiz S2M / ITSP (1x per channel)	TDM User
ITSP 1 to 8			X	
S0 networking				
QSIG		X		
CorNet-NQ		X		
S2M - Networking				
QSIG-Network		X		
CorNet-NQ		X		
SIP Networking				
SIP-Q		X		
native SIP		X		

Xpressions Compact

- **Xpressions Compact Announcement**
  For the use of Xpressions Compact Announcements features such as recording special announcements for information or attendant mailboxes. One license is required per Xpressions Compact.
- **Xpressions Compact Conferencing**
  For the use of Xpressions Compact Conference features such as managing and conducting conferences and controlling conferences through a web client. Six licenses can be purchased per Xpressions Compact.
- **Xpressions Compact Mobility**
  For the use of Xpressions Compact Mobility features such as the One Number Service (which enables a subscriber to be reached via a single phone number for all calls on all phones associated with that subscriber). Six licenses can be purchased per Xpressions Compact.

Contact Center Options

- **Contact Center Mail**
  For setting up one or more email boxes to send and receive emails for Contact Center agents. A station license and a myAgent license are required for this. One license is required per node.
- **Contact Center Fax**
  For setting up one or more fax boxes to send and receive faxes for Contact Center agents. A station license and a myAgent license are required for this. One license is required per node.
- **myReports**
  For the compilation of statistics on the utilization of Contact Center resources based on different criteria. Using the Schedule Manager, reports can be created from over 100 predefined report templates for telephone, email and fax contacts. The report templates are managed via the Report Manager, with

functions for regrouping as well as adding and deleting newly created report templates.

UC Client Options

- **Open Directory Connector**
  For connecting to the Open Directory Service (ODS) in order to enable access to an external database or an external directory A maximum of four databases can be connected per node.
- **Company AutoAttendant**
  For the use of a central UC Smart or UC Suite based AutoAttendant to automatically transfer calls. One license is required per node.
  Announcements of the type "music on hold" (endless loop) are only played with this license.
- **Gate View cameras**
  For video surveillance, which provides real-time video images on your OpenStage phone, PC or smartphone. A separate license is required for each of the eight possible cameras within a node.
- **OpenScape Business Attendant**
  For using the OpenScape Business Attendant (PC attendant). Up to 8 OpenScape Business Attendants may be licensed per node.
  If OpenScape Business Attendant should also have access to presence information, a UC Smart or UC Suite User license is additionally required.
- **OpenScape Business BLF**
  For use of the additional Busy Lamp Field indicator of OpenScape Business BLF. For each subscriber, one BLF license and one UC Smart or UC Suite User license is required. Up to 50 OpenScape Business BLFs may be licensed per node.

4.2.5 Evaluation Licenses

An evaluation license can be used to test special features with full functionality over a fixed time period (called the evaluation period) free of charge. If a regular license for the feature is activated during the evaluation period, the evaluation license will be disabled.

The following evaluation licenses are available:

- **OpenScape Business V2 Service Evaluation**
  This evaluation license is intended for partners who want to first preconfigure the communication system in their own company and put it into service at the customer site later. The 30-day activation period begins during the preconfiguration. In order to restart the activation period of 30 days after commissioning the system, this evaluation license must be activated from the customer site after starting up the system.
  The activation is possible once per system and only within the activation period. If the activation period has expired, the system must be licensed with permanent licenses.

- **OpenScape Business V2 UC Smart Evaluation**
  This evaluation license is intended for customers who want to test the UC features of UC Smart. All UC Smart features can be used with this evaluation license.

  INFO: This evaluation license cannot be used if the communication system is located in an internetwork and the "Networking" license is active. If voicemail licenses are already available, they are used in combination with the new UC evaluation licenses.

- **OpenScape UC Suite V2 Business Evaluation**
  This evaluation license is intended for customers who want to test the UC features of UC Suite. All UC Suite features can be used with this evaluation license.

  INFO: This evaluation license cannot be used if the communication system is located in an internetwork and the "Networking" license is active. If voicemail licenses are already available, they are used in combination with the new UC evaluation licenses.

- **OpenScape Business V2 UC Gate View Evaluation**
  This evaluation license is intended for customers who want to test the UC features of Gate View. All Gate View features can be used with this evaluation license.

  INFO: This evaluation license cannot be used if the communication system is located in an internetwork and the "Networking" license is active.

- **OpenScape Business V2 UC Suite Contact Center Evaluation**
  This evaluation license is intended for customers who want to test the Multimedia Contact Center. All features of the Multimedia Contact Centers can be used with the evaluation license.

  INFO: If the Multimedia Contact Center is not licensed within the evaluation period, the administrator must undo the Contact Center settings (e.g., delete schedules and queues, deactivate agents, etc.) before the evaluation license expires. Otherwise, errors may occur in OpenScape Business.

- **OpenScape Business V2 CRM Evaluation**
  This evaluation license is intended for customers who want to test Application Launcher, Open Directory Service and TAPI.
- **OpenScape Business V2 Attendant Evaluation**
  This evaluation license is intended for customers who want to test the OpenScape Business Attendant application.

- **OpenScape Business V2 BLF Evaluation**
  This evaluation license is intended for customers who want to test the OpenScape Business BLF application (e.g., to independently display the busy lamp field and presence information).

Rules

- The activation of an evaluation license occurs at the Customer License Server (CLS) and can only be performed once.
- The evaluation period is 90 days. After 60 days, the remaining time in days is counted backwards on the display of system telephones.
- When the evaluation period expires, the feature is automatically disabled.
- Multiple evaluation licenses may be active simultaneously in the system, but may then end at different times.
- If a perpetual license is active, the evaluation license is not started or, if already present, is stopped.

4.2.6 Upgrade Licenses

Upgrade licenses are required to upgrade HiPath 3000 V9, OpenScape Office V3 and OpenScape Business V1 systems to OpenScape Business V2 systems.

The license migration of HiPath 3000 systems requires a running and possibly licensed HiPath 3000 V9 system. The steps for the hardware and license migration must be carefully observed (see also the *Administrator Documentation, Migration*). Pure HiPath 3000 TDM systems without licenses must be first upgraded to Version 9 and can then be migrated to OpenScape Business with an upgrade license.

The following upgrade licenses are available:

- **HiPath 3000 V9 Upgrade to OpenScape Business V2**
  For the migration from HiPath 3000 V9 to OpenScape Business V2 X3/X5/X8.
- **HiPath 3000 V8 Upgrade to OpenScape Business V2**
  For the migration from HiPath 3000 V8 to HiPath 3000 V9 and then to OpenScape Business V2 X3/X5/X8.
- **HiPath 3000 V7 Upgrade to OpenScape Business V2**
  For the migration from HiPath 3000 V7 to HiPath 3000 V9 and then to OpenScape Business V2 X3/X5/X8.
- **OpenScape Office V3 MX/LX Upgrade to OpenScape Business V2**
  For the migration from OpenScape Office V3 MX/LX to OpenScape Business V2.

4.2.7 Possible License Combinations

The licenses can be combined as desired. This section contains some suggestions for possible license combinations that will allow you to use the desired functions.

Please note that multiple licenses are required for some functions.

Telephony

- Required: IP User, TDM User or DeskShare User station license

  INFO: Without a valid license, the phone can only be used for internal connections.

Telephony with UC Smart

- Telephony with voicemail box (UC Smart)
  - Required: IP User, TDM User or DeskShare User station license
  - Required: user-oriented VoiceMail license

- Telephony with Mobility Entry (DISA-based mobility)
  - Required: Mobility User station license

- Telephony with myPortal Smart
  - Required: IP User, TDM User or DeskShare User station license
  - Required: user-oriented UC Smart User license
  - Optional: user-oriented VoiceMail license

- Telephony with myPortal to go
  - Required: Mobility User station license
    No Mobility User license is required in the **Desk phone** (control of the Office telephone) mode.
  - Required: user-oriented UC Smart User license
  - Optional: user-oriented VoiceMail license

- Telephony with optiClient Attendant
  - Required: IP User, TDM User or DeskShare User station license
  - Required: OpenScape Business Attendant system license
  - Optional: user-oriented VoiceMail license
  - Optional: user-oriented UC Smart User license (for displaying the presence status)

Telephony with UC Suite

- Telephony with voicemail box (UC suite)
  - Required: IP User, TDM User or DeskShare User station license
  - Required: user-oriented VoiceMail license

- Telephony with myPortal for Desktop
  - Required: IP User, TDM User or DeskShare User station license

  - Required: user-oriented UC Suite User license
  - Optional: user-oriented VoiceMail license
  - Optional: user-oriented Fax license
  - Optional: user-oriented Conference license

- Telephony with myPortal for Outlook
  - Required: IP User, TDM User or DeskShare User station license
  - Required: user-oriented Groupware User license
  - Optional: user-oriented VoiceMail license
  - Optional: user-oriented Fax license
  - Optional: user-oriented Conference license

- Telephony with myPortal to go
  - Required: Mobility User station license
    No Mobility User license is required in the **Desk phone** (control of the Office telephone) mode.
  - Required: user-oriented UC Smart User license
  - Optional: user-oriented VoiceMail license

- Telephony with myAttendant
  - Required: IP User, TDM User or DeskShare User station license
  - Required: user-oriented myAttendant license
  - Optional: user-oriented VoiceMail license

Using the Contact Center

- Required: IP User, TDM User, DeskShare User or Mobility User station license
- Required: user-oriented myAgent license
- Optional: Contact Center Email system license
- Optional: Contact Center Fax system license
- Optional: myReports system license

Using the Company AutoAttendant

- Required: Company AutoAttendant system license

4.3 Licensing a Communication System (Standalone)

The licensing of a standalone system must be performed in a specific order. This order is given in our example for one of the OpenScape Business X communication systems.

The following subsections describe how Step 3 and Step 4 can be performed using the WBM.

1. **License Authorization Code (LAC)**
   On purchasing licenses, the customer receives a License Authorization Code (LAC). The information on the licenses purchased are stored in the database of the Central License Server (CLS).
2. **Installation and Configuration**
   The customer or service technician uses the WBM wizard to install and configure the communication system (including the stations and lines). When you first launch the WBM, you must enter the current date. This starts the activation period (i.e., the period of 30 days during which the licensing has to be completed).
3. **License Activation**
   The customer or service technician uses the WBM to activate the licenses either online using a License Authorization Code (online license activation) or offline using a license file (offline license activation).
4. **Assigning Licenses**
   The customer or service technician uses the WBM to assign the purchased licenses to stations and lines. Once the licenses have been assigned successfully, the licensed features are activated.

Related Topics

- Activating Licenses (Standalone)
- Assigning Licenses (Standalone)

4.3.1 Activating Licenses (Standalone)

After purchasing a product or feature, you must first activate the licenses provided with the product or feature. After successful activation of the licenses, the licenses are assigned.

Licenses can be activated by one of the following two methods:

- **Online license activation** (via the license authorization code)
  Using the WBM, the customer or service technician transmits the license authorization code to the Central License Server (CLS) via the Internet. Together with the LAC, the Locking ID of the communication system is used for license activation. The CLS creates a license file from the data and sends this back to the system, which then activates the licenses purchased.
  To access the CLS, you will need an Internet connection. The IP address of the CLS is saved in the WBM under **License Management > Settings** and can be changed by an administrator with the **Expert** profile if required.

  INFO: By default, port 7790 is used for the online license activation. This port must be enabled in the firewall of the customer network.

> ***INFO:*** Before the online licensing can be performed, the registration data must first be entered correctly.

- **Offline license activation** (using the license file)
  The customer or service technician logs in at the Central License Server (CLS) and enters the license authorization code there along with the Locking ID of the communication system. The CLS generates a license file from the data entered. The customer or service technician downloads the license file and copies it into the WBM. The system then actives the purchased licenses.
  The IP address of the CLS is saved in the WBM under **License Management > Settings** and can be changed by an administrator with the **Expert** profile if required.

If the communication system is to be expanded, further licenses can be purchased. On purchasing more licenses, an additional License Authorization Code (LAC) with which the newly procured licenses can be activated is supplied.

> ***INFO:*** Additionally purchased licenses can also be activated remotely.

Related Topics

- Assigning Licenses (Standalone)
- Licensing a Communication System (Standalone)

4.3.2 Assigning Licenses (Standalone)

Once the purchased licenses have been activated successfully, they must be assigned to the stations and lines. In a standalone system, system-wide features are enabled automatically upon activation.

Assigning Station Licenses and User-oriented Licenses

Subscribers can be assigned station licenses and user-oriented licenses.

Station licenses can be assigned to the following subscriber types:

Icon	Station license	Description
	IP stations	For the use of IP system telephones (HFA or SIP) and SIP telephones
	TDM stations	For the use of UP0 system phones, ISDN phones, analog phones and DECT phones
	Mobile stations	For the use of myPortal to go, Mobility Entry and DISA (One Number Service)
	DeskSharing stations	For the use of Desk Sharing by IP stations

The station licenses are permanently assigned to the numbers of the subscribers. If a subscriber is deleted or if another subscriber type is assigned to a call number, the associated station license is released.

With the flexible licensing, TDM, Mobility and Deskshare users can also be licensed with IP user licenses. If all the acquired TDM, DeskShare and Mobility user licenses have already been assigned to subscribers, and further TDM, DeskShare and Mobility users are required, then any remaining IP User licenses can be used to meet this demand.

After a station license has been assigned to the subscriber, a user-oriented license can also be assigned to that subscriber.

The following user-oriented licenses can be assigned to the stations:

Icon	User-oriented license	Description
	Voicemail	For the use of the voicemail box.
	UC Smart	For the use of the UC Smart features via myPortal Smart.
	Groupware user	For the use of the UC Suite features via myPortal for Outlook.
	UC Suite	For the use of the UC Suite features via myPortal for Desktop.
	Fax	For use of a fax box within the UC Suite. As a prerequisite, one UC User or Groupware User license is required.

Icon	User-oriented license	Description
	Conference	For use of the UC Suite conference features. As a prerequisite, one UC User or Groupware User license is required.
	myAttendant	For use of the UC Suite Attendant features.
	myAgent	For the use of Contact Center functions.
	Application Launcher	For call-related control of applications on a client PC during incoming and outgoing calls, e.g., launching an application or displaying caller information.
	TAPI 120/170	For the use of TAPI compliant applications and for PC-supported telephony with the customer's own applications from various software vendors.

You can have an overview of all station licenses and user-oriented licenses displayed (via **Local User Licenses > Overview)**.

This overview also shows the statuses of the licenses for each subscriber.

Possible license states:

Symbol	Explanation
	Successfully licensed.
	Unsaved license release.
	Not licensed
	Unsaved license demand release.
	License demand configurable.
	Unsaved license demand.
	License demand not configurable.

Assigning System Licenses

System licenses include licenses for trunks and for system-wide features.

Licenses can be assigned to the following types of trunks:

- S_{2M}/T1 trunks: number of B channels
- ITSP trunks: number of simultaneous calls conducted via a single ITSP

In a standalone system, licenses for system-wide features will have already been unlocked by default during the license activation. Consequently, no further assignment is required.

License assignment procedure

Prerequisite: The license file is activated and the stations are configured.

- How to License Stations

  a) Assign a station license to a subscriber. This assignment triggers the generation of a license request for the subscriber while at the same time enabling the assignment of the user-oriented licenses.

  b) Assign the user-oriented licenses to a subscriber. These assignments cause further license requests to be generated for the subscriber. Please note that some licenses require other licenses (see *Possible License Combinations*).

  c) Check and unlock license requests.

  d) If there are not enough licenses to be unlocked, the invalid assignments will be displayed via the license statuses (in red). Correct the license assignments and then check and unlock the licenses again.

  INFO: To obtain a better overview, you can have the license assignments for all subscribers printed out as a preview (via **Local User Licenses > Overview > Print**). At the end of the printout, all invalid assignments are listed in a separate table.

- Assign trunk licenses
  The trunk licenses must be distributed to the required S_{2M}/T1 and ITSP trunks.

Related Topics

- Licensing a Communication System (Standalone)
- Activating Licenses (Standalone)
- Station Licenses

4.4 Licensing Multiple Communication Systems (Internetwork)

The licensing of a multiple communication systems must be performed in a specific sequence. This sequence is shown below for a sample internetwork consisting of one OpenScape Business S (master) and two OpenScape Business X3 (slave) systems.

When multiple OpenScape Business (nodes) systems are combined into an internetwork, licensing occurs centrally via a network license file, which is activated on the master node. In addition, each slave node in the internetwork needs its own networking system license. The node with the largest bandwidth should be the master node.

The nodes in the internetwork are configured as a master node and slave nodes via the Network Wizard of the WBM. The master node contains the central license agent (central CLA; central Customer License Agent). All slave nodes in the internetwork use this CLA for the licensing. To enable this, the IP address of the master node must be made known to the slave nodes using the WBM.

Only one network license file exists for the entire internetwork. This file is bound to the master node via the node's locking ID. If an OpenScape Business S (SoftSwitch) is the master node, the network license file is bound to the master node via either the Locking ID of the Linux server of the SoftSwitch or the Advanced Locking ID of the SoftSwitch if the SoftSwitch is used in a virtual environment. The network license file is stored in the central CLA and contains all the license information of the internetwork. It can be activated only at the master node via the WBM. Only the master node has access to the CLS; at all other nodes, the access is disabled.

No node-specific licensing should be performed in the internetwork. If separate network files exist for each node, you can combine them into a network license file at the CLS.

Behavior during Network Problems (Failover)

If the connection to the master node and thus to the central CLA fails, the message "Failover Period" appears on the displays of the system telephones. During this failover period (max. 30 days), all nodes and their features continue to operate normally. Once the network problems have been resolved and the connection to the central CLA is restored, all nodes revert to the regular license status.

If the network problems cannot be resolved within the failover period, the nodes switch to operating in emergency mode. The entire internetwork will then need to be relicensed.

Licensing Procedure in the Internetwork Based on the Above Example

OpenScape Business S (Master) and both OpenScape Business X3 (Slave) systems are already installed, configured and combined to form an internetwork.

1. **License Authorization Code (LAC)**
   On purchasing licenses, the customer receives a License Authorization Code (LAC). The information on the licenses purchased are stored in the database of the Central License Server (CLS).
2. **OpenScape Business S as master node**
   The customer or service technician logs into the WBM of the OpenScape Business S and installs the OpenScape Business S as the master node by using the Network Wizard.
   For a description, see *Administrator Documentation, Networking*
   The system has already been installed and configured and is running in the Activation Period (period of 30 days during which the licensing has to be completed).
3. **Locking ID of the master node**
   The customer or service technician notes the Locking ID or the Advanced Locking ID of the OpenScape Business S.
   For a description, see *Administrator Documentation, Networking*
4. **OpenScape Business X3 as slave nodes**
   The customer or service technician first logs into the WBM of the first OpenScape Business X3 and installs the first OpenScape Business X3 as a

slave node by using the Network Wizard. This process is then repeated at the WBM of the second OpenScape Business X3.
For a description, see *Administrator Documentation, Networking*
The systems have been installed and configured and are running in the Activation Period.

5. **Locking IDs of OpenScape Business X3**
   The customer or service technician notes the Locking IDs of the two OpenScape Business X3 systems.
   For a description, see *Administrator Documentation, Networking*
6. **License Activation**
   The customer or service technician logs in at the CLS and generates a network license file together with the license authorization code and the locking IDs. He or she then loads this file into the master node using the WBM.
   For a description, see *Administrator Documentation, Licensing*
   The system then actives the purchased licenses.
7. **Assigning Licenses**
   The customer or service technician now distributes the licenses to the nodes. To do this, he or she logs into the WBM of each node and assigns the desired number of licenses to the node. Note that it is important that each node be assigned a networking system license; otherwise, it will not be integrated into the internetwork.
   For a description, see *Administrator Documentation, Licensing*

4.4.1 License Activation (Internetwork)

After purchasing a product or feature, you must first activate the licenses provided with the product or feature. A license file is is used for license activation. After successful activation of the licenses, the licenses are assigned.

Licenses can be activated as follows:

- **Offline license activation** (using the license file)
  The customer or service technician logs in at the Central License Server (CLS) and enters the license authorization code there along with the Locking IDs of the communication systems. The CLS generates a license file from the data entered. The customer or service technician downloads the license file and copies it into the WBM of the master node.
  The master node is checked to see whether the Locking IDs stored in the license file match those of the systems. If the check is successful, the licenses are activated, and the systems switch to the regular license status. If the check is not successful, the systems continue to run in the activation period until it expires and then only in emergency mode.
  The IP address of the CLS is saved in the WBM under **License Management > Settings**.

License files can be combined as follows:

- **How to Combine License Files into a Network License File**
  If one or more nodes that have already been licensed are to be combined into an internetwork, the administrator must combine the individual license files

via the CLS into a single license file and load it into the central CLA. The IP address of the master node with the central license agent must then be entered at all other nodes by using the WBM's network wizard.

4.4.2 Assigning Licenses (Internetwork)

Once the purchased licenses have been activated successfully, they must be assigned to the stations and lines. License assignment must be performed separately on each node.

Assigning Station Licenses and User-oriented Licenses

Subscribers can be assigned station licenses and user-oriented licenses.

Station licenses can be assigned to the following subscriber types:

Icon	Station license	Description
	IP stations	For the use of IP system telephones (HFA or SIP) and SIP telephones
	TDM stations	For the use of UP0 system phones, ISDN phones, analog phones and DECT phones
	Mobile stations	For the use of myPortal to go, Mobility Entry and DISA (One Number Service)
	DeskSharing stations	For the use of Desk Sharing by IP stations

The station licenses are permanently assigned to the numbers of the subscribers. If a subscriber is deleted or if another subscriber type is assigned to a call number, the associated station license is released.

With the flexible licensing, TDM, Mobility and Deskshare users can also be licensed with IP user licenses. If all the acquired TDM, DeskShare and Mobility user licenses have already been assigned to subscribers, and further TDM, DeskShare and Mobility users are required, then any remaining IP User licenses can be used to meet this demand.

After a station license has been assigned to the subscriber, a user-oriented license can also be assigned to that subscriber.

The following user-oriented licenses can be assigned to the stations:

Icon	User-oriented license	Description
	Voicemail	For the use of the voicemail box.
	UC Smart	For the use of the UC Smart features via myPortal Smart.
	Groupware user	For the use of the UC Suite features via myPortal for Outlook.
	UC Suite	For the use of the UC Suite features via myPortal for Desktop.
	Fax	For use of a fax box within the UC Suite. As a prerequisite, one UC User or Groupware User license is required.
	Conference	For use of the UC Suite conference features. As a prerequisite, one UC User or Groupware User license is required.
	myAttendant	For use of the UC Suite Attendant features.
	myAgent	For the use of Contact Center functions.
	Application Launcher	For call-related control of applications on a client PC during incoming and outgoing calls, e.g., launching an application or displaying caller information.
	TAPI 120/170	For the use of TAPI compliant applications and for PC-supported telephony with the customer's own applications from various software vendors.

You can have an overview of all station licenses and user-oriented licenses displayed (via **Local User Licenses > Overview)**.

This overview also shows the statuses of the licenses for each subscriber.

Possible license states:

Symbol	Explanation
	Successfully licensed.
	Unsaved license release.
	Not licensed

Symbol	Explanation
	Unsaved license demand release.
	License demand configurable.
	Unsaved license demand.
	License demand not configurable.

Assigning System Licenses

System licenses include licenses for trunks and for system-wide features.

Licenses can be assigned to the following types of trunks:

- S_{2M}/T1 trunks: number of B channels
- ITSP trunks: number of simultaneous calls conducted via a single ITSP

System-wide licenses are assigned to every system (node) in the network. This configuration must be performed in direct succession (i.e., one after the other) at each node. The total number of system-wide licenses stored in the network license file on the master node is reduced by the number configured at the node.

License assignment procedure

Prerequisite: The license file is activated and the stations are configured.

- How to License Stations

  a) Assign a station license to a subscriber. This assignment triggers the generation of a license request for the subscriber while at the same time enabling the assignment of the user-oriented licenses.

  b) Assign the user-oriented licenses to a subscriber. These assignments cause further license requests to be generated for the subscriber. Please note that some licenses require other licenses (see *Possible License Combinations*).

  c) Check and unlock license requests.

  d) If there are not enough licenses to be unlocked, the invalid assignments will be displayed via the license statuses (in red). Correct the license assignments and then check and unlock the licenses again.

  INFO: To obtain a better overview, you can have the license assignments for all subscribers printed out as a preview (via **Local User Licenses > Overview > Print**). At the end of the printout, all invalid assignments are listed in a separate table.

- Assign trunk licenses
  The trunk licenses must be distributed to the required S_{2M}/T1 and ITSP trunks.

4.5 License information

Information on the available and assigned licenses, products and features is displayed with the WBM. The license information on all nodes available in the internetwork can be retrieved.

The following information can be displayed:

- **MAC Address**: MAC address of the hardware platform or the Linux Server SoftSwitch to which the licenses are bound.

  INFO: If the communication system is in the activation period, a wrong MAC address may possibly be shown here. The correct MAC address can be checked via the Service Center under Inventory (*Inventory*).

- **Advanced Locking ID**: Advanced Locking ID of the softswitches in a virtual environment, to which the licenses are bound.
- **Locking ID**: Locking ID of the Application Server to which the licenses are bound.
- **Node**: Name of the communication system to which the license is bound.
- **Product Name**: Name of the product for which the license is assigned.
- **Feature**: Feature for which the license has been assigned.
- **Used licenses**: Shows the number of used and available licenses.
- **Available for distribution**: Shows the licenses still available in the internetwork.
- **Status**: Status of the license.

The OpenScape Personal Edition product is licensed by its own license file. The license information for this is displayed under **Additional Products**.

4.5.1 License Information without a Network (Standalone)

All licenses assigned to the communication system and the relevant licensing information can be displayed.

4.5.2 License Information in an Internetwork

In an internetwork, all existing licenses and the relevant license information can be displayed. This information is read from the network license file.

All licenses of an internetwork (with the exception of the base licenses) are "floating" licenses and are managed in a license pool. If a license is no longer required by a node (communication system), it is released and can thus be used another node.

All the licenses of the internetwork as well as any shared (floating) licenses or licenses that are bound to a specific node can be displayed in an internetwork.

In addition, station licenses and user-oriented licenses can be sorted by node and displayed in a list.

4.6 Assigning License Profiles

License profiles contain predefined license assignments and can be assigned to one or more stations. License profiles are useful if more than one subscriber is to receive same license.

You can use predefined license profiles or create new license profiles.

A license profile only applies to one station type and can only be assigned to stations of this type. Several license profiles can be created and named appropriately for a station type.

License profiles can be created for the following types of stations:

- IP stations (IP system phones, SIP phones)
- TDM stations (UP0 phones, ISDN phones, analog phones, DECT phones)
- DeskSharing stations
- Mobile stations

Within a license profile, you can assign assign user-oriented licenses to the station type as needed.

If the license assignment for a station within a license profile is changed, the assignment of the station to the license profile is automatically revoked.

4.7 Rehosting after Replacement of Hardware

Licenses must be updated whenever the mainboard of the hardware platform or the network card of the Linux server is replaced at the communication system. Rehosting requires the MAC address of the old hardware, the MAC address of the new hardware and the login credentials for the central license server (CLS).

After replacing the hardware, the configuration data must be restored using the latest backup set (see *Restore*).

Since the licenses are bound to the MAC address of the hardware, the MAC address changes on replacing the hardware, and the licenses are thus are no longer valid. After a hardware replacement, the communication system reverts to the activation period. After the old and new MAC addresses have been entered at the CLS, the new license file can be generated. This is loaded into the communication system through via an offline update, and all existing licenses are then activated automatically. When a system is identified as re-hosted all licenses expire and an indication is available in the notification area of the landing page of WBM.

For the softswitch, the MAC address of the network card of the Linux server, which was selected on installing the Linux operating system (visible via YaST), is used. The MAC address can also be read by using the WBM.

INFO: Every rehost is logged on the CLS. A license can be used for a rehost up to three times.

INFO: The IP address of the CLS can be checked via the WBM under **License Management > Settings** and changed if required.

4.8 License Server (Central License Server, CLS)

The Central License Server (CLS) generates and manages the license files.

A license file is generated when the customer sends the License Authorization Code (LAC) to the CLS via the WBM. The transmission of the license file to the communication system occurs automatically via the Internet. If an automatic transmission is not possible, the license file can also be loaded manually into the communication system.

4.9 Customer License Agent (CLA)

The Customer License Agent (CLA) is part of the OpenScape Business communication software and runs automatically in the background. It manages the license file and the licenses contained therein. The CLA checks the license requirements, and if sufficient licenses are available, it activates the licenses. There is only one CLA (local CLA) for each communication system. If several communication systems (nodes) are present in one internetwork, only one CLA (central CLA) should be used on the master node.

The following configurations are possible:

- **How to Configure the Connection to the Local License Agent**
  When a node is removed from the internetwork, the connection to the central CLA will be cleared. The local CLA installed on the node is used automatically instead. If this automatic mechanism fails, the connection to the local CLA can also be made manually.
- **How to Change the Connection to the Central License Agent**
  Every node in the internetwork requires the connection to the Central CLA on the master node. This connection is automatically established on running the WBM wizard **Network**. If the IP address of the master node changes, the connection to the central CLA must be reconfigured at all slave nodes.

4.10 Locking ID and Advanced ID Locking

Each communication system is assigned a Locking ID or an Advanced Locking ID. To ensure a unique assignment of licenses, the licenses are tied to these Locking IDs.

Locking ID

With hardware platforms, the Locking ID is the MAC address of the communication system.

With softswitches, the Locking ID is the MAC address of the network card of the Linux server. If the Linux server has multiple network cards, the network card that was used at initial startup of the Linux server must be selected.

If the communication system is in the activation period, a wrong MAC address may possibly be shown under the license information. The correct MAC address can be checked via the **Service Center** under **Inventory**.

Advanced Locking ID

If a softswitch runs in a virtual environment, the Advanced Locking ID (ALI) is used instead of the Locking ID. The Advanced Locking ID is generated at the CLS using the ALI Calculator.

The following system and network parameters must be configured, since they are used to generate the 24-digit Advanced Locking ID.

- IP address of the default gateway (Linux server)
- Host name of the Linux server
- IP address of the Linux server
- IP address of the DNS server (configured in the Linux server)
- Time zone (Linux server)

If one or more of these system and network parameters are not set, then the Advanced Locking ID cannot be generated.

The Advanced Locking ID is displayed in the WBM. In some cases, it is possible that the ALI which was generated at the CLS for the license file may differ from the ALI which is displayed during the activation period in the WBM. The license file containing the deviant ALI is accepted by the system anyway.

If any of the system and network parameters listed above changes, the softswitch reverts to the unlicensed state, and a new Advanced Locking ID is generated. In order to be able to use the purchased license again, a rehost from the old to the new Advanced Locking ID must be conducted at the Central License Server (CLS).

If the system detects a change in ALI, a message is displayed on the WBM home page in Licensing area to inform the user that ALI has been changed. The user has to click on Confirm, to verify for being informed about the change. Then the message is removed from the WBM home page, until a new instance of ALI change is detected. If the user does not click on Confirm, the message is permantly displayed on the home page.

IMPORTANT: If a user presses the confirm button, no email will be sent afterwards. An email will only be sent if the user hasn't confirmed the changes via Home page. Email mechanism is triggered every day with an 24h interval, starting from the last system restart.

5 Integration into the Internal Data Network (LAN)

The integration of the communication system in the existing internal network (LAN) enables the use of UC solutions and the administration of the communication system on PCs in the internal network.

The following network parameters must be set up in the WBM:

- OpenScape Business X hardware platform: IP address and network mask of the mainboard and the UC Booster Card (if present). These settings are made during the initial installation, but can be changed later.
  Softswitch OpenScape Business S: IP address and subnet mask of the Linux server on which the communication software is running. These settings are made during the Linux installation, but can be changed later.
- The communication system can be optionally set up as a DHCP server (supplied with network-specific parameters such as the subnet mask, default gateway, DNS server) or as a DHCP relay agent. The setup as a DHCP server is performed during the initial installation, but can be changed later. The setup as a DHCP relay agent is performed in Expert mode.
- IP address of the default router and the (external) DNS server for access to other IP networks (e.g., the Internet). These settings are made during the initial installation, but can be changed later.

5.1 LAN Interface

In order to integrate the communication system in the LAN infrastructure, the IP address and internal IP address range of the communication system must be adapted to the IP address scheme of the internal network (LAN).

5.1.1 IP Address and Subnet Mask of the LAN Interface

The IP address and the subnet netmask of the communication system are defined during the initial installation but can also be changed later. You may need to adapt the IP address and/or subnet mask to the IP address range of the LAN.

Hardware Platform

By default, the hardware platform is assigned an IP address and a subnet mask. The UC Booster Card also requires an IP address. The IP address of the UC Booster Card can be configured regardless of whether the UC Booster Card is installed or not.

The hardware platform uses the "LAN" interface of the mainboard for integration into the LAN. Whenever the UC Booster Card is installed, the "LAN" interface of the UC Booster Card must also be connected to the LAN. The hardware platform and UC Booster Card must be located in the same subnet.

To activate the changes to the IP address or subnet mask, a restart of the hardware platform is required.

The changes to the IP address and the subnet mask remain in effect after a software update, but will be reset to the default values in the event of a hardware platform reload. These changes cannot be stored in a backup set.

Softswitch

For a softswitch, the Linux server on which the communication software runs is integrated into the LAN via its network card.

The change of IP address or subnet mask takes effect after a restart of the application (see *Restart, Reload, Shutdown*).

5.1.2 Internal IP Address Range of the LAN Interface

The internal IP address range of the LAN interface that is used by the hardware platform for the internal communication of its modules can be changed if necessary.

The hardware platform uses the internal IP address range 192.168.3.xxx by default. This address range can also be edited and set to a desired IP address range. The internal subnet mask is 255.255.255.0 and cannot be changed.

To activate the changes to the internal IP address range, a restart of the hardware platform is required.

The changes to the internal IP address range remain in effect with a software update, but will be reset to the default values in the event of a reload. These changes cannot be stored in a backup set.

5.2 DHCP

DHCP (Dynamic Host Configuration Protocol) is a protocol that enables the dynamic allocation of network-specific data to the IP stations of a network (e.g., a LAN) with the aid of a DHCP server.

DHCP thus makes it possible to automatically integrate IP stations (e.g., IP phones or PCs) in an existing LAN. The IP station must be configured to automatically receive the network-specific data and is thus a DHCP client. The DHCP server provides the IP stations with the network-specific data on request.

5.2.1 DHCP Relay Agent

When using the internal DHCP server of the hardware platform, the internal DHCP server and the DHCP clients must be on the same network segment. If this is not the case, the hardware platform must be configured as a DHCP relay agent. The DHCP requests of the IP stations are then forwarded from the hardware platform to the actual DHCP server.

5.2.2 DHCP Server

The DHCP server assigns network-specific information such as the IP address and subnet mask of the IP station, the IP address of the default gateway, the IP address of the SNTP server, etc., dynamically to the IP stations (i.e., the IP phones, SIP phones, PCs, WLAN access points, and so on).

The internal DHCP server of the communication system or an external DHCP server can be used as DHCP server (e.g., the DHCP server of the Internet router).

In the hardware platform, the integrated DHCP server is enabled by default. If an external DHCP server is to be used, the internal DHCP server must be disabled. Otherwise, conflicts may arise with the external DHCP server.

For the softswitch, the Linux server can be configured as an internal DHCP server.

The decision as to whether the internal DHCP server of the communication system or an external DHCP server is to be used should be made during the initial startup. The internal DHCP server can also be enabled or disabled later. Even the network-specific data can be configured later.

Internal DHCP Server

If the internal DHCP server is used, the IP stations are automatically supplied with the following network-specific data:

- IP address and subnet mask of the IP station
- IP address of the communication system (default gateway)
- IP address of the SNTP server (to obtain the date and time)
- IP address of the DNS server (for name resolution)
- IP address of the SIP server (for the authentication of SIP stations)
- IP address of the internal DLI or the external DLS server (for the software update of the IP system phones)
- Routing rules

External DHCP Server

If an external DHCP server is used, it must support a vendor-specific option space to enable the provision of vendor-specific parameters. The following network-specific data should be entered in the external DHCP server:

- IP address and subnet mask of the IP station
- IP address of the default router = Option 3
- IP address of the communication system (default gateway) = Option 33
- IP address of DNS server (for name resolution) = Option 6
- IP address of the internal DLI or the external DLS server (for the software update of the IP system telephones) = Option 43
- Only for SIP phones: IP address of the SIP server (SIP registrar, for the authentication of SIP stations) = Option 120

- Only for SIP phones: IP address of the SNTP server (to supply the SIP phones with the date and time) = Option 42

> ***INFO:*** Additional information on DHCP server in a Windows environment can be found here: http://wiki.unify.com/wiki/DHCP_Server_in_a_Windows_environment.

If no such entries can be made at the external DHCP server, this data must be entered directly at the IP system phones. Only then can the IP system phones be automatically supplied with the current date and time and the latest software updates, for example.

For further information please refer to the following Unify Experts Wiki page under: http://wiki.unify.com/wiki/DHCP

DHCP Address Pool (IP Address Ranges)

Whenever an IP station logs in at the DHCP server, it receives, among other things, a dynamically assigned IP address. The administrator can optionally define an IP address range from which the DHCP server can assign IP addresses to the IP stations. In this case, for example, not all IP addresses from the range 192.168.1.xx are to be assigned, but only those from 192.168.1.50 to 192.168.1.254, since the lower IP addresses up to 192.168.1.49 are to be reserved for IP stations with static IP addresses.

In fact, even multiple IP address ranges can set up for the internal DHCP server under **Network Interfaces** in expert mode.

5.3 DNS - Name Resolution

The Domain Name Service (DNS) serves to the translate names to numerical addresses. This enables host names or domain names to be converted to IP addresses, and vice versa.

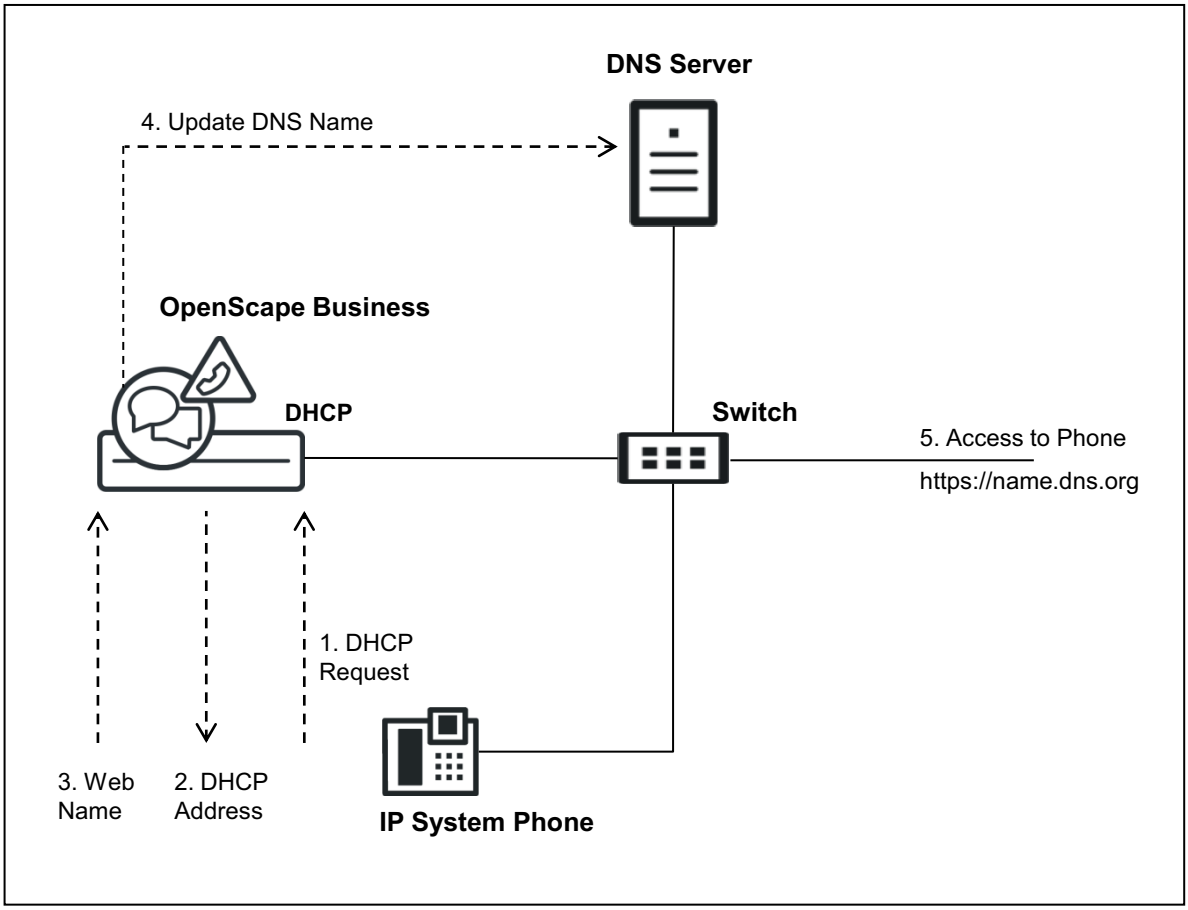
The DNS uses a hierarchical database that manages the Internet name space and is distributed over a collection of servers worldwide. This name space is divided into so-called zones (domains). Separate Internet-independent DNS servers are usually operated for local requirements – for example, within a corporate network.

Name Resolution for IP System Phones

The following prerequisites must be met:

- Windows 2008 DNS Server (with the current patch level and the "Allow unsafe update" setting enabled)
- The internal DHCP server is enabled
- The "Enable Dynamic DNS Update" functionality is activated in the internal DHCP server (see *DHCP Server*)
- The web name is entered in the IP system telephone.

The IP system telephone sends a DHCP request (1) and receives a valid IP address and other network-specific data (2) from the internal DHCP server. After receiving this data, the IP system telephone sends the set web name to the internal DHCP server (3), which then forwards the name automatically to the configured DNS server (4). The DNS server now knows the name associated with the IP address of the IP system telephone. The IP system telephone can now be accessed via the WBM by using its web name (5).



DNS Server

The DNS server, also called a name server, is a program that responds to requests about domain names or computer names. Even the PC on which this program runs can be designated as a DNS server.

For requests about a domain name or a host name, the DNS server returns the corresponding IP address.

Example: for `www.wikipedia.org`, DNS server on the Internet will return the IP address `91.198.174.2`.

If the preferred DNS server cannot answer a request, it forwards the request to another DNS server.

For a softswitch, the Linux server on which the communication software runs can be configured as a DNS server. The hardware platform cannot be used as a DNS

server. An external DNS server can be specified for both the softswitch as well as the hardware platform.

5.4 IP Routing

In data technology, IP routing describes the definition of paths (routes) for data streams within networks. IP routing is required when the sender and recipient are on different networks.

Default Router

To ensure that IP stations can also reach destinations outside their own networks that are not explicitly listed in a route table, a gateway must be specified for forwarding packets of this kind (default router). The default router will then redirect the data to the parent network.

You can enable or disable IP routing via a default router for both the mainboard and the Application Board.

Static Routes

Static routes are used to establish the path along which data will travel to a network that cannot be reached via the default router.

You can create static routes for both the mainboard and the Application Board.

5.5 Deployment Service (DLS and DLI)

DLI and DLS can be used to manage IP components centrally and to deploy their software. The DLI is integrated in the communication system. The DLS is a standalone application which must be installed on an external server PC.

DLI (Deployment Server Integrated)

The DLI is a component which is integrated in the communication system and provides limited DLS functionality. The internal DLI can be used to centrally configure all IP system phones connected to the communication system and to equip them with the latest phone software.

The internal DLI also works with the integrated FTP server on which the latest phone software is stored.

If the IP address of the DLI is known to the DHCP server, the DHCP server sends this data to the IP system telephone (HFA, SIP) as soon as the phone logs into the internal network. This enables the telephone to retrieve the current software from the FTP server of the communication system. The DLI is configured by default in the internal DHCP server. If an external DLS server is to be used instead, its IP address must be configured in the internal DHCP server.

DLS (Deployment Service)

The DLS is a client/server application for the central administration of the IP components. The DLS server is not integrated in the communication system and must be installed on a server PC. The DLS client runs on the IP components. Administration occurs via a web browser.

IP components can be IP system phones, SIP phones, SIP clients and IP gateways.

> ***INFO:*** The properties and features of the DLS can be found in the product description of the DLS and are not described in this documentation.

DLI or DLS with External DHCP Server

In order to ensure that the software of IP system telephones (HFA, SIP) can be updated automatically even when using an external DHCP server, you have the following alternatives:

- Configure the IP address of the DLI or DLS in the external DHCP server
  When using an external DHCP server, the network-specific data and the IP address of the external deployment server (DLI or external DLS server) must be entered. In addition, the latest phone software must be stored on the external DLS server.
- Configure all system phones
  The IP address of the deployment server must be entered as the DLS address for each IP system phone (IP address of the communication system for the internal DLI or IP address of the external DLS server).

Features and Restrictions

Function	DLI	DLS
Central configuration of the parameters of IP components The parameters of the IP components can be configured via customizable XML templates.	yes	yes
Plug&Play commissioning of the IP components Using a DHCP server, the IP components can log into the system automatically after being connected to the system for the first time or after an IP component is replaced, for example.	Yes	Yes
Central and automatic software update for IP components Whenever a new software version is available, the IP components are automatically supplied with the latest version of the software the first time the user logs on. The IP address of the DLI/DLS must be configured in the IP component.	Yes	Yes The latest phone software must be stored on the DLS.

Function	DLI	DLS
Centralized inventory management of IP components The data on the hardware configurations of the IP components can be accessed and retrieved centrally.	no	Yes
Support for IP Mobility (Desk Sharing) The telephony data of a user (e.g., program keys, directory entries, journals) is stored centrally and can be retrieved at other phones).	Yes Not for SIP phones, Not possible in the internetwork.	Yes Not for SIP phones, In homogeneous networks (only OpenScape Business systems), only with closed numbering, Not in heterogeneous networks (with OpenScape 4000 or OpenScape Voice).
SPE support in networks	SPE in networks is possible. DLS has to be used (no DLI).	SPE in networks is currently not possible because the SDES protocol has not been implemented. This applies regardless of whether the DLS is used.
Central supply for several different platforms	no	Yes
Activation of the 2nd LAN interface of IP system phones (PC Ethernet mode). See ***Expert Mode > Telephony Server > Basic Settings > Phone Parameter Deployment***	Yes	Yes

Deployment- und Licensing Client (DLSC)

To use DLS functions such as the element manager, for example, the communication system must allow the external DLS to access the configuration data. The communication system is then operated as Deployment and Licensing Client.

6 Connection to Service Provider

The communication system supports connection to public communication networks. The connection to the IP network provides access to the Internet and Internet telephony, ane the connection to the Central Office provides access to the ISDN network and the analog network.

Access to the Internet occurs via either an Internet modem or an Internet router.

ISDN trunk access for the hardware platforms occurs via the mainboard or additional plug-in boards. ISDN trunk access is not possible with the softswitch.

The analog trunk access for the hardware platforms requires an additional plug-in board. Analog trunk access is not possible with the softswitch.

6.1 Internet Access

A broadband connection (DSL or connection) is required for access to the Internet. This enables fast data transfers within the framework of the available bandwidth.

Internet Access via a DSL Connection

Conventional telephone lines are used for broadband Internet access via DSL (digital subscriber line). The Internet access can be used at the same time as the normal phone. Fax, analog phone or ISDN are also available during the DSL connection. This makes it possible to implement Internet access that is permanently available as in the case of a dedicated line (flat rate).

For Internet access via DSL, you need a modular jack (analog or ISDN) and an Internet Service Provider (ISP). The ISP provides a splitter and an Internet modem (DSL modem) or an Internet router with a built-in Internet modem. The splitter divides the signal into DSL and telephony parts and forwards the DSL signals to the Internet modem.

The communication system can be connected directly to the Internet modem or to the Internet router with an integrated Internet modem. In the first case, the access data of the ISP must be entered in the communication system; in the second, the Internet router must be made known to the communication system. The access data of the ISP is saved in the Internet router.

To use Internet telephony, you will also need an Internet Telephony Service Provider (ITSP, SIP provider).

Internet Access via a Cable Connection

The broadband connection to the Internet is implemented via the TV cable. In addition to transmitting TV signals, the TV cable connection can be used for accessing the Internet and making calls. This means you do not need a telephone line to surf and for telephony.

For Internet access via cable, you need a cable provider that offers this feature. The cable provider is also your Internet Service Provider (ISP). This cable

provider supplies you with a cable port with a back channel and a cable modem that transmits the data over the TV cable network. The cable port and the communication system are connected to the cable modem over Ethernet. Internet data filtration takes place directly in the cable modem.

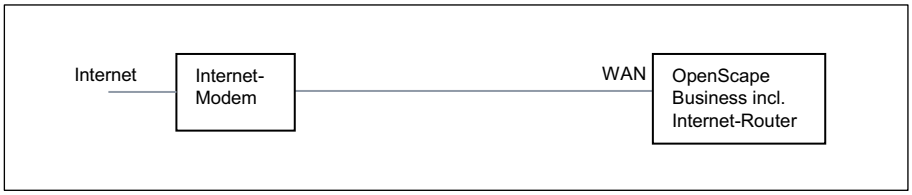
The communication system can be connected directly to the cable modem or to an Internet router that is connected to the cable modem. In both cases, the cable modem or the Internet router must be made known to the communication system.

To use Internet telephony, you will also need an Internet Telephony Service Provider (ITSP, SIP provider).

Configuring Internet Access

The configuration of Internet access in the WBM depends on whether the Internet connection has already been set up in an external router or whether it occurs via an Internet modem and thus needs to be set up in the WBM.

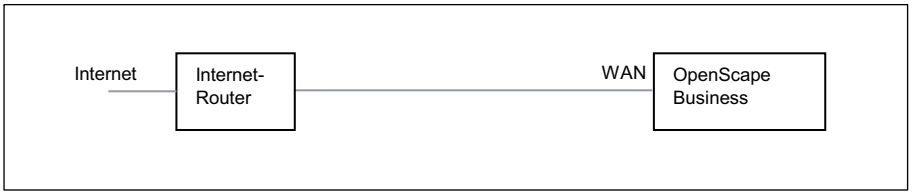
- **Internet access through an Internet modem** (**DSL at WAN port directly**)
  You want to operate the communication system directly at an Internet modem (DSL, cable, UMTS ...). OpenScape Business has the Internet router integrated. Enter the access data of the Internet Service Provider (ISP) directly in the communication system and use the WAN port of the communication system. This option is not available with the softswitch.



  You have the following options:
  - Internet access via a preconfigured ISP
  - Internet access via the standard ISP PPPoE
  - Internet access via the standard ISP PPTP

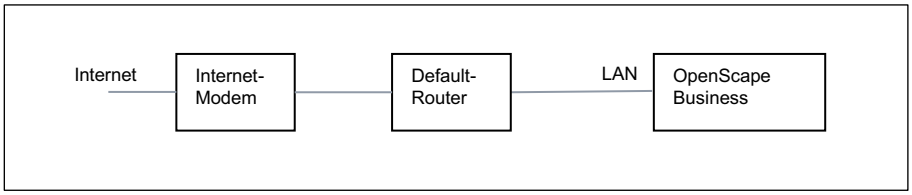
  If your ISP is not listed under the preconfigured ISPs, use the default ISP PPPoE or PPTP.

- **Internet access via an external Internet router**
  You want to operate the communication system at an external Internet router. The Internet Service Provider is already configured in the Internet router.
  You have the following options:
  - **Internet access via an external Internet router at the WAN port** (**TCP/IP at WAN port via an external router**)



    To do this, you use the WAN port of the communication system. OpenScape Business either knows the Internet router or works as a DHCP client. This option can be used if the Internet router is located in another network segment and has its own DHCP server.

– **Internet access via an external Internet router at the LAN port** (**TCP/IP at LAN port via an external router**)



To do this, you use the LAN port of the communication system. OpenScape Business knows only the default router and not the underlying infrastructure. To activate the connection to the Internet router, the IP address of the default router and that of the DNS server must be made known to the communication system.

- **Disable Internet access** (default setting)
  You do not want to use the Internet. Then leave the Internet access disabled.

6.1.1 Internet Access via an External Internet Router

The **Internet Configuration** wizard helps you configure your Internet access via an additional Internet router.

To set up Internet access, you have the following options:

- **Internet access via an external Internet router at the LAN port**
  To do this, you use the LAN port of the communication system. To activate the connection to the Internet router, the IP address of the default router and that of the DNS server must be made known to the communication system.
- **Internet access via an external Internet router at the WAN port**
  To do this, you use the WAN port of the communication system. This option can be used if the Internet router is located in another network segment and has its own DHCP server.

6.1.2 Internet Access via an Internet Modem

The **Internet Configuration** wizard helps you configure your Internet access via an Internet modem. An Internet modem is directly connected for this to the WAN port on your communication system. You can use an ISP that was preconfigured in the communication system or a standard ISP type (consult ISP for type).

To set up Internet access, you have the following options:

- **Setting up Internet Access via a Preconfigured ISP**
  You are using an ISP preconfigured in the communication system. You can then select your preconfigured ISP from a list.
- **Setting up Internet Access via the Standard ISP PPPoE**
  You are using the standard ISP type **Provider PPPoE**. Obtain the required settings from your ISP.

- **Setting up Internet Access via the Standard ISP PPTP**
  You are using the standard ISP type **Provider PPTP**. Obtain the required settings from your ISP.

Connection Clear-down Depending on the Tariff Model

Depending on the tariff model, you can define whether or not the connection to the ISP should be maintained in the event of inactivity.

- With the flat-rate tariff model, the Internet connection does not have to time out on inactivity. Many ISPs require forced timeout every 24 hours. You can enter the time when the connection should time out.
- With the time-based tariff model, the Internet connection should time out on inactivity. You can specify the inactivity timeout for connection clear-down (for instance, 60 seconds). The connection is automatically reestablished the next time an Internet request is made. If VPN is configured, the connection should not be cleared due to inactivity; the flat rate tariff model should hence be selected here.

> ***INFO:*** Network-based programs or services can automatically set up an Internet connection and thereby incur additional connection charges for you if your tariff is time-based.

Bandwidth

Different bandwidths for downloading and uploading are usually provided by the ISP. The bandwidth is specified in Kbps. If Internet telephony is also used, the bandwidth is shared by voice and data transmission. We therefore recommend reserving sufficient bandwidth to guarantee good voice quality during voice transmission. However, this can lead to data transfer bottlenecks (for example, slower downloads) during periods with a high volume of voice transmissions.

You can choose whether bandwidth control for voice connections should be enabled only for uploading for both uploading and downloading. If the download bandwidth is high and the upload bandwidth is low, bandwidth control should be enabled only for uploading to prevent an unnecessarily high amount of download bandwidth from being reserved for voice transmissions.

> ***INFO:*** About 128 Kbps of bandwidth is reserved for an Internet call.

6.1.3 WAN port

WANs (**W**ide **A**rea **N**etwork) are used to network different LANs (**L**ocal **A**rea **N**etwork) as well as individual PCs with one another. An Internet modem for access to the Internet can be connected to the WAN port.

The WAN port must not be used for the networking of network nodes and for connecting IP stations or IP clients.

6.1.4 DynDNS

DynDNS (Dynamic Domain Name Service) is an Internet service that assigns a fixed DNS name to an IP address that changes dynamically.

OpenScape Business X makes the DynDNS service available if an Internet modem is connected to the WAN port of OpenScape Business X and the communication system is used as an Internet router. If this is not the case, DynDNS is set up in the external Internet router in the infrastructure of the customer.

DNS Name

With DynDNS, a client who is connected to the Internet with a dynamic IP address can always be addressed with the same name, the DNS name. A DynDNS account with a DynDNS provider (such as www.dyndns.org) is needed for this. If the communication system is assigned a new IP address (for example, by the Internet Service Provider), this IP address is automatically sent to the DynDNS provider and saved in the DynDNS account. The refresh interval is adjustable. If a DNS name is addressed, a request is sent to the DynDNS provider to translate the name into the IP address currently valid. The entire DNS name (also known as the domain name) is composed of a host name of your choice (myhost, for instance) and the selected DynDNS provider (dyndns.org, for instance), producing, in this instance, myhost.dyndns.org. More information on this can, for example, be found at the Internet address:

`http://www.dyndns.org/services/dyndns`

DynDNS also lets you set up a virtual private network (VPN) over an Internet Service Provider that supplies dynamic IP addresses. This enables teleworkers, for example, to access the internal network via the Internet. More Information can be found under *Virtual Private Network (VPN)*.

Mail Exchanger

The Mail Exchange entry (MX record) in the Domain Name Service (DNS) specifies the IP address to which e-mails should be sent for the domain name configured (myhost.dyndns.org, for instance). The mail server (Mail Exchanger) must be located at the IP address specified. An e-mail address for this domain name could be as follows: mymail@myhost.dyndns.org.

The Backup MX function buffers e-mails that could not be delivered to the Mail Exchanger specified above (because of temporary unavailability, for instance) and delivers them as soon as Mail Exchanger availability is restored.

6.2 CO Access via ITSP

In order to make calls over the Internet, you will need access to an Internet Telephony Service Provider (ITSP, SIP Provider). To do this, an Internet telephony connection and a user account must be applied for from the ITSP.

Connection to the ITSP

The communication system uses the options described in the section on "Internet Access" to reach the ITSP (OpenScape Business X: via LAN or WAN / OpenScape Business S: exclusively via LAN).

The ITSP access based on SIP (Session Initiation Protocol) for signaling and RTP (Realtime Transport Protocol) for voice and data.

Internet Telephony Service Providers do not always offer the same range of SIP features. Consequently, only ITSPs certified for the communication system should be used. A list of certified ITSPs as well as the certification process can be found at the following link:

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

> ***INFO:*** Special numbers and emergency numbers, which are not supported by the ITSP, should be routed over fixed network connections.
>
> In the event of ITSP failure, fixed network connections via least cost routing (LCR) can be used as a fallback solution.

ITSP user account

The ITSP user account (SIP User Account) must be applied for from the ITSP. The ITSP provides a SIP Registrar server at which the communication system must first log in (provider-specific) for this purpose.

> ***INFO:*** A registration is not necessary if static IP authentication or a VPN tunnel is used by the ITSP.

Mobile Extension (MEX)

This feature is offered by some mobile phone operators in connection with the MDA (mobile direct access) service. It enables mobile phones/smartphones to be integrated as internal subscribers in a communication system.

This feature can only be used only with an Internet telephony DID connection. To do this, the MEX number provided by the ITSP must be entered when configuring the ITSP. At the ITSP, the call number of the mobile phone is associated with the MEX number. In addition, the mobile phone or smartphone must be configured in the communication system as a Mobility station (see *Configuring myPortal to go and Mobility Entry*).

Short Description:

- The mobile phone operator offers a flat-rate for the mobile phone.
- One Number Service: the mobile phone can be reached under a single fixed network number, which is also communicated to the other party.
- The presence status and connection status of mobile phones are visible exactly as for normal internal subscribers.

- Every phone call from or to the mobile phone is performed exclusively via OpenScape Business in combination with a certified ITSP.
- The mobile phone number of the mobile phone is not known to the outside, i.e., the mobile phone cannot be called directly. It can also not make any direct outbound calls. All calls are conducted through OpenScape Business.
- The mobile phone can be integrated into system-internal teams.
- UC applications such as myPortal for Desktop and myPortal for Outlook can be used in the same way as for internal subscribers. myPortal Smart is currently not supported.
- myPortal to go is available on the road.
- Embedded mobile phones identify themselves by name when calling an internal subscriber.
- The digit analysis and call routing in the system or network occurs as for any other internal station (e.g., allowed numbers, denied numbers, LCR rules)
- The ITSP uses special call signaling from/to the OpenScape Business, which must be administered accordingly.
- Every integrated mobile phone requires a Mobility User license.
- To use UC applications, a UC Client license is additionally required.

6.2.1 Configuring an ITSP

It is possible to configure predefined and new Internet Telephony Service Providers (ITSPs). You can configure one or several accounts for each ITSP. Up to 8 ITSPs may be active simultaneously.

Additional information on ITSPs and their features can be found here:

`http://wiki.unify.com/index.php/Collaboration_with_VoIP_Providers#Overview`

> ***INFO:*** Configuration examples can be found on the Internet at the **Unify Experts Wiki** under *OpenScape Business - SIP / ITSP Connectivity - PDF "OSBiz V2 Configuration for ITSP"*.

Assigning the ITSP Phone Numbers

- In the case of an **Internet Telephony Station Connection**, the ITSP provides individual numbers such as 70005555, 70005556, etc. These individual call numbers are then assigned manually as the internal call numbers of the subscribers.
- In the case of an **Internet telephony point-to-point connection**, the ITSP provides a call number range, e.g., (+49) 89 7007-100 to (+49) 89 7007-147. The call numbers from the range are then assigned manually as the internal call numbers of the subscribers.

These two connection types can be combined as appropriate.

Alternatively, the ITSP phone numbers can be entered as the DID call numbers of the subscriber for both connection types during the station configuration.

Internal call number	Name	DID
100	Andreas Richter	897007100
101	Susanne Mueller	897007101
102	Buddy Miller	897007102
104	Juan Martinez	70005555
105	Emilio Carrara	70005556

The ITSP call numbers thus result from the configured PABX number (e.g., country code 49) and the entered DID numbers in long format. This has advantages for the digit analysis and call management, even in an internetwork. The ITSP connection is thus DID-enabled for another node, for example.

A further CO trunk connection via ISDN is only possible to a limited extent in this case.

Multisite Management

The subscribers of the communication system can be assigned to different sites (with different area codes, for example). Each site is assigned a route, and each route is assigned an ITSP registration. A maximum of 8 ITSP registrations can be managed. One registration per ITSP is possible or even multiple registrations at one ITSP. Each ITSP registration can be assigned an area code, and multiple subscribers can then be assigned to it. The connection between the subscribers at the different sites and the communication system occurs via a VPN. All sites must be located within one country and use the same CO access code (see also *Networking OpenScape Business in Hosting Environments*, Scenario 1b).

Using ITSP Templates

The default is to use a preconfigured ITSP template. To do this, the own access data and phone numbers are entered in the template, and this is then activated.

In Expert mode, you can also edit a preconfigured ITSP template and save it as a new template.

Updating ITSP Templates

The preconfigured ITSP templates are automatically updated after a software update of the system if there are new preconfigured ITSP templates in that update or more recent default values for existing preconfigured templates.

If the ITSP of a template is already activated, the update is not done automatically, since important changes could otherwise be overwritten when updating the default values. Consequently, the update can be performed manually in the Expert mode if required. The default values will then need to be customized again to suit individual requirements.

6.2.2 STUN (Simple Traversal of UDP through NAT)

When operating the communication system behind a NAT router, STUN determines its own public IP address/port (which is required for some ITSPs). The functionality is made available on the Internet on STUN servers, whose addresses must be stored in the configuration of the communication system.

The required STUN mode depends on the ITSP infrastructure and the used Internet router. STUN is not required for ITSPs that resolve NAT traversal using infrastructure components in the provider network such as the session border controller.

The following STUN modes can be set at the communication system:

- **Automatic (Default)**
  If no ITSP is active, STUN is fully disabled. With an active ITSP, STUN determines the used firewall type (NAT type) at system startup and detects IP address changes during runtime. Depending on the detected NAT type, STUN changes certain parameters in SIP messages (NAT traversal).

  INFO: Symmetric NAT is not supported.

- **Always**
  STUN is always active, for example. Depending on the detected NAT type, some parameters in SIP messages are adapted.
- **Use static IP**
  The DSL modem or Internet router uses a static a static IP address (public IP address), and the ITSP requires a static IP authentication. The static IP address and port that is used by the modem or router must be specified in addition.
- **Port Preserving router**
  The public IP address is determined using STUN. The port is entered in SIP messages unchanged.

6.3 CO Access over Digital and Analog Lines

The CO Access over ISDN or analog lines connects the hardware platforms with the public network (PSTN).

Wizards are available to facilitate the configuration of an ISDN outside line or analog outside line.

6.3.1 Trunks

Trunks connect the hardware platforms with the public network (PSTN). Every trunk must be assigned a route through which different properties can be assigned to the trunk.

By default, all trunks are assigned a seizure code and a route. These assignments can be changed by the administrator.

In the case of an ISDN trunk connection, the trunks are also referred to as B-channels.

Trunk code

Using the trunk code, the communication system seizes the specific trunk assigned to that trunk code. The trunk code is also used to program a trunk key or to test a trunk.

MSN Allocation

The service provider assigns one or more MSN (Multiple Subscriber Number) to each ISDN point-to-multipoint (PMP) connection. These can be assigned directly to a line.

System Phone Numbers

System phone numbers include the international prefix, the country code and area code, and the PABX number or one or more MSNs.

ISDN Protocol

The ISDN protocol used depends on the country code. It should only be changed if the PSTN connection explicitly requires some other deviant protocol. Several protocol templates, which can be adapted to individual requirements, are available. The requisite information for this can be obtained from your Service Provider.

B Channel Seizure Mode

Individual B channels of an ISDN trunk can be blocked for outgoing and/or incoming traffic.

The following B channel seizure modes are possible:

- outgoing only
- incoming only
- outgoing and incoming (default)

The B channel seizure mode is only evaluated when the communication system must offer a B-channel. The applies in the following situations:

S_2 outgoing:	The communication system must offer a B-channel.
S_2 incoming:	The remote station must offer a B-channel. This B-channel is accepted by the communication system without checking the setting. It is thus of no direct significance.
S_0 outgoing:	Since the communication system does not pre-assign a B-channel (any channel), this setting is of no direct significance.
S_0 incoming:	When the remote station sets up a call without specifying a B-channel, the communication system offers a B-channel, while taking the set B channel seizure mode into account.

Dialing Method for Analog CO Trunks (MSI)

The dialing method is automatically detected by the communication system whenever the line is seized. For special cases, the dialing method can also be set directly to Dual Tone Multifrequency (DTMF) or Dial Pulsing (DP).

6.3.2 Routes

Routes enable trunks (B channels) to be grouped. Separate parameters can be configured for each trunk group (= route).

Each trunk can be assigned to exactly one route. By default, all trunks are assigned to route 1.

For each route, a name and a seizure code can be assigned.

> ***INFO:*** Seizure codes only work for outgoing trunk seizures if LCR has not been activated.

B Channel Allocation

The allocation of B channels to different trunk groups is also called B-channel allocation. For ISDN trunk connections with multiple B-channels, e.g., S_{2M} ports, it may be useful to allocate B channels to different trunk groups (called B-channel allocation).

For outgoing calls, only B-channels that are included in the trunk group can be selected (e.g., trunk group selected via the seizure code, overflow trunk group or trunk group selected using LCR)

Incoming calls are always accepted, regardless of the trunk group. As a rule, the B-channel offered by the peer is seized. Consequently, the B-channel allocation configured in the system must also be supported on the peer side (system or public network). If this is not the case, the correct allocation of the call to the correct trunk group cannot be guaranteed.

Trunk group key

A subscriber can program a trunk group key on the telephone. One trunk group key is reserved for outbound calls. Calls placed via trunk group keys are subject to COS toll restriction levels and rules.

When a subscriber presses a trunk group key (or dials a seizure code), the communication system seizes an available trunk that is assigned to the appropriate route. The telephone shows the trunk number in the display. If all trunks of the route are seized, the corresponding LED lights up, even in the case of a successful overflow.

Overflow Route with LCR Disabled

For each route, the administrator can also define an overflow route. If all the trunks of a route are busy during a seizure attempt, the search for trunks

continues among all trunks in the overflow route. If all the trunks in the overflow route are busy as well, no further overflow occurs.

Overflow Route with LCR Enabled

As part of the LCR configuration, the administrator configure up to 16 entries per route table that are then processed sequentially within the context of an overflow.

Type of Seizure

For an outgoing route seizure, the administrator can specify the criteria to be used by the communication system when searching for an available trunk in the required direction. This is done by defining the type of seizure as follows:

- cyclic:
  after the last outbound seized trunk - search begins at the next higher trunk number, as of the last outgoing trunk reserved for that direction. Consequently, all trunks are used with similar frequency.
- linear:
  always the first free trunk - search begins at the lowest trunk number assigned to that route.

Entering a PABX Number, Incoming and Outgoing

The administrator can configure the PABX number incoming and the PABX number outgoing separately. Thus, the own number for outgoing calls can be represented differently than is needed for accessibility by incoming calls. The portions for the country code, local area code and the PABX number must each be entered separately in this case. Different entries for the PABX number incoming and outgoing require the availability of the "CLIP no screening" feature at the Central Office. If no PABX number outgoing is configured, the communication system always uses the data of the PABX number incoming.

In the case of an incoming seizure on an ISDN line, the communication system truncates the PABX number portion (left-aligned) from the received phone number in accordance with the incoming phone number type (Type Of Number = TON, see table below Caller ID) and interprets the remaining portion as the Direct Inward Dialing number. For call number information to the PSTN, the communication system automatically inserts the outgoing PABX number portion as the leading portion of the call number in accordance with the configured type of number (TON). In Germany, the PABX number portion must be specified at the trunk connection without the local area code and the intercept code (0).

Station Number Transmission

The station number that is sent to the PSTN and to the receiver can be composed as follows:

Type Of Number (TON), outgoing	Station number transmitted to the PSTN
Unknown TON = Unknown	only DID number (default setting)
PABX number TON = Subscriber	PABX number + DID number
Local area code TON = National	+ Local area code + PABX number + DID number
Country code TON = International	Country code + Local area code + PABX number + DID number
Internal TON=Internal	Only for networked system: number prefixes may not be added for closed numbering plans. Call number prefixes are suppressed here.

In addition, you can specify which call number information is to be transmitted from the dialing station to the destination station.

Call number type	Call number transmitted to the PSTN
Internal	In this case, only the internal call number is transmitted. If the destination is an external station, either no number is transmitted or only that of the Attendant Console. The internal call number can be displayed when the destination is an internal station.
Direct inward dialing	In this case, only the DID number is transmitted. The internal call number is not provided for display at internal destinations in other nodes. The call number information is sufficient for external destinations.
Internal / DID	This setting is useful for networking purposes. Both the internal call number and the DID call number are transmitted to the destination station. If an internal station is called within the network, the internal call number of the caller can be displayed for this station. If the internal destination station has activated call forwarding to an external destination, for example, a DID number can also be transmitted in this case.

In addition, the desired handling of the route prefix can be configured:

- Incoming call
  The caller's number is supplemented with the seizure code (-> dialable format for callback) or passed through transparently when it is transmitted to the S0 bus. Default: enabled.
- Outgoing call
  The display of the dialed phone number on the system telephone occurs with or without the route prefix. Default: enabled.

Second CO Code

A second trunk code (CO code) is defined if the communication system is a subsystem of another communication system or is networked with several other communication systems. It is only relevant for networking routes (route type =

PABX). In this case, the second trunk code is the seizure code for the main system. Within a network, the codes for the trunk seizure, the route seizure code(s) and the second CO code must be configured uniformly. The default in Germany is 0.

6.3.3 Dial Tone Monitoring

When setting up a connection over an analog trunk line, the dialed digits can be sent to the Central Office only when a dial tone (audible signal) has been detected. Since the time until the arrival of the dial tone varies depending on the network provider and network state, the arrival of the dial tone can be monitored.

The dial tone monitoring time and the digit dialing time are configured using Manager E.

Delay Period for Dial Tone Monitoring

The monitoring of the dial tone can be done immediately or only after a pause. In some cases, additional tones may need to be played back to the subscriber after the line is seized, for example, to inform him or her that call forwarding has been enabled at the Central office. For such cases, a delay period for the dial tone monitoring (Analog trunk seizure, 1-9 seconds) can be programmed. The dialed digits will then be sent to the CO only after this pause.

INFO: Notes for Brazil:

If the DTMF dialing method is used from analog phone devices in conjunction with analog trunks (TLAx and TML8W) and pulse dialing after the dial tone monitoring, problems may arise with toll restriction when the country code is set to Brazil. In this case, the DTMF signals from the analog devices go directly to the analog trunk lines. All DTMF signals that were dialed before receiving the dial tone are lost. Consequently, for such cases, least cost routing (LCR) must be enabled for the dialing method and toll restriction to operate properly at the device.

Dial tone monitoring time

This parameter indicates how long the system will wait for the dial tone and is configurable. If no dial tone is detected during the configured dial tone monitoring time, the line is taken out of service. The system checks at cyclical intervals whether the dial tone is once again present. If this is the case, the line in question is put back into operation.

Digit dialing time

This parameter defines how many seconds after detection of the dial tone the first dialed digit is to be sent to the Central Office (default setting: 0 s).

Analysis of the Second Dial Tone

The communication system can recognize an additional dial tone (2nd dial tone). This is relevant for public network providers who transmit at a second dial tone for international calls, e.g., for Belgium after 00 and for France after 16 or 19. For Germany, this feature is not relevant.

6.4 Prioritizing the Exchange Line Seizure with LCR Enabled

The prioritization for exchange line seizure defines in what order different network providers (ISDN/analog or ITSPs) are selected.

The exchange line seizure normally occurs by dialing the prefix "0". Within this code, different providers are prioritized (depending on what is preset). For example, an outbound call may be first routed via an ITSP and, if the exchange line seizure fails, be then sent via ISDN.

7 Stations

A subscriber or station is a communication partner connected to the communication system. In general, every station (apart from virtual stations) is assigned a terminal. A terminal is, for example, a telephone, a PC or fax device. The stations may also be users of the UC Clients.

The following types of stations exist:

- IP stations (also known as IP clients)
- SIP stations (a subset of IP stations)
- UP0 stations
- DECT stations
- ISDN stations
- Analog stations
- Mobility stations (mobile stations, see *Mobility*)
- Virtual stations

The data of subscribers (name, station number, DID number, e-mail address, etc.) can be imported as an XML file during the initial installation (see *Individual Dial Plan*). In addition, the subscriber data can also be exported to an XML file (see *Exporting Subscriber Data*).

Licensing Procedure for Stations

All stations are subject to licensing. To begin with, stations can be set up during the initial installation or later by using the Station wizards. After a successful setup, the subscribers can make internal calls. In the next step, the station licenses must be activated and assigned to the stations. Once the licenses have been assigned successfully, the subscribers can also make external calls.

Related Topics

- Licensing
- Mobility

7.1 Dial Plan

A dial plan, which is also called a numbering plan, is a list of all phone numbers and codes available in the communication system. It includes, among other things, the internal call numbers, DID numbers and group call numbers. In the communication system, the call numbers and codes are preset with default values. However, these values can be adapted to suit individual requirements as needed.

When setting up call numbers or codes, error messages may be produced if the desired number is already being used. The dial plan can be used to check which call numbers can still be assigned.

7.1.1 Default Dial Plan

The default dial plan includes all call numbers and codes that are predefined n the communication system with default values.

These default values can be edited as necessary. Some numbers can be also deleted completely so that they no longer appear in a dial plan overview.

Default dial plan for the hardware platforms and the softswitch:

Type of call numbers	X1	X3/X5/X8/S	Action
Internal station numbers	11-30	100-742	deletable
User direct inward dialing numbers	11 -30	100-742	deletable
Group call numbers 1-90 Group call numbers 91-800	31-40 -	350-439 not preset	deletable
Trunk station number	700-703	from 7801 onward	deletable
Seizure codes (external codes): Trk. Grp 1 (trunk: ISDN, analog) Rte. 8 (UC Suite) Trk. Grp 12-15 (trunk: ITSP) Rte. 16 (Networking)	 0 = World / 9 = USA - not preset not preset	 0 = World / 9 = USA 851 855-858 859	only editable
Attendant code (Intercept position), Internal	9 = World 0 = USA	9 = World 0 = USA	only editable
Attendant code (Intercept position), Direct inward dialing	0 = ROW – = USA	0 = ROW – = USA	only editable
Station numbers for online users	not preset	749	only editable
Call number for remote access	not preset	not preset	only editable
Call number for voicemail UC Smart UC Suite	 351 -	 351 not preset	 only editable only editable
Conference call numbers	-	not preset	only editable
Call number for parking	-	not preset	only editable
AutoAttendant numbers	-	not preset	only editable
Station number for Attendant Console	9 = World 0 = USA	9 = World 0 = USA	only editable
Substitution for "#" (for service codes)	75	75	deletable
Substitution for "#" (for service codes)	76	76	deletable
Service codes			only editable

7.1.2 Individual Dial Plan

The communication system allows you to set up an individual dial plan by editing the default values of the call numbers and codes. A reload of the communication system resets the values to the defaults.

The following actions are useful for this purpose:

- Delete defaults: apart from some exceptions (special default numbers), default call numbers can be deleted. These call numbers are identified as "deletable" in the "Action" column of the default dial plan table.
- Edit special defaults: these call numbers must not be deleted. However, their values may be edited. These call numbers are identified as "only editable" in the "Action" column of the default dial plan table.
- Import call numbers and station data: station data can be imported via an XML file during the initial installation. The call numbers and DID numbers of the stations are imported as well. This is usually performed during the initial installation.

Importing Station Data via an XML File

An individual dial plan can be imported into the communication system via an XML file in UTF-8 format during the initial installation.

The OpenScape Business Assistant administration program makes the file `csv-templates.zip` available under **Service Center > Documents > CSV Templates**. This zip file contains, among other things, the following files, including descriptions:

- `portdata_xml_import_empty.xml`
  This template contains registers without sample records. New records can be entered using Microsoft Excel, for example.
- `portdata_xml_import_example.xml`
  This template contains registers with sample records. These records can be edited using Microsoft Excel, for example. Data records that are no longer needed should be deleted.
- `portdata_xml_import_syntax.txt`
  Descriptions in German and English on how to create records correctly.

7.2 LAN Telephony Requirements

The term LAN telephony refers to the communication between IP stations in an internal network (LAN). To ensure the quality of the voice transmission in LAN telephony, the IP networks being used and the communication system must meet certain requirements. The voice quality and voice communication reliability always depend on the network technology in use.

To guarantee loss-free transmission and good voice quality, voice signals are digitized using audio codecs and marked using special procedures (Quality of Service) so that voice transmission has priority over data.

Requirements

- LAN with at least 100 Mbps and full duplex
- Every component in the IP network must be connected to a separate port on a switch or to a router; a hub should not be used.
- Not more than 50 msec delay in one direction (One Way Delay); not more than 150 msec total delay
- Max. 3% packet loss; if a fax/modem via G.711 is used, the packet loss must not exceed 0.05%.
- Not more than 20 msec jitter
- Support for Quality of Service (QoS): IEEE 802.p, DiffServ (RFC 2474) or ToS (RFC 791)
- Maximum 40% network load

7.2.1 Audio Codecs

An audio codec is a program that encodes and decodes voice in digital data packets (IP packets). The data compression rate can vary depending on the audio codec used. The bandwidth requirement for transferring an IP packet is lower if the packet is compressed. The decoding of data packets can, however, have a negative impact on voice quality and the playback continuity.

The recipient and sender must use the same codec to ensure that the data can be correctly decoded back into voice after transport.

Supported Audio Codecs

The following audio codecs are supported:

- G.729A, G.729AB: voice encoding at 8 Kbps - good voice quality.
- G.711 (A-law and µ-law): voice encoding at 56 or 64 Kbps - very high voice quality. G.711 is also used in fixed networks (ISDN).

The audio codecs can be assigned priorities between 1 (high) and 4 (low). The communication automatically tries to use the audio codec with the highest priority available for every connection. Using an audio codec with low voice compression (good voice quality) increases network load. In the case of intensive IP telephony, this can lead to diminished voice quality in a network already overloaded by data transfers.

The communication system can enable voice activity detection (VAD) for certain codecs. This can reduce network load during long voice pauses.

You can specify a frame size (IP packet size) of 10 to 90 msec for every codec. This specifies the sampling rate at which the audio codec splits the voice signal into IP packets. While a higher value (90 msec, for instance) results in a better

relationship between payload and the IP packet overhead, it also increases the transfer delay.

It is possible to disable the resource-hungry G.729 codecs and to only use the G.711 codecs. This optimizes the number of possible simultaneous calls. If this function is enabled, the system must be restarted.

7.2.2 Transmission of Tones According to RFC 2833

The transmission of DTMF tones and fax/modem tones according to RFC 2833 can be enabled or disabled.

7.2.3 Quality of Service

Quality of Service (QoS) encompasses various procedures for guaranteeing the highest possible quality and integrity during the transmission of data packets (IP packets). For good voice quality during voice transmission, QoS is used in the IP network to give IP voice packets priority over IP data packets from other applications.

The IP packets are assigned a special marker (code point) for prioritization. Categorization in different classes is performed based on priority information. If the components available in the IP network (communication system, SIP stations, and Internet routers, for instance) support QoS, you can assign different bandwidth to these classes and thus transport the IP voice packets first.

Priority Classes According to DiffServ

For DiffServ-based prioritization, different code points are defined for the Type of Service (ToS) field so that IP-packet transmission can be split into different classes.

- Expedited Forwarding (EF) Code point: guarantees constant bandwidth. The bandwidth is always the same for IP packets marked with this code point. Once the set value is reached, all IP packets that exceed this bandwidth are dropped.
- Assured Forwarding (AF) Code point: guarantees minimum bandwidth. IP packets that are marked with this code point have a lower priority than EF and must share the bandwidth not used by EF. Once the set value is reached, all IP packets that exceed this bandwidth are rejected.
  Four classes are reserved for AF: AF1x (low priority), AF2x, AF3x and AF4x (high priority), where "x" stands for one of three dropping levels: low (1), medium (2) and high (3). In the case of "low", packets are buffered over an extended period, in the case of "high", packets are promptly rejected if they cannot be forwarded.
- Best Effort (BE): Unmarked IP packets (Type of Service (ToS) field=00) are handled in the same way as the lowest priority.

Priority Classes According to IP Precedence

In addition to the DiffServ method, there are several older definitions, which perform the prioritization based on the ToS field. To achieve the best possible adaptation of the communication system to any required settings in the customer network, classes 3 to 7 (CS3-CS7) can be selected for IP Precedence, for example.

Individual Priority Classes

If none of the preset options is used in the customer network, the ToS value can also be set directly and manually. The set value is set to decimal 0-63 and transferred to the upper 6 bits of the ToS byte (e.g., 41 = 101-001-00 = 0xA4).

Table of Possible Priority Classes

Priority class	ToS value, binary	ToS value, hexadecimal
AF (Assured Forwarding)		
AF11	001-010-00	28
AF12	001-100-00	30
AF13	001-110-00	38
AF21	010-010-00	48
AF22	010-100-00	50
AF23	010-110-00	58
AF31	011-010-00	68
AF32	011-100-00	70
AF33	011-110-00	78
AF41	100-010-00	88
AF42	100-100-00	90
AF43	100-110-00	98
EF (Expedited Forwarding)		
EF	101-110-00	B8
Best Effort (BE)		
BE	000-000-00	00
CS (Class Selector)		
CS3	011-000-00	60
CS4	100-000-00	80
CS5	101-000-00	A0
CS6	110-000-00	C0
CS7	111-000-00	E0
Manual entry	xxx-xxx-00	0-63 (decimal)

7.3 IP Stations

IP stations are connected to the communication system via the LAN. An IP station is generally a LAN or WLAN phone.

The following IP protocols are supported:

- Vendor-specific communication system protocol
  The communication system uses CorNet-IP (CorNet Internet Protocol) for LAN telephony within the internal network. CorNet-IP, which was developed on the basis of H.323, supports all telephone features of the communication system.
- SIP (Session Initiation Protocol)
  SIP is usually used in Internet telephony but is not restricted to it. It can also be used for telephony in the internal network, for example. However, SIP does not support all telephony features associated with the communication system.

The following types of IP stations exist:

- **System Client**: A system client is an IP station that can use all the features of the communication system via CorNet-IP. This can be an IP system phone such as an OpenStage 60 HFA, for instance, or a PC with CTI software such as OpenScape Personal Edition.
- **SIP client**: A SIP client is an IP station that uses the SIP protocol. It can access only limited functionality of the communication system via SIP. A SIP client is a SIP phone such as the OpenStage 15 S, for example.
- **Deskshare User**: A Deskshare User is an IP user who can log in at another IP system telephone (mobile login) and then use this phone as his or her own phone (including the call number).
- **RAS User**: A RAS user (Remote Access Service user) is granted access to the IP network via the ISDN connection. This allows the communication system to be maintained remotely.

For each connected IP station, an "IP User" station license is required.

Two IP stations are reserved for the Online User and for remote access via ISDN. These IP stations do not require a station license. If one or several of these three reserved IP stations are not required, these stations can be converted to normal IP stations in Expert mode. However, station licenses are then required for these IP stations.

Configuring IP Stations

The following configurations can be performed for an IP station:

- Configuration of standard parameters with the **IP Telephones** wizard (see *Administrator Documentation, Stations*).
- Configuration of all parameters (standard and advanced parameters in Expert mode (see *Administrator Documentation, Stations*).

OpenScape Desk Phone IP system phones are supplied with the SIP software by default. As soon as an OpenScape Desk Phone IP system phone is configured in the WBM as a **System Client**, the HFA software stored in the communication system is automatically loaded onto the IP system phone.

7.4 SIP Stations

SIP stations are IP stations that use the Session Initiation Protocol (SIP) for communication. SIP stations can use this protocol to access a limited number of the communication system's functions. SIP stations, like IP stations, are connected to the communication system over the LAN.

A SIP station is a WLAN phone or a LAN phone such as the OpenStage 15 S, for example.

For each connected SIP station, an "IP User" station license is required.

SIP Authentication

In order to ensure the security of the internal network, it is important that SIP subscribers are authenticated at the communication system with the values described below. These values must be configured in the WBM of the communication system for each SIP subscriber and also at every SIP phone itself. To protect against SIP attacks, authentication is strongly recommended!

- Password
  Password for authentication: assigned freely; at least 8 characters up to a maximum of 20 characters. The password should contain at least one uppercase letter, one lowercase letter, one digit and one special character. A separate password should be assigned for each SIP subscriber.
- SIP User ID / Username
  User name for authentication: preassigned; can be changed if required, maximum 20 characters. Each SIP subscriber has a different preassigned SIP User ID.
- Realm
  Zone or domain for authentication: assigned freely; can be changed if required, max. 20 characters. The realm for all SIP subscribers is preassigned with the same value. It can be changed as required, e.g., in the host name or domain name of the communication system.

Configuration of SIP Stations in the Communication System

The following configurations can be performed in the WBM of the communication system for an IP station:

- Configuration of standard parameters with the **IP Telephones** wizard (see *Administrator Documentation, Stations*).
- Configuration of all parameters (standard and advanced parameters in Expert mode (see *Administrator DocumentationStations*).

Configuration of the SIP phone

The data used to authenticate a SIP subscriber at the communication system must be additionally entered directly at the SIP phone.

Configuration of authentication data at the SIP phone (see *Configuring the Authentication Data at the SIP Phone*).

Features that can be used with SIP Telephones

The following features can be used with SIP telephones:

- Incoming and outgoing calls with display of call number and name
- Hold, Toggle/Connect, Consultation
- Call transfer (screened/unscreened)
- Take Call
- Immediate call forwarding, on busy and after timeout
- Three-party conference
- Call lists, message waiting indicator
- Ringer cutoff at phone, reject call, call forwarding
- Call waiting
- Membership in groups (without display of the group number)
- Different calls for internal, external and recall
- Mailbox LED - Message Waiting Indication
- DTMF dialing, e.g., for the operation of voicemail boxes
- Use of the UC clients
- Automatic software updates (when using the DLI)

> ***INFO:*** Deployment with a multichannel Contact Center has not been released.

Depending on the telephone, there may be some restrictions on the available functions; see the wiki at: `http://wiki.unify.com/wiki/SIP_devices_configuration_examples`

The following features, which are activated using codes with * or #, can be used with SIP phones:

- Reset services: #0
- Join/Leave hunt group: *85/#85
- Station number suppression (CLIR) on/off: *86/#86
- Speed dial: * 7nnnn (nnnn = speed dial number)
- Door opener: *61

Features that can be used with SIP Telephones and myPortal/myAttendant

SIP phones to be used with myPortal and myAttendant must meet the following requirements:

- 3PCC as per RFC 3725 is supported.
- The "call waiting" feature is supported.
- The local Do Not Disturb is disabled.

The full functionality of the features depends on the SIP phone used and cannot be guaranteed. A successful test of the features listed below was performed with the OpenStage SIP telephones.

Connection-/call-oriented features:

- Making Call
- Redirect call
- Take Call
- Resume call
- Application-controlled conference
- Place call on hold
- Alternate (Toggle/Connect)
- Consultation
- Disconnect
- Transfer

Phone-oriented features:

- Do Not Disturb
- Call forwarding

7.5 UP0 stations

A UP0 station uses a $U_{P0/E}$ line to transmit digital signals. UP0 stations are connected to the communication system via UP0 interfaces and are system telephones such as an OpenStage 60T, for example. UP0 stations can therefore use the complete functional scope of the communication system.

The following connectivity options are available for UP0 stations:

- OpenScape Business X1
  To the $U_{P0/E}$ interfaces on the mainboard.
- OpenScape Business X3/X5
  To the $U_{P0/E}$ interfaces on the mainboard or, if several UP0 stations are involved, to an additionally inserted $U_{P0/E}$ board.
- OpenScape Business X8
  To additionally inserted $U_{P0/E}$ boards.
- OpenScape Business S
  No connection possible.

For each connected UP0 station, a "TDM User" station license is required. Even system telephones that are connected in slave mode require a station license.

Configuring the UP0 Stations

The following configurations can be performed for a UP0 station:

- Configuration of standard parameters with the **UP0 Devices** wizard (see *Administrator Documentation, Stations*).
- Configuration of all parameters (standard and advanced parameters in Expert mode (see *Administrator DocumentationStations*).

7.6 DECT stations

A DECT station uses a Cordless base station to transmit digital signals. A DECT station is a DECT telephone.

The following connection options are available for DECT stations:

- OpenScape Business X1/X3W/X3R/X5R
  Cordless base station to a $U_{P0/E}$ interface of the mainboard.
- OpenScape Business X5W
  Cordless base station to a $U_{P0/E}$ interface of the mainboard or to an SLC16N board.
- OpenScape Business X8
  Cordless base station to one or more SLCN boards.
- OpenScape Business S
  DECT IP base station on the LAN

The connection of a Cordless base station is called the integrated Cordless solution. This means that almost all functions of the communication system are available.

The integration of an IP DECT base station in the internal network is called Cordless IP. Since only the SIP protocol can be used in this case, not all communication system features are available.

For each connected DECT station, a "TDM User" station license is required.

For the description and configuration of the integrated Cordless solution, see *Integrated Cordless Solution*.

Configuring DECT Stations

The following configurations can be performed for a DECT station:

- Configuration of standard parameters with the **DECT Devices** wizard (see *Administrator Documentation, Stations*).
- Configuration of all parameters (standard and advanced parameters in Expert mode (see *Administrator DocumentationStations*).

DECT IP stations are configured as normal SIP stations.

7.7 ISDN Stations

An ISDN station uses the $_0$ bus for transmitting digital signals and is therefore often referred to an S_0 station The ISDN station is connected to the communication system via the S_0 interfaces

The following connection options are available for an S_0 station:

- OpenScape Business X1
  To an S_0 interface of the mainboard.

- OpenScape Business X3/X5
  To an S_0 interface of the mainboard or to an S_0 board.
- OpenScape Business X8
  To one or more S_0 boards.
- OpenScape Business S
  To additionally required gateways or adapters

The following ISDN stations can be connected:

- ISDN phone
- Fax Group 4
- ISDN modem
- PC with ISDN card

The following types of ISDN stations can be defined:

- Default: for ISDN phone, Fax Group 4, ISDN modem or PC with ISDN card
- Fax: prerequisites for setting up the "Info from Fax/Answering Machine" key. If a PC with an ISDN card and Fax software is attached to the S_0 bus and assigned the type "Fax", for example, then an "Info from Fax/Answering Machine" key could be set up on every device. When this key lights up, this indicates that a fax has been received.
- Answering machine: prerequisites for picking up a call when the answering machine has already accepted it If a Gigaset ISDN phone with an answering machine is connected and assigned the type "Answering Machine", for example, a call that has already been accepted by the answering machine can be picked up at any terminal. To do this, the terminal must be programmed with the internal call number of the Gigaset.

For each connected ISDN station, a "TDM User" station license is required.

Connecting ISDN Stations to the S_0 Port

To be able to connect an ISDN station to the communication system, you must configure at least one of the S_0 ports that are used for the ISDN subscriber line or the ISDN point-to-point connection as an internal S_0 bus (S_0 EURO bus).

INFO: If there is more than one ISDN station connected to an S_0 port (up to 8 ISDN stations are possible) in an ISDN point-to-multi-point connection, each individual ISDN station must be assigned to a unique MSN. This assignment must be made in the configuration menu of the ISDN station.

Configuring ISDN stations

The following configurations can be performed for an ISDN station:

- Configuration of standard parameters with the **ISDN Devices** wizard (see *Administrator Documentation, Stations*).
- Configuration of all parameters (standard and advanced parameters via Expert mode (see *Administrator DocumentationStations*).

Allowing only Configured Numbers for MSNs

The administrator can specify that further MSNs at an S0 bus may only be configured for call numbers that already exist there. This prevents subscribers from adding an MSN without authorization through an outgoing seizure of the S0 bus with a further MSN. Without this restriction, the communication system would normally assign a free internal call number to the S0 bus for that MSN.

Terminal Portability

The communication system supports Terminal Portability (TP), that is, it lets you park a call on the S_0 bus, unplug the terminal, and plug it back in at a new location to resume the call. The parked station receives a message indicating that the user is porting. Three minutes are available for the entire operation.

The feature is not supported for services such as telefax, teletex or data transfer.

7.8 Analog Stations

An analog station uses a two-core analog cable to transmit analog signals. The communication system connects the analog station via the analog ports.

The following connectivity options are available for analog stations:

- OpenScape Business X1
  To an analog interface of the mainboard.
- OpenScape Business X3/X5
  To an analog interface of the mainboard or to an analog board.
- OpenScape Business X8
  To one or more analog boards.
- OpenScape Business S
  To additionally required gateways or adapters

The following analog stations can be connected:

- Analog telephone
- Analog Fax (Group 3)
- Answering Machine
- Modem, 9600 bps or higher
- Entrance Telephone (Door Opener)
- Loudspeaker

The following types of analog stations can be defined:

- Standard: for analog phone, Group 3 fax, answering machine or loudspeakers
- Fax: prerequisites for setting up the "Info from Fax/Answering Machine" key. If a Fax Group 3 device is connected and assigned the type "Fax", for example, then an "Info from Fax/Answering Machine" key could be set up on every device. When this key lights up, this indicates that a fax has been received.
- Answering machine: prerequisites for picking up a call when the answering machine has already accepted it If a Gigaset phone with an answering

machine is connected and assigned the type "Answering Machine", for example, a call that has already been accepted by the answering machine can be picked up at any terminal. To do this, the terminal must be programmed with the internal call number of the Gigaset.

- Modem: Analog modems with a fixed speed of 56 kbps or higher are not supported, since speeds of 56 kbps or higher cannot be processed.

For each connected analog station, a "TDM User" station license is required.

Availability of an Analog Fax Device in the System with Previous Fax Number

Since it is not possible to forward an analog fax device to a fax number in the system, the following workaround exists: The previous fax number is configured in the system and receives the incoming fax messages. For the analog fax device, a port is configured with the previous number as the CLIP. The Configurable CLIP check box must be selected for this purpose. Outbound fax messages show the previous number as the sender; internal recipients see the internal number of the fax machine.

Configuring Analog Stations

The following configurations can be performed for an analog station:

- Configuration of standard parameters with the **Analog Devices** wizard (see *Administrator Documentation, Stations*).
- Configuration of all parameters (standard and advanced parameters via Expert mode (see *Administrator DocumentationStations*).

7.9 Virtual Stations

Virtual stations behave like real stations, but have no physical telephones assigned to them.

Virtual stations are required for mobile phone integration and call forwarding no answer (CFNA), for example. These stations must be configured like real stations so that they can be used for the signaling of calls, for example.

Configuring Virtual Stations

The parameters associated with a virtual station are configured in Expert mode (see *Administrator DocumentationStations*).

7.10 Key programming

Every system phone comes with a certain number of function keys. A number of these function keys are programmed by default with functions. You can modify this default setting and program the remaining function keys that were not preprogrammed.

The individual keys can be programmed as follows:

- Key programming via WBM
  The keys on connected system telephones can be programmed in the WBM via the **Key Programming** wizard.
  This wizard can also be used to program a key assignment for a subscriber even though no system telephone has been connected for that subscriber.
- Key programming via the UC clients
  Users of the UC clients **myPortal Smart**, **myPortal for Desktop**, **myPortal for Outlook** and **myAttendant** can also program the keys on their system telephone via these UC clients (see the respective User Guides for the UC clients).
- Key programming directly at the system telephone
  System phones with display allow you to program certain function keys directly at the phone.

Programming Function Keys on Different Levels

The function keys of the system telephones can be programmed twice, that is, on the first and second levels. You can program all available functions on the first level. You can program external phone numbers on the second level. The Shift key must be programmed on the system phone before you can use the second level. The function key LEDs are always assigned to the first level.

INFO: In case of a **user it is not possible to copy key programming as the automatic key assignment feature is MULAP specific and should not be copied at any station. The prefix ** should be removed manually from these users in order the key copy to be enabled.

7.11 Station Profiles

The values and properties of subscribers are stored in profiles. One or more members can be assigned to a profile. The same values and properties then apply to all members of that profile.

Station profiles can be assigned to subscribers with system telephones. Up to 20 station profiles can be created. The station profiles can be exported or imported individually or collectively. The files are of type `xml`.

Every subscriber can be a member of exactly one profile. If the values and properties of a station that is a member of a profile are changed directly, i.e., not through the profile, the station is deleted from the profile.

7.12 Configuring Stations

You can define specific values (for example, phone number, name, and DID number) and properties (for example, type of call signaling) for the station.

Station configuration is split into standard configuration and advanced configuration. The default settings can be configured using wizards with the **Advanced** profile. The Advanced settings can only be configured in Expert mode with the **Expert** profile.

The default settings can be conveniently edited in a list for all stations of a station type (e.g., IP stations or analog stations). Additional settings (such as call signaling or the station flags, for example) can be changed individually for each subscriber.

Virtual stations are configured entirely in Expert mode (both the standard and the advanced settings).

Although the **Basic** profile cannot be used to configure stations, it can be used to edit the names of stations.

A dial plan (also called a numbering plan) should be available for the stations connected to the communication system. The station numbers, names and DID numbers of all configured subscribers can be displayed in Expert mode via **Stations > DDI Extensions**.

DID numbers which are not provided by the service provider and which are not used in the system should be deleted; otherwise, there may be conflicts with MSN or Internet telephony phone numbers. DID numbers that are provided by an Internet Telephony Service Provider (ITSP) must be assigned to the individual stations when configuring the ITSP (see *Configuring an ITSP*).

IMPORTANT: Whenever the phone number of a station is changed, the Smart VM (Voicemail) configured for that station is automatically reset. All personal voice messages, greetings and announcements are lost, and the password is reset.

Default Settings

The default settings should be verified for every station and adapted if required.

- **Station Number, Name, DID Number**
  Every station is assigned a station number by default (such as 101). The station can be reached internally under this call number. In system phones, this phone number appears both on the actual display and the communication partner's display. If a station number other than the actual station number is to be displayed at the external station called, this number can be defined here. You can also assign a DID number to each station. The station can be accessed directly from an external location with the DID number. The station can be reached internally via the call number 101, for example, and externally via the DID number `3654321` (MSN in a point-to-multipoint connection) or `<PABX number>-101` (in a point-to-point connection). In the case of a point-to-point connection, you can configure whether the internal phone number should be automatically entered as a DID number during initial installation. The DID number may also differ from the phone number. If you are using Internet telephony, you can also define a DID number that can be used to

reach the station via Internet telephony. This phone number is made available by the Internet Telephony Service Provider.
You can also assign a name to each station. This name appears on the communication partner's display (system phones only).
If a dial plan exists, the phone numbers, DID numbers, and names of the subscribers should be adjusted based on the dial plan.

- **Type**
  The station type can be selected for every station. For example, an IP station could have a station type of **System Client** or **SIP Client**; an analog station may be an analog phone or an analog fax machine, and an ISDN station could be an ISDN phone or ISDN fax.
- **Fax call number; Fax DID number**
  If the a fax box is to be set up for a subscriber (which can be used with the UC clients myPortal for Desktop or myPortal for Outlook, for example), assign a fax call number (for receiving internal faxes) and a fax DID number (for receiving external faxes).
- **Classes of Service**
  A station can be assigned one out of 15 possible classes of service. This determines whether a station may accept and make external calls, for example, or which numbers may be dialed by the station and which are not allowed (see *Classes of Service (Toll Restriction)*).
- **Call pickup group**
  Every station can be assigned to a call pickup group.
- **Language, call signaling**
  The language used for the menu controls of the attached system telephones can be set.
  The ring tone for an internal or external call can be selected.
- **Voicemail box (only with UC Smart)**
  With the UC solution UC Smart, you can set up a voicemail box for each subscriber and choose between different greetings. For more detailed information on the voicemail box, see *Voicemail Box (SmartVM)*
  With the UC solution UC Suite, a voicemail box is assigned automatically to each subscriber. Consequently, there are no voicemail box settings in this case.
- **Station flags**
  The station flags of each subscriber can be changed. For a description of the station flags, see *Expert mode: Station > Station > Station Parameters*.

Advanced Settings

You can configure all settings for all types of stations in Expert mode. The advanced settings can be left unaltered for default operation and only have to be changed if required. For information on the advanced settings, see *Administrator Documentation, Expert Mode*.

Related Topics

- Classes of Service (Toll Restriction)

7.13 Configuring Station Profiles

The values and properties of IP stations are stored in station profiles.

Using the **Profiles** wizard, an administrator with the **Advanced** profile can perform the following configuration tasks:

- Create a new profile
- Display profiles and their members
- Add members to a profile
- Delete members from a profile
- Export or import a single profile

In Expert mode, an administrator with the **Expert** profile can also perform the following configuration tasks:

- Change values and settings of a station profile
- Export or import all profiles

Station profiles that have already been created cannot be deleted, but can be overwritten.

7.14 Configuring the Authentication Data at the SIP Phone

The data used to authenticate a SIP subscriber at the communication system must also be entered directly at the SIP phone. The must be done by using the data that was entered in the WBM for each SIP subscriber.

The following data must be taken from the WBM and entered at the SIP phone (separately for each SIP phone):

- Password
  Password for authentication.
- SIP User ID / Username
  User name for authentication.
- Realm
  Zone or domain for authentication.

The configuration can be performed via the WBM of the SIP phone or directly on the display of the SIP phone.

7.15 Exporting Subscriber Data

Important subscriber data can be exported to an XML file.

In addition to the user data, such as the names and phone numbers of the subscribers, e-mail addresses and phone types, for example, the XML file may

also contain additional information such as group phone numbers and license assignments.

The XML file can be edited using a spreadsheet program such as Microsoft Office Excel, for example.

A template with sample data sets and a description thereof can be found in the file `csv-templates.zip` under **Service Center > Documents > CSV Templates**.

8 UC Smart

UC Smart is integrated in all OpenScape Business models (with and without the UC Booster) and offers unified communications features such as presence status and voice messages as well as conferencing, for example.

Clients for UC Smart

The UC Smart features can be used with the following clients:

- myPortal Smart
- myPortal to go (as Mobile UC App or Web Edition)
- myPortal for OpenStage
- Application Launcher
- OpenScape Business Attendant / BLF
- 3rd Party WSI Clients

The capacity limits (for expansion) depend on the OpenScape Business model being used and any possibly installed OpenScape Business UC Booster variants.

Special Aspects of UC Smart with OpenScape Business S

Due to the system architecture, the following restrictions apply to OpenScape Business S:

- The number of voicemail messages is not shown on the phone's display (MWI).
- No fax, busy or idle detection is supported for the voicemail box (SmartVM). Incoming fax calls cannot be switched to a default fax device after being answered by the SmartVM. The SmartVM records for 2 minutes.
- When connections are switched by the Company AutoAttendant to busy subscribers, the caller receives a busy signal. There is no way to leave a voice message.
- If, when checking a voice message, you want to be redirected to the phone number stored in the SmartVM (calling party number), this number must be identical to the phone number of the user that was configured for the SmartVM.
- For connections to the voicemail box (SmartVM), SIPQ trunks are occupied at the UC Booster Server and OpenScape Business S. No trunk licenses are required for this.
- MEB channels are occupied for simultaneous announcements.
- Sixty MEB channels are available for voice connections to the voicemail box (SmartVM) or AutoAttendant.

INFO: After changes in configuration of Stations, Groups, Mobility or other system parameters like trunk access codes, the UC Data for either UC Smart or UC Suite need to be synchronized. Synchronization occurs five minutes after the last configuration change. If a later configuration change occurs before the 5 minutes timer, the timer is restarted. UC Data may outdated until

synchronization starts. During the synchronization the UC Application and the Web Services Interface API are not available and any connected UC clients lose their connection until UC Data synchronization is finished. Connections are restored automatically after UC Data Synchronization is finished.

Related Topics

- UC Features (Overview)

8.1 Basic Settings for UC Smart

The basic settings for UC Smart can be customized.

UC Smart can be enabled or disabled. If UC Smart is used, UC Suite must be disabled.

Password Settings

The administrator must assign an initial password for all users of UC Smart and communicate this password to the users. The initial password may be the same for all users or different for each user. The initial password must be changed by the user when logging in at a UC Smart client for the first time. Without the assignment of an initial password, the user cannot log into to a UC Smart client.

The new password assigned by the user should meet stringent password policies.

Advanced Settings for Application-controlled Conferences (Optional)

During the basic installation, the administrator must set up the **Functional number for MeetMe Conferencing** (MeetMe dial-in number) and at least one **Functional number for Conferencing** (conference room) in the WBM.

For OpenScape Business X systems, the MeetMe dial-in number must be assigned a call destination list in which the first entry is empty and the second entry matches the call number of the voicemail box (SmartVM).

For OpenScape Business S systems, the MeetMe dial-in number must be assigned a call destination list in which the first entry matches the call number of the voicemail box (Route: Application Suite).

Finally, the MeetMe dial-in number must also be assigned a standard voicemail box.

The description of the configuration can be found here: *How to Configure Application-controlled Conferences*,

License Assignments

The administrator must assign a UC Smart User license to each UC Smart user.

Additional licenses can be optionally assigned for:

- Voicemail (also usable without UC Smart)

- Conference
- Application Launcher

8.2 UC Smart Clients

UC Smart clients provide subscribers with convenient user interfaces for unified communications.

The system offers the following UC Smart clients for the following devices:

Client type	Client	Device
Communications Client	myPortal Smart	PC
	myPortal for OpenStage (UC Smart)	OpenStage telephone
Mobile Client	myPortal to go (UC Smart) (see *Mobility*)	Smartphone, Tablet PC
Communications Client	OpenScape Desk Phone CP 400/ 600 HFA(integrated Client to phone software)	OpenScape Desk Phone CP 400/600 HFA

8.2.1 myPortal Smart

myPortal Smart is an Adobe AIR-based PC application (Microsoft Windows and Mac OS X) for unified communications using the UC solution UC Smart. Besides convenient dialing aids via phone directories and favorites and information on the presence status of colleagues, you can, for example, also access your voicemails.

Depending on the licenses assigned to you, the scope of the available features may vary slightly.

myPortal Smart supports the following features:

- Presence status
- Status-based call forwarding
- Directories
- Favorites List
- Journal
- Search by phone number and name
- Call Functions
- One Number Service (ONS)
- Voicemail
- Text messages

INFO: Some features such as consultation holds and conferencing are not available in myPortal Smart in conjunction with SIP telephones.

8.2.2 myPortal for OpenStage

myPortal for OpenStage is the user portal for accessing unified communications functions on your system telephone.

The configuration of myPortal for OpenStage is possible directly on the system telephone via the administrator settings or via the WBM of the system telephone.

myPortal for OpenStage provides the following features:

- Presence status

8.2.3 Prerequisites for myPortal Smart

In order to use the UC client, the client PC must be equipped with the appropriate hardware and software configurations. Depending on the configuration, administration rights are required for the installation and automatic updates. The available functionality depends on the licenses being used.

INFO: Please make sure that you refer to the latest information in the Experts wiki.

INFO: In case of Windows OS, TLS 1.2 in Internet Options (in control panel) must be activated and the latest patches from Microsoft must be installed or activated manually.

If above actions are not performed then HTTPS access will be rejected.

Telephones

myPortal Smart can be used in combination with the following telephones:

- OpenStage HFA and SIP
- OpenScape Desk Phone IP 35G/55G HFA and SIP
- OpenScape Desk Phone IP 35G Eco HFA and SIP
- OpenScape Desk Phone CP 200/400/600 HFA and SIP
- SIP phones with 3PCC support
- Analog telephones
- ISDN Phones
- OpenScape Personal Edition HFA and SIP

- OpenStage S5/M3/SL4 (OpenScape Business Cordless)
- optiPoint WL3 professional SIP

Older devices (such as optiPoint 410/420/500, Gigaset M2/SL3/S4 and optiPoint WL2 SIP) are supported. Optiset E devices cannot be operated. For details on the tested and released devices, please refer to the Release Notice.

INFO: OpenScape Desk Phone CP 400/600 HFA integrated Client does not have any special prerequisites, apart from the standard client configuration and license.

INFO: Some features such as consultation holds and conferencing are not available in myPortal Smart in conjunction with SIP telephones.

INFO: For analog and DECT telephones, the Message Waiting Indication (MWI) is not supported, and only limited support is available for displaying information on the phone.

Additional Software

- Adobe AIR V16.0 or later

Minimum Hardware Requirements

According to the requirements of Adobe AIR.

Web Browsers

The following web browsers have been released for programming telephone keys via the UC client:

- Microsoft Internet Explorer Version 10 (or later)
- Mozilla Firefox Version 19 (or later)
- Google Chrome

Installation Files

The administrator can download the installation files from the **Service Center > Software** and make them available to users via a network drive, for example.

Related Topics

- Licenses

8.2.4 Prerequisites for myPortal for OpenStage

In order to use myPortal for OpenStage, the phone must be equipped with the appropriate hardware and software.

Telephones

myPortal for OpenStage can be used with the following telephones:

- OpenStage 60/80
- OpenScape Desk Phone IP 55G

Web Browsers

myPortal for OpenStage can be used in combination with the following web browsers (for configuration and administration):

- Microsoft Internet Explorer Version 10 (or later)
- Mozilla Firefox Version 19 (or later)
- Google Chrome

8.3 Users of UC Smart

Users of UC Smart are subscribers who use the UC Clients of UC Smart.

The following settings for UC Smart clients are available in UC Smart Assistant:

Settings	Explanation
Settings	
Users	The setting is only displayed here.
Name	The setting is only displayed here.
Password	Password for UC Smart clients and UC Smart Assistant.
Language	Language of the user interface.
The user must assign a new password	The setting is only displayed here.
UC Smart Assistant access	User permission for the use of UC Smart Assistant in the web browser for configuration tasks.
Configured as Mobility stations	The setting is only displayed here.
Voicemail licence	The setting is only displayed here.
Associated Services	The setting is only displayed here.
Profile details	
Mobile phone number	Mobile phone number of the subscriber in canonical format (e.g., `+ 49 173 1234567`).

Settings	Explanation
Private/External phone number	Additional phone number of the subscriber in canonical format (e.g., `+ 49 89 987654321`).
E-mail Address	E-mail address of the subscriber.
Voicemail to e-mail	Enable/disable the e-mail notification when a new voice message is received.
Presence visibility	Setting that determines whether the presence status is visible to both internal and external subscribers or just to internal subscribers or not visible to any subscribers.
Licence information	
Display of licenses assigned to the user	

8.4 Presence Status (Presence)

The Presence status in the internal directory provides information on the availability of internal subscribers (including Mobility Entry stations). The Presence status also controls the availability of internal subscribers using status-based call forwarding.

As a subscriber, you can change your Presence status in myPortal Smart, myPortal to go or myPortal for OpenStage. For every change in the presence status (except for **Office**), you can also define the scheduled time of your return to the **Office** status if required.

As a subscriber, you can select the following statuses:

- **Office**
- **Meeting**
- **Sick**
- **Break**
- **Gone Out**
- **Vacation**
- **Lunch**
- **Gone Home**
- **Do Not Disturb** (not available on MULAP configurations)

Using the status-based call forwarding, calls can be forwarded to the personal voicemail box, for example. Subscribers who have no personal voicemail boxes can forward calls to a group mailbox or a system mailbox. However, they have no access to these voicemail boxes via myPortal Smart.

8.5 Directories and Journal

Directories and the Journal organize contacts and calls.

8.5.1 Directories

Directories are used to organize the contacts of subscribers. Subscribers can access these contacts with UC Smart clients.

The system provides the following directories, which support the following functions and with the below priority for lookup number (lookup number will be supported only for external call and in case that CO/ITSP does not provide the name):

Directory	UC Smart Clients	System telephone with a display
Personal directory	Outlook contacts imported via the Personal Assistant.	
Internal directory	Contains all internal subscribers and groups (with their phone numbers) for which the display has been activated in the system. Internal subscribers with system telephones are shown with presence status. The Presence status of a subscriber can only be shown if allowed by that subscriber.	Contains all internal subscribers and groups for which the display has been activated in the system.
Favorites list	Contains the contacts selected by the subscriber from his or her personal contacts and the internal directory. Internal subscribers with system telephones are shown with their respective presence statuses. The Presence status of a subscriber can only be shown if allowed by that subscriber.	
System Directory	Contains all central speed-dial numbers.	

INFO: Phone numbers in directories should always be entered in canonical format wherever possible.

8.5.2 Internal Directory

The internal directory contains the contact details of the internal subscribers and MULAP groups of the communication system. UC Smart clients can access the internal directory.

As an administrator, you have unrestricted access to all data in the internal directory. As a subscriber, you can dial from the internal directory.

The station parameter **Entry in telephone directory** (which can be set in the WBM via the Stations wizard) determines whether or not internal subscribers and groups are displayed in the internal directory.

In an internetwork, the internal directory applies across all nodes.

Related Topics

- Group Call

8.5.3 Favorites List

The Favorites list contains the contacts selected by the subscriber from the personal contacts and the internal directory. UC Smart clients have access to the Favorites list.

A UC Smart user can call a contact directly from the Favorites list. When an internal subscriber receives a call, the ringing state of the subscriber is displayed. The UC Smart user can then accept this call. In addition, the presence status for internal subscribers is displayed.

8.5.4 System Directory

The system directory contains all central speed-dial numbers for which a name was assigned. UC Smart clients can access the system directory.

The administrator individually disable the display for every subscriber and every speed-dial number with a name.

8.5.5 Unified Directory

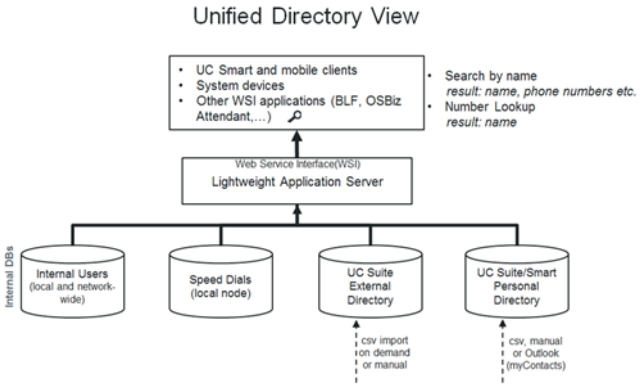
OpenScape Business provides different data sources to store and to retrieve user or contact related data, starting with the internal user data in the internal user configuration, via the internal speed dial list, up to the different directories of the UC applications.

Each data source within OpenScape Business is used by a specific client application either located within the system SW itself in the phone devices or within a UC client application. Depending on the used data sources and the used clients, the retrieved data and their presentation is different.

The "Unified Directory" service within OpenScape Business comprises the existing OpenScape Business data sources for common search and name resolution functions. It provides the same search result or name resolution information to all system devices and OpenScape Business clients.

The Unified Directory service can either be accessed via the Web Service Interface (WSI) from externally located clients like myPortal to go or internally via

the call processing mechanisms (e.g. from OpenStage



Phones).

Unified Directory uses following internal databases and directories of OpenScape Business:

- Internal user directory (network wide)
- Speed dial lists
- UC Smart Personal Directory (optional)
- UC Suite External Directory (optional)
- Personal Outlook Contacts (if imported via myContacts)

The Unified Directory service is available within every OpenScape Business system from V2R2 on. It does not require specific HW-SW or license prerequisites.

In order to get best results when using the Unified Directory some rules regarding phone number formats and writing of names have to be followed.

8.5.5.1 Features

Unified Directory Service provides:###P###

- Directory Search in several internal data sources of OpenScape Business
- Unified offering of the search result to all supported clients
- Phone number Look-Up / Name Resolution in several internal data sources
- Unified offering of name resolution results for all supported clients
- External data access via the WebServices Interface (WSI)

The features are available for single node systems as described in the following. Within OpenScape Business networks, the availability of the features depends mainly on the kind of connection of the trunks, devices and clients within the network.

Supported Devices / Clients

Unified Directory supports following clients / system devices of Unify using the indicated interfaces:

Device/Client	Used Interface/Protocol	Remarks
OpenStage phones	Call Processing / HFA protocol	WSI / HTTP(S) is optional on OpenStage 60/80 for caller images
OpenScape Deskphone IP	Call Processing / HFA protocol	WSI / HTTP(S) is optional on DeskPhone IP 55 for caller images
Cordless (CMI) devices	Call Processing / CMI protocol	
CP200	Call Processing / HFA protocol	
DeskPhone CP200/CP600	WSI / HTTP(S)	
myPortal Smart	WSI / HTTP(S)	
myPortal to go	WSI / HTTPS	
Openscape Business Attendant/BLF	Call Processing / CorNet protocol	WSI / HTTP(S) is optional

INFO: The UC Suite myPortal, myAttendant and myAgent clients use their own mechanisms for directory search and name resolution.

Search function

The Unified Directory search is always performed by using the specific device / client user interface. The search criterions and the used character set could be restricted, depending on the used clients.

After the search criterion is entered the search is performed within subsequentdirectories

- Internal user directory (network wide)
- Speed dial lists
- UC Smart Personal Directory (optional)
- UC Suite External Directory (optional)
- Personal Outlook Contacts (if imported via myContacts)

All matches within the directories above are shown as search results together with their origin. The matches contain either the full contact data set or only parts of it. The information depth of the results depends on the data souce.

The matches are presented at the devices or clients depending on display capabilities.

	Internal UserDirectory	SpeedDials	UC SmartPersonalDirectory	UC SuiteExternalDirectory	PersonalOutlookContacts (viamyContacts)
Last Name	X	---	X	X	X
First Name	X	---	X	X	X
Short/ Displayname	X	X	---	---	---
Office Phone No.	---	---	X	X	X
Home/Ext. PhoneNo.	---	---	X	---	X
Mobile Phone No.	---	---	X	X	X
XMPPID	---	---	---	X	---
Email-Adr.	---	---	X	X	X
Company name	---	---	X	X	X
City	---	---	---	---	---
Contact Picture	---	---	X	---	X
Contact Picturepreview	---	---	X	---	X

Phone Number Look-Up

Unified Directory Phone number Look-Up resolves the transferred calling party (CLI) by a number search in all supported internal data sources . The search is perfomed within following phone number fields:

- Office number
- Mobile number
- Home number

The Phone number Look-Up is triggered in case of incoming or outgoing calls in general, whereas specific routing and forwarding features are considered in addition.

A fixed prioritization of the data sources that are used for Phone number Look-Up is implemented in order to get the result as fast as possible. The result contains either only lastname, firstname, displayname or ,if available, the full related contact data.

Table: Supported Data Sources and Prioritization

Priority	Data Sources	Remark
1	CO/ITSP name (as sent by provider)	Prerequisite is to enable flag "Name in CO".
2	Speed dial list	
3	Personal Contacts	
4	UC User detail	

The retrieved data are presented on the user's device and/or in the UC client. The information depth depends on the display capabilities.

- **Incoming calls**
  Supported scenario for single node systems:
  - Basic call
  - Group call/ MULAP call
  - Ringing Group
  - Single Step Call Transfer (SSCT)
  - Attended/Supervised/Consultation Transfer
  - Call Forwarding Unconditional (CFU)
  - Call Forwarding No Reply (CFNR)
  - Call Forwarding Busy (CFB)
  - Blind transfer
  - Call Pickup

  Supported scenario for multi node (network) scenarios is a Gateway Call.
- **Outgoing call**
  In case of an Outgoing Call the Phone number Look-Up of the called partynumber happens only once.
  Supported scenario for single node systems is a Basic Call to externalnumber.

The presentation of the Phone number Look-Up result depends on display capabilities of the phones.

8.5.5.2 Rules and Conventions

Some conventions regarding number and name formats within the data sources have to be observed in order to get optimal results using the Unified Directory service.

Supported Number Format

All external phone numbers within the data sources must be entered in the canonical format including country and area code. e.g.+4989700712345

INFO: Speed Dial list supports only system dialable format e.g. 0089700712345 or 0004989700712345

Supported Name Formats

The following conventions regarding name formats and character sets have to beobserved:

- **Speed dial name format**
  Name search within the Speed Dial List is supported only with specific configuration rules. The first and last names have to be entered within the existing name field using the following pattern:
  <Last Name>, <First Name> (comma separated)
- **Internal Users in case of Migrations**
  Migration to V2R1 and onwards with internal users that do not follow these configuration rules will not be supported in the expected way. This means the administrator should convert internal names to the following pattern before migration:
  <Last Name>, <First Name> (comma separated)

Availability of directory changes

After creating, updating or deleting contacts in the various data sources it can take up to 10 minutes until all changes appear on Phone number Look-Up results.

8.5.5.3 Functional Boundaries

The following functional boundaries do exist regarding Unified Direcrories:

Name Search

- Group name support
  Group names (not MULAP names) can currently not be searched in all kindof configurations
- Support of special characters
  On most phone devices the user can only search for standard characters "a-z". Special (diacritical) characters like German characters Ää,Öö,Üü, ß are not accessible via phone device user interface. Therefore special characters are not supported in search filter.
  Names including special characters cannot be searched via the Unified Directory.
- Support of Speed Dial Name format
  Name search within the Speed Dial List is supported only with specific configuration rules. The first- and last names have to be entered within the existing name field using one of the following patterns
  - <Last Name>, <First Name> (comma separated)
  - <First Name> <Last Name> (space separator on this case)

Name Presentation

Personal Contacts in UC Smart and from external offline directory, with length of first name plus length of last name greater than 24 characters, will be truncated to 24 characters length to fit the display length of the devices.

Phone number Look-up

The Phone number Look-Up feature (retrieve contact name from calling party number) is not supported in Unified Directory for SIP and S0 devices.

8.5.5.4 Unified Directory in Networked Systems

The Unified Directory Service is active within every node of an OpenScape Business Network and uses the datasources of the own system. Phone Devices and Client use always the Unified Directory Service within their own node.

Therefore it depends on the kind of datasource content if netwide contacts are available.

Table: Local and Netwide Datasource

Data source	Local data	Netwide data
Internal user directory	X	X
Speed dial lists	X	---
UC Smart Personal Directory	X	---
UC Smart Personal Directory	X	---
Personal Outlook Contacts (via myContacts)	X	---

Phone number Look-up

In Networking scenarios the Phone number Look-Up functionality is not used. In such scenarios the name is transported via normal networking mechanisms between the network nodes.

For internal users the configured Display Name is used so Lookup is not required.

8.5.6 Journal

The journal is the list of all incoming and outgoing calls of a subscriber. It enables subscribers to quickly and easily respond to missed calls and call back their contacts or call them again directly from within the journal.

A maximum of the last 100 calls are displayed to UC Smart users.

Folder for Call Types

The calls can be arranged in the following groups:

- **Open**
- **Missed**
- **Accepted**
- **All Calls**

Call Details

Every call is shown with the Date and Time and, if available, with the call number. If a directory contains further details on the call number such as the **Last Name** and **First Name**, then this information is also shown. In addition, the **direction** and **duration** of the calls are displayed, as well as any redirections and call pickups that may have occurred.

8.6 Calls

For calls, the call number format is of particular importance.

8.6.1 Call Number Formats

Call numbers can be specified in different formats.

Format	Description	Example
Canonical	Begins with + and always includes the country code, area code and the full remaining station number. Blanks and the special characters + ( ) / - : ; are allowed.	+49 (89) 7007-98765
Dialable	Exactly as you would dial the call number on the system telephone in your office, always with the trunk access code.	• 321 (internal) • 0700798765 (own local network) • 0089700798765 (external local network) • 0004989700798765 (international)

INFO: If possible, you should always use the canonical call number format. This ensures that a phone number is always complete, unique and consistent for networking and mobile stations in every situation.

When dialing an external station (dialable format) manually, the CO access code must always be dialed as well.

When dialing an external phone number in dialable format from a directory (and when using the Desktop Dialer and Clipboard Dialer for certain UC clients), the communication system automatically adds the CO access code (route 1).

> ***INFO:*** For calls within the USA via CSTA to a number in canonical format, phone numbers are converted to the dialable format.

8.7 Conferences

In a conference, multiple participants (including external parties) can communicate with one another at the same time. The Conference Management function enables you to quickly and easily host conferences and also to schedule them in advance.

Phone-controlled and Application-controlled Conferences

As a subscriber, you can initiate conferences both via the phone and via the myPortal Smart application.

You can initiate a phone-controlled conference in the following ways, and then control that conference via the phone:

- Call the desired conference participant and connect him or her to the conference
- Extend a consultation call into a conference
- Extend a second call into a conference

You can initiate, control and manage application-controlled conferences via the Conference Management of myPortal Smart. A Conference license is required for the use of Conference Management.

Differences between the conference types:

	Phone-controlled conference	Application-controlled conference
Direction of connection setup from the viewpoint of the system	• Outbound	• Inbound (dial-in by the participant)
Authentication of conference participants	-	• Personal PIN (conference ID) • Guest PIN (optional)
Predefined invitation to the conference participants	-	• Conference Name • Dial-in number (MeetMe) • Personal PIN (conference ID) • Guest PIN (optional)
Max. number of participants per conference	8	16

Scheduled Conference

Scheduled conferences are created as permanent conferences. The conference can be used as needed at any time without further scheduling. Scheduled

conferences do not occupy any conference channel so long as no participant has dialed into the conference. The order of dialing in determines the assignment of the conference channels.

Administrators can change the specified dial-in number (MeetMe) for conferences via the WBM during the initial setup. The dial-in number with which the participants can dial into the conference is shown to the participants. They are then required authenticate themselves with their personal PIN or with the general guest PIN if allowed.

Moderators

The initiator of a conference is automatically the moderator and can:

- Create, edit and delete scheduled conferences.
- Add and remove conference participants.
  Removed participants do not remain in the conference.
- Disconnect conference participants.
  Disconnected participants can dial back into the conference.
- Specify another internal participant on the same node as the moderator
- Leave the conference without ending it immediately.
  If the last moderator leaves the conference, it ends after 5 minutes.
- End active conferences.
- Start a web collaboration session in an active conference.
- Send predefined invitations to all or individual conference participants.

All internal participants within a node can be moderators. However, a conference license is required for this.

Conference participants whose contact details were entered manually are treated as external participants and cannot be set as moderators.

Conference Participants

Conference participants can leave the conference and dial-in again. In addition, they can participate in a web collaboration session has already been started. As long as a conference has only one participant, the participant hears music on hold. The maximum number of external conference participants is limited, inter alia, by the number of available trunks.

Symbol	Status	Description
	Inactive	The participant is not in the conference. No conference channel is used.

Symbol	Status	Description
	Dialing in	The participant is just dialing into the conference.
	Waiting	The participant is in the conference and is currently listening to music on hold.
	Active	The participant is in the conference. A conference channel is in use.

Automatic Termination without a Moderator

If the last moderator leaves the conference, the other participants are notified with an info text that the conference will end after about 5 minutes.

Notification of Conference Participants

The moderator can send all or some conference participants an invitation by email. This requires an email program to have been installed on the client PC. Known email addresses are automatically added to the distribution list. In an invitation to all conference participants, only the general guest PIN (if allowed) is included; for individual invitations, the personal PIN is also sent.

Alternatively, a predefined invitation text can be copied to the clipboard for further use in other programs (e.g., a chat program).

8.8 Web Collaboration

myPortal Smart supports the integration of the separate product Web Collaboration for simultaneous multi-media collaboration during phone calls and conferences. This provides quick access to functions such as desktop and application sharing, file sharing, co-browsing, whiteboarding, URL push, IM chat and video chat with multiple participants.

Web collaboration can be started by a subscriber during a phone call via the Call window of the UC PC client or by the moderator of an active conference from within the conference. A Web page from which the download of the web collaboration client can be initiated is opened. A local installation of Web Collaboration on the UC PC client is not required. If an email program is available on the UC PC client, an email with the link to the web collaboration client can be sent to the communication partners. Detailed information on web collaboration can be found in the Web Collaboration product documentation.

On deleting or ending a conference, the associated web collaboration session is automatically deleted as well.

Integration of Web Collaboration

In order to integrate web collaboration, the license number and password for the hosted web collaboration connection must be entered by the administrator in the

WBM. The vendor offers the web collaboration server as a service on the Internet (Public Server). The license number and password are transmitted over a secure https connection. By default, TCP port 5100 is used for this purpose. Local web collaboration servers are not supported.

INFO: In order to use web collaboration, the UC PC clients and the communication system require an Internet connection. Connections via a proxy are not supported by the communication system.

Instant Messaging and Web Collaboration

Note that Instant Messaging of the system and Instant Messaging of a web collaboration session are mutually independent, i.e., the instant messages from a UC PC client do not appear in a web collaboration session of the same participant, and vice versa.

8.9 Instant Messaging

Instant Messaging refers to communicating with instant messages (usually called a chat).

8.9.1 Instant Messaging

Using instant messaging, you can chat with other users of UC Smart.

The sent and received instant messages are presented to the communication partners as an interactive dialog. On selecting a recipient, the client shows whether the communication partner is currently online. If a communication partner is offline, no instant message can be transmitted to him or her. The IM overview page displays the most recent streams. The system stores a limited number of instant messages. A maximum of up to 100 of the last instant messages of a user are displayed.

8.10 Voicemail Box (SmartVM)

The voicemail box (also called SmartVM) plays a greeting to callers and offers them the option of recording a message or being routed to another number. Internal subscribers can access the voicemail box via a telephone and with the UC Smart client myPortal Smart. Subscribers who want to use a voicemail box require a voicemail license.

Voicemail Box Types

The following different voicemail box types exist:

- Standard voicemail box:
  The standard voicemail box is the personal voicemail box of a subscriber. It accepts the call, greets the caller with a personal or standard announcement and offers the caller the option to leave a message. The standard voicemail box can be configured by the subscriber (by recording a personal greeting, for example) via the telephone or via myPortal Smart.
- Group voicemail box:
  The group voicemail box has the same features as the standard voicemail box, except that it is not assigned to a single user, but a group of users. Messages can be recorded for a group voicemail box only if at least one member of the group has a voicemail license. The info of the voicemail box is displayed to all group members with a voicemail license. Message playback is possible through the phone menu of the personal voicemail box of the group members.
- Attendant voicemail boxes (AutoAttendant / Company AutoAttendant):
  The Attendant voicemail box offers callers a greeting with or without subsequent routing options. A special form of the AutoAttendant voicemail box is the Company AutoAttendant. Here, the caller can be optionally forwarded automatically (to the switchboard, for example) or selectively to another station (e.g., to the service or hotline) by dialing an internal call number or speed dial number (digits 0-9). These dialing options must, of course, be explained with a corresponding announcement. It is also possible to configure an intercept destination to which the caller will be redirected if he or she fails to enter a digit or enters an invalid (i.e., unassigned) digit. The administrator can configure up to 100 Attendant voicemail boxes.
- Announcement voicemail box:
  The announcement function is configured by assigning an announcement index to an announcement port and configuring a voicemail box with the call number of the announcement port. The greeting of the mailbox is used as the announcement. Depending on the type of announcement, the playback may occur once (outgoing message) or cyclically (music). The phone menu of an announcement voicemail box can only be used from a different phone, since there is no associated phone. Consequently, a different PIN must be used for the announcement voicemail box than for the voicemail box of the used telephone.
- System voicemail box:
  The voicemail box with the call number of the hunt group of the SmartVM is used as a system voicemail box. The system voicemail box must be a standard voicemail box (not an AutoAttendant) with voice recording enabled. The info of the voicemail box is displayed to the owner of the voicemail box with index 1 and can also be checked from there. This first voicemail box should not be a Group, Attendant or Announcement voicemail box. If the system voicemail box is not to be used, then no voicemail box should be configured with the call number of the SmartVM hunt group.

Features of the Voicemail Box

- Checking and control via a telephone
  (from external location: own telephone number required)
- Manual or automatic selection of different greetings
- Phone menu (Telephone User Interface, TUI) with a system-wide switchable menu structure:
  - Phone menu, UC Smart: **SmartVM** (similar to Xpressions Compact / EVM)
  - Phone menu, UC Suite: **OSO** (similar to UC Suite)
- Up to 320 voicemail boxes can be set up per system
- Up to 32 hours of voice recording capacity per system
- Up to 100 stored messages per voicemail box
- Up to 2 minutes of recording time for a voicemail per voicemail box
- Up to 10 simultaneously possible switching and call answering operations
- Announcement/music before answering
- Playback of individual announcements
- Forwarding of fax calls through automatic fax tone recognition to a preconfigured fax destination

> ***INFO:*** Details on the phone menu can be found in the two Quick Reference Guides, UC Smart Telephone User Interface (TUI) and UC Suite Telephone User Interface (TUI).

Code Number Settings

Before the first use of the voicemail box, every subscriber must change the preassigned code number (default: `123456`).

The code number consists of a six digit sequence. Repeated digits (e.g., `333333`) and digit sequences in ascending or descending order (e.g., `987654`) are not allowed. After an invalid code number has been entered six times, access to the corresponding voicemail box is locked until the password is reset by the administrator. After two incorrect entries of the password via the phone menu, the connection is dropped.

Ports

The voicemail box uses the S_0 ports 500 to 509, which are assigned the call numbers 739 to 748, respectively. The ports 504 and 505 are assigned by default to the Company AutoAttendant (call number 352), and the remaining 8 ports are assigned to the voicemail box of the hunt group (call number 351). The call number 351 is the general call number of the voicemail box via which the phone menu is accessible.

Toll restriction

For security reasons, the ports of the voicemail box only have outward-restricted trunk access by default. The following features require the assignment of a COS group with direct trunk access:

- Call sender of a voice message
- Mobility users can listen to voice messages via callback
- Messages are transferred to an external destination using the Company AutoAttendant

Greetings / Announcements

Custom greetings (= announcements) can be either recorded from a phone or loaded into the system with the WBM. The configuration of a custom greeting via the phone occurs by dialing the voicemail box number and then using the user prompts of the voicemail box to record a new greeting over the phone.

Greetings can, however, also be loaded into the system separately for each voicemail box and subsequently saved or deleted in Expert mode.

8.10.1 Configuring the Voicemail Box (SmartVM)

Configuring the voicemail box (SmartVM) includes the configuration of standard/ group voicemail boxes and the Attendant voicemail boxes.

The general settings for the voicemail box (SmartVM) such as the adaptation of the voicemail box call number to a 4-digit dial plan, for example, are made via the **SmartVM** wizard.

The special settings for the voicemail box (SmartVM) and the setup of standard/ group voicemail boxes and Attendant voicemail boxes are performed in Expert mode.

> ***INFO:*** Changing a call number resets the voicemail box of the corresponding subscriber. All personal voice messages, greetings and announcements are lost, and the password is reset.

You can also load individual greetings into the SmartVM, save and delete them, as well as back up and restore the greetings and messages of individual or all voicemail boxes. In addition you can check the loaded languages of the user prompts and display the 10 voicemail boxes with the most messages as well as the amount of storage space used by the messages and greetings.

The setup of Attendant voicemail boxes can be found in the section Attendants - AutoAttendants - Company AutoAttendant (UC Smart).

Assigning the Mailbox to Subscribers

Once the voicemail box (SmartVM) has been configured, the subscribers can be assigned their default mailboxes. This is possible through

- call forwarding for the subscriber with the aid of a call destination list (set up by the administrator). In this case, the call is forwarded sequentially to the selected call destinations (e.g., first to the subscriber and then - after a definable time period - to the mailbox).

- Call forwarding set up at the phone of the subscriber (which can be done by the subscribers themselves). In this case, the call goes immediately to the mailbox.
  If the subscriber is a member of a hunt group and the hunt group is called, the call is not redirected to the voicemail box of the hunt group.

8.10.2 Notification Service for Messages

The system can optionally notify a UC Smart user about a new voicemail by e-mail.

Prerequisites for the Notification Service

- The delivery of e-mails (e-mail forwarding) has been configured by the administrator in the system.
- The user's e-mail address must be known to the system. The administrator can import all e-mail addresses in the WBM during the initial installation via an XML file or enter an e-mail address for each user in the UC Smart Assistant (see *Administrator Documentation: UC Smart - Users of UC Smart*). Alternatively, users can specify their own e-mail addresses in their UC Smart client.
- A Voicemail licence is assigned to the user.
- The **Voicemail to e-mail** feature is enabled. The administrator can activate the feature for each user in the UC Smart Assistant (*Administrator Documentation: UC Smart - Voicemail Box / Smart VM*). Alternatively, users can activate the feature themselves in their UC Smart client.

The UC Smart user receives an e-mail with the voicemail as an attached WAV file (16 bit, mono), together with the date and time of receipt, duration of the voicemail and, if available, the phone number and name of the sender.

9 UC Suite

The UC Suite provides unified communications features such as the Presence status and CallMe, conferencing, as well as voicemail and fax functionality in the myPortal for Desktop and myPortal for Outlook clients. myAttendant also provides Attendant Console functions.

INFO: For the OpenScape Business hardware models X3/X5/X8, the UC solution UC Suite requires the UC Booster hardware (UC Booster Card or UC Booster Server). With OpenScape Business S (softswitch), the UC solution UC Suite is already integrated.

INFO: After changes in configuration of Stations, Groups, Mobility or other system parameters like trunk access codes, the UC Data for either UC Smart or UC Suite need to be synchronized. Synchronization occurs five minutes after the last configuration change. If a later configuration change occurs before the 5 minutes timer, the timer is restarted. UC Data may outdated until synchronization starts. During the synchronization the UC Application and the Web Services Interface API are not available and any connected UC clients lose their connection until UC Data synchronization is finished. Connections are restored automatically after UC Data Synchronization is finished.

9.1 Basic Settings for UC Suite

The basic settings for UC Suite can be customized.

UC Suite can be enabled or disabled. If UC Suite is used, UC Smart must be disabled.

In addition, for all UC calls initiated by the system (e.g., via the Call-Me service), a check can be performed before dialing to determine whether the requesting UC user has the requisite class of service for that call. If the UC user does not have the required class of service, the call is not executed.

9.2 UC Suite Clients

UC Suite clients provide subscribers with convenient user interfaces for comprehensive unified communications functions.

The system offers the following UC Suite clients for the following devices:

Client type	Client	Device
Communications Client	myPortal for Desktop	PC
	myPortal for Outlook	
	Fax Printer	
	myAttendant	
	myPortal for OpenStage (UC Suite)	OpenStage telephone
Mobile Client	myPortal to go (UC Suite) (see *Mobility*)	Smartphone, Tablet PC
Contact Center Client	myAgent (see *Multimedia Contact Center*)	PC
	myReports (see *Multimedia Contact Center*)	

Subscribers with a configured e-mail address receive a welcome e-mail with Getting Started instructions.

Custom Settings

The custom (i.e., subscriber-specific) settings for myPortal for Desktop are stored in ini files on the PC. A separate ini file is created for every user. The custom settings for myPortal for Outlook, myAttendant and Fax Printer are stored in the registry of the PC. This enables different users to use the myPortal for Desktop, myPortal for Outlook, myAttendant and Fax Printer applications on a single PC (Desk Sharing) and also the deployment in Windows Terminal Server and Citrix Server environments. This allows different users to access the applications from their PCs without a local installation.

9.2.1 myPortal for Desktop

myPortal for Desktop is a client for unified communications on your PC. Besides convenient dialing aids via phone directories and favorites and information on the presence status of other subscribers, users can, for example, also access their voicemails and fax messages.

myPortal for Desktop provides the following features:

- Directories
- Favorites List
- Journal
- Desktop Dialer
- Screen Pops
- Presence status
- CallMe service with ONS (One Number Service)
- Status-based call forwarding

- Personal AutoAttendant
- Conference management
- Recording conferences
- Record calls
- Instant Messaging
- Voice and fax messages

9.2.2 myPortal for Outlook

myPortal for Outlook is the client for unified communications in Microsoft Outlook (plug-in) and is analogous to myPortal for Desktop.

myPortal for Outlook provides the following features in addition to those of myPortal for Desktop:

- How to Call an Outlook Contact
- How to Create an Outlook Contact from the Sender of a Voice Message
- How to Send a Voice Message as an E-mail
- How to Send a Fax Message as an E-mail

9.2.3 Fax Printer

Fax Printer is a Windows application for sending fax messages with individually created cover sheets from other Windows applications such as Microsoft Word, for example.

Fax Printer consists of the following components:

- Fax Printer Cover Editor
- Fax Printer Driver - with the following features:
  - Sending faxes to individual recipients
  - Directories
  - Use of central cover sheets
  - Using predefined headers
  - Merge fax
  - Control via the user interface
  - Control via the command line

9.2.4 myAttendant

myAttendant is a unified communications solution for Attendant functions. Besides convenient Attendant functions, dialing aids via phone directories and information on the presence status of other subscribers, myAttendant can, for example, also be used to access voicemails and faxes. Instant Messaging supports the communication with internal subscribers.

myAttendant provides the following features:

- Attendant functions
- Directories
- Journal
- Pop-up windows
- Change the presence status of subscribers
- Record calls
- Message Center
- User Buttons
- Manage voice and fax messages
- Instant Messaging
- Team functions
- Conference management

9.2.5 myPortal for OpenStage

myPortal for OpenStage is the user portal for accessing unified communications functions of the system on your system telephone.

The configuration of myPortal for OpenStage is possible directly on the system telephone via the administrator settings or via the WBM of the system telephone.

myPortal for OpenStage provides the following features:

- Presence status
- Voicemail

9.2.6 Prerequisites for UC Suite PC Clients

In order to use UC Suite PC clients, the client PC must be equipped with the appropriate hardware and software configurations. Depending on the configuration, administrator rights are required for the installation and automatic updates. The available functionality depends on the licenses being used.

INFO: Please make sure that you refer to the current notes in the `ReadMe first` file, which is located in the storage directory of the install files.

Telephones

The UC clients can be used in combination with the following telephones:

- OpenStage HFA and SIP
- OpenScape Desk Phone IP 35G/55G HFA and SIP
- OpenScape Desk Phone IP 35G Eco HFA and SIP

- OpenScape Desk Phone CP 200/400/600 HFA and SIP
- SIP phones with 3PCC support
- Analog telephones
- ISDN Phones
- OpenScape Personal Edition HFA and SIP
- OpenStage S5/M3/SL4 (OpenScape Business Cordless)
- optiPoint WL3 professional SIP

Older devices (such as optiPoint 410/420/500, Gigaset M2/SL3/S4 and optiPoint WL2 SIP) are supported. Optiset E devices cannot be operated. For details on the tested and released devices, please refer to the Release Notice.

INFO: OpenScape Desk Phone CP 400/600 HFA integrated Client does not have any special prerequisites, apart from the standard client configuration and license

INFO: For analog and DECT telephones, the Message Waiting Indication (MWI) is not supported, and only limited support is available for displaying information on the phone.

Operating Systems

The UC Suite PC clients can be used in conjunction with the following operating systems:

- Apple Mac OS X 10.10 / 10.9 / 10.8 / 10.7
- Microsoft Windows 10 / 8.1 / 8 / 7 (both 32-bit or 64-bit are possible)
- Microsoft Windows Vista (32 bit)
- Office 365 (local installation = Office 2013)

INFO: The used operating system always requires the latest version of all available updates (Service Packs and patches).

Support for the UC Suite PC clients for Microsoft Office 2003, Microsoft Windows XP and Microsoft Windows Server 2003 will end at the same time as the end of support for these products by Microsoft. The product will still be supported, but will no longer be tested in detail.

Local administrator rights on a client PC are required for the installation under Windows, but not for automatic updates. The Russian and Chinese user interfaces of myPortal for Outlook require a corresponding Russian or Chinese Windows installation.

myPortal for desktop for Apple MAC is available with same interface as under Microsoft Windows. However, due to the Apple MAC OS system architecture, the following functions are currently not supported:

- Sending faxes
- Outlook, Entourage Integration

myPortal for Outlook is supported in Microsoft Office 365 environments. Microsoft Office 365 is a cloud application It includes, among other things, an Exchange server for the centralized distribution of e-mails as well as the traditional Microsoft Office products. OpenScape Business supports Microsoft Office 365.

The following functions can be used under Microsoft Office 365:

- Exchange Calendar Integration
- E-Mail Forwarding

Web Browsers

The following web browsers have been released for programming telephone keys via the UC clients:

- Microsoft Internet Explorer Version 10 (or later)
- Mozilla Firefox Version 19 (or later)
- Google Chrome

Additional Software

Additional Software	myPortal for Desktop	myAttendant	myPortal for Outlook
Oracle Java: latest version (32 bit / 64 bit)	X	X	
Microsoft Office 16, including Outlook (32 bit / 64 bit) or Microsoft Office 2013 / 2010 (32 bit / 64 bit) or Microsoft Office 2007 (32 bit) or Microsoft Office 365			X
Access to Microsoft Exchange Server (for Outlook contacts and appointments) Exchange 2015 / 2013 / 2010 (64 Bit) Exchange 2007 (32 bit)	X		X
Microsoft .NET Framework >= 3.5 (as of Outlook 2007) or Microsoft .NET Framework >= 4.0 (as of Outlook 2010)			X

INFO: In order to use the Exchange Calendar integration with Microsoft Small Business Server, FBA (Form Based Authentication) may need to be disabled there under some circumstances.

Note about Oracle Java 32 bit or 64 bit

In order to use the myPortal for Desktop function "Import Outlook Contacts at Startup" in conjunction with the 64-bit version of Microsoft Office 2013, an installation of the 64-bit variant of Oracle Java is required. If this function is not used, the Oracle Java 32 bit version is recommended, since the memory

requirements for it are significantly lower. For this reason, the 32-bit version of Oracle Java is generally recommended for all other installations as well.

Minimum Hardware Requirements

- 2 GHz CPU
- RAM: 2 GB
- 100 Mbps LAN (1 Gbps LAN recommended)
- XGA (1024x768) screen resolution, myPortal for Outlook: SVGA (800x600) screen resolution

> ***INFO:*** 4K monitors are not supported for myPortal and myAttendant.

Microsoft Terminal Server, Citrix XenApp Server

The UC Suite PC clients can be used in Microsoft Terminal Server and Citrix Server environments under the following preconditions:

> ***INFO:*** Terminal Server and Citrix Server environments, including hosted services and virtual environments are the responsibility of the customer.

> ***INFO:*** Citrix server environments can decode some regional characters (e.g., German umlauts) correctly.

Operating systems:

- Microsoft Windows Server 2015 (32 bit / 64 bit) as Microsoft Terminal Server
- Microsoft Windows Server 2012 (32 bit / 64 bit) as Microsoft Terminal Server
- Microsoft Windows Server 2008 R2 (64 bit) as Microsoft Terminal Server
- Microsoft Windows Server 2008 R2 (64 bit) with Citrix XenApp 6.5 Server (Desktop Mode)

Office applications:

- Microsoft Office 16, including Outlook (32 bit / 64 bit)
- Microsoft Office 2013 (32 bit / 64 bit)
- Microsoft Office 2010 (32 bit / 64 bit)
- Microsoft Office 2007 (32 bit)

Hardware Prerequisites: The number of installable clients depends on the server performance and on the amount of available memory. If the server is also being used for other applications, their memory requirements must also be taken into account.

More information on the configuration of Citrix XenApp Server can be found under:

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

Installation Files

The following options are available for providing installation files to users:

- The administrator downloads the installation files from the **Service Center** and makes them available to users via a network drive, for example.

9.2.7 Prerequisites for myPortal for OpenStage

In order to use myPortal for OpenStage, the phone must be equipped with the appropriate hardware and software.

Telephones

myPortal for OpenStage can be used with the following telephones:

- OpenStage 60/80
- OpenScape Desk Phone IP 55G

Web Browsers

myPortal for OpenStage can be used in combination with the following web browsers (for configuration and administration):

- Microsoft Internet Explorer Version 10 (or later)
- Mozilla Firefox Version 19 (or later)
- Google Chrome

9.2.8 Silent Installation/Uninstallation for UC Suite PC Clients

Silent installation/uninstallation is a command-line based method to automatically install, uninstall or modify UC Suite PC clients on a PC without requiring any further user inputs.

INFO: Please make sure that you refer to the notes in the `ReadMe first.rtf` file.

The silent installation/uninstallation option is available as of V3 and requires local administration rights on the relevant PC. The silent installation/uninstallation process can also be logged in a file.

The following parameters are available for silent installations / uninstallations:

Parameters	Components
`ALL`	• myPortal for Desktop / myAttendant • myPortal for Outlook • Fax Printer • myAgent • Automatic Updates
`myPortal`	myPortal for Desktop / myAttendant
`OutlookIntegration`	myPortal for Outlook
`FaxPrinter`	Fax Printer
`myAgent`	myAgent

9.2.9 Automatic Updates

Automatic updates ensure that the UC clients are always kept up-to-date with the latest version.

If a new version is available, the update will either be installed automatically or you will be notified that an update is available. If necessary, a message is displayed indicating that one or more applications must be closed to perform the update.

INFO: We recommend that you always perform the updates offered. This also applies to software that is required for certain UC clients.

9.3 Users and User Profiles of the UC Suite

Users of UC Suite are the subscribers who use the UC clients of UC Suite. User profiles store the settings of the users of UC Suite.

9.3.1 Users of UC Suite

UC Suite users use the UC clients of UC Suite. The settings of the UC Suite users are configurable in the user directory.

The user directory contains all the subscribers in the system. In order to use the UC clients, additional user data must be configured in the user directory.

The following information is displayed in the user directory for every user:

- Symbol for presence status
  The administrator can change the presence status for every user.
- **Extension**
- **User name**
  Freely definable.
- **Name**
  First and last name, as configured for the subscriber.
- **Department**
  If a department is assigned to the user.
- **E-mail**
  E-mail address
- **Is Agent**
  Agent level for Multimedia Contact Center.
- **Voicemail**
  The user can receive voicemail.
- **Call Forwarding**
  Call forwarding is configured for the user.

The following settings can be configured:

Values and settings	Keywords
Personal details	
My Personal Details	Own name, user name, password, e-mail address, department, additional phone number, XMPP ID
My Picture	My Picture
User Level	Receiving voicemails: see *Stations* User as Attendant Console: see *Stations* User as agent: see *Stations*
My Preferences	
Presentation	Skin colors, language of the user interface
Notifications	Screen Pops
Calendar connectivity	Automatic creation of Outlook appointments when absent, automatic update of presence status via Outlook/iCal appointments
Hotkeys	Hotkey for functions
Miscellaneous	Automatic reset of the presence status, transfer method, retention period for Journal entries, server address, function keys of the telephone
Call Rules	
Forwarding destinations	Status-based Call Forwarding
Rules Engine	Rule-Based Call Forwarding
Communications	

Values and settings	Keywords
Voicemail settings	Recording or announcement mode, language of the voicemail box
VM Notification	Notification Service for Messages
Fax Notification	Notification Service for Messages
Profiles	
Busy, No Answer, Meeting, Sick, Break, Away, Vacation, Lunch, Home Ph.	profile for personal AutoAttendant
Sensitivity	
Security and Access	Retrieval of your voice and fax messages by the Attendant; password check for the voicemail box
Presence Visibility	Visibility of your Presence Status for Others
VoiceMail Presence	Announcement of your presence status for external callers; announcement of your presence status for specific callers
myAttendant	
LAN Messages	Text module for Instant Messaging
DIDs	MSN
Communications	Call forwardings

Additional information on user settings can be found in the User Guides of the UC clients and under the keywords listed in the table.

The password for UC clients consists of six digits by default. The password length can be adapted as required (6-10 characters). An administrator with the **Advanced** profile can change the password of a user (if the user has forgotten it, for example).

> ***INFO:*** The First Name and Last Name of a user are overwritten in the User Directory when they are changed by using a wizard or in Expert mode. By contrast, if the First Name and Last Name of a user are changed in the User Directory, the user data displayed when using a wizard or in Expert mode are not overwritten. This results in the existence of two different user names for the same user. Additionally, if the length of first name and the length of last name is greater than 16 characters in total, then it will be truncated to 16 in order to fit to dispay of the device.

Subscribers for whom an e-mail address has been configured and who use myPortal for Desktop receive a welcome e-mail with Getting Started Instructions.

Resetting User Data

The settings of a user can be reset to default values. All the user's voicemail messages, personal greetings for the voicemail box, journal entries, scheduled conferences, e-mails and faxes are deleted in the process.

9.3.2 User Profiles for the UC Suite

User profiles of the UC Suite store the settings of the UC Suite users. One or more users (members) can be assigned to a user profile. All members of this profile have the same settings.

Every user can be a member of no more than one user profile. Direct changes to the settings of a user - i.e., not via the assigned profile - automatically delete the user from the profile.

The following values and settings can be configured:

Menu items	Values and settings for
Personal details	
My Personal Details	Visibility of phone numbers
My Preferences	
Appearance	Skin colors, language of the user interface
Notifications	Screen pops
Outlook connectivity	Automatic creation of Outlook appointments when absent, automatic update of presence status via Outlook/iCal appointments
Miscellaneous	Automatic reset of the presence status, transfer method, retention period for Journal entries, server address
Call Rules	
Forwarding destinations	Status-based call forwarding
Communications	
Voicemail settings	Recording or announcement mode, language of the voicemail box
VM Notification	Notification Service for Messages
Fax Notification	Notification Service for Messages
Profiles	
Busy, No Answer, Meeting, Sick, Break, Away, Vacation, Lunch, Home Ph.	Profile for personal AutoAttendant
Sensitivity	
Security and Access	Retrieval of your voice and fax messages by the Attendant; password check for the voicemail box
Presence Visibility	Visibility of your Presence Status for Others
VoiceMail Presence	Announcement of your presence status for external callers; announcement of your presence status for specific callers

Additional information on user profile settings can be found in the User Guides of the UC clients and under the keywords listed in the table.

9.4 Presence Status and CallMe Service

The Presence status and CallMe service display and optimize the availability of subscribers. The Presence status enables simple status-based call forwarding as well as rule-based call forwarding, which can be flexibly configured with myPortal for Desktop or myPortal for Outlook.

9.4.1 Presence Status (Presence)

The Presence status indicates the availability of internal subscribers (including mobile stations) in the Favorites list, the internal directory, the virtual conference room and via voicemail announcements. In addition, the Presence status controls the availability of internal subscribers with status-based call forwarding, rule-based call forwarding and the personal AutoAttendant.

As a subscriber, you can change your Presence status in myPortal for Desktop and myPortal for Outlook or via the menu controls of the voicemail box. Deactivating call forwarding at the telephone returns you to the **Office** presence status. For every change in the Presence status (except for **Office** and **CallMe**), you also define the scheduled time of your return to the **Office** or **CallMe** status.

As a subscriber, you can select the following statuses:

- **Office**
- **Meeting**
- **Sick**
- **Break**
- **Gone Out**
- **Vacation**
- **Lunch**
- **Gone Home**
- **Do Not Disturb** (not available for Mobility Entry or MULAP)

Mapping of the External XMPP Status Internally

Subscribers can see the presence status of external XMPP communication partners in the Favorites list or in the external directory, for example, provided XMPP has been configured. The following mappings apply (from left to right):

XMPP status	Represented as presence status
Online	Office
DND	Meeting
Away	Out of the Office
Extended Away	Vacation

INFO: Outlook contacts must include the XMPP ID In the IM address in accordance with the following pattern: `xmpp:john.public@oso.example-for-a-domain`.

Mapping of the Internal Presence Status Externally

External XMPP communication partners can see the XMPP status of internal subscribers, provided XMPP has been configured. The following mappings apply (from left to right):

Presence status	Represented as XMPP status
Office	Online
Meeting	DND
Sick	Away
Break	Away
Out of the Office	Away
Lunch	Away
Gone Home	Away
Vacation	Extended Away

Call Forwarding to the Voicemail Box

If Presence status of a subscriber is not **Office** or **CallMe**, the communication system redirects calls for him or her to the voicemail box by default and notifies the callers via status-based announcements about the nature of absence and the scheduled time for return.

Info Text

You can enter any info text for your current presence status, e.g., "I am in Room No. ..." when attending a meeting. The info text is displayed in the Favorites list, in the internal directory and in the virtual conference room. The info text is deleted when you change your presence status.

Automatic Reset of the Presence Status

As a subscriber, you can have your Presence status automatically reset to **Office** at the end of your scheduled absence. Otherwise, the system extends the current Presence status in increments of 15 minutes until you change it yourself.

Visibility of your Presence Status

As a subscriber, you can specify for each subscriber in the internal directory whether or not that subscriber can see your Presence status other than **Office** and **CallMe** as well as the scheduled time of your return and any info text you may have entered.

Automatic Update of Presence Status via Outlook / iCal Appointments

As a subscriber, you can automatically control your Presence status via appointments (but not for those that have been proposed or declined) by using the specific keywords in the Subject line. You can choose between the following calendars:

- Exchange calendar (on the Microsoft Exchange Server)
  The automatic update of the presence status via Outlook appointments occurs independently, regardless of whether or not your PC is running. The administrator must configure the Exchange Calendar Integration for this function.

  INFO: Information on the usage of the various Microsoft Exchange servers can be found in the Unify Experts wiki at `http://wiki.unify.com/wiki/OpenScape_Business#Microsoft_Exchange_Server`.

- Outlook calendar
  The automatic update of the presence status via Outlook appointments requires myPortal for Desktop or myPortal for Outlook to have been started on your PC.
- iCal calendar (myPortal for Desktop)

You can use the following keywords:

- **Meeting**
- **Sick**
- **Break**
- **Gone Out**
- **Vacation**
- **Lunch**
- **Gone Home**

The keywords depend on the language set for the user interface. The keywords may be located anywhere in the Subject line. If the Subject line contains more than one such keyword, only the fist takes effect. When this function is enabled, your Presence status changes automatically at the start and end time of the relevant appointment. The check for calendar appointments occurs at 30-second intervals.

NOTICE: When enabling this function, please bear in mind that any appointments with corresponding keywords in the Subject line could lead to undesirable changes in your Presence status. Consequently, you may nee to change the Subject line if needed.

Automatic Creation of Outlook Appointments when Absent)

As a subscriber, you can have appropriate Outlook appointments created automatically when you are absent by a change in your Presence status. The Subject line of the corresponding Outlook appointment consists of your Presence

status and the text "(Auto)", for example: "Meeting (Auto)". The start and end times for the appointment involved correspond to your entries in myPortal for Desktop or myPortal for Outlook. The end time of the Outlook appointment remains unchanged in the event of a possibly delayed return. You can define whether the Outlook appointments should be stored in the local PST file or on the Exchange server. If you are using a local PST file, your Outlook must be open when creating the Outlook appointments. If you are using a PST file on the Exchange server, the Outlook appointments are created, regardless of whether or not your Outlook is open. The administrator must configure the Exchange Calendar Integration for this function.

INFO: Information on the usage of the various Microsoft Exchange servers can be found in the Unify Experts wiki at `http://wiki.unify.com/wiki/OpenScape_Business#Microsoft_Exchange_Server`.

Screen Pops on Changing the Presence Status

As a subscriber, you can have changes to your Presence status indicated by a screen pop.

9.4.2 CallMe Service

The CallMe service enables subscribers to define any phone at an alternative workplace as the CallMe destination at which they can be reached through their own internal phone numbers. The subscriber can use myPortal for Desktop or myPortal for Outlook at his or her alternative workplace exactly as in the office and thus also make outgoing calls from the CallMe destination.

Inbound Calls

Inbound calls to the internal phone number are forwarded to the CallMe destination. The internal phone number of the called subscriber is displayed to the caller. Unanswered calls are forwarded to the voicemail box after 60 seconds.

Outbound Calls

For outbound calls with myPortal for Desktop or myPortal for Outlook, the communication system sets up two connections. It first calls the subscriber at the CallMe destination. If the call is answered, the communication system then calls the desired destination and connects the subscriber with it. The internal phone number of the caller is displayed at the destination (One Number Service).

Presence Status

When the CallMe service is enabled, the message "`CallMe active`" appears in the display of the relevant phone (not for analog and DECT phones). Other subscribers see the presence status **Office**.

Activation

As a subscriber, you can activate the CallMe service manually. In addition, the Call-Me service is also reActivated by an automatic reset of the Presence status following an absence, provided it was active earlier. Then following types of CallMe destinations are not supported:

- Group
- Redirected telephone

Displaying the CallMe Destination in the Favorites List

As a subscriber, you can have the number of your CallMe destination displayed in the Favorites list of other subscribers instead of your own phone number.

Deactivation

The CallMe service remains active until your Presence status changes.

NOTICE: CallMe function should not be used when dialing or caling in an open conference.

9.4.3 Status-based Call Forwarding

Status-based call forwarding enables subscribers to forward calls based on their Presence status to one of their additional phone numbers or their voicemail box.

As a subscriber, you can configure status-based call forwarding for every presence status except **Office**, **CallMe** and **Do Not Disturb**. When you change your Presence status, the communication system activates call forwarding to the destination defined by you for this purpose. For example, if you are away from the office, to your mobile phone or if you are on vacation, to your representative.

9.4.4 Rule-Based Call Forwarding

Rules-based call forwarding enables subscribers to forward calls based on numerous conditions and exceptions even more flexibly than with status-based call forwarding.

In addition, rule-based call forwarding also supports:

- Any destinations
- Presence status **Office**, **CallMe** and **Do Not Disturb**

As a subscriber, you can define rules and activate or deactivate them at any time by using the Rules wizard. A rule can only be active if your phone has not been forwarded. Status-based call forwarding (except to the voicemail box) overrides rule-based call forwarding.

When a call forwarding rule is active, **"rule active"** appears on the display of your telephone.

When an inbound call is received, the communication system checks the applicability of the active rule in accordance with its sequential order in the Rules wizard. Only the first applicable rule is executed. In this case, your phone will ring once, and the communication system will then forward your call to the defined destination.

You can define several types of conditions and exceptions (except when ...) in one rule. However, you cannot define a condition with an exception of the same type. For example, it is not possible to define a condition of the type "On certain weekdays" together with an exception of the type "Except on certain weekdays".

Types of Conditions and Exceptions

- (except) for certain Presence status
- (except) from certain people (in the internal directory, external directory, personal directory or from any station number)
- (except) when transferred to you from certain people (in the internal directory, external directory, personal directory or from any station number)
- (except) from a certain type, i.e., **internal**, **external** or **Unknown Contact**
- (except) on a certain date (also on multiple dates)
- (except) on certain weekdays
- (except) between a certain Start and End date
- (except) between a certain Start and End time

9.5 Directories and Journal

Directories, the Favorites List and the Journal organize contacts and calls.

9.5.1 Directories

Directories are used to organize the contacts of subscribers. Subscribers can access these contacts with UC Suite clients and via system phones with displays.

The system provides the following directories, which support the following functions and with the below priority for lookup number (lookup number will be supported only for external call and in case that CO/ITSP does not provide the name):

Directory	myPortal for Desktop, my Attendant, Fax Printer	myPortal for Outlook	System telephone with a display
Outlook Contacts MAC OS contacts (myPortal for Desktop)	If required, the subscriber can import Outlook/Mac OS contacts on starting myPortal for Desktop when using Microsoft Windows.	Contains the personal Outlook contacts of a subscriber. Only the subscriber involved has write access to this data.	Contains the personal Outlook contacts of a subscriber. Only the subscriber involved has write access to this data.
Personal directory	The subscriber can either import Outlook/Mac OS contacts on starting myPortal for Desktop or maintain personal contacts manually. Imported contacts cannot be edited.	-	Outlook contacts imported via the Personal Assistant.
Internal directory	The internal directory of UC Smart offers additional features with the UC Suite. Contains all internal subscribers, and groups for which the display has been activated in the system, possibly with additional phone numbers, provided the subscriber has made this information visible to other internal subscribers. Internal subscribers (with system telephones) are displayed with their Presence status and can be contacted through Instant Messaging. The Presence status of a subscriber can only be shown if allowed by that subscriber. If relevant, the scheduled time of return and any info text that may have been entered by the subscriber are also displayed. A subscriber is only provided read-access to this directory.		Contains all internal subscribers and groups for which the display has been activated in the system.
External directory	Contains contacts from a corporate directory and must be configured by the administrator. A subscriber is only provided read-access to this directory.		-
Public Exchange folder (not usable with Office 365)	Contains contacts of the public Exchange folder if configured by the administrator. These are shown in the external directory. Information on the usage of the various Microsoft Exchange servers can be found in the Unify Experts wiki at `http://wiki.unify.com/wiki/OpenScape_Business#Microsoft_Exchange_Server`.		-
External Offline Directory (LDAP)	Contains contacts from the LDAP corporate directory and must be configured by the administrator. The external offline directory can only used for searches. The administrator can enable and disable the display of the external offline directory for system telephones.		
System Directory	-		Includes all internal stations and all central speed-dial numbers. The administrator can enable and disable the display of a subscriber in the system directory.

INFO: Phone numbers in directories should always be entered in canonical format wherever possible.

NOTICE: In case the number is called from system phones it must be configured in canonical or diable format.

Simple Search

As a subscriber, you can search the directories by **First Name**, **Last Name** or a call number. The directories are searched in the order shown in the table above. The search can be conducted using whole words and also with partial search terms such as a part of a station number, for example. The set search options remain in effect for subsequent searches. Al search terms used are saved. You can optionally delete the list of search terms used.

Advanced Search

You can selectively search in the **Title**, **First Name**, **Last Name**, **Company**, **Extension**, **Company Ph.**, **Business Ph. 1**, **Business Ph. 2**, **Home Ph. 1**, **Home Ph. 2**, **Mobile Number** and **Email** fields and limit the maximum number of hits. The modern interface of myPortal for Desktop does not support the advanced search.

Sorting

The contacts of a myPortal for Desktop and myPortal for Outlook directory can be sorted by any column in ascending or descending alphanumeric order. The modern interface of myPortal for Desktop does not support sorting.

9.5.2 Internal Directory

The internal directory contains the contact details of the internal subscribers of the communication system. UC Suite clients can access the system directory.

As an administrator, you have unrestricted access to all data in the internal directory. As a subscriber, you can dial from the internal directory.

The administrator can disable the display for all analog stations or for analog stations without an associated name. Subscribers whose names begin with - are not displayed in the latter case.

9.5.3 External Directory

The external directory includes contacts from outside the communication system.

The data of the external directory is available to all subscribers in all UC Suite clients and the phone display. Subscribers can dial from the external directory. Users with the UC Suite clients myAttendant and myAgent can also edit data in the external directory.

Importing a CSV File

As an administrator, you can import contacts from a CSV file in UTF-8 encoding from the local file system or a network share into the external directory.

A header in the CSV file allows the mapping of field names in the CSV file to fields in the system. A typical CSV file may be structured as follows:

- Header line:
  "Customer ID","Last Name","First Name","Company Phone Number","Company Name":
- Data line:
  "987654","Dubios","Natalie","+498977712345","Company"

You can map the data being imported from the CSV file to the following fields in the system:

- Customer ID
- Title
- First Name
- Last Name
- Company
- Business Ph.
- Business Ph2
- Mobile Ph.
- Home
- XMPP ID
- Fax Ph.
- E-mail
- City

After processing the CSV template, the file must be in saved in UTF-8 format in order to ensure the correct import of any existing special characters.

If you want the import to overwrite data, the corresponding **Customer IDs** should be identical.

INFO: A CSV template and a description of the syntax required for importing data into the external directory can be found under **Service Center > Documents > CSV Templates**.

9.5.4 External Offline Directory (LDAP)

The external offline directory (LDAP) contains contacts from an LDAP server for myPortal for Desktop, myAgent, Fax Printer, myPortal for Outlook and for system telephones with displays.

The system supports LDAP Version 2 with authentication.

LDAP (Lightweight Directory Access Protocol) is a TCP/IP-based directory access protocol for accessing network directory services. LDAP has a unique format world-wide in which all names can be represented. It provides for different layouts and enables unique associations between names and their internal representation. This data is defined by the administrator together with the IT administrator of the customer when planning and setting up a project. LDAP can be used under the MS Windows and Linux operating systems.

In a Microsoft environment, the Active Directory Server (ADS) or the Exchange Server also serves as the LDAP server. Under Microsoft Windows, user data can be administered with the Active Directory (AD) application or ESTOS Metadir, for example. The administration of this data is generally performed by the IT administrator of the customer.

Under Linux, the user data can be administered with OpenLDAP, for example.

Setting up an LDAP directory service can be simplified with an LDAP browser (e.g., the freeware from Softerra).

Phone numbers on the LDAP server may only include "-" and blanks as delimiters. Other delimiters cannot be filtered out by the system.

As an administrator, you can adapt the mapping of fields to the names of the used LDAP server during the configuration of an external offline directory. Deleted fields are ignored when searching for names via phone numbers. The search always occurs with the last 4 positions of the phone number preceded by a wildcard. You can deactivate the search for names via phone numbers for incoming calls.

If the default port 389 is already being used, some other port must be configured

---

INFO: More information can be found on the Internet at `http://wiki.unify.com`.

The data of the external directory is available to subscribers in myPortal for Desktop, myAttendant, Fax Printer and myPortal for Outlook during the search.

System Telephones with Displays

As a subscriber, you can select between the internal directory and the LDAP directory via the menu., provided these have been configured for system telephones. The LDAP directory supports searches in the appropriate contacts and the subsequent calling of a contact.

The name information provided by the LDAP server is not displayed in ringing or call status. The call numbers for incoming calls are also not replaced by the name information provided by the LDAP server (as when call numbers are replaced by SSD names).

A system subscriber can only be reached from the LDAP directory if a DID number was configured for him or her and if this entry corresponds to the entry in the LDAP database. Call numbers provided by the LDAP server can only be routed within the network if the internal call number and the DID number are identical.

9.5.5 System Directory

The system directory contains all internal stations. UC Suite clients can access the system directory.

The administrator individually disable the display for every subscriber and every speed-dial number with a name.

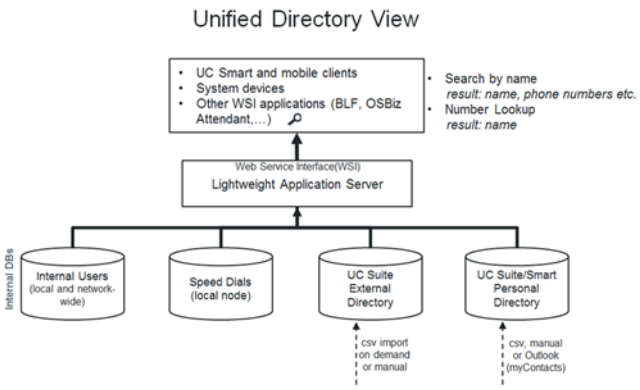
9.5.6 Unified Directory

OpenScape Business provides different data sources to store and to retrieve user or contact related data, starting with the internal user data in the internal user configuration, via the internal speed dial list, up to the different directories of the UC applications.

Each data source within OpenScape Business is used by a specific client application either located within the system SW itself in the phone devices or within a UC client application. Depending on the used data sources and the used clients, the retrieved data and their presentation is different.

The "Unified Directory" service within OpenScape Business comprises the existing OpenScape Business data sources for common search and name resolution functions. It provides the same search result or name resolution information to all system devices and OpenScape Business clients.

The Unified Directory service can either be accessed via the Web Service Interface (WSI) from externally located clients like myPortal to go or internally via the call processing mechanisms (e.g. from OpenStage



Phones).

Unified Directory uses following internal databases and directories of OpenScape Business:

- Internal user directory (network wide)
- Speed dial lists
- UC Smart Personal Directory (optional)
- UC Suite External Directory (optional)
- Personal Outlook Contacts (if imported via myContacts)

The Unified Directory service is available within every OpenScape Business system from V2R2 on. It does not require specific HW-SW or license prerequisites.

In order to get best results when using the Unified Directory some rules regarding phone number formats and writing of names have to be followed.

9.5.6.1 Features

Unified Directory Service provides:###P###

- Directory Search in several internal data sources of OpenScape Business
- Unified offering of the search result to all supported clients
- Phone number Look-Up / Name Resolution in several internal data sources
- Unified offering of name resolution results for all supported clients
- External data access via the WebServices Interface (WSI)

The features are available for single node systems as described in the following. Within OpenScape Business networks, the availability of the features depends mainly on the kind of connection of the trunks, devices and clients within the network.

Supported Devices / Clients

Unified Directory supports following clients / system devices of Unify using the indicated interfaces:

Device/Client	Used Interface/Protocol	Remarks
OpenStage phones	Call Processing / HFA protocol	WSI / HTTP(S) is optional on OpenStage 60/80 for caller images
OpenScape Deskphone IP	Call Processing / HFA protocol	WSI / HTTP(S) is optional on DeskPhone IP 55 for caller images
Cordless (CMI) devices	Call Processing / CMI protocol	
CP200	Call Processing / HFA protocol	
DeskPhone CP200/CP600	WSI / HTTP(S)	
myPortal Smart	WSI / HTTP(S)	
myPortal to go	WSI / HTTPS	
Openscape Business Attendant/BLF	Call Processing / CorNet protocol	WSI / HTTP(S) is optional

INFO: The UC Suite myPortal, myAttendant and myAgent clients use their own mechanisms for directory search and name resolution.

Search function

The Unified Directory search is always performed by using the specific device / client user interface. The search criterions and the used character set could be restricted, depending on the used clients.

After the search criterion is entered the search is performed within subsequentdirectories

- Internal user directory (network wide)
- Speed dial lists
- UC Smart Personal Directory (optional)
- UC Suite External Directory (optional)
- Personal Outlook Contacts (if imported via myContacts)

All matches within the directories above are shown as search results together with their origin. The matches contain either the full contact data set or only parts of it. The information depth of the results depends on the data souce.

The matches are presented at the devices or clients depending on display capabilities.

	Internal UserDirectory	**SpeedDials**	**UC SmartPersonalDirectory**	**UC SuiteExternalDirectory**	**PersonalOutlookContacts (viamyContacts)**
Last Name	X	---	X	X	X
First Name	X	---	X	X	X
Short/ Displayname	X	X	---	---	---
Office Phone No.	---	---	X	X	X
Home/Ext. PhoneNo.	---	---	X	---	X
Mobile Phone No.	---	---	X	X	X
XMPPID	---	---	---	X	---
Email-Adr.	---	---	X	X	X
Company name	---	---	X	X	X
City	---	---	---	---	---
Contact Picture	---	---	X	---	X
Contact Picturepreview	---	---	X	---	X

Phone Number Look-Up

Unified Directory Phone number Look-Up resolves the transferred calling party (CLI) by a number search in all supported internal data sources . The search is perfomed within following phone number fields:

- Office number
- Mobile number
- Home number

The Phone number Look-Up is triggered in case of incoming or outgoing calls in general, whereas specific routing and forwarding features are considered in addition.

A fixed prioritization of the data sources that are used for Phone number Look-Up is implemented in order to get the result as fast as possible. The result contains either only lastname, firstname, displayname or ,if available, the full related contact data.

Table: Supported Data Sources and Prioritization

Priority	Data Sources	Remark
1	CO/ITSP name (as sent by provider)	Prerequisite is to enable flag "Name in CO".
2	Speed dial list	
3	Personal Contacts	
4	UC User detail	

The retrieved data are presented on the user's device and/or in the UC client. The information depth depends on the display capabilities.

- **Incoming calls**
  Supported scenario for single node systems:
  - Basic call
  - Group call/ MULAP call
  - Ringing Group
  - Single Step Call Transfer (SSCT)
  - Attended/Supervised/Consultation Transfer
  - Call Forwarding Unconditional (CFU)
  - Call Forwarding No Reply (CFNR)
  - Call Forwarding Busy (CFB)
  - Blind transfer
  - Call Pickup

  Supported scenario for multi node (network) scenarios is a Gateway Call.
- **Outgoing call**
  In case of an Outgoing Call the Phone number Look-Up of the called partynumber happens only once.
  Supported scenario for single node systems is a Basic Call to externalnumber.

The presentation of the Phone number Look-Up result depends on display capabilities of the phones.

9.5.6.2 Rules and Conventions

Some conventions regarding number and name formats within the data sources have to be observed in order to get optimal results using the Unified Directory service.

Supported Number Format

All external phone numbers within the data sources must be entered in the canonical format including country and area code. e.g.+4989700712345

> ***INFO:*** Speed Dial list supports only system dialable format e.g. 0089700712345 or 0004989700712345

Supported Name Formats

The following conventions regarding name formats and character sets have to beobserved:

- **Speed dial name format**
  Name search within the Speed Dial List is supported only with specific configuration rules. The first and last names have to be entered within the existing name field using the following pattern:
  <Last Name>, <First Name> (comma separated)
- **Internal Users in case of Migrations**
  Migration to V2R1 and onwards with internal users that do not follow these configuration rules will not be supported in the expected way. This means the administrator should convert internal names to the following pattern before migration:
  <Last Name>, <First Name> (comma separated)

Availability of directory changes

After creating, updating or deleting contacts in the various data sources it can take up to 10 minutes until all changes appear on Phone number Look-Up results.

9.5.6.3 Functional Boundaries

The following functional boundaries do exist regarding Unified Direcrories:

Name Search

- Group name support
  Group names (not MULAP names) can currently not be searched in all kindof configurations

- Support of special characters
  On most phone devices the user can only search for standard characters "a-z". Special (diacritical) characters like German characters Ää,Öö,Üü, ß are not accessible via phone device user interface. Therefore special characters are not supported in search filter.
  Names including special characters cannot be searched via the Unified Directory.
- Support of Speed Dial Name format
  Name search within the Speed Dial List is supported only with specific configuration rules. The first- and last names have to be entered within the existing name field using one of the following patterns
  - <Last Name>, <First Name> (comma separated)
  - <First Name> <Last Name> (space separator on this case)

Name Presentation

Personal Contacts in UC Smart and from external offline directory, with length of first name plus length of last name greater than 24 characters, will be truncated to 24 characters length to fit the display length of the devices.

Phone number Look-up

The Phone number Look-Up feature (retrieve contact name from calling party number) is not supported in Unified Directory for SIP and S0 devices.

9.5.6.4 Unified Directory in Networked Systems

The Unified Directory Service is active within every node of an OpenScape Business Network and uses the datasources of the own system. Phone Devices and Client use always the Unified Directory Service within their own node.

Therefore it depends on the kind of datasource content if netwide contacts are available.

Table: Local and Netwide Datasource

Data source	Local data	Netwide data
Internal user directory	X	X
Speed dial lists	X	---
UC Smart Personal Directory	X	---
UC Smart Personal Directory	X	---
Personal Outlook Contacts (via myContacts)	X	---

Phone number Look-up

In Networking scenarios the Phone number Look-Up functionality is not used. In such scenarios the name is transported via normal networking mechanisms between the network nodes.

For internal users the configured Display Name is used so Lookup is not required.

9.5.7 Departments

Departments classify subscribers in the internal directory into groups based on their organizational affiliation. The internal directory allows you to search and sort by department.

9.5.8 Favorites List

The Favorites list provides you (as a subscriber) with a constant view of selected contacts. These contacts can also be called very easily directly from the Favorites list. All internal subscribers with system telephones and external XMPP communication partners are shown together with their Presence status and can be contacted via instant messaging.

As a subscriber, you can add contacts from all directories to the Favorites list. For favorites that do not come from the internal directory, instead of the symbol for the Presence status, the symbol for the source of the contact is displayed.

The Favorites list manages contacts in groups. The contacts in all groups can be sorted by First Name, Last Name or their original sorting order.

When an internal subscriber is absent, you can determine the scheduled time of his or her return by positioning the mouse pointer over the entry for that subscriber, provided the subscriber has allowed his or her Presence status to be visible to you.

For favorites with multiple phone numbers, you can specify a default number with which the contact is to be called. The default phone number of a favorite can be determined in the context menu from the symbol with the activated check box.

9.5.9 Journal

The journal is the list of all incoming and outgoing calls of a subscriber. It enables subscribers to quickly and easily respond to missed calls and call back their contacts or call them again directly from within the journal.

Folder for Call Types

The calls are arranged in the following groups:

- **Open**
  Contains the unanswered missed calls for which a call number was transmitted. As soon as one of these calls is answered, all associated entries with that call number are dropped from the list.
- **All calls**
- **Missed**
- **Answered**
- **Internal**
- **External**
- **Inbound**
- **Outbound**
- **Scheduled**
  Contains all the calls that you (as a subscriber) have scheduled for specific dates/times. The Scheduled Calls feature is not available to Contact Center agents. In order for the communication system to execute a scheduled call, myPortal for Desktop or myPortal for Outlook must be open at the scheduled time; your presence status must be **Office** or **CallMe**, and you must confirm the execution of the call in a dialog. If you are busy at the time the scheduled call is to be made, the system defers the scheduled call until you are free again. myPortal for Desktop or myPortal for Outlook informs you of any pending scheduled calls on exiting the program. On starting the application, myPortal for Desktop or myPortal for Outlook notifies you about any scheduled calls for which the scheduled time has elapsed. You can then either delete such calls or save them with a new scheduled time.

Not all folders for call types are available in the modern user interface myPortal for Desktop.

Retention Period

The system saves a record of the calls in the Journal for a maximum period of time, which can be configured by the administrator. As a subscriber, you can reduce this time. After the retention period expires, the system automatically deletes all associated entries.

> ***INFO:*** The retention period also determines the maximum time period for evaluations with myReports.

Grouped by time period

The calls in each group are arranged by time, e.g.: Today, Yesterday, etc., Last Week, Last Month and Older. Your administrator can set the duration for which calls should be saved in the Journal. After this set time period expires, the entries are automatically deleted. The grouping by time period is not available in the modern user interface of myPortal for Desktop.

Call Details

Every call is shown with the Date and Time and, if available, with the call number. If a directory contains further details on the call number such as the **Last Name**,

First Name and **Company**, then this information is also shown. In addition, the **Direction**, **Duration** and **Call Complete** columns are also displayed in most folders. Not all call details are available in the modern user interface of myPortal for desktop.

Sorting

You can sort the calls in the Journal by any column in ascending or descending alphanumeric order.

You can jump within the Journal to the first call whose entry begins with a specific character in the sorted column, e.g., to the first Last Name beginning with "P". By entering subsequent characters, you can then narrow the search. Sorting is not available in the modern user interface of myPortal for Desktop.

Export

As a subscriber, you can export the journal as a CSV file using myPortal for Desktop or myPortal for Outlook:

9.6 Calls

For calls, convenient features such as a desktop dialer, screen pops and the option to record calls and conferences are available to subscribers.

9.6.1 Desktop Dialer and Clipboard Dialer

The Desktop Dialer and Clipboard Dialer enable users with myPortal for Desktop (Windows) or myPortal for Outlook to call a selected destination or a destination copied to the Windows clipboard via a key combination from many Windows applications, e.g., from an Outlook e-mail.

Depending on the type of string used, the Dialer works as follows:

- A phone number in canonical format is dialed directly.
- A station number in dialable format is dialed directly if the communication system can decide whether an internal or external destination is involved. Otherwise, the user is asked to make the appropriate selection.
- A string containing letters is searched in the directories as a first name or company.

The Desktop Dialer and Clipboard Dialer are executed after a definable time period. During this period, the dialing can still be canceled. If the preset value of 3s is changed to 0s, the dialing will be executed immediately. The value is changed in the settings of the UC Suite clients.

Windows applications that were implemented with standard Windows-compliant components usually support the Desktop Dialer and Clipboard Dialer, but 16-bit applications do not. The Desktop Dialer is only supported by 32-bit applications.

9.6.2 Screen Pops

Screen pops in the UC Suite clients offer you convenient ways to respond to incoming calls or new voicemails with a single mouse click, for example.

Screen pops appear in the lower right corner of the screen. There are different types of screen pops. Screen pops for calls and messages show phone number, name and image of the caller, if possible. The buttons in the screen pops change, depending on the situation.

Screen pops can be minimized to a tray icon. As soon as more than three screen pops are opened for calls, they are automatically minimized and shown as icons on the task bar.

9.6.3 Record calls

A subscriber can record calls. Recorded calls appear in the voicemail box.

INFO: Note that in most countries you are legally required to notify the other party that you are recording the call. In some countries (such as France, for example), the other party is automatically notified by the system.

As an administrator, you can allow or prevent the recording of calls and conferences on a system-wide basis. In addition, you can optionally configure the playback of an announcement or warning tone at the start of the recording.

As a subscriber, you can control the recording of calls via myPortal for Desktop or myPortal for Outlook. Recorded calls are identified in the voicemail box with a red dot and show the call number of the other party if available.

Ongoing recordings are automatically stopped by a consultation hold, placing a call on hold, transfers and the initiation of a conference.

INFO: Call recording is not supported with DTMF.

9.7 Conferences

In a conference, multiple participants (including external parties) can communicate with one another at the same time.

9.7.1 Conference Management

Conference management enables subscribers to use different types of conferences.

Types of Conferences

The different types of conferences offer the following features:

	Ad-hoc	Scheduled	Permanent	Open
Usage	• Phone-controlled • application-controlled	• application-controlled	• application-controlled	• application-controlled
Start	• Manually	• Scheduled	• Manually	• Manually
End	• Manually	• Scheduled • Manually	• Manually	• Manually
Duration of the reservation of conference channels	• 1 hour by default	• Scheduled	• Until the deactivation or deletion of the conference	• Until the deactivation or deletion of the conference
Extension	x	x	-	-
Recurrence	• Manually	• Scheduled	-	-
Direction of connection setup from the viewpoint of the system	• Outbound	• Outbound • Inbound	• Inbound	• Inbound
Set of participants	• Fixed	• Fixed	• Fixed	• Open
Authentication of conference participants	-	• Individual conference ID (optional) • Password (optional)	• Individual conference ID (optional) • Password (optional)	• Shared conference ID (optional)

	Ad-hoc	Scheduled	Permanent	Open
Recording, if enabled in the system	• Manually (On Demand Conference Recording)	• Automatically (Auto Conference Recording) • Manually (On Demand Conference Recording)	• Automatically (Auto Conference Recording) • Manually (On Demand Conference Recording)	• Automatically (Auto Conference Recording) • Manually (On Demand Conference Recording)
Invitation by E-mail with:	• Conference Name • Link for Web Collaboration session	• Conference Name • Dial-in number • Conference ID • Password • Date and time of the start and end of the conference • Link for Web Collaboration session	• Conference Name • Dial-in number • Conference ID • Password • Link for Web Collaboration session	• Conference Name • Dial-in number • Conference ID • Password
Outlook appointment as an e-mail attachment (.ics)	-	x	-	-

Application-controlled Conference

As a subscriber, you can initiate, control and manage a conference with the Conference Management feature of myPortal for Desktop or myPortal for Outlook.

Phone-controlled Conference

As a subscriber, you can initiate a phone-controlled conference and then control it via the phone by the following methods:

- Call the desired conference participant and connect him or her to the conference
- Extend a consultation call into a conference
- Extend a second call into a conference

Virtual conference room

The virtual conference room enables you to follow a conference and its participants in a graphical environment (for application-controlled conferences) and to also manage the conference if you are the conference controller. The virtual conference room shows the phone number, name and presence status to the conference participants, where available.

Dial-in Number

As an administrator, you can change the conference dial-in numbers that were set up during basic installation. As a subscriber, you can display the dial-in number for a conference.

Conference Controller

The initiator of the conference is automatically the conference controller until this is explicitly changed. Depending on the type of conference, the controller can:

- Add or remove conference participants (for application-controlled conferences):
  Removed participants do not remain in the conference.
- Disconnect or reconnect conference participants:
  Disconnected participants remain in the conference. When the conference controller is connecting a conference participant, all other conference participants remain connected to one another. If there is only one participant connected, that participant will hear music on hold.
- Record a conference
  Recorded conferences are identified in the voicemail box with a red dot and show the call number of the first conference participant, if available. Conferences in which a participant is on hold cannot be recorded.
- Set another internal participant on the same node as the conference controller
- Extend the conference
- Leave the conference without ending it:
  The longest attending internal participant of the conference automatically becomes the conference controller.
- End the conference

Conference Participants

Conference participants can leave the conference and optionally dial-into it again (scheduled and permanent conferences). As long as a conference has only one participant, the participant hears music on hold. As an administrator, you can specify whether multiple external conference participants are allowed. The maximum number of external conference participants is determined, among other things, by the number of available trunks.

Conference tone

When connecting or disconnecting a conference participant, the other participants hear the conference tone. As an administrator, you can activate or deactivate the conference tone.

Automatic Termination without a Conference Controller

If there are only external subscribers left in a conference, the participants will hear an alert tone after a specified time period. Following a further timeout, the conference is automatically terminated by the system. As an administrator, you can edit these time values.

Notification by E-mail and Outlook Appointment

The system can automatically notify conference participants by e-mail and, for scheduled conferences, additionally through an Outlook appointment as an attachment (.ics):

Event	Notified conference participants	Outlook appointment
New conference	all	Automatic creation
Delete the conference		Automatic deletion
Reschedule the conference		Automatic update
Adding conference participants	Those affected	Automatic creation (those affected)
Remove conference participants		Automatic deletion (those affected)

This requires the administrator to have configured the sending of e-mails. In addition, an internal conference participant must have specified his or her e-mail address. For external conference participants, the initiator of the conference must enter their individual e-mail addresses.

INFO: For e-mail notifications, no return acknowledgments are obtained for failed deliveries or absence messages, since the e-mails are sent directly from the system due to the integration of Web Collaboration.

Further Calls

While participating in a conference, making a call or accepting another call disconnects the participant from the conference.

Park, Toggle/Connect

The Park and Toggle/Connect features are not available in a conference.

Call Charges

Toll charges are assigned to the party who set up the toll call. When a conference is transferred to another conference controller, all further charges are assigned to that controller.

System Load

As an administrator, you can display both active and saved conferences. Inactive conferences can be deleted.

INFO: Permanent conferences occupy system resources permanently. Since every subscriber can configure permanent conferences with myPortal for Desktop or myPortal for Outlook, you should, as the administrator, review the saved conferences regularly to avoid resource bottlenecks.

Video Monitoring

Any ongoing video transmission must be terminated before participating in a conference.

9.7.2 Ad-hoc Conference

An ad-hoc conference occurs spontaneously and is started manually by the conference controller. The conference controller can save ad-hoc conferences in order to set them up again at some later point in time.

Starting the Conference

The system opens the window with the virtual conference room automatically for all internal conference participants, provided they have started myPortal for Desktop with the classic user interface or myPortal for Outlook. The system calls all conference participants simultaneously. On joining the conference, each conference participant hears a greeting announcement with the name of the conference controller.

Recording the Conference

Conference controllers can record a conference manually for themselves or for all connected internal conference participants, provided the live recording of calls has been activated in the system. Participants located in the own node receive the recording in the voicemail box; participants in other nodes, via email. The duration of the recording is only limited by the available storage capacity of the system.

Ending the Conference

The conference controller can end the conference in the client or simply hang up. Alternatively, the conference ends when all conference participants have left the conference.

Expanding a Call to a Conference

An internal subscriber who is conducting a call can convert the call to an ad-hoc conference and add further subscribers. For this, the subscriber must have a UC Suite Conference license. This feature is not available for CallMe.

9.7.3 Scheduled Conference

A scheduled conference (Meet-Me conference) occurs at a pre-defined point in the future with a defined duration and may be set up to recur repeatedly at the same time.

A scheduled conference will run for the entire scheduled duration even if there are no connected participants. The conference controller saves a scheduled conference under a specified name.

Options for Configuring a Scheduled Conference

The initiator of the conference can define the following properties:

- Start time and End time
- Recurring conference
- Presence of conference controller required
- Authentication of conference participants on joining the conference required (by entering a conference ID and password via the phone keypad).

  INFO: Mobility Entry users must enter the code for DTMF suffix dialing before their authentication.

  The default password for conferences is 123456. The conference controller can change this for the conference participants individually.
- Language of announcements before the conference begins
- Direction for the connection setup for each conference participant (default: **outbound**).

Starting the Conference

The system opens the window with the virtual conference room at the scheduled time automatically for all internal conference participants, provided they have started myPortal for Desktop with the classic user interface or myPortal for Outlook. If the presence of the conference controller is required, the system first calls the controller. After the successful authentication of the controller, all the other conference participants are called simultaneously. Conference participants who have forwarded their calls to their voicemail boxes or who are determined to be absent by their presence status are not called. Depending on how the connection setup has been configured, the system calls the conference participants or the participants can dial in themselves. The system announces every participant who joins the conference by name, as in: "`...` `has joined the conference`", provided the initiator has recorded his or her name announcement.

INFO: Conference participants of a scheduled conference without authentication can only hear the announcement with the name of the conference controller at the start of the conference, provided they have already initiated a conference with authentication earlier on one occasion.

Dialing In

Every conference participant can use the dial-in number to dial into the conference within the scheduled time period, regardless of which direction for the conference setup was set for that participant. Attempts to dial into the conference outside the scheduled time period result in a corresponding announcement. To dial in via an ITSP, the ITSP must support RFC 2833 (DTMF characters).

Forcing Authentication with the Star (*) Key

The conference controller can set the conference so that each conference participant is forced to provide authentication by at least by pressing the * key. This ensures that only the participants who are actually present are connected to the conference, as opposed to a voicemail box, for example.

Extending the Conference

Ten minutes before the scheduled end of the conference, the participants hear an announcement indicating that the conference is about to end and are offered the option of extending the conference by dialing a specific digit. Any conference participant can extend the conference by dialing that specific digit. The conference controller can extend the conference in myPortal for Outlook at any time.

Recording the Conference

Conference controllers can record a conference automatically or manually for themselves or for all connected internal conference participants, provided the live recording of calls has been activated in the system. Participants located in the own node receive the recording in the voicemail box; participants in other nodes, via e-mail. The duration of the recording is only limited by the available storage capacity of the system.

Ending the Conference

The conference ends at the time scheduled for the end of the conference or if the conference controller terminates the conference.

9.7.4 Permanent Conference

A permanent conference is not subject to time restrictions. The conference participants can dial in at any time.

The conference controller saves a permanent conference under a specified name. The conference is retained until it is explicitly deleted.

Options for Configuring a Scheduled Conference

The initiator of the conference can specify:

- whether the conference participants need to authenticate themselves by entering a conference ID and password via the phone keypad when joining the conference.

  INFO: Mobility Entry users must enter the code for DTMF suffix dialing before their authentication.

  The default password for conferences is 123456. The conference controller can change this for the conference participants individually.
- in which language the announcements before the start of then conference are to be made.

Starting the Conference

As soon as the first conference participant dials in, the system opens the window with the virtual conference room automatically for all internal conference participants, provided they have started myPortal for Desktop or myPortal for Outlook. All conference participants dial in themselves. The system announces every participant who joins the conference, as in: "`... has joined the conference.`"

Dialing In

Every conference participant can use the dial-in number to dial into the conference at any time. To dial in via an ITSP, the ITSP must support RFC 2833 (DTMF characters).

Recording the Conference

Conference controllers can record a conference automatically or manually for themselves or for all connected internal conference participants, provided the live recording of calls has been activated in the system. Participants located in the own node receive the recording in the voicemail box; participants in other nodes, via e-mail. The duration of the recording is only limited by the available storage capacity of the system.

9.7.5 Open Conference

Open conferences are intended for a fixed number of arbitrary participants. Any participant who has the requisite access data can dial into them.

The conference controller saves an open conference under a specified name. The conference is retained until it is explicitly deleted.

Options for Configuring an Open Conference

The initiator of the conference can specify:

- The number of conference participants (max. 16).
- whether the conference participants need to authenticate themselves by entering a conference ID and password via the phone keypad when joining the conference.

  INFO: Mobility Entry users must enter the code for DTMF suffix dialing before their authentication.

  The default password for conferences is 123456. The conference controller can change this for the conference participants individually.
- what common conference ID is valid for all conference participants.
- in which language the announcements before the start of then conference are to be made.

Starting the Conference

All conference participants dial in themselves. The system announces every internal participant who joins the conference, as in: "`... has joined the conference.`"

Dialing In

Every conference participant can use the dial-in number to dial into the conference at any time. To dial in via an ITSP, the ITSP must support RFC 2833 (DTMF characters).

Recording the Conference

Conference controllers can record a conference automatically or manually for themselves or for all connected internal conference participants, provided the live recording of calls has been activated in the system. Participants located in the own node receive the recording in the voicemail box; participants in other nodes, via e-mail. The duration of the recording is only limited by the available storage capacity of the system.

9.8 Web Collaboration

The UC PC clients myPortal for Desktop (Windows) and myPortal for Outlook support the convenient integration of the separate product OpenScape Web Collaboration for simultaneous multi-media collaboration during phone calls and conferences. This provides quick access to functions such as desktop and application sharing, file sharing, co-browsing, whiteboarding, URL push, IM chat and video chat with multiple participants.

Web collaboration can be started by a subscriber during a phone call via the pop-up window of the UC PC client or by the conference controller of an active conference from within the conference. This opens the web collaboration session. A local installation of Web Collaboration on the UC PC client is not required. If an email program is available on the UC PC client, an email with the link to the web collaboration client can be sent to the communication partners. Detailed information on web collaboration can be found in the Web Collaboration product documentation.

When creating or editing a conference, the conference controller can also schedule a web collaboration session. On deleting or ending a conference, the associated web collaboration session is automatically deleted as well.

INFO: In order to enable UC PC clients to start web collaboration automatically, proxy authentication must be disabled whenever the UC PC clients access the Internet via a proxy server.

Supported Types of Connections

The web collaboration integration supports phone calls and phone-controlled conferences as well as the following types of application-controlled conferences:

- Ad-hoc conference
- Scheduled conference
- Permanent conference

Integration of Web Collaboration

For the integration of Web Collaboration, the address of the Web Collaboration server must be known to the communication system. The vendor offers the web collaboration server as a service on the Internet (Public Server). Alternatively, it may also be possible to use a Custom Server located on the customer's own network or with a partner. If the server is on the customer's own network, it is usually addressed by the communication system on TCP port 5004 using http. In the case of a hosted solution on the Internet (Public Server), a secure https connection is used instead, since the license number and password are transmitted over this connection. By default, TCP port 5100 is used for this purpose.

INFO: In order to use web collaboration, the communication system requires an Internet connection (default router and DNS server). Connections via proxy are not supported.

Internal conference participants with UC PC clients are automatically connected to the appropriate web collaboration session on starting the conference. To do this, FastViewer is automatically downloaded and opened in the background, which may take several seconds. External conference participants with known email addresses receive an email with an appropriate link to the Web Collaboration session.

INFO: Users working under a MAC OS must close the alert dialog for the terminated session manually after completion of a web collaboration session.

For a scheduled conference, it is possible to connect to the Web Collaboration session as early as 5 minutes before the start of the scheduled conference.

Instant Messaging and Web Collaboration

Note that Instant Messaging of the system and Instant Messaging of a Web Collaboration session are mutually independent, i.e.: the instant messages from a UC PC client do not appear in a web collaboration session of the same participant, and vice versa.

9.9 Instant Messaging

Instant Messaging refers to communicating with instant messages (usually called a chat).

9.9.1 Instant Messaging

Instant Messaging enables you to chat with other peers. The system supports instant messaging with users of UC Smart and external communication partners via XMPP and multi-user chats (or a combination of both).

Instant Messaging is possible with the following clients:

- myPortal for Desktop
- myPortal for Outlook
- myAgent
- myAttendant

As an administrator, you can enable or disable instant messaging on a system-wide basis. The sent and received instant messages are presented to the communication partners as an interactive dialog. On selecting a recipient, the client shows whether the communication partner is currently online. If one of the communication partners is offline, the following occurs with the instant message, depending on the type of the selected recipient:

Recipients	Behavior
Individual subscribers	The instant message is displayed at the next login.
Group in Favorites	The instant message is never displayed for the subscribers who are offline.

External Instant Messaging

As a subscriber, you can also chat with *one* external XPP communication partner (e.g., a Google Talk user).

Multi-user chat

A multi-user chat is the exchange of instant messages with multiple communication partners. Here too, the system supports a maximum of one external XMPP communication partner.

Instant Messaging and Web Collaboration

Note that Instant Messaging of the system and Instant Messaging of a Web Collaboration session are mutually independent, i.e.: the instant messages from a UC client do not appear in a Web Collaboration session of the same participant, and vice versa.

9.10 AutoAttendant

Depending on the presence status of the called party, the AutoAttendant offers callers options to route voice calls to fixed numbers or their voicemail box. Callers signal their choice by entering digits at the phone.

9.10.1 Personal AutoAttendant

The personal AutoAttendant is the customized AutoAttendant, which can be configured by subscribers.

Personal AutoAttendant

As a subscriber, you can do the following for your station number with myPortal for Desktop or with myPortal for Outlook:

- Record or import announcements for the personal AutoAttendant.
- Configure profiles for the personal AutoAttendant

The relevant calls are first handled by the central AutoAttendant.

9.11 Voice and fax messages

The Voicemail and Fax services integrated in the system enable subscribers to receive and manage voicemails and fax messages via myPortal for Desktop and myPortal for Outlook. Fax messages can be sent by subscribers using Fax Printer.

9.11.1 Voicemail Box

The voicemail box records central voicemail and recorded calls. Subscribers can access it by phone and via UC Smart clients.

Only voice messages longer than two seconds are recorded.

Managing Voicemail Messages

As a subscriber, you can listen to your voicemails:

- via a PC with myPortal for Desktop or myPortal for Outlook
- via your phone if your Presence status is **Office** or **CallMe**
- via any external telephone

Using myAttendant, the Attendant can also listen to voicemails of other subscribers who have explicitly allowed this.

The subscriber uses folders such as Inbox, Played, Saved or Deleted to manage incoming voicemail messages.

Voice messages can also be played back, paused and forwarded to another subscriber. The subscriber can also save voicemail messages in .wav format and redirect them to any selected email account.

The voicemail box can also be used by subscribers to manage recorded calls. Recorded calls are identified in the voicemail box by an appropriate symbol.

> ***INFO:*** Information on the Phone menu can be found in the Quick Reference Guide documentation of the UC Suite Telephone User Interface (TUI).

Calling Back the Sender of a Voice Message

When listening to a voicemail, the subscriber can directly call back the person who left a message.

As an administrator, you can configure on a system-wide basis whether or not callbacks can be executed from the voicemail box

- from any phone number
- only from the own phone numbers of a subscriber configured under My Personal Details in the myPortal for Desktop, myPortal for Outlook, myAttendant and/or myAgent clients (**Extension**, **Mobile number**, **External Number 1**, **External Number 2**, **Private Number** and **Assistant Number**).

Retention Period

As an administrator, you can configure the retention period for voice messages.

Prioritizing voicemail messages

Callers can flag their voicemail messages as normal, urgent or private.

In myPortal for Desktop and myPortal for Outlook, the prioritization of existing voicemail messages is represented by different colors.

Subscribers who listen to their voicemail messages through the phone are first notified how many messages are urgent, private and normal. Urgent messages are played back first.

If the voicemail messages are forwarded as emails, the voicemails identified as urgent are flagged as emails with high priority.

Functionality of the Voicemail Box

The administrator can define the scope of the voicemail box. He or she can choose between:

- **Full**
  Full functionality of the voicemail box (default value)
- **Short Menu**
- After the status-based or personal announcement is made, a connection to the operator is offered.
- **No Menu**
- After the greeting announcement is played, the caller is directly taken to record a message.

Displaying New Messages at the Telephone

Voicemail messages are signaled at the telephone. As soon as the voicemail has been played, the indicators are deleted.

The type of signaling used for new voicemail messages depends on the phone

- For all telephones, acoustic signaling occurs using a special dial tone.
- For system telephones without a display, the Mailbox key also lights up (if configured).
- For system telephones with a display, the Mailbox key lights up (if configured), and a message appears on the display.

Notification Service

Subscribers who are using myPortal for Desktop or myPortal for Outlook can define whether the notification about the arrival of new voicemails should be forwarded and, if so, to what destination.

Subscribers can also define whether the message should be forwarded as an email. In addition, they can choose to be notified about the arrival of new voicemails by a phone call or an SMS.

Language of the Voicemail Box

As an administrator, you can select the default language of the voicemail box for the menu prompts and the internal system announcements on a system-wide basis.

Dependencies

Topic	Dependency
Playing a message over the phone	Subscribers can play back voicemails through the phone only in the **Office** or **CallMe** presence status. For all other settings, the message can only be played back via the PC.

9.11.2 Voicemail Announcements

Voicemail announcements notify callers about the Presence status of a subscriber, for example.

Standard announcements are available in all languages. As a subscriber, you can also record or import personal announcements for your voicemail box. The corresponding standard announcement is overwritten by the personal announcement in the process. As an administrator, you can change the standard announcements by importing different announcements. The personal announcements of subscribers are overwritten in the process. The system performs the automatic level control and normalization needed to meet the "USA / TIA 968 Signal Power Limitations" requirements.

INFO: Before using announcements or music from other sources, make sure that you do not infringe on any copyrights.

System Language for Voicemail Announcements

The system language for the voicemail box is set at the country initialization. In addition, the subscriber can set the language of his or her own voicemail box. A caller will then hear the station-specific announcements in the language set by the subscriber and the system-specific announcements in the system language.

Announcements Depending on Presence Status and Profile

Depending on the Presence status, the announcements for the voicemail box change automatically; for example, if the Presence status is **Meeting**, then the announcement may be something like: The subscriber is in a meeting until 3.00 p.m. today. If the entered end of a meeting is reached, but the subscriber has not yet changed his or her status back to "In Office", then the voicemail announcement is adapted automatically or the voicemail announcement reverts automatically to "In Office" (this is configurable by the subscriber).

The following table describes which greeting is heard by the caller, depending on the set Presence status and profile. The caller menu refers to the central AutoAttendant. The profile refers to the personal AutoAttendant of the subscriber here. The default greeting, name and custom greeting for profiles must be recorded by the subscriber. Depending on the configuration, the caller menu may vary in length or may not be available at all.

	Busy **No answer** **Do Not Disturb**	**Meeting** **Sick** **Break** **Gone Out** **...**
Voicemail with Presence status	Default greeting + Caller menu	Name + Presence status + Caller menu
Voicemail box with blocked Presence status	Default greeting + Caller menu (if enabled)	
Profile with dynamic greeting	Custom Profile Greeting	Name + Presence status + Custom Profile Greeting
Profiles if dynamic greeting is to be skipped	Custom Profile Greeting	

If a subscriber has set his or her presence status to not be displayed to external callers, the external caller will always receive the "Busy" greeting for all presence states other than "Office" even if the called subscriber may not be actually busy in some cases. In this case, the subscriber should set up an announcement for the "Busy" greeting to indicate that he or she cannot accept the call.

9.11.3 Fax Box

The fax box enables subscribers to receive and send fax messages via myPortal for Desktop or myPortal for Outlook without a fax machine.

As an administrator, you can configure a fax box for licensed subscribers. In addition, you can connect fax devices or fax servers via the a/b or ISDN interface.

As a subscriber, you can access your fax messages via myPortal for Desktop or myPortal for Outlook. myAttendant can access the fax messages of subscribers who have explicitly allowed this.

Managing Fax Messages

The subscriber can manage received fax messages by moving them to different folders (Saved or Deleted, for instance). The fax messages can also be forwarded to another subscriber. The subscriber can also save fax messages as PDF or TIFF files and redirect them to any selected e-mail account.

The administrator can configure whether the fax message is to be stored as a TIFF file (default) or as a PDF file on a system-wide basis.

Retention Period for Fax Messages

The system automatically deletes fax messages for which the following retention periods are exceeded:

Fax message	Retention period (days)
New	120
Read	365
Sent	365
Deleted	60

9.11.4 Sending Fax Messages with Fax Printer

Fax Printer is an application for sending fax messages with centrally provided or individually created cover sheets from Windows applications such as Microsoft Word, for example.

Fax Printer consists of the following components:

- Fax Printer Cover Editor
- Fax Printer Driver

Fax Printer can be used from all the usual Windows programs. Fax groups make distribution easier. Fax messages are sent as an e-mail or directly to the Desktop. A screen pop notifies the subscriber when the fax is sent successfully.

Header Rows

As an administrator, you can configure different header lines for Fax Printer users. You can also define a header line as the default. Header lines may include the following elements:

Details	Placeholder
Date / Time	{{date_time}}
Company Name	{{company_name}}
User name	{{user_name}}
Company Ph.	{{company_number}}
Page number	{{page_number}}
Number der pages	{{page_count}}

The header lines of fax messages sent with Fax Printer may only include characters from the ANSI character set. In other words, no special or diacritical characters such as umlauts are allowed. Since the header line may basically include the sender's name, no special or diacritical characters should appear in the names of the subscribers as well.

9.11.5 Notification Service for New Messages (UC Suite)

The system can optionally notify you (as a subscriber) about a new message by e-mail, by phone or with an SMS.

The Notification Service works as follows:

Notification	for voicemail	for fax message	Prerequisites
E-mail	You receive an e-mail with the message as a WAV file, the date and time it was received, the duration of the message and, if available, the phone number and name of the sender. If the size of the WAV file exceeds 10 MB (average 1MB/min), it is not attached to the e-mail. Voicemails with "urgent" priority are flagged as e-mails with "High" importance. E-mails with a voicemail have a separate symbol in Outlook. If you are using an IMAP mailbox that shows only the e-mail headers, the usual e-mail icon will appear instead.	You receive an e-mail with the message as a PDF or TIFF file, the date and time it was received, the number of pages and, if available, the phone number and name of the sender. If the size of the PDF or TIFF file exceeds 10 MB, it is not attached to the e-mail. E-mails with a Fax message have a separate symbol in Outlook. If you are using an IMAP mailbox that shows only the e-mail headers, the usual e-mail icon will appear instead.	The delivery of e-mails has been configured in the system. The corresponding address is used as the sender.
SMS	You receive an SMS about the received message at the phone number defined by you.		The SMS template has been configured.
by phone	Your voicemail box calls you at the number you have specified and plays back the message to you.	-	

As a subscriber, you can enable or disable every type of notification for each Presence status individually. The notification by phone can be restricted to the business hours configured by the administrator. You can define the number and intervals for the repeated attempts for the notification by phone.

9.11.6 Sending E-mails

The feature for sending e-mails enables e-mail notifications about new voice and fax messages to be sent to subscribers and system messages to be sent to administrators by e-mail.

9.11.7 SMS Template

An SMS template enables subscribers to be notified about new voicemails with an SMS.

In order to receive SMS messages, a personal mobile e-mail address of the respective provider must be first activated. To do this, the subscriber sends an activation SMS to a speed-dial number. The subscriber then receives an SMS with his or her personal e-mail address, which is usually composed of the call number and the gateway name. For example, the mobile e-mail address for a T-Mobile customer with the phone number 0171/1234 567 would be: 01711234567@t-mobile-sms.de. This applies analogously to other networks as well.

An SMS template consists of the Template Details and SMS Details areas. The administrator must enter the name of the template in the Template Details area. This is usually the name of the E-mail-to-SMS Provider.

The specifications in the SMS Details area depend on the Provider. Under Recipient, the administrator must enter the e-mail address to which the SMS is to be sent. The entry for the Subject line may be freely selectable or require the customer number to be entered by the administrator.

INFO: Every Provider requires a specific template. The required data can be obtained from the respective mobile service provider.

Placeholder

SMS templates may include the following placeholders in the **Recipient**, **Subject** or **Text** field:

Details	Placeholder
Mobile number to which the message is to be sent	`{{MobileNumber}}`
Name or call no. of the sender	`{{Sender}}`
Date and time of receiving a message	`{{DateTime}}`
Caller number	`{{CallingNumber}}`
Priority of message	`{{Priority}}`

System-Specific Information

The length of the message is reduced to the first 160 characters.

9.11.8 Fax over IP (T.38 / G.711 Fax)

Fax over IP enables the transmission of fax messages over the Internet in accordance with the G2 and G3 standards by using the network protocol IFP (Internet Facsimile Protocol).

UC Suite can generally handle up to 8 simultaneous fax connections. Depending on the DSP module, OpenScape Business X3/X5/X8 as an ISDN gateway can handle from 3 to 12 concurrent faxes. Both parameters determine the number of simultaneous T.38 or G.711 fax connections.

INFO: It is highly recommended to use T.38 fax, if possible.

The system supports the following scenarios for T.38 or G.711:

- A subscriber receives fax messages via an ITSP (Internet Telephony Service Provider) at his or her fax box and sends faxes to external locations with Fax Printer via the ITSP.
- A subscriber receives fax messages via a Mediatrix 4102S (SIP) at his or her fax box and sends faxes with Fax Printer via a Mediatrix 4102S (SIP).
- Stations can receive Fax messages via an ITSP (Internet Telephony Service Provider) on a fax device that is directly connected to an analog or ISDN interface and send faxes from this fax device via the ITSP to external destinations.
- Stations can receive fax messages via an ITSP on a fax device that is connected to a Mediatrix 4102S and send faxes from this fax device via the Mediatrix 4102S and ITSP to external destinations.
- Stations can receive fax messages via ISDN on a fax device that is connected to a Mediatrix 4102S and send faxes from this fax device via the Mediatrix 4102S and ISDN to external destinations.
- A station can send fax messages from a fax device that is connected to a Mediatrix 4102S to another fax device that is also connected to a Mediatrix 4102S.
- Internal fax message from a fax device at an ISDN port to a fax device at a Mediatrix 4102S and vice versa.
- Internal fax message from a fax device at an ISDN port to a fax box and vice versa.

INFO: T.38 must be activated in the system for the fax box. In order to send faxes from the communication system via an ITSP, the ITSP must support T.38. In case the ITSP cannot switch to T.38, then the fax will be handled as G.711.

10 Functions at the Telephone

The communication system offers a comprehensive set of telephony features extending from the usual features such as hold, toggle/connect and consultation hold, etc., through various call signaling mechanisms, down to call transfers, call deflections and call forwarding.

10.1 Making Call

The communication system offers many ways to make calls, including, among other things, direct station selection and speed dialing.

10.1.1 Digit Dialing

In the case of digit dialing, every digit is transmitted as soon as it is dialed.

The call setup begins immediately after the input of the first digit. Consequently, the subscriber has no way to edit the dialed number.

10.1.2 En-Bloc Dialing

In en-bloc dialing, connections are only established after the complete phone number has been entered. The call number is transferred as a single block.

The transmission of the dialed number can be initiated by entering the end-of-dialing code (#).

En-bloc dialing is mandatory for:

- ITSP trunk connection
- ISDN Primary Rate Interface in the U.S.

After 5 seconds without the input of a digit, the last entered digit is interpreted as the final digit of the number block.

10.1.3 Keypad dial

In some countries, the services of digital trunk connections are controlled using keypad dialing instead of functional control. To activate these services in the PSTN, you can use the stimulus interface.

The feature must be configured in E Manager.

Subscribers acknowledge the message traffic using the display. As a result, keypad dialing can only be performed on telephones with a display (optiPoint, OpenStage), mobile telephones (Cordless) with optiPoint menu navigation and IP telephones with stimulus interfaces. ISDN telephones are not supported. Each network provider determines which services can be used with keypad dialing.

An authorized station can activate keypad dialing using the service menu or using the *503 code. This is possible only in the idle state. Then the station must select an ISDN trunk that the feature can use.

Depending on the messages sent by the central office (such as when connecting), keypad dialing can create CDR entries. The number of the station using keypad dialing, the line used, and the time period when the feature was used are logged.

INFO: Actions triggered by keypad dialing are not monitored by the system. The system cannot prevent improper use, such as call charges fraud or trunk blocking.

Customers must be informed that they are liable for damages resulting from the improper use of this feature.

10.1.4 End-of-Dialing Recognition

End-of-dialing is either recognized automatically after five seconds or indicated manually by the user with the end-of-dialing code "#".

10.1.5 Editing the Telephone Number

This option lets subscribers modify the digits entered for the station number. This function is common in mobile phones. A call number can only be corrected as it is being entered.

After entering a sequence of digits, the user can edit it from right to left by pressing a key; each time the key is pressed, one digit is deleted. Once the correct digit sequence is entered in full, the user can press the confirm key or lift the handset to start digit transmission.

It is not possible to edit a saved call number, for example, for number redial.

INFO: This feature can be individually activated for every station.

Dependencies

Topic	Dependency
Call waiting	Call waiting is possible during editing because the telephone is in digit input state and is busy for incoming traffic.
Consultation	The telephone is in digit input state after a consultation. This makes it possible to edit station number digits.

10.1.6 Redialing

The phone number dialed is saved after an external call is set up. If the destination is busy or not reachable, a user can press the Redial key to redial the same number.

Speed dial numbers are also stored in the redial memory.

Dialing internal call numbers has no effect on the redial memory.

Post-dialed digits (also called DTMF characters), if any, are not seen as part of the dialing information and are therefore not saved (e.g., digits sent to a connected voicemail box).

The Redial function can only be activated via a key, not via an access code.

To retrieve a specific number and use it to set up another call, press the Redial key. Press the key once to dial the last number dialed. Press the key twice to dial the next-to-the-last number dialed. Press the key three times to dial the number that was stored the longest.

The station number saved is automatically dialed after 2 seconds when you press the Redial key. If you need more time to read the displayed station number, select "scroll" with the Confirm Key. Click "Next" to display the next phone number saved. This is phone number is dialed only on selecting the "Make Call" command. This gives you much more time to check if the correct phone number was selected.

In the case of a call routed via LCR, only the number dialed by the station is stored.

Account codes are also stored in the redial memory. This is true only if the appropriate system-wide flags are set.

10.1.7 System Speed Dialing

You can save frequently needed external phone numbers in the communication system. Every number is then represented by a speed-dial number which is used instead of the full phone number.

Speed-dial numbers consist of 4-digit numbers.

All subscribers are members by default of a group that is assigned all SSD numbers. This means that every subscriber can use all SSD numbers.

SSD overrides toll restriction rules.

The numbers for system speed dialing are configured by the administrator in groups. The subscribers can each be assigned to one of these groups. A subscriber can only use the speed-dial numbers of his or her allocated group. A group can only be assigned a single SSD range.

Entries in speed dials are searchable by first and last name if name is configured in <Last Name>, <First Name> or <First Name>, <Last Name> format.

Used speed dial numbers are stored in the redial memory.

To program a "dial pause" and DTMF changeover for suffix dialing of DTMF characters (e.g., for controlling voicemail boxes), you can use the Repdial "P-key" or "#" (pound) key.

Translation of station numbers to names

You can assign a name to each speed-dialing destination. As soon as a call is received from a saved phone number, the system automatically enters the name and displays it instead of the phone number if CLIP is set.

Suffix-dialing

Suffix-dialing is also possible:

- Manual suffix-dialing
  The user can select additional numbers by selecting the access code and entering the index number (speed-dial number). These are added to the station number saved in this index and dialed.
- Automatic suffix-dialing
  When configuring an SSD, the number entered can be split into two parts. A dash "-" is used as the separator. The first part is always sent. A timer then starts. If the user does not dial any more digits before the timer expires, the second part of the number entered is automatically suffix-dialed, otherwise the manually dialed digits are transmitted.

  For example: SSD = 7007–0
  If the station does dial a DID (manual suffix-dialing) after selecting the SSD and before the specified time has expired, 0 is automatically dialed (automatic suffix-dialing).

Importing Speed Dial Numbers

You can import speed-dial lists from an XML or CSV file in UTF-8 format. Existing speed dial numbers are deleted before the import.

File structure:

4-digit speed dial (use leading zeros)**;**CO access code with long number*;* last name, first name

Example:

```
0001;08970070;Schmidt, Marcus
```

```
1010;006768970070;Schmoll, Lucas
```

> ***INFO:*** An XML template with the appropriate explanations can be found in the WBM under **Service Center > Documents > CSV Templates**. You can enter your speed dial destinations in these templates by using Microsoft Excel, for example.

Exporting Speed Dial Numbers

As an administrator with the **Expert** profile, you can export speed-dial numbers to an XML file in UTF-8 format in the **Expert mode**. The export always includes all the records.

10.1.8 Individual Speed Dialing (ISD)

Individual Speed Dialing (ISD) enables every subscriber to save 10 external numbers as individual speed-dial numbers in addition to the system speed-dial numbers.

For telephones without a display, the station user must wait for the confirmation tone following station number entry.

External numbers can be programmed in the ISD pool. Access depends on the station's dial-up access rights. Before entering the station number, the subscriber must enter the CO access code (e.g., 0).

The Redial key or the pound (#) key is used to program a dial pause or DTMF changeover.

10.1.9 Direct station select

The function keys on a telephone or add-on device can be programmed as DSS keys. These are programmed with the phone number of an internal subscriber or a group for this. Press a key of this kind to initiate an immediate call to the programmed destination (DSS). The current status of the subscriber or of the group is indicated by the LED associated with the DSS key.

A DSS (direct station selection) key can also be used to transfer a call quickly to the programmed subscriber or group. Pressing a DSS key during a call with an external party places the ongoing call on consultation hold. The transferring subscriber can transfer the call to the transfer destination by replacing the handset (unscreened transfer). He or she can also wait until the transfer destination responds before transferring the call (screened transfer). If the transfer destination does not answer, an automatic recall is enabled.

Statuses of a DSS Key LED

The DSS key LED shows the current status of the programmed station:

- Off: the associated subscriber is not conducting a call.

- Lit: the associated subscriber is conducting a call or has activated Do Not Disturb.
- Flashing fast: the associated subscriber is conducting a call. The call can be accepted by pressing the Direct Station Select (DSS) key.
- Flashing slowly: the associated subscriber is being called and has not yet answered. The call can be accepted by pressing the Direct Station Select (DSS) key.

Dependencies

Topic	Dependency
ISDN phones, SIP phones	Direct Station Select (DSS) keys cannot be programmed for ISDN or SIP telephones.

10.1.10 Speaker Calls / Direct Answering

The Speaker call function lets you set up an internal connection without the called subscriber lifting the handset. The loudspeaker on the called station is automatically activated.

On phones equipped with a speakerphone (microphone), direct answering of the called station is possible by switching on the microphone. On lifting the handset, the call becomes a normal two-party call.

Speaker calls can be used via a function key programmed for this purpose, the associated menu item or by entering the code and then dialing the station number of the destination station or group. A function key can also be programmed with a station number. A connection to the programmed destination is immediately set up when you press a function key of this kind.

Speaker calls also enable the broadcasting of announcements to all internal members of a group.

Direct answering can be activated via the menu item provided for this in the display or via a function key programmed for this purpose.

Speaker calls can be prevented for a subscriber by enabling an option to prevent voice calling. In this case, speaker calls are signaled like a normal call.

Dependencies

Topic	Dependency
Do Not Disturb, Override Do Not Disturb	Speaker calls are not possible at stations where Do Not Disturb is active. If the subscriber who wants to use the "Speaker calls" feature is authorized to override Do Not Disturb, he or she hears the busy tone for five seconds. The destination station is then called, but not directly addressed.
Toggle, consultation hold, transfer	The specified features cannot be used in a speaker calls/ direct answering connection.
ISDN phones, SIP phones	The "Speaker call" and "Direct answering" features cannot be used with ISDN or SIP telephones.

10.1.11 Associated Dialing

Associated dialing enables an authorized subscriber to dial a phone number on behalf of any other subscriber. The effect is the same as when the other subscriber dials the phone number.

The user accesses the function by dialing a code and specifying the station for which a number should be dialed. The system then interprets this information as though the station specified earlier were dialing.

10.1.12 Trunk Queuing

A subscriber can reserve a trunk in advance if there are no free trunks available (busy signal). As soon as a trunk becomes free, it is offered to the subscriber through an automatic recall.

If the user is busy at the time of the recall, the trunk will camp on to the busy station. If the camp-on tone is not answered, the reservation is canceled, and the trunk is offered to the next station in the queue. If the user activated DND prior to receiving the recall from the queued trunk, the trunk reservation is canceled and the trunk is offered to the next station in the queue.

If a number of stations queue a trunk, the trunk is assigned in the order that the requests were received.

Only one queue/reservation request is accepted per telephone. If a second reservation is attempted, it overwrites the first.

It is not possible to invoke the Trunk Queuing feature if the attempted call was placed through LCR (least cost routing).

The Trunk Queuing feature ignores an existing call forwarding—no answer instruction. Trunk reservation is canceled if not answered within 20 seconds.

A recalling trunk cannot be picked up by either Call Pick up - group or Call pick up - Directed.

Trunks can be reserved in one of the following ways:

- Manual reservations only work in telephones with a display
- Automatic reservation (for all other telephones)
  When this flag is activated and if a station is not assigned a free trunk after the usual simplified dialing procedures, the busy tone is signaled at the station. After five seconds, a positive acknowledgment tone is applied and the trunk is reserved, provided that the station has the appropriate CO call privilege.

INFO: Trunk queuing is not possible for S_0 phones.

10.1.13 Private Trunk

A private trunk is a CO trunk that is available exclusively to a specific subscriber.

10.2 Call Signaling, Calling Line ID

The communication system offers various options for call signaling and call number display such as CLIP, CLIR, COLP and COLR, for example.

10.2.1 Different Call Signaling

Different call signaling enables a distinction to be made between internal and external incoming calls.

Incoming calls are signaled visually and acoustically on the phone. The following displays appear on the screen:

- Caller number
- For internal call forwarding: additionally, the dialed call number

The incoming call can also be signaled via an LED. Different acoustic signals are used for internal and external calls.

Call signaling internal

Each subscriber can be assigned one of a total of eight possible acoustic call signals for internal calls. The station then uses the modified ringing tone to distinguish its calls at other internal stations. For example, a special internal ringing tone can be set for the manager so that every staff member knows when the manager is calling simply from the ringing tone.

Call signaling external

There are three different call types, each with different acoustics, that can be set for an external call. Different acoustic signals can be applied, for instance, to distinguish between calls from two different groups such as Sales and Warehouse.

- In Germany, the administrator can configure three different ring types for analog, ISDN and system phones.
- In other countries, the ring types for analog phones are the same.

10.2.2 Calling Line Identification Presentation (CLIP)

Calling Line Identification Presentation (CLIP) shows the caller's number at the called station.

The CLIP (Calling Line Identification Presentation) refers to incoming calls and must be supported by the network provider.

If the caller's name and phone number are programmed as a system speed dialing (SSD) number in the communication system, you will see the name on your display.

The Calling Line Identification Presentation (CLIP) and Calling Line Identification Restriction (CLIR) features are mutually exclusive, that is, as soon as CLIP is activated, CLIR is deactivated, and vice versa.

Configurable CLIP

Configurable CLIP transmits a set call number (e.g., the call number of a hunt group) externally instead of the caller's number (e.g., the number of the hunt group member).

System-Specific Information

Country	Enabled by default
USA	LIN (Location Identification Number). If CLIP is enabled for the USA, LIN is automatically disabled.
Remaining countries	CLIP

10.2.3 Calling Line Identification Restriction (CLIR)

Calling Line Identification Restriction (CLIR) suppresses the station number of the caller at the station of the called subscriber.

CLIR (Calling Line Identification Restriction) applies to outbound calls. The PSTN must support the feature. The Calling Line Identification Restriction (CLIR) has precedence over the Calling Line Identification Presentation (CLIP).

The Calling Line Identification Presentation (CLIP) and Calling Line Identification Restriction (CLIR) features are mutually exclusive, that is, as soon as CLIP is activated, CLIR is deactivated, and vice versa.

CLIR and COLR can only be enabled or disabled together.

Calling Line Identification Restriction (CLIR) has no effect for certain call destinations (e.g., emergency numbers of the police and fire departments).

System-wide Station Number Suppression (CLIR)

As an administrator you can enable or disable the CLIR station number suppression on a system-wide basis.

INFO: The flag "System-wide station number display suppression" does not apply to the U.S.

Temporary Station Number Suppression

As a subscriber, you can activate or deactivate the temporary station number suppression (CLIR). A temporary station number suppression is only possible if the system-wide station number suppression has been deactivated.

Station Number Suppression (CLIR)

As an administrator, you can configure the CLIR for each route so that only the PABX number is transmitted instead of the subscriber's station number.

10.2.4 Connected Line Identification Presentation (COLP)

Connected Line Identification Presentation (COLP) transmits the call number of the called subscriber to the caller as soon as the two are connected.

Connected Line Identification Presentation (COLP) is an ISDN feature.

COLP makes sense with call forwarding, for example, so the caller can see the phone number of the actual communication partner instead of the originally dialed phone number.

The Connected Line Identification Presentation (COLP) and Connected Line Identification Restriction (COLR) features are mutually exclusive, that is, as soon as COLP is activated, COLR is deactivated, and vice versa.

10.2.5 Connected Line Identification Restriction (COLR)

Connected Line Identification Restriction (COLR) suppresses the display of the called station at the station of the caller.

The Connected Line Identification Restriction (COLR) applies to incoming calls.

The Connected Line Identification Restriction (COLR) has precedence over the Connected Line Identification Presentation (COLP).

The Connected Line Identification Presentation (COLP) and Connected Line Identification Restriction (COLR) features are mutually exclusive, that is, as soon as COLP is activated, COLR is deactivated, and vice versa.

CLIR and COLR can only be enabled or disabled together.

10.2.6 CLIP No Screening (Transmission of Customer-Specific Phone Number Information)

CLIP No Screening transmits a call number specified by the caller instead of the caller's own number.

The outgoing system number does not have to be identical to the incoming system number.

The "Suppress station number" flag can be activated for special customer applications. This prevents the system from sending out the DID number of the station along with the outgoing system number.

Example: You want to prevent direct customer access to a service staff member who is reached centrally with a general service number. To conceal the staff member's own DID number, enter the general service number as the outgoing PABX number and activate the "CLIP no screening" flag. Then called subscribers see only the general service number on their display as the CLIP.

Incoming and outgoing calls usually use the same system number. In this case, the entry under "System number - outgoing" is either empty or the same as the one under "System number- incoming". If this is not the case, you can

- enter a different number under "System number - outgoing".
- use the routing parameter "No. and type, outgoing" to define whether the "System number - outgoing" entered contains the station number without area code, with area code (national), or also with the international country code (international).

INFO: CLIP no screening must be supported by the Network Provider and be activated.

10.2.7 CLIP for Analog Telephones

CLIP for analog telephones transmits the call number of an analog device of the caller to the called party and displays the CLIP (Calling Line Identification Presentation) on suitable devices of the called party analogously.

The additional transmission of CNIP name information (Calling Name Identification Presentation) can be configured.

INFO: CNIP is device-independent. Please also refer to the vendor specifications.

10.2.8 Ringer Cutoff

The Ringer Cutoff feature signals incoming calls acoustically with only a brief alert tone (beep) and on the display.

Ringer Cutoff is only available on phones with displays and has no effect on the signaling of appointments.

10.2.9 Translating Station Numbers to Names for System Speed Dialing

For calls made using system speed-dials (SSD) and for incoming calls from system speed-dial numbers, the name associated with the speed-dial destination is displayed after dialing instead of the speed-dial number.

10.3 Functions During the Call

The communication system offers several functions during calls, e.g., holding, redirecting and transferring calls.

10.3.1 Placing a Call on Hold

Placing a call on hold causes the call to be held in a waiting state. During this period, the caller usually hears an announcement or music on hold.

The hold ends when the held call is retrieved (i.e., resumed).

The following types of holds are possible:

- Common hold:
  Any subscriber can retrieve the call again by pressing a trunk or call key
- Exclusive hold: (only for Team or Top function and at the Attendant Console)
  Only the initiating party can retrieve the call.

Placing a Call on Hold and Automatic Recall

A parked call results in an automatic recall when the **Time for parking + change to hold** timer expires (default: 160 s).

10.3.2 Parking

Parking a call causes that call to be placed in a waiting state. During this period, the caller usually hears an announcement or music on hold. A parked call can be retrieved from any telephone.

As a subscriber, you assign a park slot (0-9) for a call to be parked. If the park slot you select is already occupied, a negative confirmation tone sounds and the number does not appear on the screen. You can then select another park slot. To retrieve a parked call, you must specify its park slot.

A parked call can be retrieved (unparked) via a code or a correspondingly programmed key and can also be retrieved if another call is waiting at the same time.

Parking and Automatic Recall

A parked call results in an automatic recall when the **Time for parking + change to hold** timer expires (default: 160 s).

Parking and Call Forwarding

In the case of a recall, a parked call does not follow call forwarding.

Parking and DISA

Parking cannot be enabled via DISA.

Parking and Conference Calls

You cannot park a conference call.

Parking and Networking

A parked call can only be retrieved in the same node. An incoming call over a network can only be parked at the destination node.

Parking and Do Not Disturb

A station with DND enabled can place a call in a park slot; however, if a recall occurs from the parked call, and no other destination was defined in the call management, the call will be automatically disconnected after the recall timer expires.

> ***INFO:*** Detailed instructions on how to park a call and how to retrieve a parked call can be found in the relevant chapter of the corresponding device's user guide (OpenStage X Hipath/ OpenScape 3000/ 4000 User Guide).

10.3.3 Consultation

In the case of a consultation hold, a subscriber initiates a second call from the same phone or accepts a waiting call. In the meantime, the first call is placed on hold.

A consultation hold is terminated on:

- retrieving the held call or
- Disconnect
  This results in either:
  - a transfer of the held call or
  - an immediate automatic recall from the party on hold to the party that has just hung up

Consultation Call using the Direct Station Select (DSS) Key

Pressing a Direct Station Select (DSS) key during a call initiates a consultation call to the corresponding destination.

Connecting two External Parties

During an external call, a consultation call to another external destination followed by a transfer connects the two external parties. This may involve call charges.

10.3.4 Toggle/Connect

The Toggle/Connect feature enables a subscriber to switch between two calls. When the subscriber is talking to one party, the other party is placed on hold.

The subscriber can toggle between the two calls by pressing the appropriate trunk key.

Toggle/Connect and Placing a Call on Hold

The Toggle function is not available to an on-hold subscriber.

10.3.5 Transfer

A transfer enables a subscriber to transfer his or her call to another destination. As soon as a subscriber initiates a transfer, the waiting party is placed on hold for the time being.

The following types of transfers are possible:

- Blind transfer (also called an unscreened transfer):
  You can transfer the call without an answer from the subscriber at the destination of the transfer. If the station at the transfer destination is busy, the call is camped on (i.e., call waiting is signaled). If a third party now tries to transfer a call to this busy station or if call waiting rejection has been turned

on at the transfer destination, an immediate recall occurs. If the subscriber at the transfer destination does not accept the transferred call within a specified time period ("Dial time during transfer before answer" timer), an automatic recall occurs. A blind transfer (also called an unscreened transfer) to an agent in another Multimedia Contact Center queue is not possible.

- Consultation transfer:
  You can transfer the call only if the subscriber at the destination of the transfer answers. The transfer is completed by hanging up the handset.

Transfer with Call Forwarding

Any call forwarding set at the transfer destination will be followed, i.e., the call will be forwarded accordingly. The display shows the final destination of the transfer.

Transfer with Do Not Disturb

Transferring a call to a station at which Do Not Disturb is enabled results in an immediate recall to the transferring station even if the transferring station itself also has Do Not Disturb enabled.

System-Specific Information

"Dial time during transfer before answer" timer: 45 seconds by default

Up to 5 calls can be transferred simultaneously to a busy station.

10.3.6 Automatic Recall

An automatic recall is received by the originator of a call if his or her call was placed on hold or parked for too long or if an attempt to transfer that call was unsuccessful.

An automatic recall occurs in the following cases:

- A held or parked call is not picked up again within a specific time period ("Time for parking + change to hold" timer).
- In the case of unscreened transfers, under the following circumstances:
  - The call is not answered before a certain time period expires ("Dial time during transfer before answer" timer)
  - The destination does not exist
  - The destination is busy with a second call
  - The digital phone at the destination is defective
  - The transfer type is not allowed

If the originator (i.e., initiating party) is busy during the recall, the automatic recall will camp on the line. As soon as the originator is free again, the automatic recall is signaled. Either the caller's phone number or that of the destination can be shown on the display or the originator. If the recalled party does not answer the call before the "Intercept time for automatic recall" timer expires, an intercept to the intercept position occurs (if the "On unanswered recall" flag is set). If the intercept position does not answer the recall before the "Time for activation of

automatic recall at attendant console" timer expires, the recall is automatically disconnected.

Automatic Recall and Call Pickup

Every station in a call pickup group with the initiating party (originator) can pick up an automatic recall if the system-wide flag "Call Pickup after Automatic Recall" is set.

Automatic Recall and Do Not Disturb

An automatic recall ignores the Do Not Disturb setting.

System-Specific Information

"Intercept time for automatic recall" timer: 30 seconds by default

"Time for activation of automatic recall at attendant console" timer: 60 seconds by default

10.3.7 Call Supervision (Selected Countries Only)

Call Supervision allows authorized subscribers to listen in on a call conducted by any internal subscriber. The microphone of the party listening in is automatically muted. The participants in the monitored call are not advised of the monitoring operation by any signal such as a tone or display.

This feature can only be activated in the following countries: Argentina, Australia, Belgium, Brazil, France, United Kingdom, Hong Kong, India, Ireland, Malaysia, New Zealand, Netherlands, Portugal, Singapore, Spain, South Africa, Thailand, United States.

Authorized subscribers need a system phone and the Override class of service.

The subscriber you want to monitor must be actively conducting a call. When you start and end call monitoring, you may encounter a lapse of up to two seconds of the conversation. The monitored connection is released as soon as one of the stations in the connection is put on hold, transferred or the call is ended. The monitored connection can only be resumed when the station to be monitored is again engaged in a call.

Dependencies

Topic	Dependency
Cordless phones	You cannot use call monitoring at cordless telephones because they do not support automatic microphone muting.

Topic	Dependency
Conferencing	Call Supervision restricts the number of possible conferences. Maximum number of conferences possible in the system = maximum number of simultaneous call monitoring stations.
Call Supervision	The call can be overridden only using code *944 + station number (not from a menu).
Call Supervision	To enable the use of features at a station, both the station flag **Call Supervision** and the flag **Override class of service** on must be activated. (Feature cannot be used with CSTA monitoring.)

10.3.8 Discreet Call (Whisper)

The Discreet Call (Whisper) feature enables a subscriber (e.g., at station C) to monitor a simple existing connection between two other stations (e.g., A and B) and to pass on information to station A that without being heard by station B. This feature is typically used in Contact Centers and Executive/Secretary systems.

The feature must be configured in E Manager.

INFO: Although there is no connection between station B and station C, user B may be able to hear the muffled tones of what user C is saying because of feedback on station A.

Destination terminals for the Whisper feature (station A) can only be system telephones with displays. Stations A and C must be in the same node.

In the idle/ready state, station C activates this feature by dialing a code. The telephone features a partially programmed key (only the code is programmed on the key, the station number must be suffix-dialed). A new menu item will be incorporated into the Service menu; the Idle/Call menu remains unchanged.

The option for activating the feature is linked to a user-specific class of service. A second class of service can be used to protect station A from a discreet call (whisper/off hook announcement).

The feature is disabled if this is initiated by the activating station C or by the impact of some other call-related feature.

INFO: If neither of the participants in the original call is a TDM station, the switching network is not involved at the time of activation, and changeover is impossible without briefly interrupting the existing connection.

INFO: Call transfer and conference functionalities are not available from UC Suite products while Discreet Call is activated.

If the Whisper/Off Hook Announcement feature is active, and station A or station B initiates another call-related feature, the Whisper feature will be deactivated. The table below provides further information on interaction with particular features:

Feature	Station A		Station B		Station C	
	Possible	Action	Possible	Action	Possible	Action
Consultation Hold, Call Hold, Park, Common Hold	Yes	Deactivate Whisper/ Off Hook Announcement	Yes	Deactivate Whisper/ Off Hook Announcement	no	Negative acknowledgement
Transfer	--	--	--	--	--	--
Conferencing	--	--	--	--	--	--
Call waiting	Yes	--	Yes	--	Yes	--
Accept call waiting	Yes	Deactivate Whisper/ Off Hook Announcement	Yes	Deactivate Whisper/ Off Hook Announcement	Yes	Negative acknowledgement
Override	no	--	no	--	no	--
DTMF transfer	Yes	--	Yes	--	no	--
FEAT counter	--	--	--	--	--	--
Associated Services	--	--	--	--	--	--
DISA/DISI	--	--	--	--	--	--

10.4 Controlling Availability

To control accessibility, the system offers features such as call forwarding, do not disturb and call rejection.

Call destination lists are used for various call forwarding types. Call destination lists define how incoming calls for the assigned station or assigned group are handled. The individual call destinations in a call destination list are processed sequentially. Different entries are possible for internal and external calls (day or night).

10.4.1 Call Forwarding

Call Forwarding—No Answer (CFNA) forwards calls that are not answered within a certain period of time.

This type of forwarding is also referred to as fixed call forwarding, since it is only configurable by the administrator.

For each call forwarding, there are one or more call destination lists, which can be assigned to the stations for the following types of calls:

- External calls during the day (when the night service is inactive)
- External calls at night (during active night service)
- Internal calls

For each call destination list, you can specify up to 4 call destinations to which the call is to be forwarded sequentially after a preset time has expired.

Under normal circumstances, the station number or name of the originally called subscriber and the station number or name of the caller are displayed at the call forwarding destination. As an administrator, you can disable the additional display of the station number or name of the caller.

Call Forwarding on Busy

Call forwarding on busy forwards an incoming call for a busy extension immediately to the next call destination.

If the call destination is also busy, the caller hears a busy signal. For an internal call, the call remains at the call destination, which is cyclically checked until the destination is free. The administrator defines the cycle.

If the call destination is not available and if no further call forwarding has been configured for it, then the call not forwarded.

Dependencies

Topic	Dependency
Analog telephones	There is no indication at these telephones that this call has been forwarded.
Call waiting	If a subscriber enabled call waiting, an incoming call is camped on if call forwarding—busy is configured for him or her.
DND	A call destination which has activated DND, will be skipped.
Call forwarding	Call Forwarding - No Answer (CFNA) is only executed when the call forwarding destination has not responded after a timeout period defined by the administrator.

Topic	Dependency
Night service	If the option "by day / by night" is enabled for a subscriber as the Call Forwarding - No Answer (CFNA) setting, external calls are forwarded in accordance with the settings for the night service. Internal calls are still handled as in the "by day" settings.
External Call Forwarding - No Answer	If external call forwarding - no answer is active, this has precedence over other call forwarding instructions.
Hunt group / Group call	If you enter a group or hunt group as the destination of a call forwarding—no answer instruction, every subscriber in the entire group is called before the next call forwarding destination is evaluated. Group calls and hunt groups can be seen as a call forwarding configuration within a call forwarding configuration. A hunt group is busy if all members are busy or have left the hunt group. A group is always busy if all members of the group are busy.

10.4.2 Call Forwarding (CF)

Subscribers can use Call Forwarding (CF) to redirect incoming calls to a destination of their choice.

If trunk keys (incl. MULAP trunk keys) have been configured, users can also activate call forwarding individually for a specific trunk (or MULAP trunk).

The following calls can be diverted:

- All calls
- External calls only
- Internal calls only

The following destinations are possible for call forwarding:

- Other phone (internal or external)
- Attendant Console
- Voicemail
- Hunt Group
- UCD group (UCD Universal Call Distribution)

Outgoing calls can still be made when call forwarding is activated.

External destination

If the call forwarding destination is external, you must enter the trunk access code followed by the external phone number of the forwarding destination.

Call Forwarding to External Destinations

If a subscriber has entered an external call forwarding destination in his or her call destination list, forwarding ends at this destination, and any further call forwarding destinations that may have been entered in call destinations list are ignored.

If call forwarding to additional destinations is to occur, the system flag **Hunting to external call forwarding destination** must be activated by the service technician.

If call forwarding to an external destination is to be followed even for a call over an analog trunk, the system flag **Call forwarding to main station interface permitted** must be activated by the service technician.

Dependencies

Topic	Dependency
Do Not Disturb	You cannot program call forwarding to a telephone where DND is active.
Appointment, automatic wake-up system	If an appointment comes due, it is signaled at the forwarded telephone, irrespective of any active call forwarding settings.
UCD group as call forwarding destination	A call is not forwarded to a UCD group in the following cases: • If a hunt group is called and a subscriber with call forwarding to a UCD group is next, this call is not forwarded. In this case, the next station in the hunt group is immediately called. • A subscriber is a member of a group call with the property "Group" and has activated call forwarding to a UCD group. • A station is a member of a group call no answer. If the group is called, the call is not forwarded to the UCD group. Exception: The first subscriber entered has activated call forwarding to a UCD group. In this case, the call is forwarded.

10.4.3 Call Forwarding After Timeout

Call Forwarding after Timeout forwards unanswered calls after a specific period of time. Call Forwarding after Timeout is analogous to Call Forwarding No Answer, the only difference being that subscribers can set the call forwarding themselves.

The subscriber can set call forwarding after timeout for his or her own phone and can also enter external destinations and groups.

The call deflection destination is not permanently saved, but deleted after you deactivate the feature.

If a subscriber is busy, the rules of call forwarding - no answer apply, that is, the system proceeds to the next destination.

System-Specific Information

You can set three destinations for each station. In addition, there is also a special ID "User-defined", via which the administrator can release or lock the Call Forwarding after Timeout feature for a station. The feature is released by default.

If a call is not answered after the preset timeout, the system searches for and calls the call deflection destination saved. If the subscriber has not entered an individual call deflection destination, the system proceeds with the next destination in the call destination list.

The administrator must release the call forwarding after a timeout for the individual subscribers via the call destination lists.

10.4.4 External Call Forwarding - No Answer (Not for U.S.)

Every station assigned an MSN (multiple subscriber number at the ISDN point-to-multipoint connection) as a DID number can activate or deactivate call forwarding —no answer for this MSN, provided that the user is authorized to use external call forwarding—no answer.

If you have assigned an MSN to a subscriber group, any member of the group can activate and deactivate external call forwarding-no answer for this MSN.

Users can enter only one forwarding destination per MSN. A total of 10 multiple subscriber numbers can be forwarded.

There are three different versions of the feature:

- Call Forwarding Unconditional (CFU): The network provider forwards all calls to this MSN directly, regardless of the MSN status.
- Call Forwarding Busy (CFB): Calls are forwarded only if the MSN dialed is busy.
- Call Forwarding No Reply (CFNR): Calls are forwarded only if the destination does not answer the incoming call within a preset period of time.

Dependencies

Topic	Dependency
Night service	External call forwarding—no answer has a higher priority than night service.

10.4.5 Ringing Assignment / Call Allocation

The ringing assignment enables incoming calls of an analog or S_0 trunk to be forwarded to a station or group, depending on the dialed number and the activation state of the night service.

Different destinations are possible for the day and night service. An incoming call is not signaled at the called station, but according to the call destination lists for that station.

10.4.6 Ringing group on

The feature "Ringing group on" allows internal subscribers to manage a personal list of internal call numbers which are called whenever their own number is called.

Users can also enter their own station numbers. They might do this, for example, if a station number is permanently routed to another station (executive/secretary).

A button can be programmed on the IP system telephones, OpenStage TDM telephones and optiPoint 500 telephones to activate/deactivate this feature. More than one Ringing Group button can be programmed on one telephone to allow for different variations. More than one button can be activated at one time; however, the maximum number of telephones with call signaling cannot exceed five.

This feature can be activated/deactivated via a DISA connection by its own station user or for another user with the aid of the feature Associated Services.

The Forwarding screen is one of three screens in the System Status pathway in Manager E that provides station-specific (rather than system-specific) status information. You can use the Call Forwarding screen to see if a phone has a Ring Group activated or if it is part of a Ring Group.

If the feature is used frequently, the subscribed can assign the feature to a free button on the telephone. The name of the key is "Ringing group on" under Key Programming. When the feature is enabled, the LED is lit.

The station flag “no group ringing on busy” determines which stations in a call ringing group receive a call when the master telephone (the one activating the feature) is busy, and which ones do not. If the same station is in the ringing group of more than one master telephone, the flag applies to all calls signaled at this station.

If the flag is not set, group ringing always takes place, provided the station in the call ringing group is available (default behavior).

If the flag is set, group ringing depends on the availability of the master telephone:

- If the master telephone is available, group ringing takes place immediately
  If the primary telephone has activated call waiting, group ringing takes place after a 5-second delay.
  If the primary telephone cannot receive a call, or if call waiting is inactive, call ringing does not take place.

Topic	Dependency/Restriction
Automatic recall System search Callback	Group ringing is not carried out with an immediate recall (operator error), system search or callback.
Call forwarding	If the station that activated group ringing has also activated call forwarding, group ringing does not occur.
Do Not Disturb (DND)	If a station in the call ringing group has activated DND, group ringing is not carried out at that station.
Timed reminder	An active timed reminder does not follow group ringing.
No group ringing on busy	If the flag is set, no group ringing will take place if the station is busy.

10.4.7 Rejecting Calls

The subscriber can reject internal and external incoming initial calls. These calls can be rejected by pressing the Disconnect key.

The rejected call is then forwarded in accordance with the CFNA instruction. If there is no other call forwarding destination, an external call is intercepted by the attendant console, provided the relevant intercept criteria were configured. If no destination can be called, the caller continues to receive a busy signal.

Transferred recalls, queued callbacks, held or parked calls cannot be rejected. An intercepted call sent to the Intercept position cannot be rejected.

Dependencies

Topic	Dependency
Group call, hunt group call, MULAP	In these cases, the entire group call is terminated and the call follows the call forwarding instruction configured. The call is terminated if there is no other call destination.

10.4.8 Deferring a Call

Subscribers are provided the option of deferring an incoming call. The subscriber called can set up a connection without picking up the incoming call.

The waiting call is then signaled as a camped-on call.

If an incoming call is signaled, the subscriber can press a call or trunk key to conduct the external call. Two call keys and one trunk key must be programmed for this. One of the relevant keys must be free to execute the feature.

The calling party does not notice a change in signaling if call waiting is set for ringing on call waiting.

10.4.9 Do Not Disturb

Do Not Disturb prevents incoming calls from being put through.

A subscriber who has activated DND hears a special dial tone when he or she lifts the handset. When active, the Do Not Disturb feature is also indicated on display phones. In all other phones, the LED on the DSS key flashes with a brief interruption on stations where Do Not Disturb is active.

The Do Not Disturb feature, if set, can be overridden by the Attendant or an authorized subscriber. The call can also be immediately put through for a subscriber with an active Do Not Disturb feature.

A caller who dials a telephone with DND activated receives a busy signal and is not allowed to camp on.

Dependencies

Topic	Dependency
Attendant/night destination	The attendant and the current intercept position cannot activate the Do Not Disturb feature.
Call forwarding	You cannot specify DND if call forwarding is active on the same telephone. You cannot activate call forwarding to a telephone with DND.
Callback	If a callback is initiated to a station with DND activated, the callback is not executed until DND is deactivated. If the subscriber with DND activated initiates a callback, this will override the DND function.
Appointment, automatic wake-up system	If a station has set an appointment and activated DND, an audible signal is sent to the telephone when the appointment comes due.
DISA	DISA can be activated by the subscriber for his or her own phone or by a user for another phone (associated services).

10.5 Optimizing Communication

The communication system offers various options to conveniently and effectively handle calls, e.g., through callbacks or call waiting.

10.5.1 Callback

A callback can then be activated if the subscriber called does not answer or is busy. An active callback triggers a call as soon as the called subscriber is available.

Automatic Callback When Free or Busy

If a call cannot be set up because the subscriber called is busy or does not accept the call, the calling subscriber can activate a callback to set up the call at a later time. If the subscriber called was busy, the Callback function monitors the call to see when it ends. The calling subscriber receives a signal in the form of a call from the communication system when the other subscriber's line is free. If he or she accepts this call, the subscriber who was previously busy is redialed. If a call set up via the Callback function is not successful, this function remains active. The callback attempt is repeated once the required subscriber has conducted another call.

A telephone can initiate up to two Callback requests and be the destination for up to two requests. Any further outgoing requests are rejected.

Callback requests are deleted when

- the call is completed; if not, the callback remains in effect (for an internal callback),
- the callback was established without a call being completed (for an external callback),
- the initiator cancels the request,
- the system deletes all callbacks daily at 23:57.

Callback requests can be made for internal subscribers and groups. Callback requests for a group call are stored at the first subscriber. When a callback is made to a group, the ring is heard at all phones that are free.

Automatic Call Completion on No Reply (CCNR) on the Trunk Interface

An internal subscriber who cannot reach an available external subscriber can activate a callback request at the central office. The system then monitors the connection of the called subscriber. As soon as the called subscriber initiates a connection setup and then ends this connection, the central office attempts to establish a connection between the two subscribers. This feature must be supported by the central office.

Callback on busy

This feature sets enables a manual callback to be set on an external station that is busy. When the station becomes free, the trunk attempts to set up a connection between the two stations. The feature must be supported and enabled by the central office and peer.

10.5.2 Call Waiting

Call waiting signals the arrival of a further incoming call to a subscriber who is on the phone.

The incoming call is visually signaled by a message on the display. It can also be signaled acoustically by a short call waiting tone. The call waiting tone can be heard every 5 seconds.

The subscriber called can accept this second call or ignore it. To answer the second caller, the subscriber can optionally end the first call and answer the second or select the **Call waiting** function offered in the display. In the latter case, the first call is placed on hold.

You cannot camp on to a subscriber if someone is already camped on (a maximum of 4 subscribers can camp on) or if the subscriber has activated call waiting rejection. The caller receives a busy signal if call forwarding—busy is not configured.

Enabling Call Waiting

If the **Call waiting rejection** flag is set, the subscriber can use a menu or code to either enable or suppress call waiting. If a subscriber has enabled call waiting, an incoming call is camped on if call forwarding—busy is configured.

Call Waiting (Camp On) by Attendant Console

The default setting is always "call waiting after timeout". However, the Attendant Console can also camp on immediately.

Dependencies

Topic	Dependency
Call waiting tone	The subscriber can activate/deactivate the call waiting tone with a code. Call waiting is still visually signaled on the phone's display. The call waiting tone is active by default.
Override	If call waiting rejection is active, an ongoing call by this subscriber cannot be overridden.
Group Call	If one or more stations in a group call are free, the call will be offered to them. If all stations are busy, all of them receive a call waiting signal, apart from any stations where call waiting rejection is active.
Speaker call	Speaker calls to busy stations are not possible.

10.5.3 Override (Intrusion)

The Override feature enables an authorized subscriber to override (i.e., intrude into) a call of another internal subscriber.

The override (intrusion) occurs by means of a code or key, and the subscriber involved is notified by a warning tone (beep) and a visual signal on the display.

The feature can be invoked during the busy signal or during the camp on state.

During an override condition, the following applies:

- If the called party hangs up, he or she receives a call from the switching party.
- If the overriding party (who wants to switch the call and overrides) hangs up, the call is switched through to the destination station.
- If the party which was connected to the called party hangs up, the overridden and called parties remain connected.

An override can be performed by any internal subscriber and the intercept position (attendant console). However, in order to use this feature, the internal subscriber and even the intercept position must be authorized for this.

It is not possible to prevent an override to a particular telephone.

Dependencies

Topic	Dependency
Voice Channel Signaling Security	You cannot override a call if the called station or the internal party it is connected to is entered as a data station (voice channel signaling security), or if the called party is dialing a number.
Do Not Disturb	If the called station has activated Do Not Disturb, only one call can be overridden when the subscriber is conducting a call.
Hunt group	Busy override is not possible if all stations are busy when a group or hunt group is called.
S_0 station	It is not possible to override an S_0 station.

10.5.4 Advisory Messages

The advisory message of a subscriber appears in the caller's display.

Variable parameters can also be assigned in advisory messages (also referred to as absence texts). These parameters (for example, time) are entered in the course of activation. Users can use the numeric keypad on the telephone to enter additional characters. The advisory message can be activated/deactivated at a phone via a code or a preconfigured function key.

Call forwarding

When call forwarding is enabled, the called subscriber's advisory message is displayed and the call is forwarded.

10.5.5 Message Texts

Message texts are internal system texts that can be selected by a subscriber and sent to internal subscribers.

A message text (also called an Info text) can be sent to one or more recipients.

If you want to send the text to all members of an internal group or an internal hunt group, you must specify the phone number of the group or the hunt group - not an individual subscriber - as the recipient.

> ***INFO:*** Only 100 phones can receive mass Message Waiting Indication (MWI) messages, any additional message will fail.

The message is sent by pressing the relevant button or via the Send Message menu.

The message can be sent in idle, ringing, talk or busy state. In ringing state it is not necessary to specify the recipient's station number.

10.5.6 Associated Services

An authorized station can control certain features on behalf of any other station, e.g., call forwarding, turning the lock code or hunt group on/off, etc. The effect is the same as if the feature involved were activated or deactivated by the other station itself.

The following features can be controlled on behalf of other stations:

- Call forwarding on / off
- COS changeover on / off
- Ringing group on / off
- Advisory message on / off
- Hunt Group and Group Call on / off
- Night service on / off
- Timed reminder on / off
- Send message / Delete sent message
- Edit lock code password
- UCD agent log in / log out
- UCD agent Available/Not available
- UCD agent Wrapup on / off
- UCD agent Night service on / off
- Forward Line Key (MULAP) on / off
- Resetting Activated Features

This is operated via a procedure. The station must specify the following:

- the code for Associated Services

- the station number of the subscriber for whom the action is to be performed.
- the code of the feature to be controlled

Before any subscriber can use the Associated Services, he or she must first disable the lock code of the other subscriber (if enabled).

10.5.7 DISA

DISA (Direct Inward System Access) allows authorized subscribers to use features of the communication system from outside, e.g., at the mobile phone using myPortal for Mobile (for mobile callback) and Mobility.

Using DISA, a subscriber can also set up outgoing connections, both internal and external. Whenever a subscriber uses DISA, he or she must enter the password for the lock code. Certain features are then available as for internal use.

DISA supports the following features:

Feature	by the subscriber him/ herself	via associated services
Call forwarding on / off	x	x
Do not disturb on / off	x	x
Hunt group on / off	x	x
Advisory message on/off	x	x
Ringing group on / off	x	x
COS changeover on / off	x	x
Reset services	x	x
System Speed Dialing	x	–
Send message text	x	–
Night service on / off	x	–

The administrator specifies under which call number the stations can access DISA. The call number may be different for external and internal use. Internal means at some other "IP-networked" node.

The password to be entered by subscribers consists of the internal call number and the PIN for the lock code. After entering the password, subscribers must either press the # key or wait until the communication system has recognized their input, depending on the security mode that was set for DISA by the administrator.

The subscriber must log in again for further action via DISA.

10.5.8 Flex Call/Mobile PIN

Flex Call (Mobile PIN) enables a system telephone to be temporarily used by other subscribers for the next outbound call as if that phone were their own phones.

Flex Call includes this subscriber's phone number, name, toll restriction, and call detail recording.

The phone being used cannot be reached at its own station number if Flex call is enabled. This status is reverted at the end of the call.

To enable Flex Call, an individual code lock must have been assigned for the mobile subscriber.

One of the following steps must be performed at the system phone to activate the feature:

- OpenStage: Service Menu > PIN and Class of Service > Flex Call + Mobile phone number + Lock code of mobile subscriber
- Code for Flex Call + Mobile phone number + Lock code of mobile subscriber

10.5.9 Relocate

The Relocate (Hoteling) feature allows an OpenStage TDM station to use a procedure to change the assignment between the physical telephone port and the logical station data (user profile).

The Relocate feature can be used if two users decide to swap their workplaces and both users share the same phone types. Relocate thus enables the implementation of DeskSharing for TDM users. The TDM users can perform the Relocate operation without the assistance of an administrator.

Only user profiles of the same phone type, i.e., with an identical key layout, may be exchanged. If you exchange user profiles from different phone types, individually programmed key functions on the basic device will be replaced by the default values. Executing the Relocate feature causes the TDM telephones involved to go out of service and restart. Enabled features are treated accordingly, i.e., current callbacks and sent infos are deleted, and all other features are preserved.

The use of Relocate requires a system-wide release of the feature. To enable the feature, select Relocate in the service menu of the phone to be exchanged and enter the internal number of the target station and the lock code PIN (the lock code PIN is not required if the default PIN 00000 is being used). After you have entered the destination call number, the Relocate feature is blocked for all other users until the procedure has completed. When executing the exchange, both telephones involved are reset. The successful exchange is indicated on both TDM phones by the display of the new number (display: New Call No.: XXXXX).

Relocate cannot be performed on system telephones with programming authorization (for Assistant T). In other words, Relocate is usually not possible on the first two active system telephones.

10.5.10 Reset activated features

You can reset specific features collectively at your terminal using a code.

This is possible for the following features:

- Call forwarding
- Delete received infos
- Advisory message on / off
- Ringing group on / off
- Hunt group on / off
- Station number suppression on / off
- Silent camp-on on / off
- Do not disturb on / off
- Ringer cutoff on / off
- Appointment
- Cancel all callbacks

10.5.11 Procedures

The communication system lets the subscriber program a key with codes, phone numbers, and other dialing information. If a subscriber presses the Procedure key as a suffix or during a call, the communication system transmits the corresponding DTMF character (DTMF = dual tone multifrequency).

Sample applications:

- Code for callback
- Code for call waiting
- Code for override
- Digit string for voicemail or answering machine
- Trunk flash code + destination station number
- Code for controlling a service + destination phone number, for example, code for send/retrieve message (message waiting) + phone number + text number
- ACCT (account code) + trunk code + destination station number

Procedures that require PIN input cannot be saved.

Only the first key level supports Procedure keys.

Depending on the situation, a subscriber can use the following features in procedures:

Feature	Ready to dial	Busy	On the phone	Outgoing call	Incoming call
Directed call pickup	x	–	x	–	–
Call Forward on, (not for tenant systems; not for individual MSNs in an S_0 trunk connection)	x	–	x	x	–
External call forwarding on / off; toggle function; (not for tenant services);	x	–	x	x	–

Feature	Ready to dial	Busy	On the phone	Outgoing call	Incoming call
Call forwarding, login/UCD (uniform call distribution), logout; toggle function	x	–	x	x	–
Call forwarding, night destination on / off; toggle function	x	–	x	x	–
Call forwarding per team configuration	x	x	x	x	x
Advisory message on / off; toggle function	x	–	x	x	–
Associated Dialing	x	x	x	x	x
Associated Services	x	–	x	x	–
Speaker call	x	–	x	–	–
Release trunk (emergency trunk access)	x	–	x	x	–
Send message (message waiting)	x	–	x	x	–
Dial station speed dialing	x	–	x	x	–
Dial system speed dialing	x	–	x	x	–
DTMF transmission	–	–	x	–	–
DTMF transmission in the talk state using procedure key	x	x	x	x	x
Night service on / off; toggle function	x	–	x	x	–
Retrieve call; toggle function	–	x	x	x	–
Account code ACCT	x	–	x	–	–
Account code ACCT in prefix	x	–	x	–	–
Callback requests - display or delete; toggle function	x	–	–	–	–
Ringing group on / off; toggle function	x	–	x	x	–
Language selection	x	x	x	x	x
Telephone Data Service TDS	x	–	x	x	–
Door opener via adapter cabinet	x	x	x	x	x
Timed reminder; toggle function	x	x	x	x	x
Retrieval of an external call from common hold	x	x	x	x	x
System Telephone Lock	x	–	x	–	–

System-Specific Information

A procedure key can store up to 32 characters.

10.5.12 Automatic Wake-up System and Timed Reminders

All users can program timed reminders (appointments). They will be reminded of the appointment at the set time. The appointment can be programmed for a single reminder (once within a 24-hour period) or for regularly scheduled daily reminders.

The time format is four-digits. The first two digits are the hour, and the second two digits are the minutes. A 12-hour clock mode is supported for the U.S.: users enter the four digits and then select "am" (key 2) or "pm" (key 7). If nothing is specified, "am" will be used as the default setting.

Analog telephones, optiPoint 500 and CMI telephones support only programming of non-repeating appointments.

The default timed reminder sounds for 20 seconds and will repeat a maximum of five repeats at one-minute intervals. The timed reminder is cleared automatically as soon as the user lifts the handset or presses the speaker button, or after the fifth repeat (number of repeats is configurable). Alternatively, a programmed timed reminder can be canceled using a procedure. Display telephones also support queries.

A timed reminder which is due but cannot be signaled (user busy, for example), is postponed until the next cycle.

11 Working in a Team (Groups)

Several features are provided by the communication system to enable and facilitate working in a team. Besides call pickup groups, group calls and hunt groups, this also includes groups with team and executive/secretary functions as well as voicemail box and fax box groups. The "UCD (Uniform Call Distribution)" feature enables incoming calls to be uniformly distributed to a group of users (UCD group).

INFO: When configuring groups, it must be noted that the first three groups are reserved:

The first group is used by default as the hunt group for Xpressions Compact.

The second group is used by default as the hunt group for OpenScape Business Smart VoiceMail.

The third group is used by default as the hunt group for the Company AutoAttendant of OpenScape Business Smart VoiceMail.

11.1 Call Pickup Group, Group Call and Hunt Group

The communication system offers several methods of combining stations into groups so that multiple subscribers and phones can be reached under one call number, for example, or a call to one station can also be signaled at other stations.

In the case of a call pickup group, a call for one member of the group is also signaled at all other group members.

With a group call, by contrast, all members can be reached via a single phone number (group phone number). The first station to answer the call is connected to the calling party.

In the case of a hunt group, an incoming call is signaled at one of the group members. If this member does not answer the call, the call is assigned to the next member. All members of the hunt group can be reached at the same phone number.

11.1.1 Call Pickup Group

A call for a member of a call pickup group is also signaled at all other group members. The call can be accepted by all group members via a function key programmed for this purpose, via the associated phone menu item or by dialing the code.

The call is signaled acoustically and visually on the display of the call pickup group member originally called. If programmed, the call is also signaled via the function key LED.

The other group members are only notified of the call by a visual signal. The phone number or name of the subscriber originally called and the phone number or name of the caller are shown on the phone's display. The display of the station number or name of the caller can be disabled by an administrator with the **Expert** profile in **Expert mode**. If programmed, the call is also signaled via the function key LED.

If the call is not accepted within four ring cycles (4 x 5 seconds), the other group members receive a warning tone (acoustic signaling). The time from the start of call signaling till the warning tone is not variable. The warning tone can be disabled for all group members by an administrator with the **Expert** profile in **Expert mode**.

If more than one call is received for a call pickup group, signaling occurs in the sequence in which the calls are received.

If recalls for members of a call pickup group are also to be picked up by other members in the group, this must be enabled by an administrator with **Expert** profile in **Expert mode**.

A station can belong to only one call pickup group.

Any call charges incurred for a picked-up call are accrued to the subscriber who picked up the call.

INFO: Double quotations (") are not supported for naming a Call Pickup Group.

SIP Phones

SIP telephones can be integrated in a call pickup group.

INFO: In addition, a function key for the call pickup group can be programmed for SIP phones, and the specific messages of a call pickup group can be shown on the displays of the corresponding SIP phones. In order to use this feature, the "Call Pickup Group" feature must be enabled on the SIP phone (see the User Guide of the SIP phone for details).

Call Pickup Outside a Call Pickup Group

Another version of the feature is the "call pickup outside a call pickup group". This permits the pickup of calls for internal subscribers that do not belong to the same call pickup group. The call can be picked up via a function key programmed for this purpose, the associated menu item or by dialing the specific call pickup code followed by the station number of the called station.

Dependencies

Topic	Dependency
Callback	Recalls and callbacks are signaled at the other group members only if the system flag **Call Pickup after automatic recall** has been activated.
Do Not Disturb	Stations that have activated DND do not receive call pickup signaling.
ISDN Phones	It is not possible to include ISDN telephones in call pickup groups.
MULAP	It is not possible to include MULAP phone numbers in call pickup groups.

11.1.2 Group Call

A group call can be defined in cases where multiple subscribers need to be reached via a single phone number (group phone number). Incoming external and internal calls are signaled at the same time at all group member phones. The first station to answer the call is connected to the calling party.

Every member of a group call can also be reached at his or her own station number.

The group must be assigned one of the following properties:

- Group
  Incoming calls are simultaneously signaled at all available group members. Available group members are subscribers who are not busy. If all group members are busy, a call is signaled by a camp-on tone. Call signaling continues at all group members (camp-on tone at busy group members) even if the subscriber hangs up.
  A caller hears the busy tone if all group members are busy and all have activated the DND feature. If a call forwarding destination has been defined for this group, the caller does not hear a busy tone, but is forwarded directly to the next call forwarding destination.
- RNA
  Incoming calls are simultaneously signaled at all group members. If a group member is busy, the entire group call is marked as busy. Other callers receive the busy tone.
- Call waiting
  Incoming calls are simultaneously signaled at all available group members. Available group members are subscribers who are not busy. A call is signaled by a camp-on tone for busy group members.
  This requires that all group members have the Do Not Disturb feature disabled.

Group calls are treated like stations by the Call forwarding—no answer function. In other words, if a call cannot be accepted by any of the members in a group call, it is redirected to a call forwarding destination in accordance with the call desti-

nation list. You can specify whether call forwarding should be performed on RNA (ring no answer) or busy.

When a call is not answered by any member of a group call, it appears as a missed call in the journal of the UC clients of all members. An accepted call appears only in the journal of the member who answered the call.

A single station can belong to several groups simultaneously. The following applies to groups of the type Group Call, Hunt Group, Team Configuration / Team Group and Executive/Secretary / Top Group: The sum of all the subscriber's memberships in these groups must not exceed 32.

The group name assigned is shown on the internal caller's display. After a call is accepted, the name of the subscriber who accepted the call is displayed.

If a member has defined rules using the AutoAttendant, e.g., to forward calls, these rules will apply only to calls to his or her own station number. The rules are ignored for group calls.

Up to 20 subscribers can be configured per group call.

Every group call can be assigned a name containing up to 16 characters.

Voicemail Box for Group Call

When setting up a group call, a voicemail box is created automatically. The call number of this voicemail box for the group call always matches that of the group call. If a group call is not accepted by any member, the call is forwarded to the voicemail box for the group call. This requires the group call voicemail box to have been defined as the CFNA (call forwarding on no answer) destination of this group call.

If a member does not accept an incoming call to his or her own station number, this call is redirected to a call forwarding destination in accordance with the call destination list.

<table>
<tr><td colspan="3">Example of a group call of type RNA (ring no answer) with the group call number 404 and the members A (call number 200), B (201) and C (202). Call Forwarding-No Answer after Timeout to the voicemail box of the group call was set up for the group call. Every member has defined Call Forwarding-No Answer (CFNA) after Timeout to his or her own voicemail box.</td></tr>
<tr><td rowspan="2">Inbound call for Member A (200)</td><td>All members are free.</td><td>Member A does not accept the call. Call Forwarding-No Answer after Timeout occurs to the voicemail box of member A.</td></tr>
<tr><td>Member A has defined Call Forwarding Unconditional (CFU) to his or her own voicemail box. Members B and C are free.</td><td>The call is forwarded immediately (CFU) to the voicemail box of member A.</td></tr>
</table>

Inbound call for the group call (404)	All members are free.	The call is signaled at all other members. No member accepts the call. Call Forwarding-No Answer after Timeout occurs to the voicemail box of the group call.
	Member A has defined Call Forwarding Unconditional (CFU) to his or her own voicemail box. Members B and C are free.	The call is signaled at members B and C. No member accepts the call. Call Forwarding-No Answer after Timeout occurs to the voicemail box of the group call.
	Member A has defined Call Forwarding Unconditional (CFU) to an external destination. Members B and C are free.	The call is signaled at members B and C and at the external destination. No member accepts the call. Call Forwarding-No Answer after Timeout occurs to the voicemail box of the group call.
	Member A has defined CFNA rules using the AutoAttendant. Members B and C are free.	The call is signaled at all other members. No member accepts the call. Call Forwarding-No Answer after Timeout occurs to the voicemail box of the group call.

Activating/Deactivating a Group Call

If a subscriber is a member of a group call, he or she can use codes to leave and rejoin the group call.

If a subscriber is a member of both multiple group calls and multiple hunt groups, he or she can use codes to leave and rejoin all group calls and hunt groups. Subscribers are added to or removed from a specific group call or hunt group by entering codes and then making a selection from the group calls and hunt groups displayed.

You can also program function keys with a shift function for joining and leaving. You can program a function key here that applies for a specific group call and hunt group or all group calls and hunt groups. Variable programming is also possible. After you press a function key of this kind, you must select one of the group calls and hunt groups displayed to define the group call or hunt group you want to leave/join.

Ring type

For every group call, an administrator with the **Expert** profile can define the acoustic signaling of incoming external calls via the ring type setting. You have the following options:

- Two rings (default setting)
- Three rings
- short-long-short ring

Only the default setting is possible for analog phones. Changes have no effect.

SIP Phones

SIP telephones can be integrated in a group call.

INFO: No programming of function keys is possible for SIP phones. Furthermore, no features can be activated or deactivated via codes. Specific display messages of a group call are not supported.

Dependencies

Topic	Dependency
Call forwarding	If a group member activates call forwarding for all calls, all calls are signaled at the destination telephone.
Do Not Disturb	If a group member activates the Do Not Disturb feature, incoming calls for his or her phone are not put through. This applies to calls via the group phone number and the member's own station number.
Override	Override is not possible if all members of a group call are busy.
ISDN Phones	It is not possible to include ISDN telephones in a group call.

11.1.3 Hunt Group

Hunt groups permit the distribution of incoming calls to associated subscribers (members). If a subscriber is busy or does not accept an incoming call, the call is automatically forwarded to the next free member of the hunt group. All members of the hunt group can be reached at the same phone number.

Every member of a hunt group can also be reached at his or her own station number.

The hunt group must be assigned one of the following properties.

- Linear
  An inbound call is always signaled first at the first member of a hunt group. Further signaling is performed on the basis of the sequence in which the members are entered in the group table.
- Cyclic
  An inbound call is always signaled first at the member that follows the subscriber who answered the last call. Further signaling is performed on the basis of the sequence in which the members are entered in the group table.

The call is automatically forwarded to the next free hunt group member when the forwarding time expires, provided the call is not answered or a member is busy or DND is activated.

You can program a call forwarding destination (call destination list) if a call cannot be answered by any of the members of the hunt group.

A single station can belong to several groups simultaneously. The following applies to groups of the type Group Call, Hunt Group, Team Configuration / Team Group and Executive/Secretary / Top Group: The sum of all the subscriber's memberships in these groups must not exceed 32.

The name assigned to the hunt group is shown on the internal caller's display. After a call is accepted, the name of the subscriber who accepted the call is displayed.

If a member has defined rules using the AutoAttendant, e.g., to forward calls, these rules will apply only to calls to his or her own station number. The rules are ignored for hunt group calls.

Up to 20 subscribers can be configured per hunt group.

Every hunt group can be assigned a name containing up to 16 characters.

Voicemail Box for Hunt Group

When setting up a hunt group, a voicemail box is automatically created for it. The call number of this voicemail box for the hunt group always matches that of the hunt group. If a call for a hunt group is not accepted by any member, the call is forwarded to the voicemail box for the hunt group. This requires the hunt group voicemail box to have been defined as the CFNA (call forwarding on no answer) destination of this hunt group.

If a member does not accept an incoming call to his or her own station number, this call is redirected to a call forwarding destination in accordance with the call destination list.

Example of a linear hunt group with the call number 404 and the members A (call number 200), B (201) and C (202). Call Forwarding-No Answer after Timeout to the voicemail box of the hunt group was set up for the hunt group. Every member has defined Call Forwarding-No Answer (CFNA) after Timeout to his or her own voicemail box.		
Inbound call for Member A (200)	All members are free.	Member A does not accept the call. Call Forwarding-No Answer after Timeout occurs to the voicemail box of member A.
	Member A has defined Call Forwarding Unconditional (CFU) to his or her own voicemail box. Members B and C are free.	The call is forwarded immediately (CFU) to the voicemail box of member A.

Inbound call for the hunt group (404)	All members are free.	The call is signaled first at member A, then at member B and then at member C. No member accepts the call. Call Forwarding-No Answer after Timeout occurs to the voicemail box of the hunt group.
	Member A has defined Call Forwarding Unconditional (CFU) to his or her own voicemail box. Members B and C are free.	The call is signaled first at member B and then at member C. No member accepts the call. Call Forwarding-No Answer after Timeout occurs to the voicemail box of the hunt group.
	Member A has defined Call Forwarding Unconditional (CFU) to an external destination. Members B and C are free.	The call is signaled first at member B and then at member C. No member accepts the call. Call Forwarding-No Answer after Timeout occurs to the voicemail box of the hunt group.
	Member A has defined CFNA rules using the AutoAttendant. Members B and C are free.	The call is signaled first at member A, then at member B and then at member C. No member accepts the call. Call Forwarding-No Answer after Timeout occurs to the voicemail box of the hunt group.

Activating/Deactivating the Hunt Group

If a subscriber is a member of a hunt group, he or she can use codes to leave and rejoin the hunt group.

If a subscriber is a member of both multiple hunt groups and multiple group calls, he or she can use codes to leave and rejoin all hunt groups and group calls. Subscribers are added to or removed from a specific hunt group or group call by entering codes and then making a selection from the hunt groups and group calls displayed.

You can also program function keys with a shift function for joining and leaving. You can program a function key here that applies for a specific or all hunt groups and group calls. Variable programming is also possible. After you press a function key of this kind, you must select one of the hunt groups and group calls displayed to define the hunt group or group call you want to leave/join.

Ring type

For every hunt group, an administrator with the **Expert** profile can define the acoustic signaling of incoming external calls via the ring type setting. You have the following options:

- Two rings (default setting)
- Three rings
- short-long-short ring

Only the default setting is possible for analog phones. Changes have no effect.

SIP Phones

SIP telephones can be integrated in a hunt group.

INFO: No programming of function keys is possible for SIP phones. Furthermore, no features can be activated or deactivated via codes. Specific display messages of a hunt group are not supported.

Dependencies

Topic	Dependency
Call forwarding	If a hunt group member activates call forwarding for all calls, all calls are signaled at the destination telephone.
Do Not Disturb	If a hunt group member activates the Do Not Disturb feature, incoming calls for his or her phone are not put through. This applies to calls for the hunt group and the member's own station number.
Queue	For cyclical and linear hunt groups, it is not possible to set up a call queue.
ISDN Phones	It is not possible to include ISDN telephones in hunt groups.

11.1.4 Configuring Call Pickup Groups, Group Calls and Hunt Groups using Wizards

Several different wizards are available to conveniently configure call pickup groups, group calls and hunt groups.

The **Call Pickup** wizard can be used to combine subscribers into a group to enable mutual call pickups. The following application cases, which can be configured using the wizard, are described here:

- *How to Configure a Call Pickup Group*
- *Add or delete a member to or from a call pickup group*

The **Group Call / Hunt Group** wizard can be used to configure group calls of the type Group. The following application cases, which can be configured using the wizard, are described here:

- *How to Add a Group Call (Group)*
- *How to Edit a Group Call (Group)*
- *Deleting a Group Call (Group)*
- *How to Add or Delete a Member to or from a Group Call (Group)*
- *How to Add a Hunt Group*
- *How to Change a Hunt Group*
- *How to Delete a Hunt Group*
- *How to Add or Delete a Member to or from a Hunt Group*

11.1.5 Configuring Call Pickup Groups, Group Calls and Hunt Groups using Expert Mode

Besides the configuration options available through wizards, administrators with the **Expert** profile are also offered additional options to configure call pickup groups, group calls and hunt groups via the **Expert mode**.

The procedure for the following application cases, which can be configured using the **Expert mode** wizard, is described here:

- *How to Enable or Disable the Display of a Caller's Station Number and Name*
- *How to Activate or Deactivate the Warning Tone*
- *How to Enable or Disable Call Pickup for Recalls*
- *How to Add a Group Call (RNA or Call Waiting)*
- *How to Display or Edit a Group Call (RNA or Call Waiting)*
- *How to Delete a Group Call (RNA or Call Waiting)*
- *How to Add or Delete a Member to or from a Group Call (RNA or Call Waiting)*
- *How to Enable or Disable Do Not Disturb for a Group Member*

11.2 Team Configuration / Team Group and Executive/Secretary / Top Group

A Team Configuration / Team Group offers several convenient team functions. The station numbers of all team members are programmed on MULAP keys (trunk keys). Every team member can thus access all trunks (for instance, for call pickup) and can also conduct calls simultaneously via multiple trunks. An Executive/Secretary or Top Group offers convenient Executive and Secretary functions (Top function) for up to three executives and up to three secretaries.

INFO: When creating a MULAP from Team/Top options in WBM / Manager E it is not allowed to enter any number beginning with ** or ***.

11.2.1 Team Configuration / Team Group

MULAP (Multiple Line Appearance) keys (trunk keys) are programmed on a telephone with team functions with the individual telephone's number and the phone numbers of all other team members. Every team member can access all trunks (for instance, for call pickup) and can also conduct calls simultaneously via multiple trunks. In addition, DSS keys with which the team members can directly call one another are programmed automatically.

The MULAP keys give team members access to the phone numbers of all members. An incoming call for a team member can thus also be accepted by all other members by pressing the flashing MULAP key. Team members can also toggle between multiple trunks. By pressing a MULAP key, a team member can

make an outbound call via the associated line. The station number of this line will then appear on the display of the called party.

Incoming calls are visually signaled at the same time on all team member phones via the MULAP key LED. You can also specify for each team member if incoming calls should also be signaled acoustically.

Every team member can use a group call key to activate or deactivate incoming call signaling for each individual trunk.

An administrator with the **Advanced** profile can configure up to 3 stations per Team configuration/Team group by using the **Team Configuration** wizard. An administrator with the **Expert** profile can configure up to ten stations per Team configuration or Team group in **Expert mode**.

An single subscriber may also simultaneously belong to several groups. The following applies to groups of the type Group Call, Hunt Group, Team Configuration / Team Group and Executive/Secretary / Top Group: The sum of all the subscriber's memberships in these groups must not exceed 32.

Every team configuration / team group can be assigned a name containing up to 16 characters.

When setting up a Team configuration or Team group, the following properties are assigned to its members (these settings can be changed by an administrator with the **Expert** profile in **Expert mode**.):

- **Master**
  This parameter changes a member into a master of the Team configuration / Team group. If a master activates call forwarding, this applies to all members (phones) in the Team configuration / Team group.
  Default setting: master is the first member of the Team configuration / Team group.
- **Acoustic ring**
  If this parameter is activated, incoming calls are signaled acoustically.
  Default setting: the parameter is activated.
- **Automatic seizure outgoing**
  If this parameter is active, a call is automatically made via the MULAP trunk of this member on lifting the handset. If the parameter is not active, the subscriber must press the MULAP key before dialing is possible.
  Default setting: the parameter is activated.
- **No automatic incoming call acceptance**
  If this parameter is activated, you cannot answer an incoming call by lifting the handset. An incoming call must be accepted by pressing the MULAP key.
  Default setting: the parameter is not activated.
- **Automatic conference release**
  If the parameter is active, you can release the seized MULAP line for a conference by pressing the MULAP key. The release of this line is signaled to all other members by the flashing MULAP key. They can join the conference by pressing the MULAP key.
  Default setting: the parameter is not activated.

- **MULAP key set up**
  If the parameter is active, a MULAP key is programmed on the associated phone. Pressing the key sets up an outgoing call via the MULAP trunk of the master. The MULAP station number of the master appears on the called party's display.
  Default setting: the parameter is not activated.

Using MULAP Keys

Every team member is assigned a separate trunk (MULAP trunk). The member's own trunk and the trunks of all other members are programmed as MULAP keys (trunk keys) for every team member. This means that every team can use all available MULAP trunks.

The LED on a MULAP key (trunk key) can have different statuses with the following meaning:

- Off: the relevant trunk is free and can be used.
- Lit: the relevant trunk is busy.
- Flashing fast: call on the relevant trunk.
- Flashing slow: an on-hold call is waiting on the relevant trunk.

Using DSS Keys

Every team member has a DSS key for every other team member. This means that team members can reach each other directly at the push of a button.

A Direct Station Select (DSS) key can also be used to quickly transfer an existing call to the team member programmed on it.

The LED on a DSS key can have different statuses with the following meanings:

- Off: the associated Team member is not conducting a call.
- Lit: the associated Team member is conducting a call or has activated Do Not Disturb.
- Flashing fast: the associated Team member is conducting a call. The call can be accepted by pressing the Direct Station Select (DSS) key.
- Flashing slowly: the associated Team member is being called and has not yet answered. The call can be accepted by pressing the Direct Station Select (DSS) key.

Ring type

For every Team configuration / Team group, an administrator with the **Expert** profile can define the acoustic signaling of incoming external calls via the ring type setting. You have the following options:

- Two rings (default setting)
- Three rings
- short-long-short ring

Only the default setting is possible for analog phones. Changes have no effect.

Fax Box for Team Configuration / Team Group

For each Team configuration or Team group, a fax box can be set up via which the members can receive Fax messages directly through myPortal for Desktop or myPortal for Outlook.

If a fax box was already configured for the master (the first member) of the Team configuration/Team group, this fax box is taken over when setting up the Team configuration/Team group. Previously configured fax boxes of other members are deleted.

After a Team configuration or Team group is dissolved, only the prior master (i.e., the first member) can use his or her fax box.

SIP Phones

SIP telephones can be integrated in a Team configuration / Team group. As a prerequisite, a system telephone (IP, HFA or SIP phone, for example) must have been defined as the first member of the Team configuration / Team group.

Dual-mode mobile phones that are configured as Mobility Entry stations, for example, can be integrated. Dual-mode mobile phones support both GSM/UMTS networks and WLAN networks. A dual-mode mobile phone can be registered as an IP station (SIP client) at the communication system over a WLAN.

INFO: No programming of MULAP keys and DSS keys is possible for SIP phones. Furthermore, no features can be activated or deactivated via codes. Specific display messages of the Team configuration / Team group are not supported.

Dependencies

Topic	Dependency
Call forwarding	One team member has activated call forwarding for all calls. In this case, all calls for his or her own station number will be forwarded.
Do Not Disturb	If a Team member activates the Do Not Disturb feature, incoming calls are not put through.
ISDN Phones	It is not possible to include ISDN telephones in Team configurations / Team groups.
Groups/Hunt groups	It is not possible to include a Basic/Executive MULAP master in Team configurations / Team groups.

11.2.2 Executive/Secretary or Top Group

Top groups can be configured if you need user-friendly executive and secretary functions (Top function).

Executive/secretary functions can be configured for groups with up to three executives and up to three secretaries.

> ***INFO:*** The terms "executive" and "secretary" also apply to groups with more than one executive and more than one secretary. The terms "executive" and "secretary" used in this document are gender-neutral.

Every Top member (every executive and every secretary) is assigned a separate trunk, known as a MULAP (Multiple Line Appearance) trunk. The member's own MULAP trunk and the MULAP trunks of all other members are programmed as MULAP keys (trunk keys) for every Top member. The MULAP phone number is shown on the called party's display for outgoing calls via the MULAP trunk. The Secretary station can make calls via its own trunk or the MULAP trunk of all executives and other secretary stations. For example, if a connection is to be set up for an executive, the MULAP trunk of that executive can be used.

DSS keys are also programmed to allow the executive to call the secretary directly, and vice versa.

Incoming calls are visually signaled at the same time on all Top member phones via the LED on the trunk key. You can also specify for each Top member if incoming calls should also be signaled acoustically. Acoustic signaling depends here on the ring transfer key.

You can use a ring transfer key to change the signaling for incoming calls. Incoming calls are signaled either at the executive or secretary phone. If the executive presses the ring transfer key, incoming calls will still be displayed to the executive via a tray pop. Accepting a call can, however, only be done via an appropriate key on the phone and not via the tray pop.

You can use a group call key on Secretary phones to add or remove the station to or from the Executive/Secretary configuration or Top group. In this case, ring transfer has priority.

> ***INFO:*** If the secretary uses the group call key to leave the Executive/Secretary configuration or Top group without activating ring transfer for the executive, incoming calls are not signaled at either the executive or the secretary.

An administrator with the **Advanced** profile can define up to two executives and two secretaries per Executive/Secretary configuration or Top group using the **Executive/Secretary** wizard. An administrator with the **Expert** profile can define up to three executives and three secretaries per Executive/Secretary configuration or Top group in **Expert mode**.

For every executive, a maximum of three phones can be set up; for every secretary, a maximum of two phones.

An single subscriber may also simultaneously belong to several groups. The following applies to groups of the type Group Call, Hunt Group, Team Configuration / Team Group and Executive/Secretary / Top Group: The sum of all the subscriber's memberships in these groups must not exceed 32.

Every Executive/Secretary configuration or Top group can be assigned a name containing up to 16 characters.

When setting up an Executive/Secretary configuration or Top group, the following properties are assigned to its members (these settings can be changed by an administrator with the **Expert** profile in **Expert mode**.):

- **Master**
  This parameter assigns executive functions to a member. The Executive MULAP trunk is automatically selected for a call on lifting the handset. Incoming calls via the associated Executive MULAP phone number are only signaled visually by default.
  Default setting: All executives of the Executive/Secretary configuration or Top group receive Executive functions.
- **Acoustic ring**
  If this parameter is activated, incoming calls are signaled acoustically.
  Default setting: the parameter is active for all members with the secretary function.
- **Automatic seizure outgoing**
  If this parameter is active, a call is automatically made via the MULAP trunk of this member on lifting the handset. If the parameter is not active, the subscriber must press the MULAP key before dialing is possible.
  Default setting: the parameter is activated for all members.
- **No automatic incoming call acceptance**
  If this parameter is activated, you cannot answer an incoming call by lifting the handset. An incoming call must be accepted by pressing the MULAP key.
  Default setting: the parameter is not activated.
- **Automatic conference release**
  If the parameter is active, you can release the seized MULAP line for a conference by pressing the MULAP key. The release of this line is signaled to all other members by the flashing MULAP key. They can join the conference by pressing the MULAP key.
  Default setting: the parameter is not activated.
- **MULAP key set up**
  If the parameter is active, a MULAP key is programmed on the associated phone. You can press the key to set up an outgoing call via the Executive MULAP trunk. The Executive MULAP phone number appears on the called party's display.
  Default setting: the parameter is activated.

Using MULAP Keys

Every Top member is assigned a separate trunk (MULAP trunk). The member's own trunk and the trunks of all other members are programmed as MULAP keys (trunk keys) for every Top member. This means that every Top member can use all available MULAP lines.

The LED on a MULAP key (trunk key) can have different statuses with the following meaning:

- Off: the relevant trunk is free and can be used.
- Lit: the relevant trunk is busy.

- Flashing fast: call on the relevant trunk.
- Flashing slowly: an on-hold call is waiting on the relevant trunk or the relevant trunk was released for a conference.

Using DSS Keys

Every Top member has a DSS key for every other Top member. This means that Top members can reach each other directly at the push of a button.

A Direct Station Select (DSS) key can also be used to quickly transfer an existing call to the Top member programmed on it.

The LED on a DSS key can have different statuses with the following meanings:

- Off: The associated Top member is not conducting a call.
- Lit: the associated Top member is conducting a call or has activated Do Not Disturb.
- Flashing fast: the associated Top member is conducting a call. The call can be accepted by pressing the Direct Station Select (DSS) key.
- Flashing slowly: the associated Top member is being called and has not yet answered. The call can be accepted by pressing the Direct Station Select (DSS) key.

Ring type

For every Executive/Secretary configuration or Top group, an administrator with the **Expert** profile can define the acoustic signaling of incoming external calls via the ring type setting. You have the following options:

- Two rings (default setting)
- Three rings
- short-long-short ring

Only the default setting is possible for analog phones. Changes have no effect.

Fax Boxes for Executive/Secretary Configuration or Top Group

For each member of an Executive/Secretary configuration or Top group, a fax box can be set up via which the members can receive Fax messages directly through myPortal for Desktop or myPortal for Outlook.

If a fax box was already configured for the first executive of the Executive/Secretary configuration or Top group, this fax box is taken over when setting up the Executive/Secretary configuration or Top group. Previously configured fax boxes of other members are deleted.

After an Executive/Secretary configuration or Top group is dissolved, only the prior first executive can use his or her fax box.

SIP Phones

SIP telephones can be integrated in an Executive/Secretary configuration or Top group. As a prerequisite, a system telephone (IP, HFA or SIP phone, for example) must have been defined as the first member of the Executive/Secretary configuration or Top group (Exec. 1).

Dual-mode mobile phones that are configured as Mobility Entry stations, for example, can be integrated. Dual-mode mobile phones support both GSM/UMTS networks and WLAN networks. A dual-mode mobile phone can be registered as an IP station (SIP client) at the communication system over a WLAN.

INFO: No programming of MULAP keys and DSS keys is possible for SIP phones. Furthermore, no features can be activated or deactivated via codes. Specific display messages of the Executive/Secretary configuration / Top group are not supported.

Dependencies

Topic	Dependency
Call forwarding	A Top member has activated call forwarding for all calls. In this case, all calls for his or her own station number will be forwarded.
Do Not Disturb	If a Top member activates the Do Not Disturb feature, incoming calls are not put through.
ISDN Phones	It is not possible to include ISDN or SIP phones in Executive/Secretary configurations or Top groups.
Groups/Hunt groups	It is not possible to include a Basic/Executive MULAP master in Executive/Secretary configurations or Top groups.

11.2.3 Configuring Team Configurations / Team Groups and Executive/ Secretary Functions / Top Groups using Wizards

Several different wizards are available to conveniently configure team configurations (team groups) and executive/secretary functions (top groups).

The **Team Configuration** wizard can be used to set up Team configurations (Team groups). The following application cases, which can be configured using the wizard, are described here:

- *Adding a Team Configuration / Team Group*
- *Editing a Team Configuration / Team Group*
- *Deleting a Team Configuration / Team Group*

The **Executive / Secretary** wizard can be used to configure convenient Executive and Secretary functions (Top function). The following application cases, which can be configured using the wizard, are described here:

- *How to Add an Executive/Secretary or Top Group*
- *How to Edit an Executive/Secretary or Top Group*
- *How to Delete an Executive / Secretary or Top Group*

11.2.4 Configuring Team configurations / Team groups and Executive/ Secretary functions / Top groups using Expert mode

Besides the configuration options available through wizards, administrators with the **Expert** profile are also offered additional options to configure Team configurations / Team groups and Executive/Secretary functions / Top groups via the **Expert mode**.

The procedure for the following application cases, which can be configured using the **Expert mode** wizard, is described here:

- *How to Add or Delete a Member to or from a Team Configuration or Team Group*
- *How to Edit a Member of a Team Configuration / Team Group*
- *How to Edit the Properties of Members in a Team Group*
- *How to Change the Programmed Feature Keys for a Team Configuration / Team Group*
- *How to Add a Fax Box to a Team Configuration / Team Group*
- *How to Add or Delete a Member to or from an Executive/Secretary or Top Group*
- *How to Edit a Member of an Executive/Secretary or Top Group*
- *How to Edit the Properties of an Executive/Secretary or Top Group*
- *How to Add a Fax Box to an Executive/Secretary or Top Group*

11.3 Basic MULAP and Executive MULAP

A Basic MULAP enables a subscriber who uses multiple telephones (e.g., a fixed-network telephone and a mobile phone) to be reached under a single phone number. You can configure Executive MULAPs if you want to use restricted executive and secretary functions.

11.3.1 Basic MULAP

Basic MULAPs can be configured if a subscriber is using a number of different phones (for example, a fixed-network phone and mobile phone) but would like to be reached at a single phone number (Basic MULAP phone number).

If a caller rings the Basic MULAP phone number, the call is visually signaled at all phones belonging to the Basic MULAP. The subscriber can also set whether or not incoming calls should also be acoustically signaled for each individual member. The status of the Basic MULAP changes to busy and other callers hear the busy signal when a call is answered.

The Basic MULAP phone number is shown on the called party's display for outgoing calls via the Basic MULAP trunk.

Up to 20 members can be configured per Basic MULAP.

Every Basic MULAP can be assigned a name containing up to 16 characters.

Each of the subscriber's phones is a member of the Basic MULAP and each member can be assigned the following properties:

- **Master**
  This parameter changes a member into a master of the Basic MULAP. If a master activates call forwarding, this feature applies to all members (phones) in the Basic MULAP. If the master activates an automatic callback on a Basic MULAP, the callback is initiated as soon as all masters are free.
  A subscriber may not be included as a MULAP master in hunt groups more than 25 times.
  Default setting: master is the first member of the Basic MULAP.
- **Acoustic ring**
  If this parameter is activated, incoming calls are signaled acoustically.
  Default setting: the parameter is active for all masters.
- **Automatic seizure outgoing**
  If this parameter is active, the Basic MULAP trunk is automatically called when the subscriber lifts the handset. If the parameter is not active, the subscriber must press the MULAP key before dialing is possible.
  Default setting: automatic outgoing seizure is assigned to all masters.
- **No automatic incoming call acceptance**
  If this parameter is activated, you cannot answer an incoming call by lifting the handset. An incoming call must be accepted by pressing the MULAP key.
  Default setting: the parameter is not activated.
- **Automatic conference release**
  If the parameter is active, you can release the seized MULAP line for a conference by pressing the MULAP key. The release of this line is signaled to all other members by the flashing MULAP key. They can join the conference by pressing the MULAP key.
  Default setting: the parameter is not activated.
- **MULAP key set up**
  If the parameter is active, a MULAP key is programmed on the associated phone. You can press the key to set up an outgoing call via the Basic MULAP trunk. The Basic MULAP number appears on the called party's display.
  Default setting: the parameter is activated.

Using MULAP Keys

The LED on a MULAP key can have different statuses with the following meaning:

- Off: the relevant trunk is free and can be used.
- Lit: the relevant trunk is busy.
- Flashing fast: call on the relevant trunk.
- Flashing slowly: an on-hold call is waiting on the relevant trunk or the relevant trunk was released for a conference.

Ring type

For every Basic MULAP, an administrator with the **Expert** profile can define the acoustic signaling of incoming external calls via the ring type setting. You have the following options:

- Two rings (default setting)
- Three rings
- short-long-short ring

Only the default setting is possible for analog phones. Changes have no effect.

SIP Phones

SIP telephones can be integrated in a Basic MULAP. As a prerequisite, a TDM, HFA or SIP phone must have been defined as the first member of the Basic MULAP.

Dual-mode mobile phones that are configured as Mobility Entry stations, for example, can be integrated. Dual-mode mobile phones support both GSM/UMTS networks and WLAN networks. A dual-mode mobile phone can be registered as an IP station (SIP client) at the communication system over a WLAN.

INFO: No programming of MULAP keys is possible for SIP phones. Furthermore, no features can be activated or deactivated via codes. Specific display messages of the Basic MULAP are not supported.

Dependencies

Topic	Dependency
Do Not Disturb	When Do Not Disturb is activated, incoming calls are no longer put through.
ISDN Phones	It is not possible to include ISDN telephones in Basic MULAPs.

11.3.2 Executive MULAP

You can configure Executive MULAPs if you want to use restricted executive and secretary functions.

All members of an Executive MULAP can be reached at the Executive MULAP phone number as well as at their personal station numbers.

INFO: The terms "executive" and "secretary" used in this document are gender-neutral.

Up to 20 members can be configured per Executive MULAP.

Every Executive MULAP can be assigned a name containing up to 16 characters.

The parameters described below define which members of an Executive MULAP can use executive functions (Executive) and which can use secretary functions (Secretary).

If a caller rings the Executive MULAP phone number, the call is visually signaled at all phones belonging to the Executive MULAP. Incoming calls are also signaled acoustically for members with secretary functions.

The Executive MULAP phone number is shown on the called party's display for outgoing calls via the Executive MULAP trunk.

The members of an Executive MULAP can be assigned the following properties:

- **Master**
  This parameter is used to assign executive functions to a member. The Executive MULAP trunk is automatically selected for a call when you lift the handset. Incoming calls via the Executive MULAP phone number are only signaled visually.
  A subscriber may not be included as a MULAP master in hunt groups more than 25 times.
  Default setting: the first member of the Executive MULAP is assigned executive functions.
- **Acoustic ring**
  If this parameter is activated, incoming calls are signaled acoustically.
  Default setting: the parameter is active for all members with the secretary function.
- **Automatic seizure outgoing**
  If this parameter is active, the Executive MULAP trunk is automatically called when you lift the handset. If the parameter is not active, the subscriber must press the MULAP key before dialing is possible.
  This parameter cannot be used by members with the secretary function.
  Default setting: the parameter is active for all members with the executive function.
- **No automatic incoming call acceptance**
  If this parameter is activated, you cannot answer an incoming call by lifting the handset. An incoming call must be accepted by pressing the MULAP key.
  Default setting: the parameter is not activated.
- **Automatic conference release**
  If the parameter is active, you can release the seized MULAP line for a conference by pressing the MULAP key. The release of this line is signaled to all other members by the flashing MULAP key. They can join the conference by pressing the MULAP key.
  Default setting: the parameter is not activated.
- **MULAP key set up**
  If the parameter is active, a MULAP key is programmed on the associated phone. You can press the key to set up an outgoing call via the Executive MULAP trunk. The Executive MULAP phone number appears on the called party's display.
  Default setting: the parameter is activated.

Using MULAP Keys

The LED on a MULAP key can have different statuses with the following meaning:

- Off: the relevant trunk is free and can be used.
- Lit: the relevant trunk is busy.

- Flashing fast: call on the relevant trunk.
- Flashing slowly: an on-hold call is waiting on the relevant trunk or the relevant trunk was released for a conference.

Ring type

For every Executive MULAP, an administrator with the **Expert** profile can define the acoustic signaling of incoming external calls via the ring type setting. You have the following options:

- Two rings (default setting)
- Three rings
- short-long-short ring

Only the default setting is possible for analog phones. Changes have no effect.

SIP Phones

SIP telephones can be integrated in an Executive MULAP. As a prerequisite, a system telephone (IP, HFA or SIP phone, for example) must have been defined as the first member of the Executive MULAP (Exec. 1).

Dual-mode mobile phones that are configured as Mobility Entry stations, for example, can be integrated. Dual-mode mobile phones support both GSM/UMTS networks and WLAN networks. A dual-mode mobile phone can be registered as an IP station (SIP client) at the communication system over a WLAN.

INFO: No programming of MULAP keys is possible for SIP phones. Furthermore, no features can be activated or deactivated via codes. Specific display messages of the Executive MULAP are not supported.

Dependencies

Topic	Dependency
Do Not Disturb	When Do Not Disturb is activated, incoming calls are no longer put through.
ISDN Phones	It is not possible to include ISDN telephones in Executive MULAPs.

11.3.3 Configuring Basic MULAPs and Executive MULAPs

The configuration of Basic and Executive MULAPs can only be performed by an administrator with the **Expert** profile and in **Expert mode**.

The procedure for the following application cases, which can be configured using the **Expert mode** wizard, is described here:

- *How to Add a Basic MULAP*

- *Display or Edit a Basic MULAP*
- *How to Delete a Basic MULAP*
- *How to Add or Delete a Member to or from a Basic MULAP*
- *How to Edit a Member of a Basic MULAP*
- *How to Add an Executive MULAP*
- *How to Display or Edit an Executive MULAP*
- *How to Delete an Executive MULAP*
- *How to Add or Delete a Member to or from an Executive MULAP*
- *How to Edit a Member of an Executive MULAP*

11.4 Voicemail Group and Fax Box Group

A voicemail group enables a subscriber group to access voicemails. When a call is placed to the call number of a voicemail group, the call is sent directly to the voicemail box (i.e., the voicemail) of the group and not to the group members. A fax box group (fax group) enables a subscriber group to access fax messages. The fax box of the group is reached directly via the station number of the fax box group.

11.4.1 Voicemail Group

A voicemail group enables a specific group of subscribers to access voicemails. When a call is placed to the call number of a voicemail group, the call is sent directly to the voicemail box (i.e., the voicemail) of the group and not to the group members. After a voicemail is left in the voicemail box of the group, it is forwarded to the voicemail boxes of all members.

All members receive the voicemail simultaneously. Whenever a member deletes a voicemail, this voicemail is also deleted from the voicemail boxes of all members and the voicemail box of the group. The personal voicemails of all members are not affected by this.

Every member of a voicemail group can be reached under his or her own station number.

Up to 20 members can be configured per voicemail group.

Every voicemail group can be assigned a name containing up to 16 characters.

At least one member of a voicemail group requires a Voicemail license.

Dependencies

Topic	Dependency
Ringing group on	The *Ringing group* feature cannot be used.

11.4.2 Fax Box Group

A fax box group (fax group) enables a specific group of subscribers to access fax messages. The fax box of the group is reached directly via the station number of the fax box group. After a fax message is left in the fax box of the group, it is forwarded to the fax boxes of all members.

All members receive the fax message simultaneously. Whenever a member deletes a fax message, this voicemail is also deleted from the fax boxes of all members and the fax box of the group.

Every member of a fax box group can be reached under his or her own station number.

Up to 20 fax box groups can be configured.

Every fax box group can be assigned a name containing up to 16 characters.

At least one member of a fax box group requires a Fax license.

11.4.3 Configuring Voicemail Box Groups and Fax Box Groups

The configuration of voicemail box groups and fax box groups can only be performed by an administrator with the **Expert** profile and in **Expert mode**.

The procedure for the following application cases, which can be configured using the **Expert mode** wizard, is described here:

- *Add a voicemail group*
- *Display or edit a voicemail group*
- *Delete a voicemail group*
- *Add or delete a member to or from a voicemail group*
- *Edit a member of a voicemail group*
- *Configure a fax box group*
- *Display or edit a fax box group*
- *Delete a fax box group*
- *Add or delete a member to or from a fax box group*

11.5 Speaker Call for Groups

Speaker call for groups enable the broadcasting of announcements to all internal members of a group.

11.5.1 Internal Paging

Internal paging enables internal members of a group to be addressed directly. This feature is also known as a group broadcast. Internal paging is not performed for group members who are busy or have activated the Do Not Disturb feature. Group members have no direct answering option. Answering is only possible by lifting the handset, which results in a transition to a normal two-way conversation.

Internal paging can be used via a function key programmed for this purpose, the menu item **Speaker call** or by entering the appropriate code and then dialing the station number of the target group. A function key can also be programmed with a group phone number. A connection to the programmed group is immediately set up when you press a function key of this kind.

Dependencies

Topic	Dependency
Do Not Disturb	Group members who have activated DND do not receive any announcements.
ISDN phones, SIP phones	The "Internal Paging" feature cannot be used with ISDN or SIP phones.

11.5.2 Transfer to Group from Announcement

A call on consultation hold can be transferred to a group via Transfer from Announcement. An announcement to the group is initiated for this (internal paging). The system sets up a two-party call when another party in the group lifts the handset or turns on the loudspeaker and the party who transferred the call hangs up. The connection is cleared down for the other group members.

Internal paging can be used via a function key programmed for this purpose, the menu item **Speaker call** or by entering the appropriate code and then dialing the station number of the target group. A function key can also be programmed with a group phone number. A connection to the programmed group is immediately set up when you press a function key of this kind.

Dependencies

Topic	Dependency
Do Not Disturb	Group members who have activated DND do not receive any announcements.
ISDN phones, SIP phones	The "Transfer to Group from Announcement" feature cannot be used with ISDN and SIP phones.

11.6 UCD (Uniform Call Distribution)

The Uniform Call Distribution (UCD) feature of the communication system enables incoming calls to be uniformly distributed to a group of stations (UCD-group).

UCD groups are primarily used in technical hotline environments (e.g., customer service hotlines), for managing complaints, in market research, order processing and acceptance (e.g., by mail-order companies and ticketing services) and even for emergency services.

As a rule, call distribution occurs by sending an incoming call to a UCD group to the station (agent) in the UCD group whose last call lies furthest in the past. It is also possible to define other distribution rules.

If there is no agent free to accept an incoming call, the call is automatically forwarded to a queue. Waiting calls are distributed to free agents on the basis of priority and wait time.

Announcements or music on hold can be played for waiting callers.

Configuration

The **UCD** wizard can be used to configure groups and stations for intelligent call distribution (UCD). The following application cases, which can be configured using the wizard, are described here:

- *Configuring Call Distribution / UCD Groups*
- *Adding/Deleting UCD Agents*
- *Changing Announcements / Music on Hold for UCD*

Besides the configuration options available through wizards, administrators with the **Expert** profile are also offered additional configuration options in **Expert mode**.

11.6.1 Call Distribution / UCD Group

A UCD group contains agents (subscribers) that belong to a work group and can be reached at a single phone number. An incoming internal or external call is automatically delivered to the agent who is idle longest.

Every UCD group can be configured using the WBM (**in Expert mode**) so that incoming calls to an agent are automatically accepted by the communication system (Unattended Incoming Call Connection AICC).

If all agents of a UCD group are busy, incoming calls can be placed in a queue. The maximum number of calls in the queue can be individually set for every UCD group. When the maximum number of queued calls is reached, further calls can be forwarded to an overflow destination (which may be an external destination, another UCD group, an internal station or a group).

If the overflow destination is another UCD group and if all other agents in this UCD group are busy, the call remains in the queue associated with the original group and is also entered in the queue of the other UCD group (overflow destination).

Announcements or music can be played for on-hold callers.

Every UCD group can be assigned a name containing up to 16 characters.

Dependencies

Topic	Dependency
Call forwarding	A call is not forwarded to a UCD group in the following cases: • If a hunt group is called and a subscriber with call forwarding to a UCD group is next, this call is not forwarded. In this case, the next station in the hunt group is immediately called. • A subscriber is a member of a group call with the property "Group" and has activated call forwarding to a UCD group. • A station is a member of a group call no answer. If the group is called, the call is not forwarded to the UCD group. Exception: The first subscriber entered has activated call forwarding to a UCD group. In this case, the call is forwarded.

11.6.2 UCD Agents

The stations of a UCD group (agents) comprise a workgroup and are typically deployed for technical hotlines, for example, or in order processing, order acceptance, CRM, etc. All incoming calls are distributed to the available stations in a UCD group.

The assignment of agents to the UCD groups occurs via identification codes (IDS). An ID can be assigned to no more than one UCD group. An agent can be assigned multiple IDs. This lets an agent work in more than once UCD group. An agent, however, can only be logged on and therefore active in one UCD group at a time.

In order to use the UCD functions effectively, agents should have phones equipped with a display, function keys and a headset.

Logging on/off

Agents can log into any phone of the communication system (except ISDN and SIP phones) by using their respective IDs (Identification Code). The agent is available following successful login and permanently assigned to the relevant phone until he or she logs off. The agent cannot log into another phone. Agents who have logged off are no longer considered for the call distribution.

The UCD functions for logging in, logging out and for changing the station status can be accessed by agents from the telephone via programmed function keys or via the associated menu items or via codes.

Subscriber states

An agent's state is **available** following successful login. If required, a agent can set his or her own station status, or the status may be changed automatically, depending on the agent's current activity. The current subscriber state is shown on the phone's display.

The following displays are possible:

Display	Meaning
available	The agent is available and can accept UCD calls.
not available	The agent temporarily logged off his or her workstation (for example, for a break).
wrap up	The agent is in wrap-up mode. He or she does not receive any UCD calls during the wrap-up time. Depending on the configuration, this can be an individual wrap-up time (the agent independently defines the length of the wrap-up time by changing his or her subscriber status) or an automatic wrap-up time (a wrap-up time is automatically available to all agents after a UCD call).
for <UCD group name>	The agent receives a UCD call.

An agent logs off after his or her shift and is therefore no longer available for UCD calls. The agent can still be reached at his or her personal station number.

If all agents of a UCD group are in the state **not available**, incoming calls are forwarded to an overflow destination (an external destination, another UCD group, an internal station or a group).

If an agent does not accept a call although he or she is logged on and available, the communication system automatically sets the status of that station to **not available**.

Dependencies

Topic	Dependency
Call forwarding	If an agent activates the Call Forwarding feature, he or she is automatically logged off and is no longer available for UCD calls.
ISDN phones, SIP phones	It is not possible to use ISDN and SIP phones here.

11.6.3 Wrap up

This feature temporarily removes an agent from the call distribution in order to allow the agent some time to wrap up the call just completed. The agent does not receive any UCD calls during the wrap-up time.

A distinction is made between:

- the individual wrap-up time.
  The agent sets the wrap-up time length by changing his or her subscriber state.
- the automatic wrap-up time.
  The Uniform Call Distribution (UCD) feature is configured for this in such a way that a wrap-up time is automatically made available to all agents in all UCD groups after a UCD call. The automatic wrap-up time is defined in ring cycles, that is, in increments of five seconds.
  An agent can manually extend the automatic wrap-up time by changing his or her subscriber state.

An agent can be reached throughout the wrap-up time via his or her personal station number.

11.6.4 Call Prioritization

You can set a priority for incoming internal and external calls for a UCD group. The queued calls are distributed to the agents in a UCD group on the basis of priority and the wait time.

A queued call with a high priority is answered before a call that has been waiting longer but has a lower priority. A queued call with low priority will be forwarded to an overflow destination before a queued call with high priority.

Priorities are assigned on the basis of trunks for external calls (per B channel), regardless of whether IP or TDM lines are involved.

Examples:

- Communication system with ISDN Primary Rate Interface (S_{2M} interface) and ISDN Point-to-Multipoint connection (S_0 interface)
  Incoming calls via the ISDN Primary Rate Interface are normal customer calls. All B channels of the $_{2M}$ interface are thus assigned a medium priority. Calls received via the ISDN point-to-multipoint connection are urgent calls, e.g., high-priority orders for spare parts. All B channels of the S_0 interface are thus assigned a high priority.
- Communication system with a point-to-point connection to an Internet Telephony Service Provider ITSP and an ISDN point-to-multipoint connection (S_0 interface)
  Incoming calls via the PABX number for IP telephony are normal customer calls. All B channels of the LAN interface are thus assigned a medium priority. Calls received via the ISDN point-to-multipoint connection are urgent calls, e.g., high-priority orders for spare parts. All B channels of the S_0 interface are thus assigned a high priority.

The priority is set system-wide for internal calls and therefore applies equally to all internal calls.

Ten priority levels (1 = high, 10 = low) are available.

By default, priority = 10 is set for internal calls, and priority = 1 for external calls.

11.6.5 Accepting UCD Calls Automatically

This feature lets agents accept incoming calls without any additional operations (Automatic Incoming Call Connection AICC).

This feature can only be used if the agent's phone has a headset and Disconnect key. An audible tone notifies the agent via the headset about an incoming call that is then automatically put through.

An agent can clear down an ongoing call by pressing the Disconnect key.

The "AICC" feature is not activated by default. Activation is performed on a group-specific basis and applies to all agents in a UCD group, irrespective of whether or not the agent's phone features a headset.

11.6.6 UCD queue

If all agents of a UCD group are busy, incoming calls can be placed in a queue. Announcements or music can be played for on-hold callers.

If a call that is waiting in the queue for a specific period (first call cycle) is not accepted by the agent longest in **available** state, this agent's state is changed to **not available** and the call is transferred to the next available agent. If this agent does not answer the call either within a set period (second call cycle), the status of this agent is changed to **not available**. The call is routed to the overflow destination if the status of all agents is **not available**.

For every UCD group, the maximum number of calls in the queue can be set individually. If the maximum number of waiting calls is exceeded, further calls can be routed to an overflow destination.

You can select an external destination, another UCD group, an internal station or a group as the overflow destination. If the overflow destination is another UCD group and if all other agents in this UCD group are busy, the call remains in the queue associated with the original group and is also entered in the queue of the other UCD group (overflow destination).

An agent can query the number of calls in the queue for his or her UCD group with a specially programmed function key of via the assigned menu item or code.

Calls in a Queue

The maximum number of calls in the queue is 30 for UCD groups 1 through 59 and 72 for UCD group 60.

The minimum number of calls in the queue is zero. There is no queue if the minimum number is set to zero. Calls are redirected or rejected directly at an overflow destination if there is no agent available.

11.6.7 UCD Overflow

UCD calls can be forwarded to an overflow destination if they are not accepted by the agents of a UCD group and if no queue was set up or if the maximum number of calls in the queue was reached.

> ***INFO:*** The UCD overflow concept defines only one overflow destination, the second CDL entry. Therefore, the announcements are played only when the call is at the UCD overflow destination and not for the whole ringing cycle. When a call leaves the UCD overflow destination then default MOH is opened.

The maximum number of calls in the queue can be individually set for every UCD group. If this number is exceeded, further calls can be routed to an overflow destination.

If you do not want a queue to be created, you can enter zero as the maximum number of calls in the queue. Unanswered calls are then immediately routed to an overflow destination.

Dependencies

Topic	Dependency
AutoAttendant	It is not possible to use an AutoAttendant as an overflow destination.

11.6.8 UCD Night Service

An individual night service can be configured for every UCD group. Night service can also be activated and deactivated by every agent in a UCD group. Following activation, all calls for this UCD group are forwarded to the night destination.

The night service destination can be defined as an internal station, another group, an announcement/MoH, the voicemail box of the communication system or an external destination.

Activating / Deactivating

Activation or deactivation of the UCD night service can be achieved via a programmed function key or via the associated menu items or via codes. The call number of the desired night service destination must be entered at activation.

For more information on the communication system's night service, see *Night Service*.

Dependencies

Topic	Dependency
Subscriber state	If you activate the UCD night answer feature, your current subscriber status does not change. A forced logout of the agents who are still logged in does not occur.
Communication system's night service	The communication system's UCD night answer and night service can be activated and deactivated independently of one another. Example: A UCD group was entered as the night service destination for the communication system. Calls that reach this UCD group via the communication system's night service remain in this UCD group, irrespective of a UCD night answer.
Existing calls	Existing calls are not affected by the activation of UCD night answer.

11.6.9 Announcements / Music on Hold for UCD

Music On Hold (MoH) or announcements can be played to callers who cannot be switched through directly to the agents of a UCD group. Music on hold and announcements can be assigned to each UCD group individually.

You have the following options:

- Music On Hold (MOH)
  Queued callers can be played music from the integrated source of the communication system. Further Music on Hold file(s) can be loaded from a PC into the communication system.
  For more information, see *Music on Hold*
- Announcements
  Queued callers can be played integrated announcements. Further announcements can be loaded from a PC into the communication system.
  For more information, see *Announcements*

The time up to the start of the announcement can be set (**Ann. delay time**). You can suppress the announcement by setting the maximum value (600 seconds). It is assumed here that the call will be accepted within this time.

11.6.10 Transfer to UCD Groups

Internal and external calls can be transferred to UCD groups. If a call is not answered within a certain period, a recall is carried out.

The recall time is defined via the time parameter **Monitoring transfer to a UCD group prior to answer**. The default setting is 300 seconds. This setting can be changed by an administrator with the **Expert** profile in **Expert mode**.

Dependencies

Topic	Dependency
Announcements	Announcements can be played for the external transferred calls. This is not possible for internal calls.
Recall time	The recall time for a transfer to UCD groups differs from the recall time for transfers to other subscribers.

11.6.11 Releasing UCD from Analog Lines

When UCD calls over analog lines are not answered within a specific time, these calls are released. This prevents analog lines from freezing up.

The release time is defined via the time parameter **Monitoring a UCD call on an analog line**. The default setting is 300 seconds. This setting (from 0 to 255 minutes) can be changed by an administrator with the **Expert** profile in **Expert mode**.

12 Call Routing

The communication system provides several ways to assign calls to a desired destination, such as classes of service (toll restriction), day and night service, least cost routing and Call Admission Control (CAC). Emergency calls can be made from any configuration.

12.1 Classes of Service (Toll Restriction)

Classes of service (Toll restriction) control subscriber access to external lines that may be subject to toll charges.

12.1.1 Class of Service (COS) Groups and Classes of Service

Every subscriber is assigned a Class of Service group that defines the class of service (i.e., the permissions) of the subscriber for incoming and outgoing calls.

For each route, one of the following classes of service is defined in the COS group:

- **Internal**
  The subscriber may only make internal calls.
- **Outward-restricted**
  The subscriber may only answer (not make) external calls.
- **Allowed list** 1-6
  The subscriber may only dial the external numbers defined in the Allowed list. Outward-restricted trunk access applies if no call number is entered.
- **Denied list** 1-6
  The subscriber is not permitted to dial the external numbers defined in the Denied list. Unrestricted trunk access applies if no call number is entered.
- **Unrestricted**
  Subscribers can answer and set up incoming and outgoing external calls without restriction.

Some of the 15 possible COS groups are preset with the same class of service for all routes and given meaningful names (e.g., COS group **International** with the class of service **Unrestricted** or COS group **Incoming** with the class of service **Outward-restricted**). The names of all COS groups can be changed by the administrator.

INFO: By default every station belongs to COS group 7 and this can be changed. Also every trunk belongs to COS group 7 but this is not configurable so as a result COS group 7 should not be used and let it have Unrestricted access to every Trunk Group.

Dependencies

Topic	Dependency
Speed Dials	System speed dial destinations can be selected independently of the assigned COS group.
LCR	The Class of Service Groups (Toll Restriction) and LCR Class of Service are different.
Call forwarding	For forwarded calls, the caller's class of service applies.

12.1.2 Allowed and Denied Lists

Allowed and Denied lists are used to define which external phone numbers may and may not be dialed by the subscribers.

Allowed lists contain the digit strings permitted at the start of a phone number. The subscriber may only dial the external numbers defined in the Allowed list. Make sure that all required emergency numbers are also included in the list!

Denied lists contain the digit strings that are not allowed at the start of a phone number. The subscriber is not permitted to dial the external numbers defined in the Denied list. Make sure that no emergency numbers are included in the list!

The **List of Emergency Numbers** is a special case of the Allowed list. The subscriber may only dial the emergency numbers entered in the list. Make sure that all required emergency numbers are included in the list!

It is not necessary to enter the complete phone numbers in the lists. To permit users to dial (toll free) 0800xxx numbers, for example, only `0800` needs to be entered here. Since these lists are only for outgoing external calls, it is not necessary to include the CO access code with the numbers you enter. Entering a `#` sign at the start of a denied number prevents the toll restriction from being bypassed for system telephones when an analog CO line is to be seized using DTMF signaling or when switching to DTMF during the dialing.

The Administrator can use **exception filters** for any Denied list to define which digits should not be compared with the corresponding Denied list. The communication system excludes the set range of digits before the digit analysis. By prohibiting the characters `*` and `#`, subscribers are prevented from entering these characters to bypass the toll restriction.

Configuration Limits

Feature	Number
Allowed list 1: long, 100 entries	1
Allowed lists 2-6: short, 10 entries	5

Feature	Number
Denied list: long, 50 entries	1
Denied lists 2-6: short, 10 entries	5
Number of characters in list entries (digits 0 - 9 and the characters * and #)	26

12.1.3 Night Service

During the night, incoming and outgoing calls can be treated differently than during the day. Incoming calls can be redirected to a night service destination, and internal subscribers can have different classes of service for their phones than during the day. The system-wide switching between the day and night service is performed automatically at a time specified by the administrator.

Any phone can serve as a night service destination, provided the associated class of service group allows incoming calls. A telephone with internal authorization only cannot be entered as a night service destination. If the night service destination has activated call forwarding, this is followed.

In order to prevent toll fraud, for example, a COS group can be assigned different classes of service for the night and day modes.

In addition, you can also specify a different intercept position for the night service as opposed to the day service. This intercept position can be an individual station or a group.

Scheduled Night Service

The communication system activates and deactivates the night service in accordance with a schedule defined by the administrator.

> ***INFO:*** With the scheduled night service, the active settings apply to ALL stations of the communication system. In the case of automatic COS changeover after time, all subscribers are combined into groups (profiles).

Variable Night Service

The variable night service is activated and deactivated manually by an authorized subscriber. The calls are handled as configured by the administrator in the call destination lists

By default, the first subscriber (with the station number "100") in the communication system can activate and deactivate the night service. The administrator can authorize up to five subscribers to activate and deactivate the night service.

UCD Night Service

An individual night service can be configured for every UCD group. It can be activated and deactivated independently of the system-wide night service. It can

also be activated and deactivated by every agent in a UCD group. The current status of the individual agents and existing calls are not affected. Following activation, all calls for this UCD group are forwarded to the night service destination.

Another UCD group, an internal station or an external destination can all be set as a night service destination.

12.1.4 Automatic COS Changeover after Time

For the "automatic COS changeover after time", the stations are grouped into so-called station profiles that define which COS group applies in which time interval of the week. For each station profile, you can configure a schedule.

Differences between "automatic COS changeover after time" and the "scheduled night service":

- Automatic COS changeover after time applies only to the day service (not the night service).
- Reaching the call destination via Call Management
  This takes place via Call Management and does not depend on automatic class-of-service changeover. There are different call lists for day and night.
- With the scheduled night service, a distinction can only be made between day and night shifts, and this applies to ALL stations.
- Intercept destinations
  The intercept destination is only defined by the scheduled night service.
- COS group:
  During the night, the COS group is in a constant (configurable) relationship with the station; the automatic class of service changeover after a timeout has no impact on this.
  During the day, the COS group may be changed during certain times of the day or also be in a fixed (configurable) relationship with the subscriber.

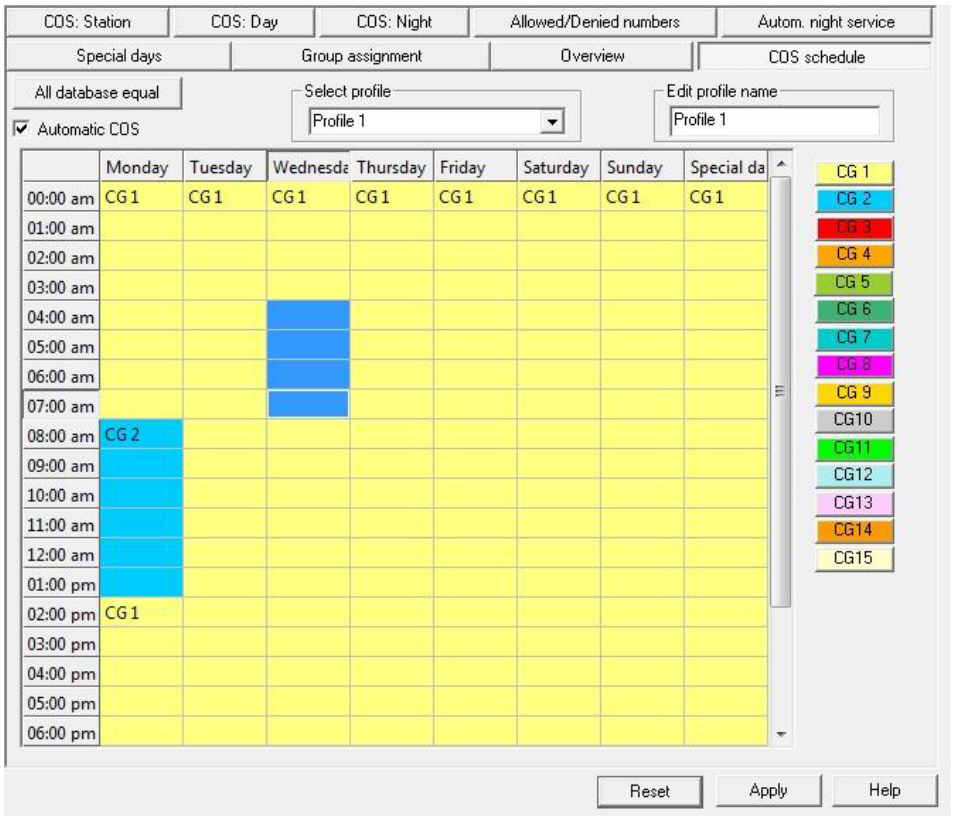
Dependencies

Topic	Dependencies
Night service	The "Automatic Night Service" feature has priority over the "Automatic COS Changeover after Time" feature. If the night service is activated, the COS group is handled normally and applied for the night. The schedule is only relevant during the day.
Networking	Automatic COS changeover and night service do not function across all nodes.

12.1.4.1 Schedule

The schedule is used to control the Classes of Service for the "automatic COS changeover after time". It is possible to configure up to eight COS changeovers per day for each day of the week.

Each day begins at 00:00 hours. Entering the end time time in each of the columns delineates the time zones. In the following example of a schedule, the individual COS changeovers are referred to as CG2, CG4 and CG5.



A station can have different class of service groups for the day and night.

If "Automatic COS changeover" is set system-wide for the day, the profile and schedule that is configured will determine the COS group that is assigned to a station. At night, the station has the same COS group as previously assigned (via the night service).

Automatic COS changeover after time is disabled by default

The communication system supports only one time zone (world time). Remote station groups working in different time zones are set to the communication system's time zone.

The schedule can only be configured using Manager E.

12.1.5 CON Groups

The CON Groups feature is used to define which subscribers of the communication system can establish connections to which other subscribers of the communication system. This feature is used for tenant systems, for example.

CON groups can also be used to configure which lines individual subscribers can access for incoming and outgoing calls..

The CON functionality does not access the applications; it is only significant for telephony. The presentation of the presence status, for example, is not prevented by an access restriction through CON.

The CON feature is implemented in two steps:

- Create CON groups
- Configure CON matrix

> ***INFO:*** The CON feature should not be used in conjunction with UC functionality, since this could result in limitations.

12.1.5.1 CON groups (traffic restriction groups)

CON groups (also referred to as traffic restriction groups) control allowed and denied connections between subscribers and lines of the communication system.

Using CON groups, specific stations and lines can be combined into groups.

You can assign a CON group to individual stations and lines in the communication system via the CON Group Assignment. When coding the connection matrix, you can then access these groups and define which subscribers can reach which other subscribers and which lines can be accessed by them.

All stations and CO trunks are assigned to CON group 1 by default. This provides all subscribers with unrestricted access to other subscribers as well as trunks, both incoming and outgoing. The CON matrix specifies which of the six CON groups can set up connections to which other CON groups.

A maximum of 64 CON groups can be configured.

12.1.5.2 Assigning Speed-Dialing Numbers to CON groups

Every CON group is assigned a range of System Speed Dialing (SSD) destinations. When a subscriber dials an SSD, the associated CON group is checked to verify if the subscriber is authorized to do so. Dialing is performed if this speed-dialing number lies within the correct range for the relevant CON group, otherwise an error message is output.

When a user dials a speed-dial number, the system identifies the ITR group for the number, which determines whether or not the user is authorized to dial that number. If not, an error message appears, and the dialing attempt is rejected

Speed-dial number ranges can overlap in the ITR groups.

By default, all speed-dial numbers are assigned to ITR group 1.

The speed-dial number ranges can overlap in the CON group. The following are permitted, for example:

CON group	SSD range
1	0000-7999
2	0050-0150
3	0200-0500

Please note, however, that you cannot enter individual system speed-dial (SSD) numbers or multiple SSD ranges in a CON group instead of a range. The following are not permitted, for example:

CON group	SSD range
1	0000, 0005, 0010
2	0050-0100, 0300-0500

12.1.6 System Telephone Lock (COS Changeover)

The central lock code enables an authorized subscriber (possibly the administrator) to set a comprehensive lock on most of the phone functions for other subscribers. Only the following features are still available: internal calls, system speed dialing and conferencing with internal subscribers. This lock code can be deactivated by either the authorized subscriber or the locked subscriber by entering their own lock codes.

The lock code of the phone for the which the lock is to be activated or deactivated by the authorized subscriber is not required to set the lock.

By default, the authorized subscriber is the subscriber with the call number "100" (reconfigured).

12.1.7 Individual Lock Code (Locking the Phone)

If the individual telephone lock is set for a phone, external calls cannot be conducted from that phone, and the user settings cannot be modified.

Emergency numbers can be dialed even if the phone is locked.

You can still conduct internal calls.

Incoming calls can be redirected to internal subscribers.

A locked telephone only supports features that do not require external dialing. The System Speed Dialing feature is the exception to this rule.

To remind subscribers that the station is locked, the phone receives a steady tone (special dial tone). In addition, on phones equipped with a display, the message "Unlock Phone" appears.

Subscribers can lock their phones via a key or code by entering their personal lock codes and then unlock the phone again as required.

The phone lock code must be configured first before the phone lock can be used. The phone lock code is set to 00000 by default for all phones and can be set individually. To do this, the must be unlocked. The phone lock code must always be 5 digits. Only digits 0-9 are allowed. If the subscriber has forgotten the phone lock code, he or she can have it reset to the default value 00000 by an authorized user (i.e., the first station in the system with the call number "100" or the administrator).

12.1.8 Collect Call Barring per Trunk (for Brazil only)

Collect call barring per trunk provides for automatic release of incoming collect calls. This feature is available only in the country settings for Brazil. The setting is ignored in all other countries.

Users can configure it individually for each analog trunk. Ringback protection can be configured individually for each analog trunk. If this feature is enabled for a trunk, the system opens the loop for two seconds (default value) one second (default value) after an incoming call is accepted. This ensures that collect calls are released in the network, while other calls continue unaffected.

12.1.9 Ringback Protection per Station (for Brazil only)

Ringback protection per station (also called call collect barring per station) makes it possible to set up ringback protection individually for each station, thus making it possible to automatically refuse incoming ringback calls. This also applies in the case of call forwarding, call pickup, an intercept, etc.

Users can also program collect call barring system-wide. This applies if a caller dials a hunt group instead of an individual station or misdials a number.

12.2 LCR (Least Cost Routing)

The Least Cost Routing (LCR) function automatically controls the paths used for routing an outgoing connection. This path can be routed via the public network, various network providers (ITSPs) or a private network. The most suitable connection path is selected for a call on the basis of the dial plan, route tables, and outdial rules.

Connections can be voice calls, analog data connections via fax and modem and ISDN data connections.

12.2.1 LCR Functionality

You can use the LCR function to specify the provider you want to use, for example, for local calls, mobile phone calls or international calls. You use the communication system to define the least-cost provider and conduct all calls via this specific path.

If a pattern that matches the dialed phone number is found in the dial plan, the route tables are searched for a suitable route (Each trunk is assigned to a route. See *CO Access over Digital and Analog Lines*). At the same time, the system checks if the LCR class of service applies to this route table entry. The LCR class of service and the difference between LCR and doll restriction are described in LCR Class of Service section.

The LCR function provides control over which stations of the communication system may use which routes or trunks (to ensure that faxes are routed exclusively via TDM trunks and not via ITSPs, for instance). It is also checked whether the caller has the required class of service as per the toll restriction to seize the route under consideration by LCR. This check can be disabled for tie trunks (PABX trunks) via the configuration.

The dialed digits are buffered until the routing tables with the LCR classes of service have been evaluated. It is only on completing this step that the connection is set up, in accordance with the outdial rules. A dial tone can be issued to signal the ready-to-dial condition to the subscriber.

When configuring outdial rules, you can enter information for the dialing station, e.g., by specifying that this connection is routed via a specific telephony provider (name of the provider) or that a connection is using a more expensive route. This information can either be displayed on the screen, output as a tone or output both on the display and as a tone.

In general:

- When LCR is activated, the check is performed for every external dialing operation. Exception: when dialing a specific trunk code or line key.
- If LCR determines that the preferred route cannot be used, the communication system will look for a (possibly more expensive) alternative from the routing table.
- Digits can be transmitted either individually or en-bloc, depending on the access method and the route table.
- If the table of DID numbers is empty, the table of internal call numbers is alternatively used. The corresponding rules apply to this table.

INFO: The location number (country code / possibly local area code / possibly PABX number) must be configured even for communication systems with analog trunks (MSI).

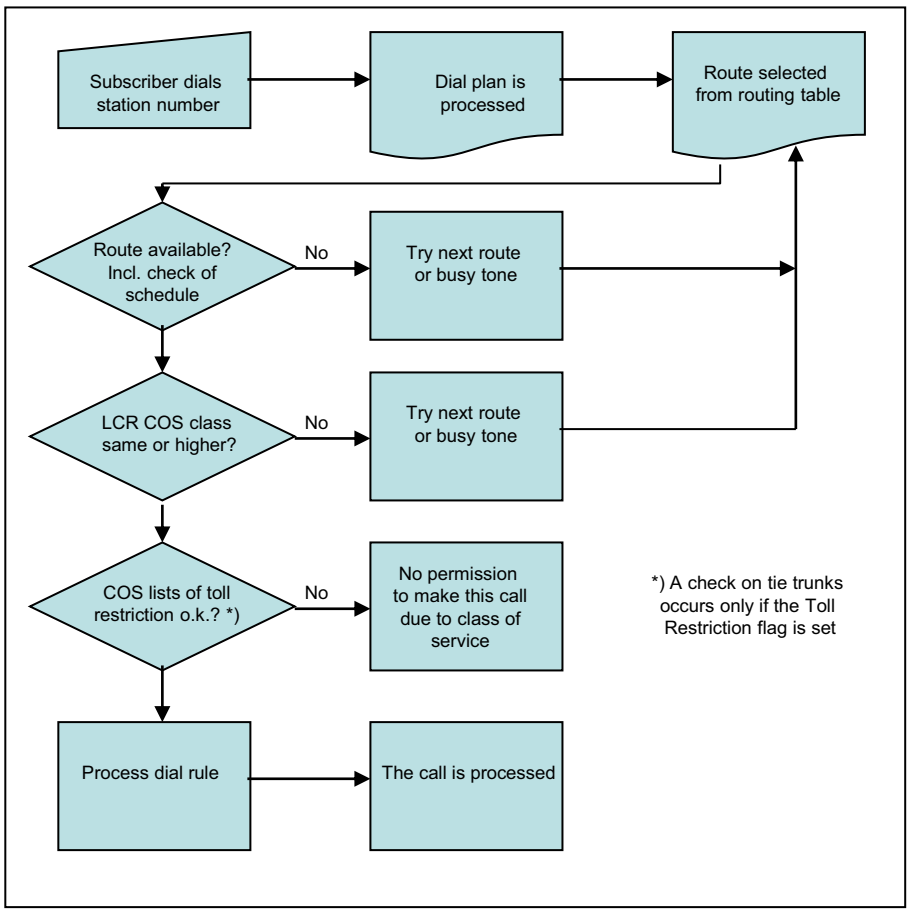
In addition, a DID number or, if the DID number table is empty, a DID number of the own analog trunk connection (MSI) must be configured. This is the only way to ensure that all external destinations can be reached.

System-Specific Information

The communication system evaluates a total of 24 characters.

The communication system can manage up to 1000 dial plans and 254 route tables with 16 entries each.

LCR Flowchart



Digit transmission

There are two types of digit transmission: digit-by-digit and en-bloc sending. For digit-by-digit transmissions, each digit is transmitted and processed directly after dialing (prerequisites: the LCR analysis is complete, the dial plan entry is uniquely

identified, and the classes of service have been checked). With block dialing, digit blocks are formed and transmitted as a block (i.e., line seizure occurs only after some time or when an explicit end-of-dialing code is recognized).

The digit transmission for ITSP routes must always be en-bloc. The setting of the route apples to the entire routing table.

For U.S. only: Carrier Select Override

Carrier Select Override can be implemented through selective line seizure (code, key). The LCR mechanism is bypassed completely in this case.

Dependencies

Topic	Dependency
Schedule	If an LCR configuration with a schedule exists in a system migrated from HiPath 3000, these entries are still effective and can be administered with Manager E.
System Speed Dialing	To ensure that system speed dial destinations work properly, the LCR access code, followed by the destination number, must be entered in the speed-dial destination.
Name keys	Repertory dial keys to external destinations must have the LCR access code for proper operation.
Class of service (Toll restriction)	The toll restriction classes of service are also applied in LCR. For PBX trunks, the toll restriction can be disabled; the configuration occurs via a flag.
Prime Line	If Prime Line to the CO is used, no LCR is possible. These features are not mutually compatible.

12.2.2 LCR Dial Plan

The dial plan is searched for patterns that match the dialed digits (dialing sequence). The result is used as a criterion for selecting the route table. At the same time, the system checks if the subscriber's LCR class of service matches for this dial plan entry.

The pattern of a dialing sequence is assigned in the dial plan to a routing table which, in turn, determines further parameters for the connection setup.

The dial plan is split into individual fields for identification and configuration purposes. The table shows the numbers 4922000 and 1603656260 entered in the dial-plan table.

Field 1		Field 2		Field 3		Field 4		Field 5
0	C	492	–	2000				
0	C	160	–	365	–	62	–	60

The following entries apply for the phone numbers:

0 . . . 9	Allowed digits
–	Field separator
C	Simulated dial tone (can be entered up to three times). This entry is also interpreted as a field separator

Global character

X	Any digit from 0 to . . 9
N	Any digit from 2 to . . 9
Z	One or more digits to follow up to the end of dialing

A digit sequence can be divided into a maximum of 10 fields.

Field separators are used to split the digit string into individual fields that can be evaluated separately. Example: After the first dialed digit, a separator is inserted so that a dialed “0” is detected as a separate field and thus simulates toll restriction.

Due to this field separation, these fields can be repeated or rearranged in the dial plan. The fields formed by the field separators "–" and "C" in the dial plan can be addressed selectively to repeat, suppress, exchange, or insert digits.

A "#" or "*" character in the digit string dialed by the subscriber is the end-of-dial code or indicates dialing method changeover. This is why these characters are not valid entries in the dial plan.

Specific dialed numbers must precede wildcard entries to prevent conflicts in matches with wildcard entries.

The account code entry can be enforced per dial plan. The Account Code Checking Procedure applies.

If there are multiple dial plan entries that match a a dial string, the closest match is used. Example: If 00894711 is dialed, and dial plan entries 0CZ and 0C089Z exist -> 0C089Z will be executed. The position of the entries within the dial plan is irrelevant; no "sorted" entry is required.

OpenScape Business can evaluate a dialing sequence of up to 24 characters.

LCR Entries for Initial Setup of the Communication System

When the communication system is started up for the first time, a number of country-specific default values are entered in the LCR dial plan. Up to and including dial plan 34, system-side entries for emergency calls, directory assistance, special numbers, default trunk seizure for PSTN and ITSP, for UC Suite, announcement connections, networking and for international dialing formats are preset to ISDN trunks. This range can be affected by configuration changes elsewhere (for example, by changes to the **Location number** flag). Consequently, whenever the location number is changed, it must be ensured that the default trunk seizure still works as expected (which is important when dialing public numbers).

INFO: From LCR dial plan 36 onwards, all entries are freely available.

12.2.3 LCR Routing Table

Least Cost Routing (LCR) is achieved by searching for a suitable route in the LCR routing tables (every trunk must be assigned a route). At the same time, the system checks if the class of service (toll restriction) matches for this route. The outdial rule is also dependent on the assigned path.

The routing table describes:

- the route assigned to the relevant path.
- the outdial rule,
- the LCR Class of Service (COS) required for seizure,
- the warning method for a more expensive route (warning tone).
- the dedicated gateway and
- the GW node ID.

The table is searched from top to bottom in hierarchical order. The system checks to determine whether the route is free and the station has the requisite LCR class of service. If this is the case, dialing occurs according to the dial rule entered in the route table if this is permitted by the toll restriction class of service and the CON group assignment between the subscriber and the line.

If the first route selection in the route table is busy, the LCR function can advance to the next (possibly more expensive) route configured in the route group table. The system can notify the user of this with an audible signal, an optical signal, or both.

Up to 254 route tables with 16 routes each can be created.

Dedicated Gateway

A dedicated gateway is a fixed partner node in an IP internetwork (Dedicated Gateway -> Forced). When a dedicated gateway with the corresponding GW node ID is entered for the IP networking route, routing to this gateway is enforced.

In a multi-gateway configuration, a dedicated gateway is determined via the subscriber configuration.

12.2.4 LCR Class of Service

Every subscriber is assigned a separate LCR class of service (COS). A subscriber can only seize a route if his or her COS is greater than or equal to the LCR COS in the route table, i.e., a subscriber with a COS 7 cannot seize a route with COS 8. By default, all subscribers are entered with the maximum LCR Class of Service (15).

Dependencies

Topic	Dependency
Toll restriction	The Toll Restriction class of service has precedence over the LCR class of service. The Toll Restriction class of service can be enabled and disabled for tie trunks.
CON Group Assignment	Dialing occurs only if allowed by the CON matrix.

12.2.5 LCR Outdial Rules

LCR outdial rules can be used to convert the phone numbers entered into random new digit strings for additional processing. Access to different carriers is enabled via digit translation. The dial rule used is defined by the path or the route in the route table.

System-Specific Information

The communication system can administer up to 254 outdial rules in the LCR dialing rules table. The name of a dial rule can contain up to 16 characters.

The dialing rules address the dial plan fields selectively for the following operations:

- Repeating digits
- Suppressing digits
- Exchanging digits
- Inserting digits
- Switching the signaling method
- Detecting a dial tone
- Inserting pauses

Dial Rule

You can define up to 254 outdial rules here with a maximum length of 40 characters each.

The LCR dialing rules table is also referred to as the routing table.

Definition of Outdial Rules (Dial Rule Format)

- A:
  Repeat remaining fields (transmit). The letter "A" causes all subsequent digit fields to be transmitted. The point of reference is the last field delimiter in the field of dialed digits in the dial plan.
  If "A" is entered without an explicit reference, it designates all digits after the acces code, i.e., "A" is then equivalent to "E2A".

- B:
  It is used for the multi-gateway network when a station number of type TON (Type Of Number) that was called from outside is "unknown" and must be routed to the multi-gateway node. To ensure that this station number is unique, it is extended to national or international in accordance with the TON in the LCR. This is required when the DID numbers are not unique and need to be configured in the national or international format.
- D (n):
  Dial digit sequence (1 to 25 digits). "D" may occur multiple times and at any position in the string.
- E (n):
  Transmit field contents (1 to 10). "E" may occur multiple times and at any position in the string. "E" can also appear in any order with relation to (n). A specific field can be addressed multiple times, including in sequence. With the exception of "E1" (access code), this letter can be surrounded by any parameters.
  With digit-by-digit dialing (opposite of en-bloc dialing), the last element in the outdial rule cannot be E(n); it may be E(n)A.
- M (n):
  Authorization code (1 to 16). This letter must not be in the final position.
- P (n):
  P (n) can occur more than once in the string and can be placed in any position. P (n) can be surrounded by any other parameters.(1 to 60 times the system-wide pause unit).
- S:
  Switch, changes signaling methods from DP to DTMF (with CONNECT, PROGRESS or CALL PROC with PI). The letter "S" may occur in the string only once and must not be in the final position. The "C" parameter cannot be used after "S".
- C:
  Carrier "C" can be inserted in the string only once. The subsequent characters are transmitted without a dial pause and are used for single stage, two-stage, DICS (not for U.S.), BRI, and PRI carrier access.
- U:
  Use subaddress signaling method. The letter "U" may occur in the string only once and must not be in the final position. The "S", "P", "M", and "C" parameters cannot be used after "U".
- N (n) (only for the U.S.):
  Network SFG (1 to 5) or Band Number (1).
- L (for U.S. only!):
  "L" must only occur at the end of a string of characters. "L" causes the call to be handled as an emergency call.

Example:

The system should automatically add a provider suffix.

Dial rule D010xxA means: the system first dials the Provider prefix (010xx), and then all the digits after the access code dialed by the subscriber (A).

12.2.6 Network carriers

You can assign network carriers to each route. The selection of the network carrier is defined by the LCR outdial rules.

Unknown

No explicit specification about a network carrier.

Main network supplier

When seizing a trunk using the main network supplier, simplified dialing into the public network is performed by en-bloc dialing or by dialing individual digits.

MCL Single Stage

With MCL Single Stage, a prefix is used to dial the desired network carrier, and the station number is then dialed. Dialing occurs in the D channel for ISDN or as normal dialing for MSI.

MCL Two-Stage

With MCL Two Stage, a prefix is used to dial the desired network carrier. After a synchronization phase, a configurable authorization code is initially sent followed by the destination call number as DTMF digits.

With synchronization during timeout, you must program a pause of 2 to 12 seconds.

Corporate Network

A corporate network is directly connected to the communication system. The LCR function determines the appropriate trunk group based on the station number dialed and then routes the call either via the trunk group in the public exchange or via the trunk group in the corporate network.

Dial-In Control Server

With this type of LCR, the desired network carrier is dialed with a prefix via a dial-in control server, and the call number and configurable authorization code are transmitted in the subaddress. Dialing occurs in the D channel.

Primary Rate Interface (PRI) (U.S. only)

In the case of the Primary Rate Interface, the selection of the network carrier or of a calling service is encoded in SETUP message using following information elements: Network Specific Facility, Operator System Access and Transit Network Selection.

Dependencies

Topic	Dependency
Receiving/forwarding call information	Temporary or permanent station number suppression cannot be activated.
ISDN/SUB addressing	The ISDN feature SUB must be applied for or released in the public network.

12.2.7 Selective Seizure of Exchange Lines

Exchange lines (aka "outside lines" or "CO trunks") can also be seized selectively by subscribers.

The prioritization for the seizure of exchange lines is handled via Least Cost Routing by default. In most cases, the least-cost provider is selected first, followed by the second-lowest cost provider, and so on.

If a subscriber wants to conduct a call over a provider that is not first in the LCR (because this provider is cheaper for long-distance calls, for example), he or she can select this provider via a specific trunk code or trunk key.

Subscribers can likewise also use selective dialing via seizure codes to reach a number that can only be dialed using ISDN (in cases where Vodafone is otherwise preset as the provider, for example).

By default, the seizure code 88 is configured for the seizure of an outside line via ISDN. All codes can be configured later by the administrator or edited as required.

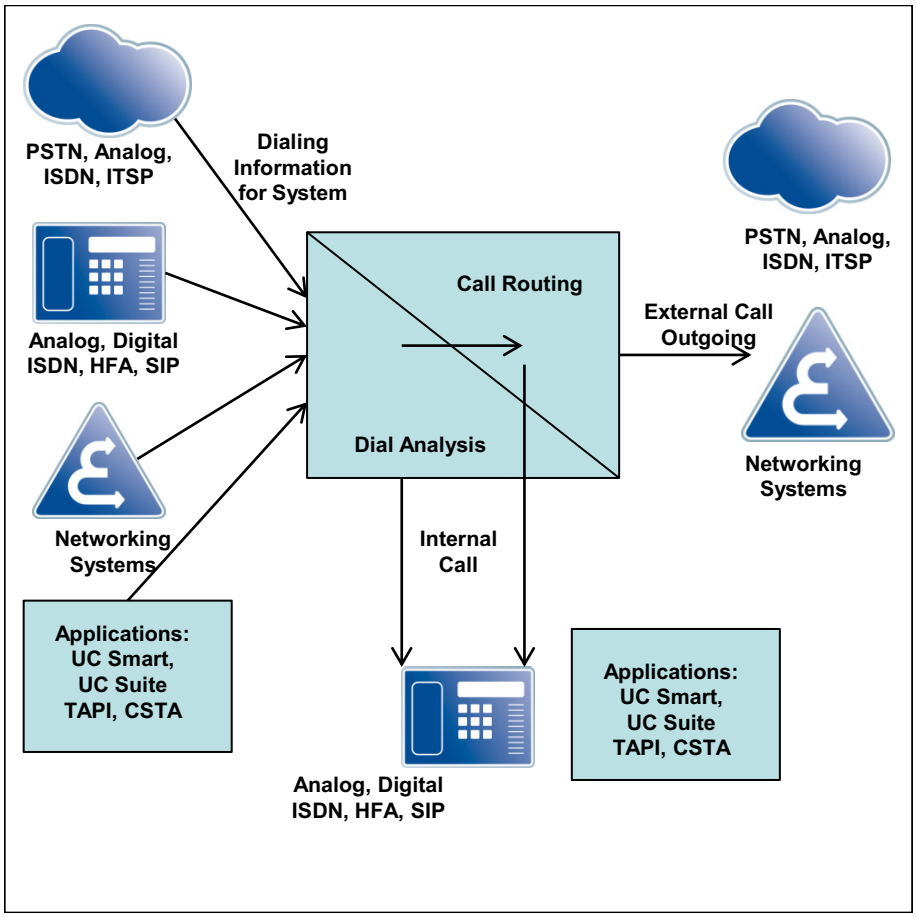
12.3 Digit Analysis and Call Routing

This section illustrates the relationship between digit analysis and call routing. It explains how the communication system analyzes call numbers dialed by subscribers, trunks and applications of various types to reach a specific destination and how the calls are routed upon completion of the digit analysis. The relevant system functions for this have already been described for the most part in the previous sections. This section describes dialing with public phone numbers within a node/network in detail.

The Digit Analysis

- of the communication system records and evaluates all dialed numbers on the basis of the configuration data
- verifies classes of services (e.g., based on classes of service for stations, station flags, day/night, allowed and denied station numbers, LCR classes of service, schedules, connection matrices, etc.).

- determines whether a number can be dialed internally or whether a line is to be seized. This applies to the dialing of internal and public call numbers as well as for network-internal call numbers.
- normalizes call numbers so that they can be dialed by the communication system. (e.g., canonical format: "+49nnn" becomes "00049nnn", where the first '0' is the main access code of the PBX)
- truncates call numbers where necessary (the leading digits of destination numbers may have to be truncated for calls with inbound trunk seizure in order to determine the DID destinations in the short format)



12.3.1 Overview of Call Routing / LCR

An incoming call is subjected to various tests in the communication system and then forwarded accordingly.

Test 1 (internal call destination?)

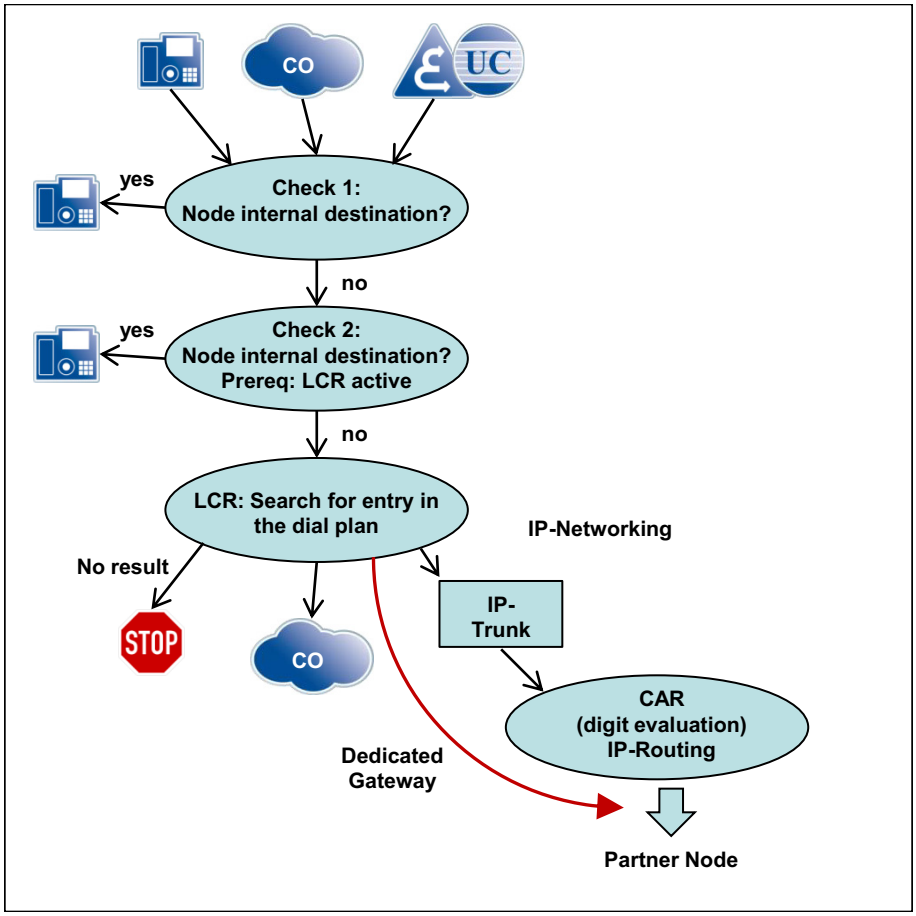
- Destinations with canonical call numbers are first converted into dialable numbers (at the station interface) or set to TON=International (ITSP interface).
- For trunk destination numbers, the call number portion of the PABX number of the corresponding route is stripped off if required.

- Internal calls are analyzed on the basis of the internal dial plan; for external calls, the dial plan for DID numbers is used.

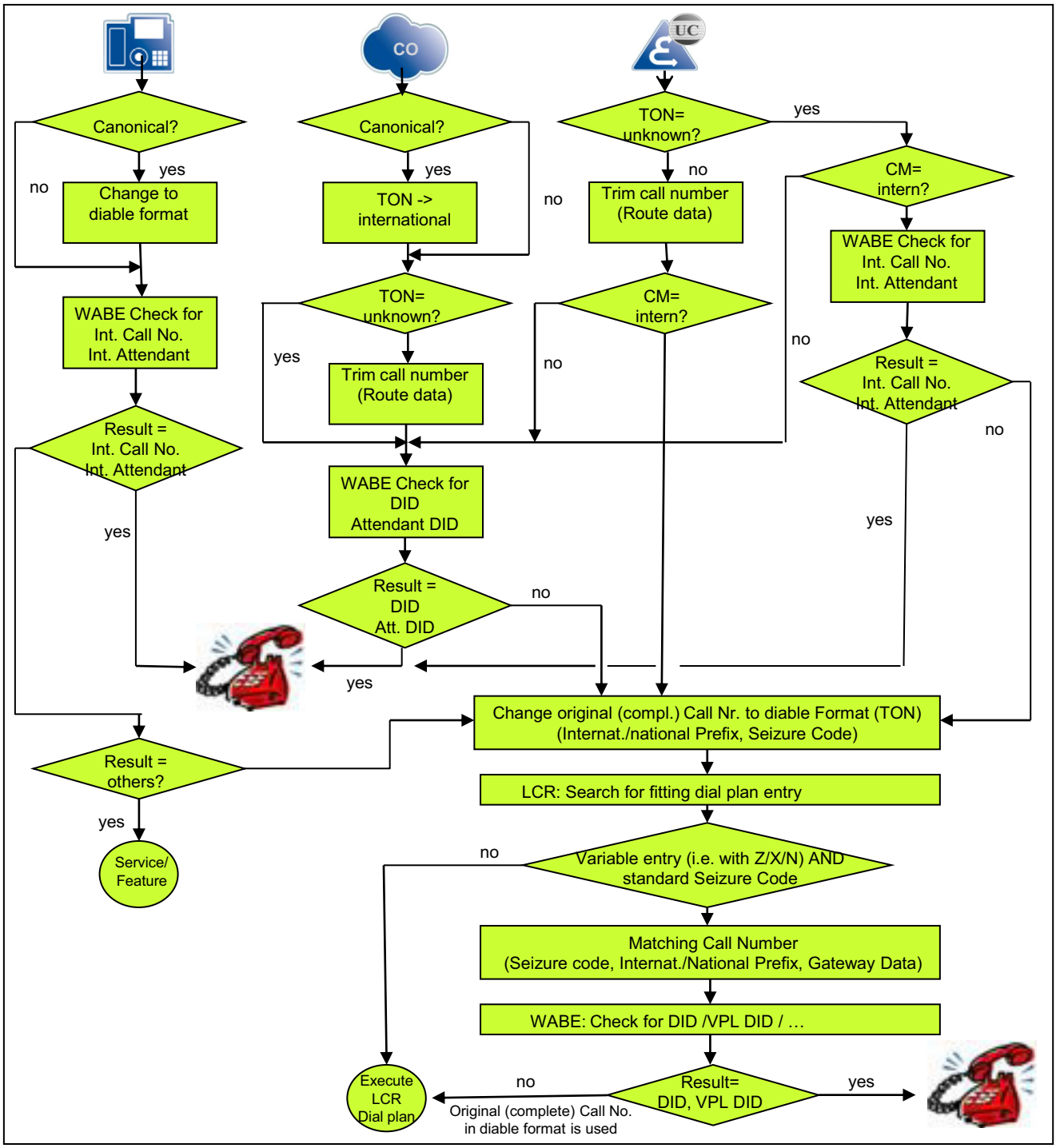
Test 2 (internal call destination?)

- Subscribers, applications, clients or other communication systems use the public format (for example, 00049nnn) for dialing destination numbers
- Precondition: the default CO access code (e.g., "0") has been set up.
- The destination number is stripped to remove the location number (gateway location) portions and evaluated based on the dial plan of the DID numbers, regardless of whether an internal or external call is involved.
- If no internal call destination is found, the dialable, unstripped (!) call number is processed in the LCR, and the call is routed further over a line accordingly.

Within an IP network, the LCR routing table parameter "Dedicated Gateway" enables the direct addressing of a node for a dialed number by bypassing the CAR digit analysis.



12.3.2 Digit Analysis Flowchart



Explanations for the flowchart:

German	English	Explanation
WABE		Digit analysis
CM	CM	Classmark identifies the caller as an external caller or (network-) internal caller
TON	TON	Type Of Number (Call number type): Unknown, Subscriber, National or International; used for both destination numbers as well as originating numbers.
DuWa	DID	DID number
TNR RNR	Int. Call No.	Internal number
Int. Attendant	VPL INT	Attendant number for internal calls
VPL DID	VPL DID	Attendant number for external calls
SERVICE	SERVICE	Service code
LCR	LCR	Least Cost Routing

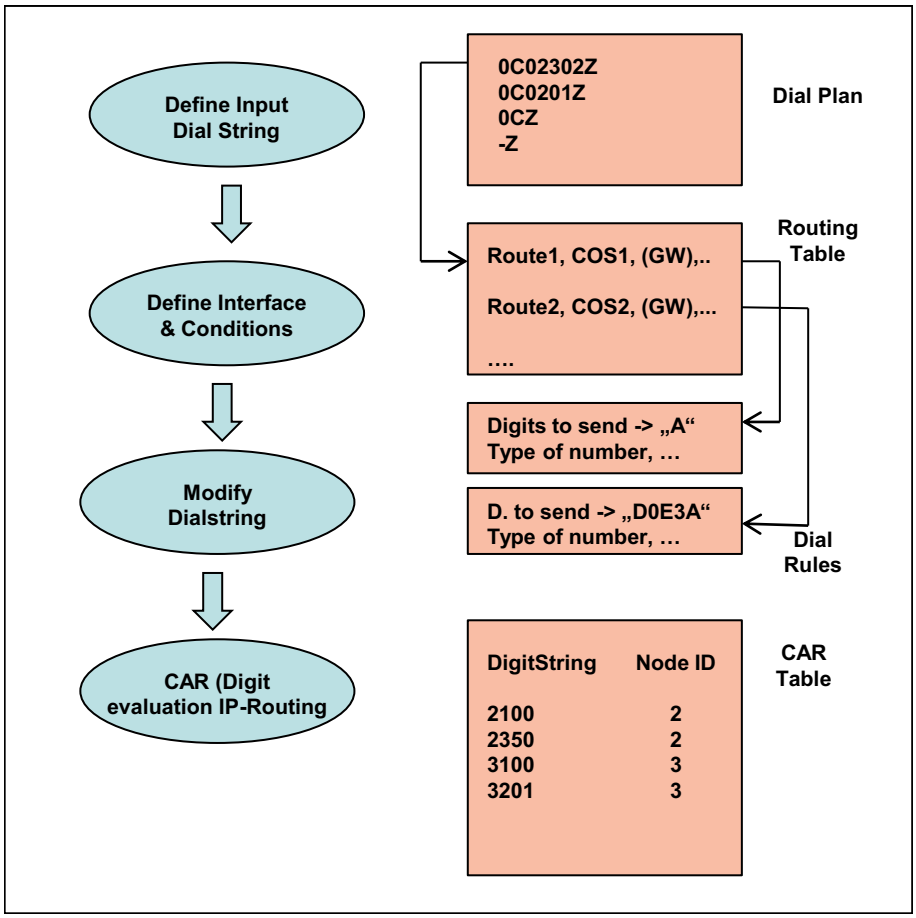
For digit analysis, UC clients are treated as subscribers controlled via CSTA.

For digit analysis, the UC Suite behaves as a SIP-Q trunk.

12.3.3 Call Routing and LCR in the Internetwork

Call routing and LCR play an important role in networking. Calls are routed by using a dial plan and dial rules. The dedicated gateway plays a special role here.

LCR Basics



If no line seizure is successful, the entries in the routing table are processed sequentially in a loop.

> ***INFO:*** -z rule must be removed from stand-alone system configuration.

LCR Entries During the Initial Setup

When the communication system is started up for the first time, a number of country-specific default values are entered in the LCR dial plan. Up to and including dial plan 35, system-side entries for emergency calls, directory assistance, special numbers, default trunk seizure for PSTN and ITSPs, for UC Suite and networking, and for international dialing formats are preset to ISDN trunks.

This range can be affected by configuration changes elsewhere (for example, by changes to the **Location number** flag. Consequently, whenever the location number is changed, it must be ensured that the default trunk seizure still works as expected (which is important when dialing public numbers).

INFO: From LCR dial plan 36 onwards, all entries are freely available.

12.3.3.1 Dedicated Gateway

The dedicated gateway is only relevant for an IP network.

Why is a dedicated gateway required?

- The CAR table of each communication system includes network-wide numbers of the other nodes and is automatically refreshed (overwritten) cyclically during updates. Consequently, CAR tables are not suitable for the permanent use of manually added entries.
- Only numbers that apply network-wide are entered, i.e., no node-specific routing is possible (e.g., "0" to the respective gateway node)

How can destinations be permanently set up through configuration?

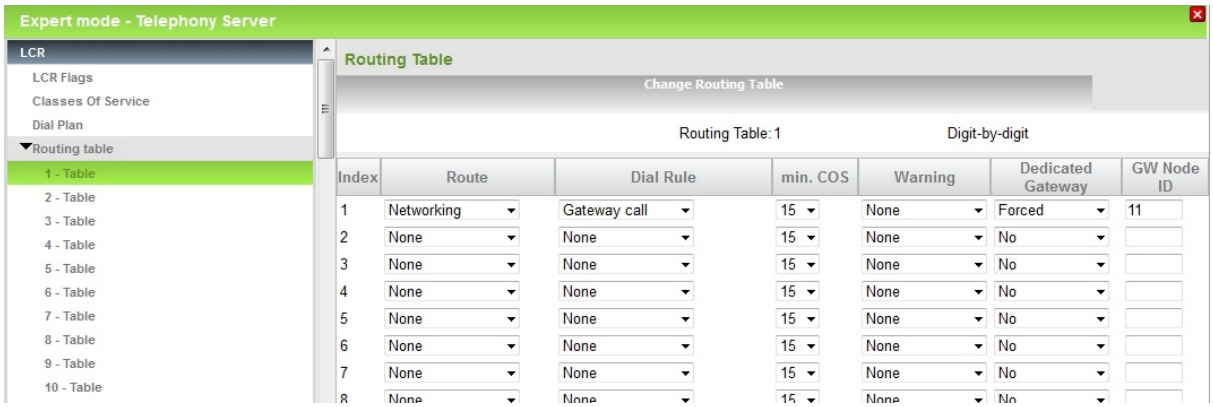
- By using direct addressing in the LCR
- The dedicated gateway directly addresses the destination node using the node ID (IP address)
- When using the dedicated gateway, CAR tables are bypassed (see previous figure).

Use cases for a dedicated gateway

Direct addressing

- of TDM gateways to seize outside lines ("0CZ")
- of TDM gateways to implement breakouts via separate codes
- of internal network nodes that are to be reached via public numbers
- of TDM gateways to which the subscribers of a multi-gateway network (to an OpenScape Business S) are assigned (e.g., subscriber 1 belongs by definition to gateway 1, and subscriber 2 belongs to gateway 2).
- of gateways and calls whose origin CANNOT be associated with a specific gateway in a mult-gateway configuration (e.g., the fax group of a UC Contact Center)

The Dedicated Gateway in the WBM



The following values can be set:

No	The station number analysis occurs on the basis of the CAR tables (no **GW node ID** required)
Forced	Routed directly to the appropriate gateway (GW node ID = n)
Multi Location	Only to be used with multi-gateway configurations: Based on the multi-gateway configuration of the OpenScape Business S subscribers, the communication system knows the assignment to their respective gateways and can selectively route outbound calls to the appropriate gateway. In the **Multi Location** configuration, the GW node ID is used only if no gateway can be identified through the assignment of the subscriber (default).

12.3.4 Scenarios: Digit Analysis and Call Routing

In order to illustrate the above processes in the communication system, the dependencies and required configuration parameters are described here on the basis of specific scenarios. The presented scenarios may build on one another, depending on the use cases involved.

Single System

1. Subscriber A calls subscriber B via an internal phone number
2. Subscriber A calls subscriber B via a public phone number
3. Subscriber A calls an external station via the CO
4. ISDN trunk calls subscriber A
5. Special configurations and their corresponding effects
   2 CO routes

Networked system as a subsystem (no CO trunk)

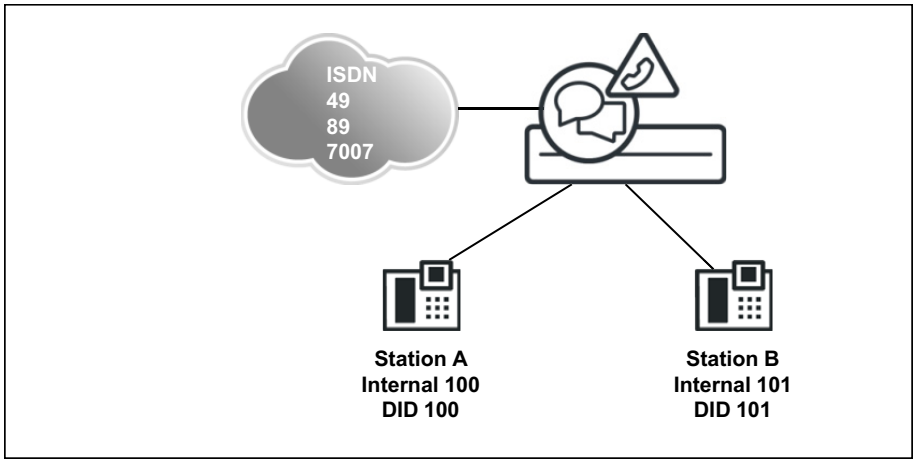
1. Subscriber A Calls Subscriber C via an Internal Phone Number
2. Subscriber A calls subscriber C via a public number in the internetwork

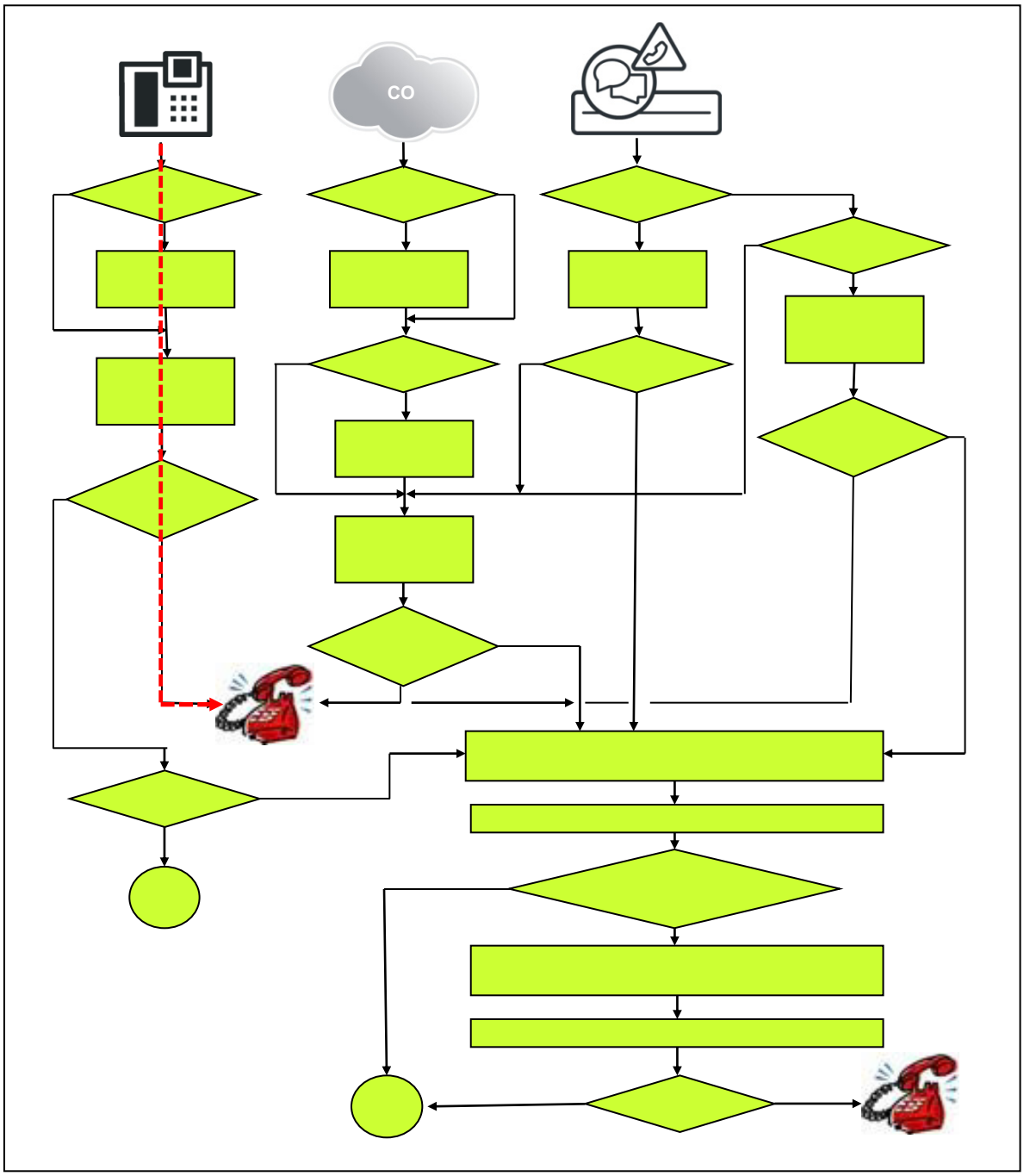
3. ISDN trunk calls subscriber C

Internetwork with multi-gateway

1. ISDN trunk gateway 1 calls subscriber D
2. Subscriber D calls external station via the CO

12.3.4.1 Subscriber A Calls Subscriber B via an Internal Phone Number

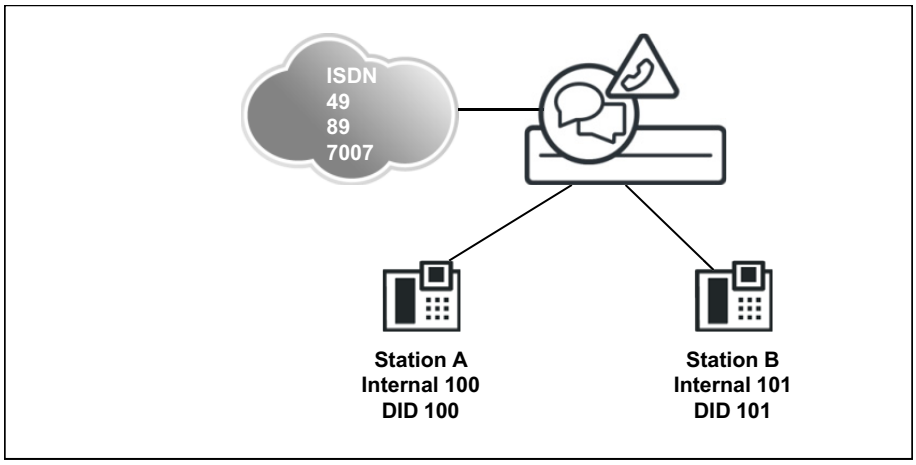




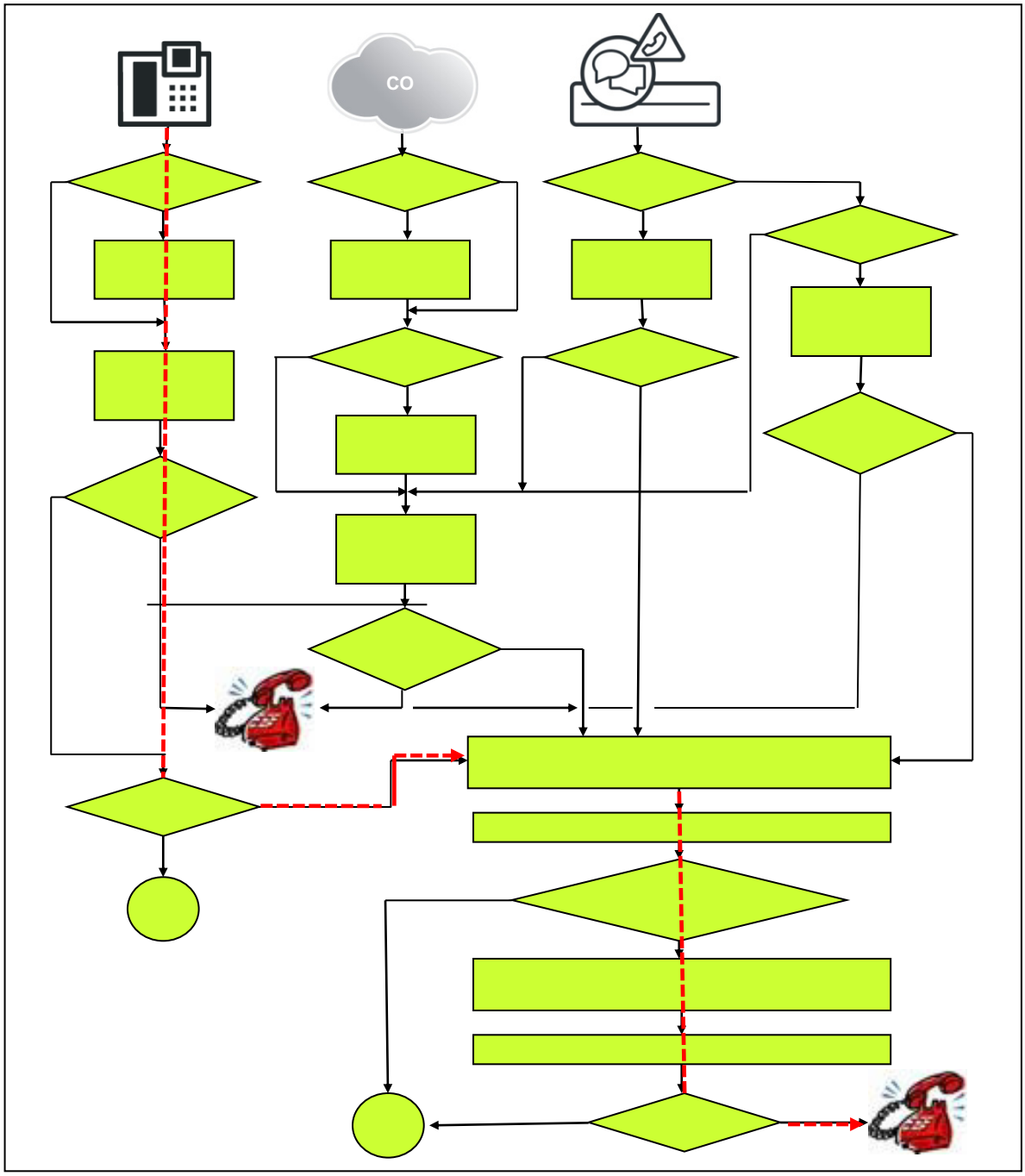
Configuration of the two internal phone numbers

	Box	Slot	CallNo	Name	DID	Type
	1	1	100	-	100	System Client
	1	1	101	-	101	System Client

12.3.4.2 Subscriber A calls subscriber B via a public phone number



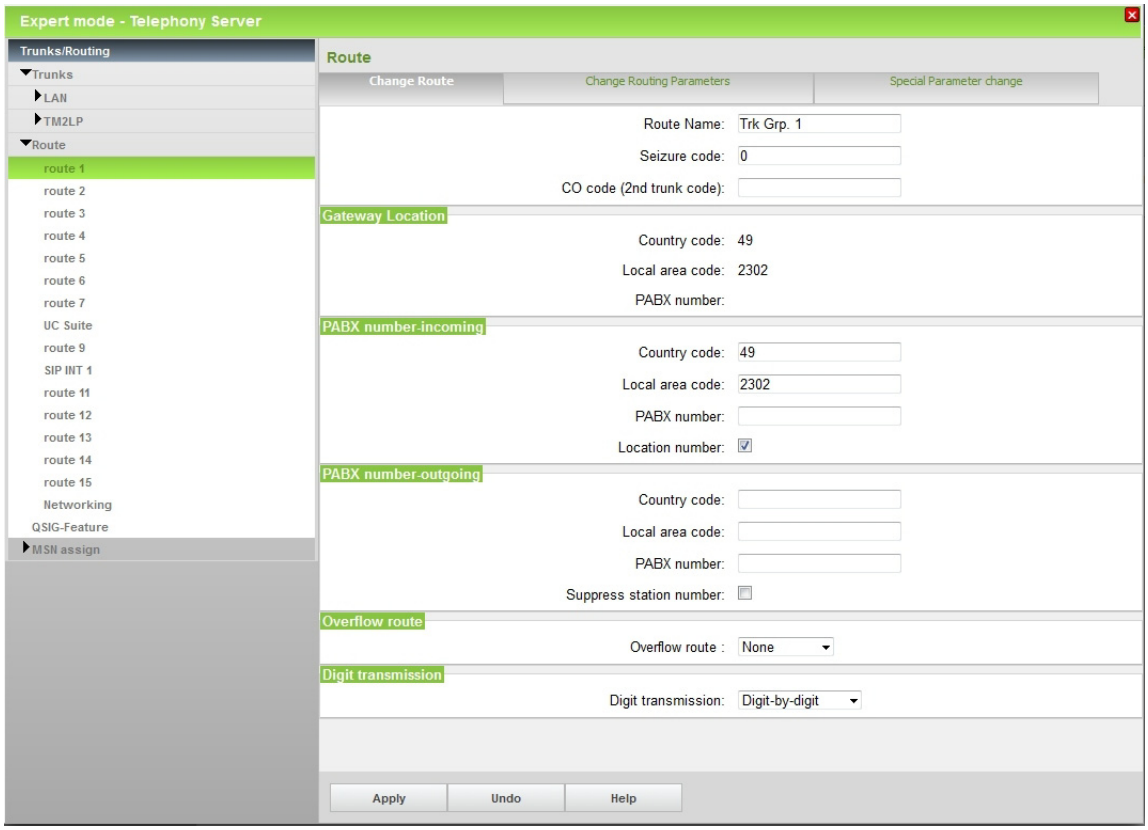
The call is delivered internally in the system, since the destination number is a DID station of the own system.



Configuration

	Box	Slot	CallNo	Name	DID	Type
	1	1	100	-	100	System Client
	1	1	101	-	101	System Client

Once the destination number has been stripped using the gateway location, the stripped call number is used to search for a destination in the DID dial plan.



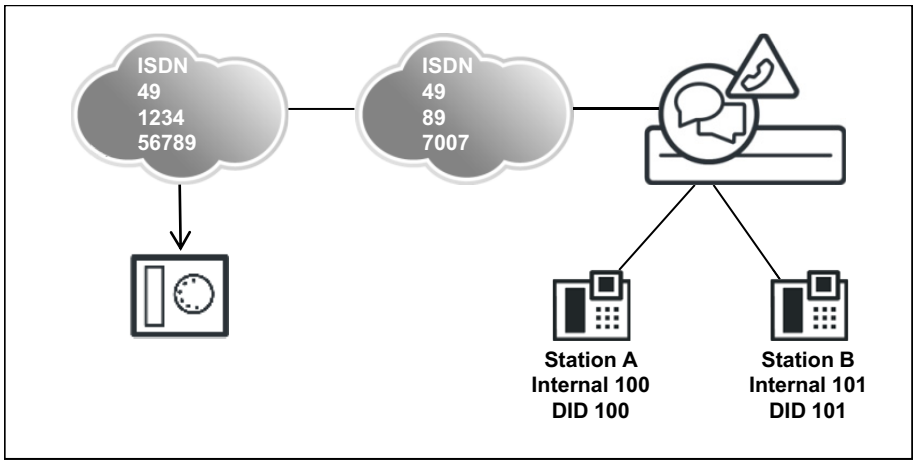
Dependencies of the "Location Number" (Gateway Location)

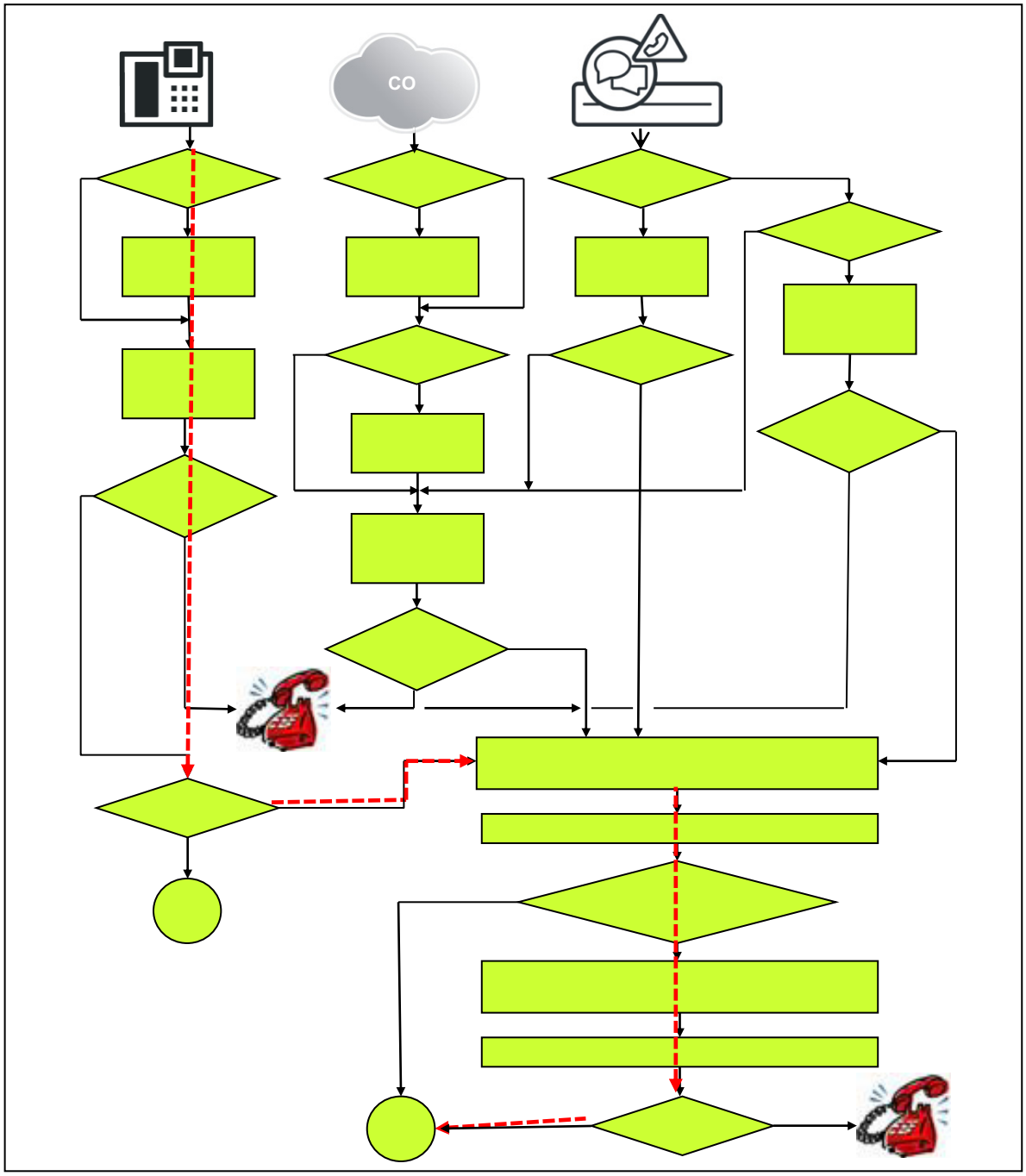
The location number (gateway location) is analyzed on dialing based on the public phone number. If the relevant portions of the dialed number matches this number, the DID table is analyzed and, if a match is found, the appropriate internal destination is dialed (without seizing a trunk!). By setting the Location Number flag, the location data is taken over automatically from the appropriate routing data (PABX number, incoming) and does not need to be changed in standard scenarios.

Consequently, only valid numbers assigned to this system should be entered in the DID tables; otherwise, masking effects could occur with numbers in the public network. For example, in some cases, an internal number identified by an invalid DID could be called even though a call via a trunk to an external destination was intended.

Changes to the "Location Number" flag may affect the preset default LCR entries. Whenever the location number is changed, it must be ensured that the default trunk seizure still works as expected. This is important when dialing public numbers.

12.3.4.3 Subscriber A calls an external station via the CO

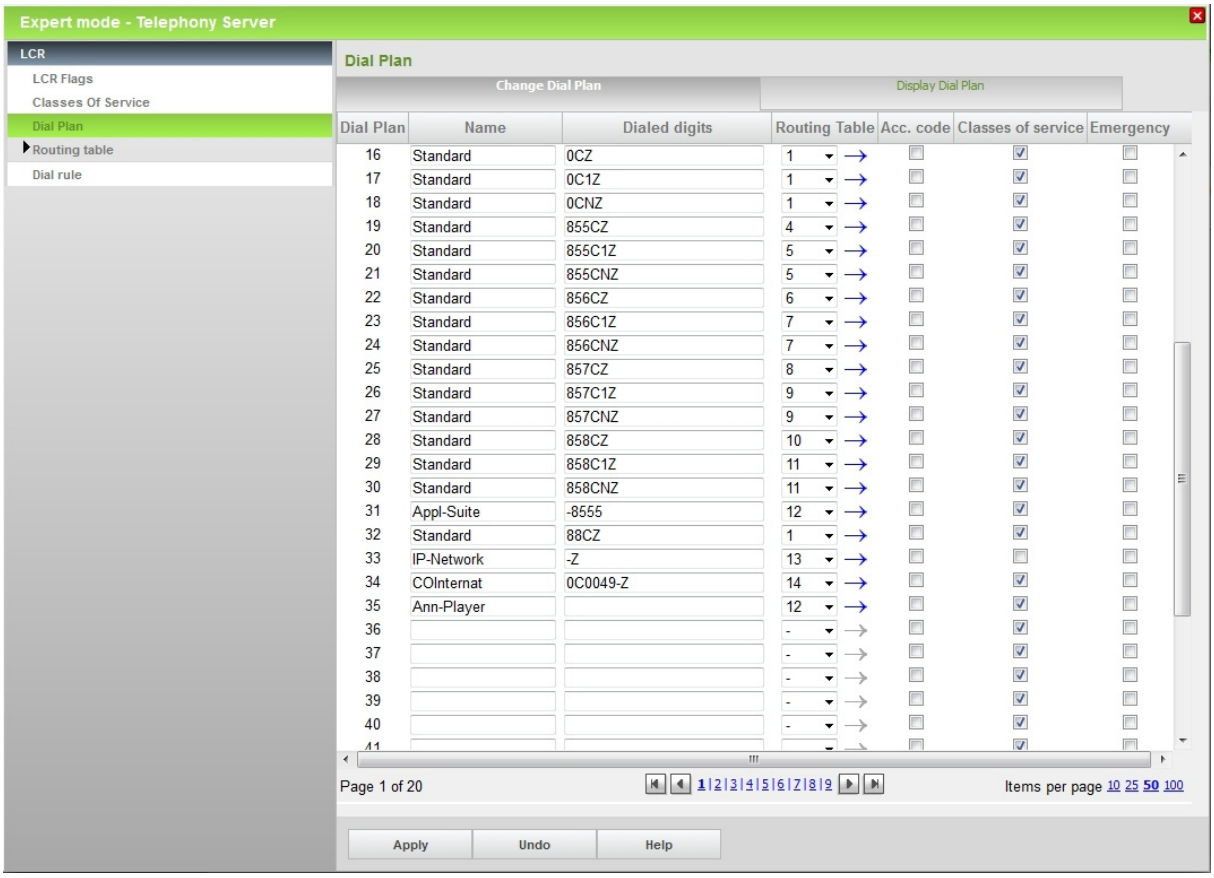




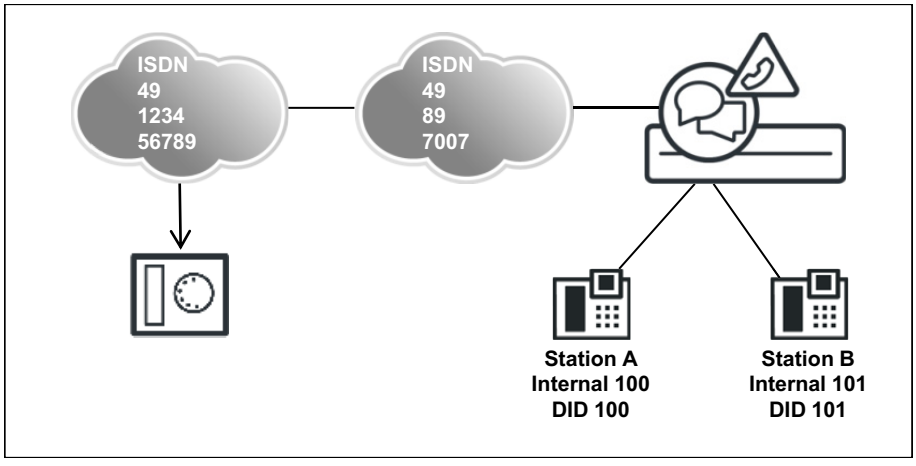
The call is routed via LCR because the destination is not in the own communication system.

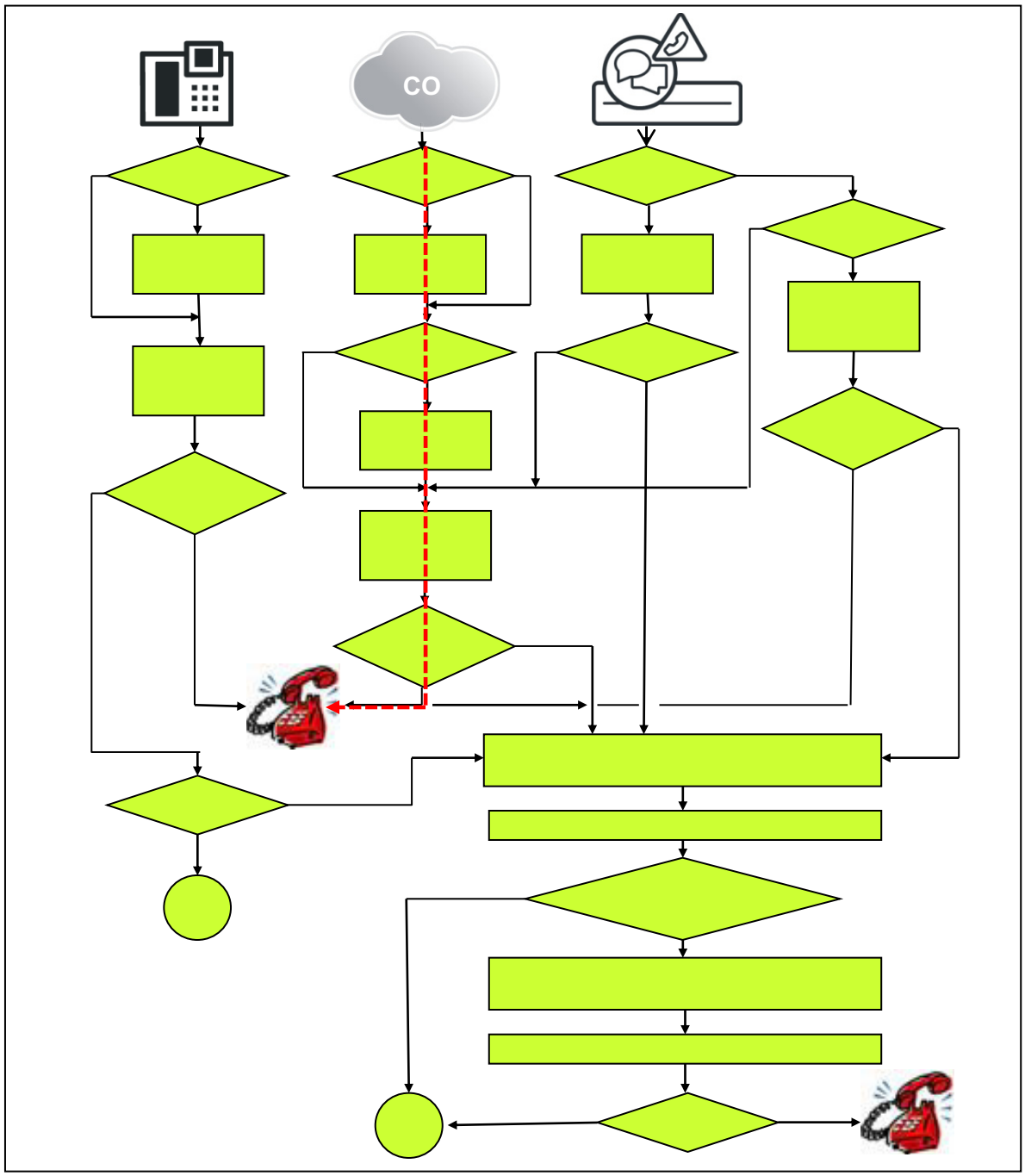
In addition to the data of the previous scenario "Subscriber A calls subscriber B via a public phone number", a suitable dial plan entry to seize the CO trunk (e.g., "0CZ") must be present in the LCR.

The LCR route table and the dial plan must be set up accordingly.



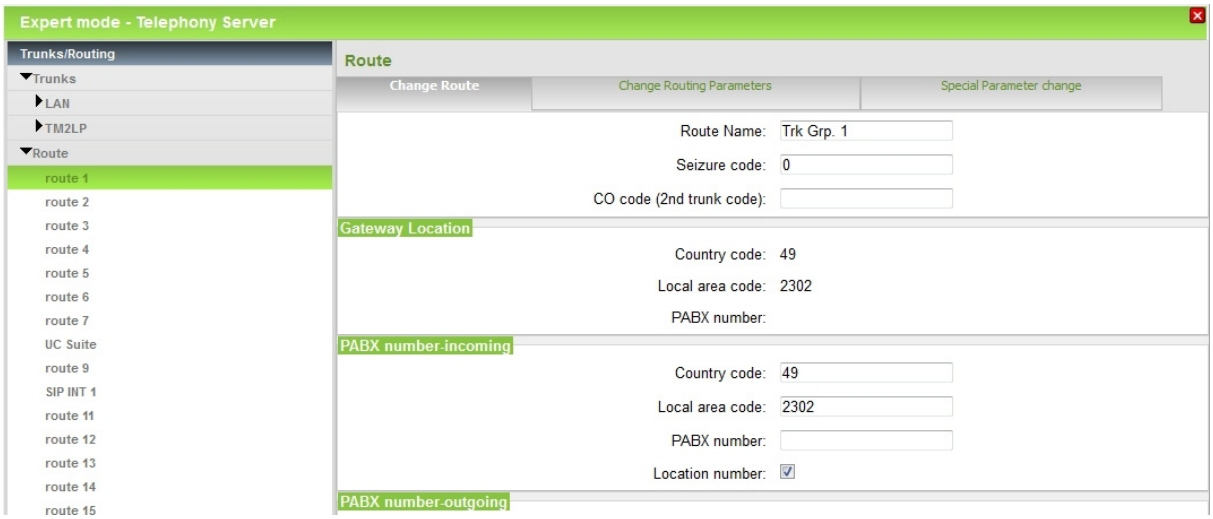
12.3.4.4 ISDN trunk calls subscriber A





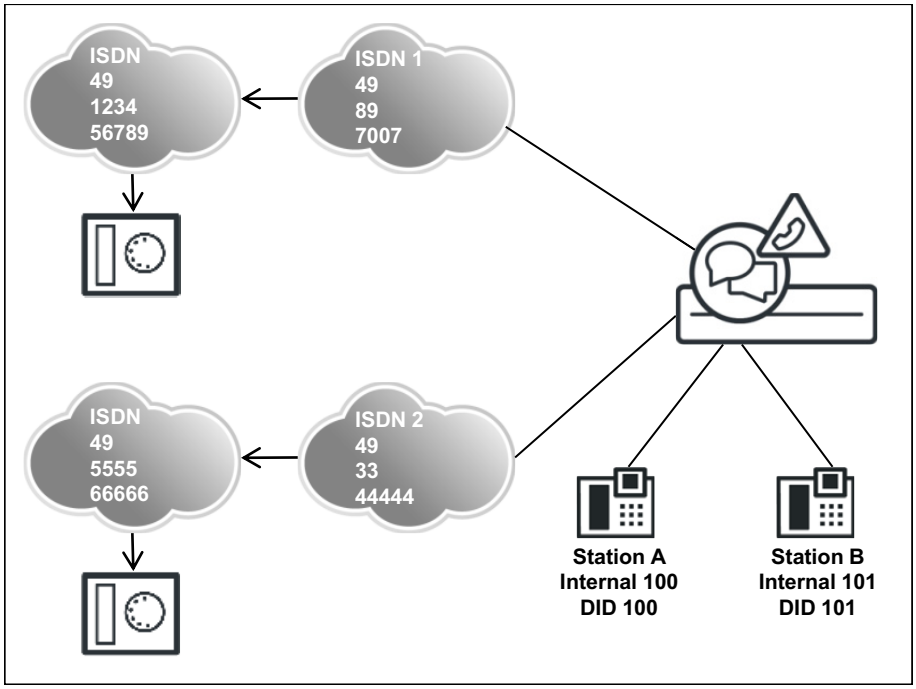
For an incoming call over an ISDN trunk, the route is stripped off from the destination number based on the configuration data of the PABX number, incoming. Using the remainder of the destination number (DID), a search for a destination is then performed in the DID dial plan.

The parameters of the gateway location and the **Location Number** flag play no role in this scenario.

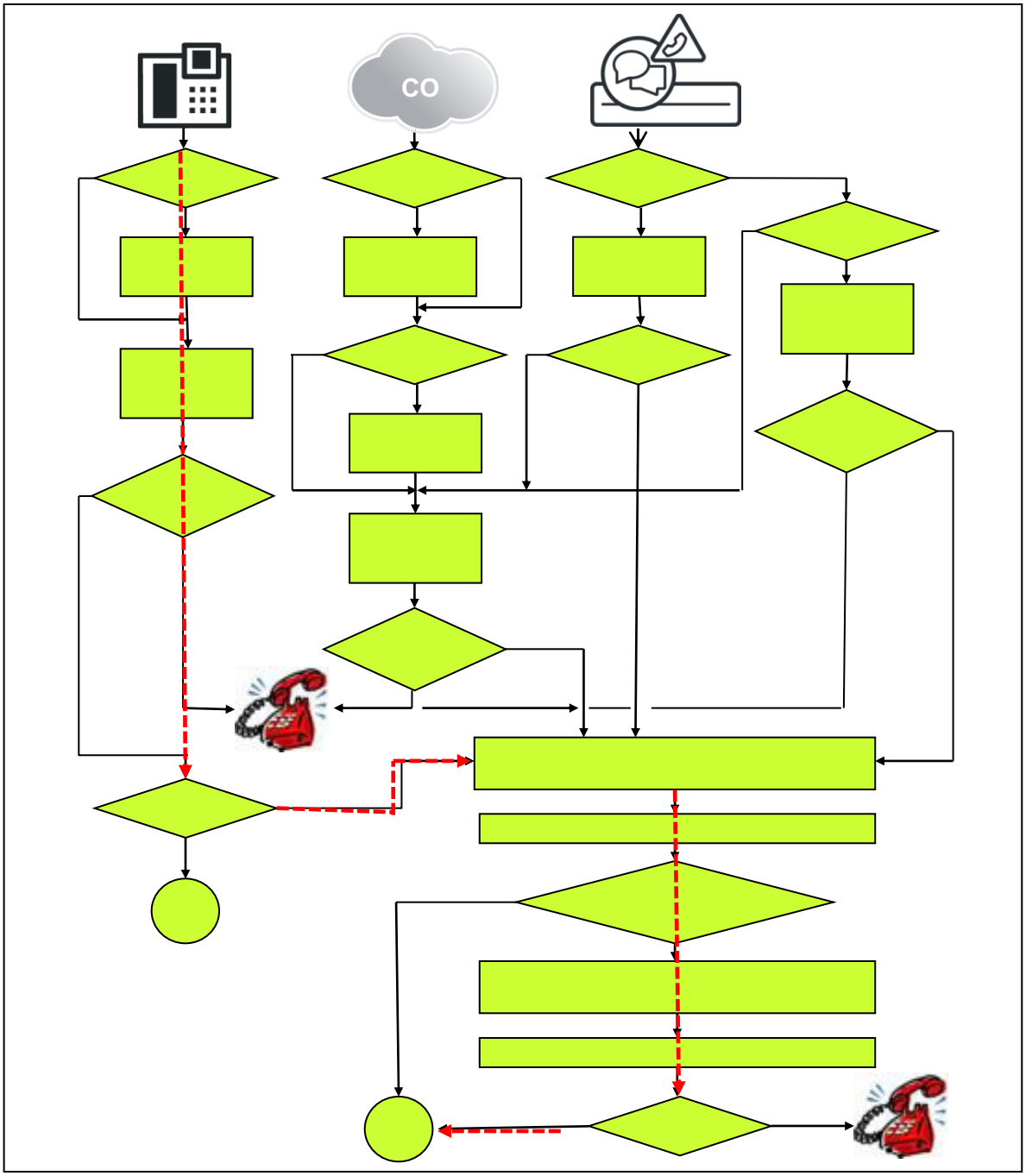


12.3.4.5 Special Configurations

Special configurations and their corresponding effects: 2 CO routes



Subscriber A calls external subscriber via the CO trunk 1 or 2



Example:

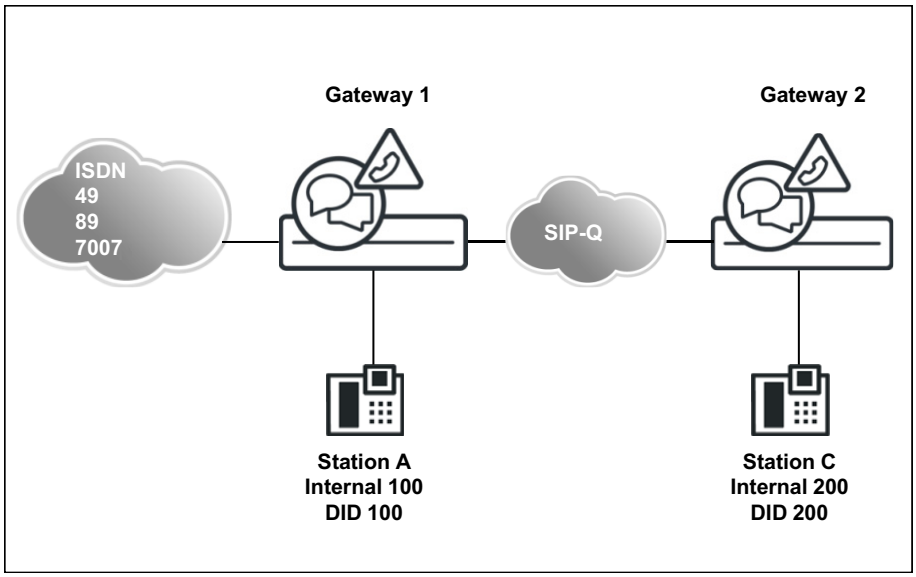
- A customer wants to use a standard ISDN 1 connection. This is set up as the location number.
- A second ISDN 2 connection is additively used for special applications.

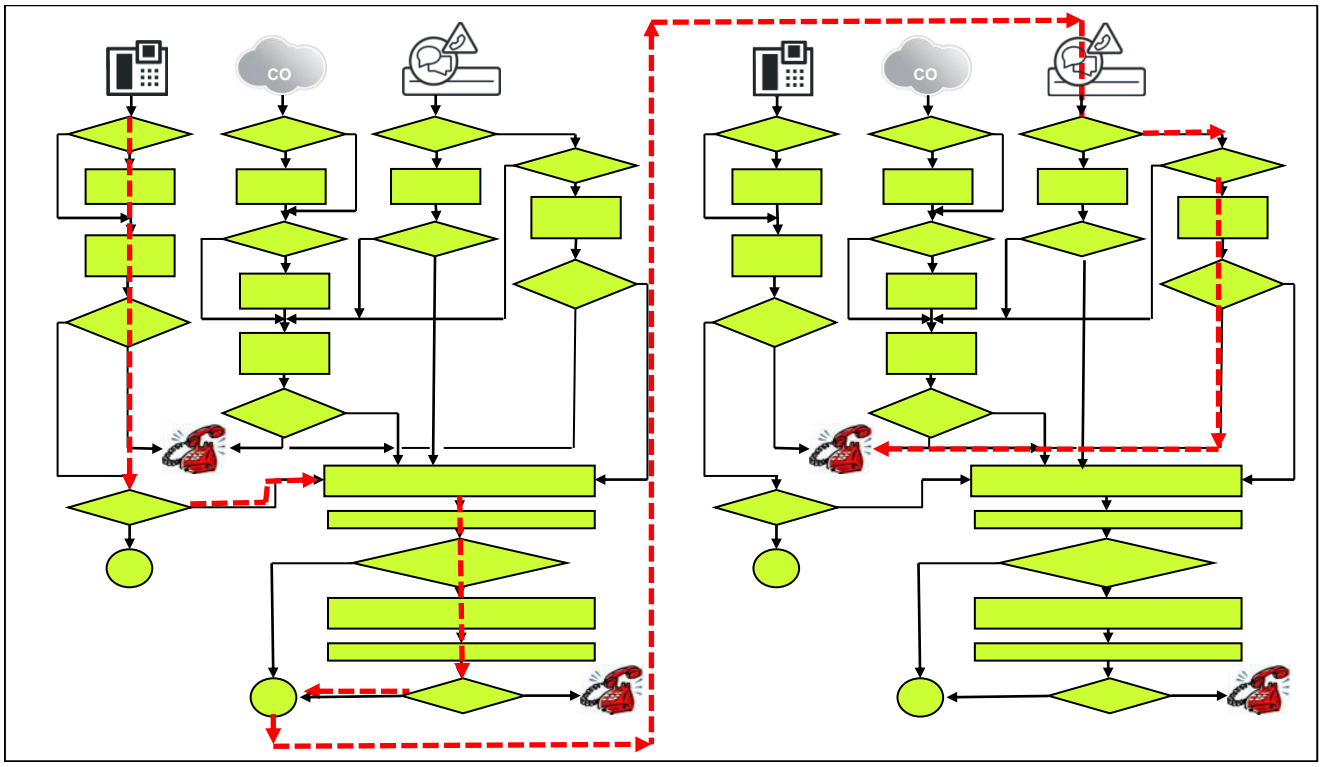
Notes and limitations:

- Only ONE CO trunk (ISDN 1 = location of the system) is fully supported, i.e., no multi-tenant configuration (tenant services) with equal trunk access rights can be configured.
- The additive ISDN 2 CO trunk can be used for Basic Call (incoming/outgoing).
- In complex switching scenarios, the correct representation of the call number may not be guaranteed under some circumstance.
- For connected applications, only the location number is supported, as is the case when dialing internal destinations with public numbers.
- The configuration with respect to the routing configuration and LCR can be derived from the previous examples.

12.3.4.6 Subscriber A Calls Subscriber C via an Internal Phone Number

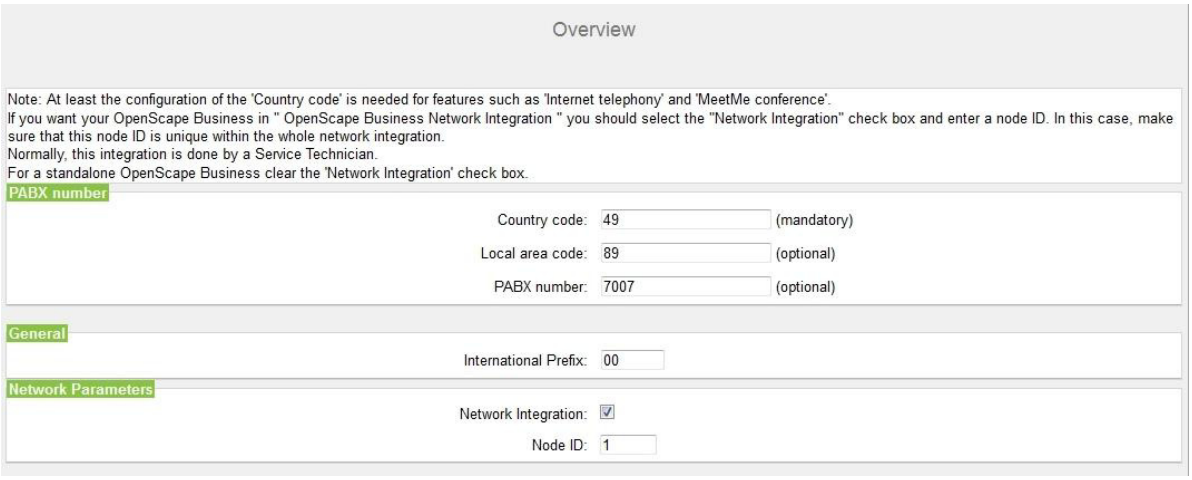
Networked communication system as a subsystem (no CO trunk)





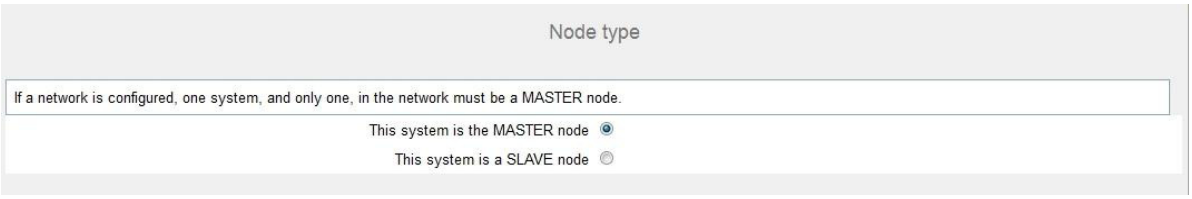
Prerequisites for standalone systems before networking:

- Both communication systems have unique IP addresses and are integrated in the IP network of the customer.
- Both communication systems can be administered in the customer network using WBM.
- A unique node ID for networking was assigned in the basic installation for each communication system (e.g., System 1 = Node ID 1 and System 2 = NID) 2).
- Defining the numbering in the basic installation of the systems 1 and 2: The numbering of the standalone systems must take the closed numbering in the future internetwork into account.
- This example assumes that closed numbering is being used (mandatory when using UC Suite!); the configuration occurs via the Network wizard. With open numbering (possible for UC Smart), the Network wizard is not used. It is also not used with a connection of OpenScape Voice and OpenScape 4000.



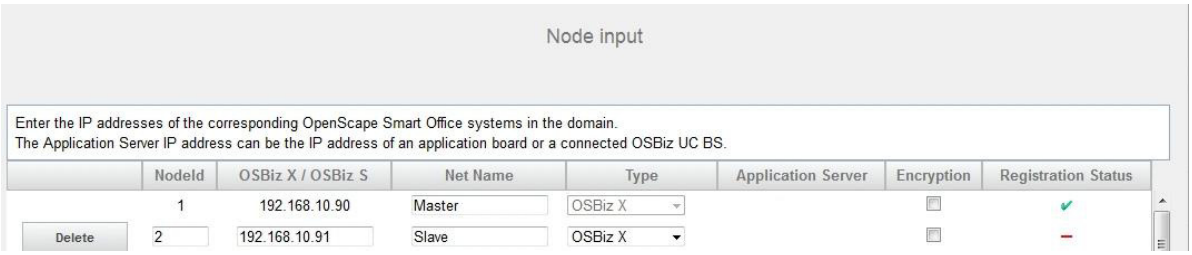
Start the Network wizard in system 1. This system (this node) is declared as the master). The master has several central functions in the network (e.g., administration, license management with centralized licensing, network-wide CSP).

If an OpenScape Business S is located in the internetwork, it should be preferentially declared as the master (for bandwidth and performance reasons).



The IP addresses are entered for each node so that the systems can find one another independently after the administration. The OpenScape Business systems are entered **Type**.

This dialog must also be completed for node 2 (slave).



Upon successful configuration, the two systems (nodes) synchronize their phone numbers and enter the call numbers of the other node into the CAR table.

With the creation of the CAR tables, network-wide telephony with internal numbers is possible. UC Suite is also launched network-wide. Further steps for the complete startup of the network are presented in the other scenarios.

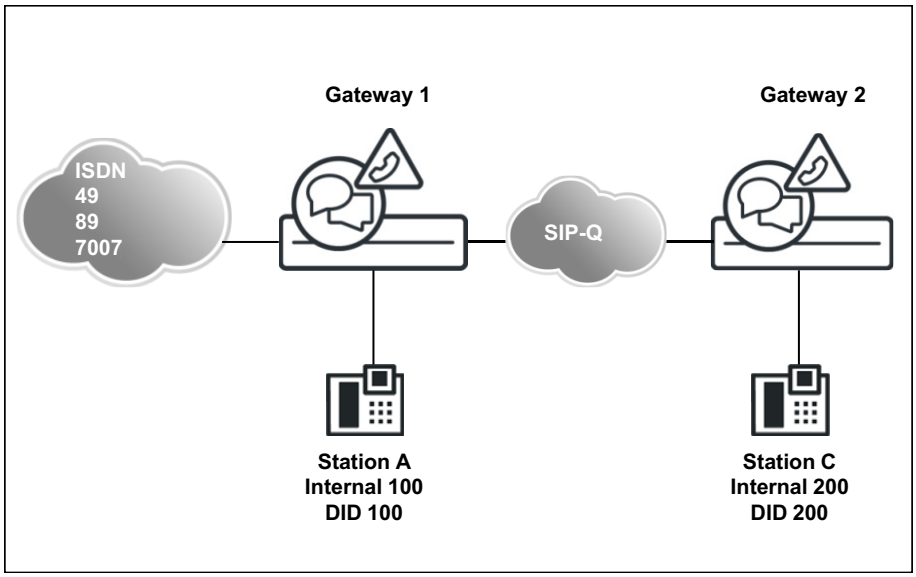
CAR entries are controlled via **Expert Mode** > **Voice Gateway** > **Networking** > **Routing**.

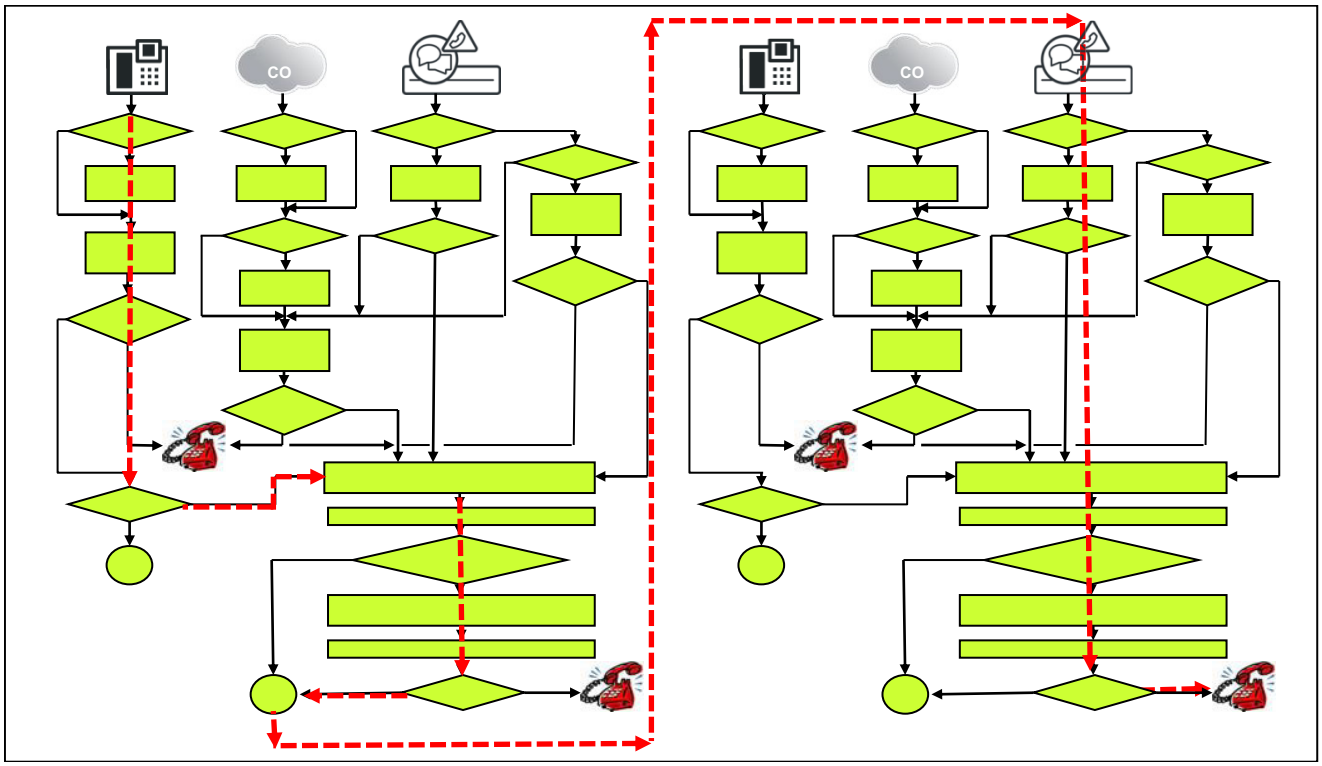
An overview of the automatic synchronization in the internetwork can be seen in the WBM (sync status).

Additional network nodes can now be administered with direct access under the menu item **Networking** in the navigation bar.

12.3.4.7 Subscriber A calls subscriber C via a public number in the internetwork

Networked communication system as a subsystem





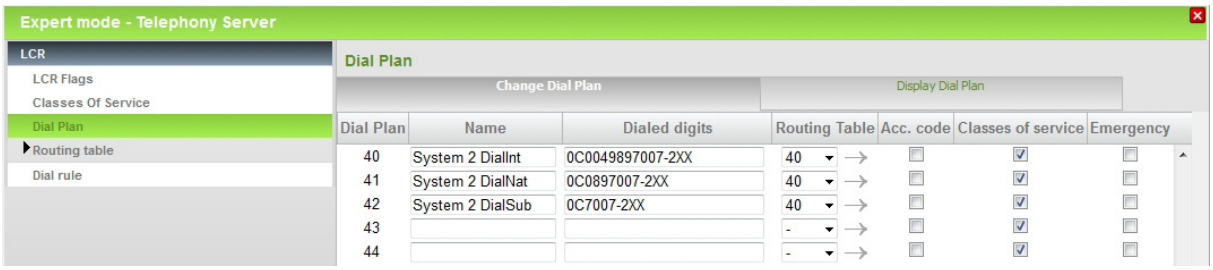
Special features of this scenario:

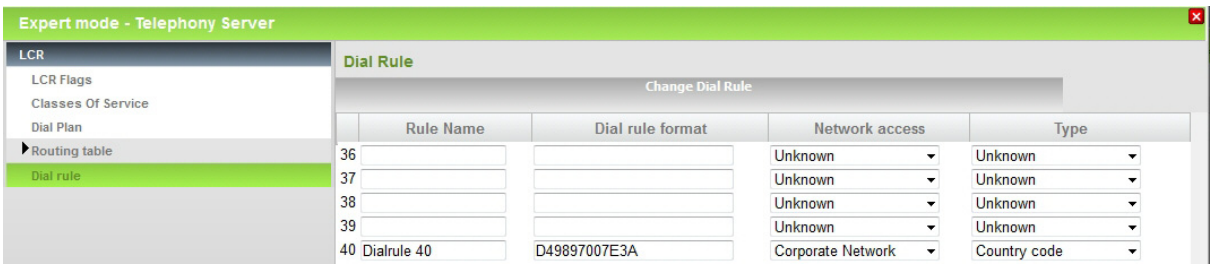
- System 1 detects that the destination phone number does not belong to the own system. A further search is thus performed in the LCR. The dedicated gateway in the LCR of system 1 must be used for the direct addressing of the node ID of system 2. The destination number is not an internal number of the network (it would otherwise be in the CAR table), but a public phone number, which can be dialed by the subscriber in three different lengths:
  Long = 00049897007nnn
  Medium = 00897007nnn
  Short = 07007nnn
  This example assumes that all 2xx DID numbers are subscribers in system 2.

  NOTICE: The dial plan entries must be configured precisely so that ALL numbers involved really belong to the subnode (internetwork). This may require a larger number of entries in a dial plan with peculiarities, e.g., when a shared trunk connection or an MSN configuration is involved.

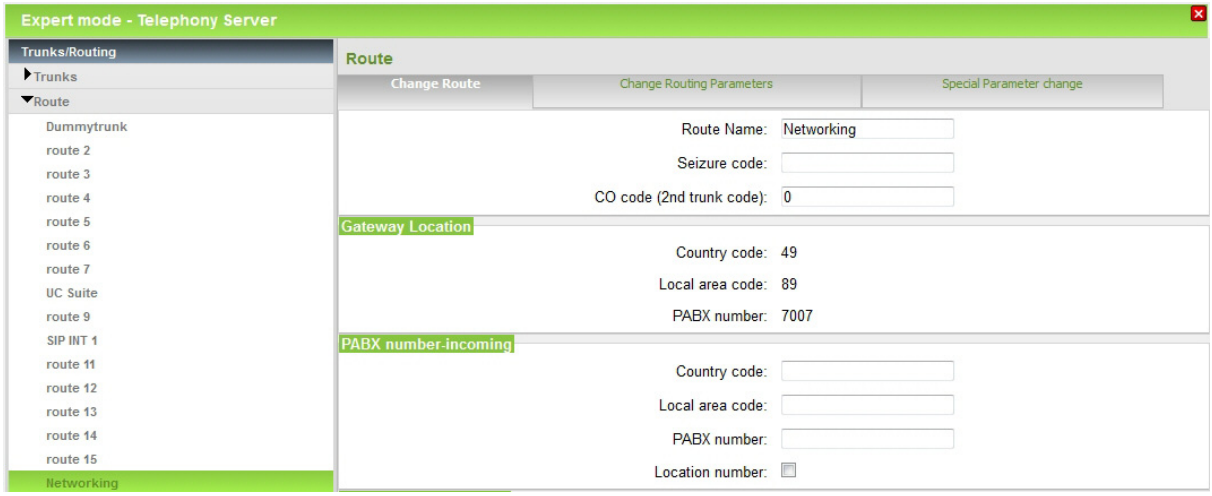
- In node 2, a location number is entered with the location data of node 1 (gateway) using a "dummy CO trunk" so that the destination number from the public dialing can be stripped before searching for an internal destination in node 2.

Configuration of Node 1, Setup in the LCR via Dedicated Gateway



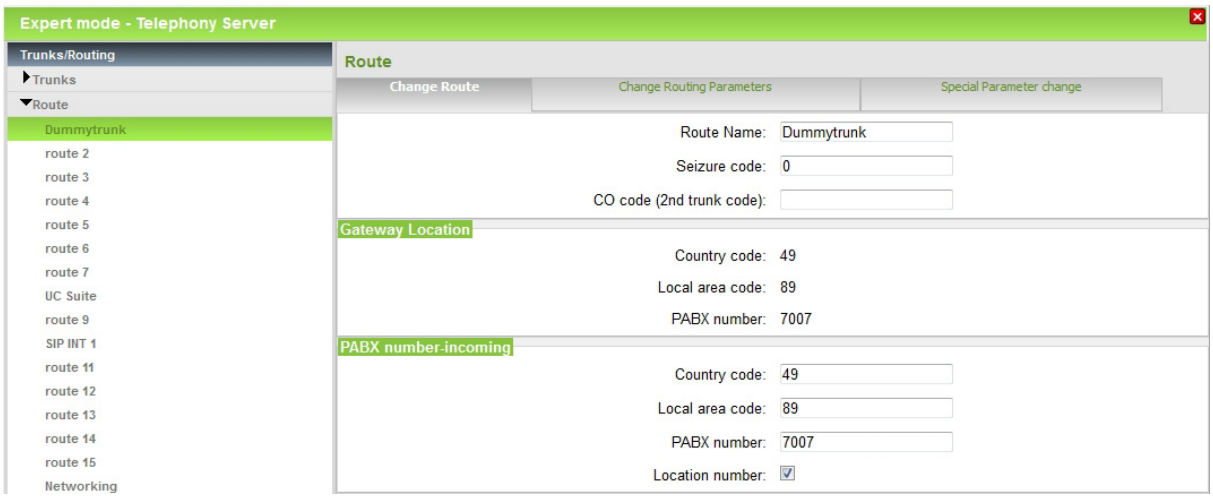


Configuration of Node 2, Setup of the "Networking" Route



The route type **PABX** must be entered on the **Change Routing Parameters** tab.

Configuration of Node 2, Setup of the Location Number at the "Dummy CO Trunk"



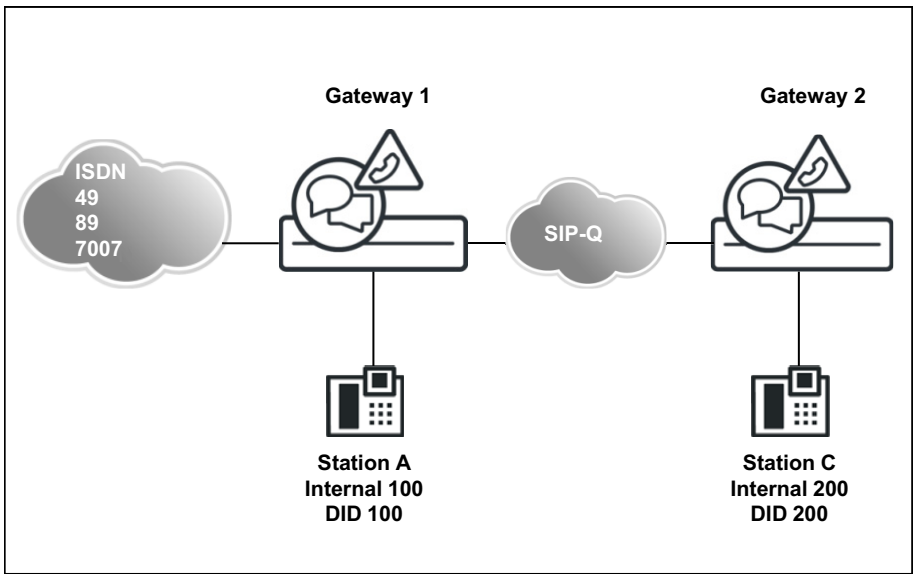
The route type **CO** must be entered on the **Change Routing Parameters** tab.

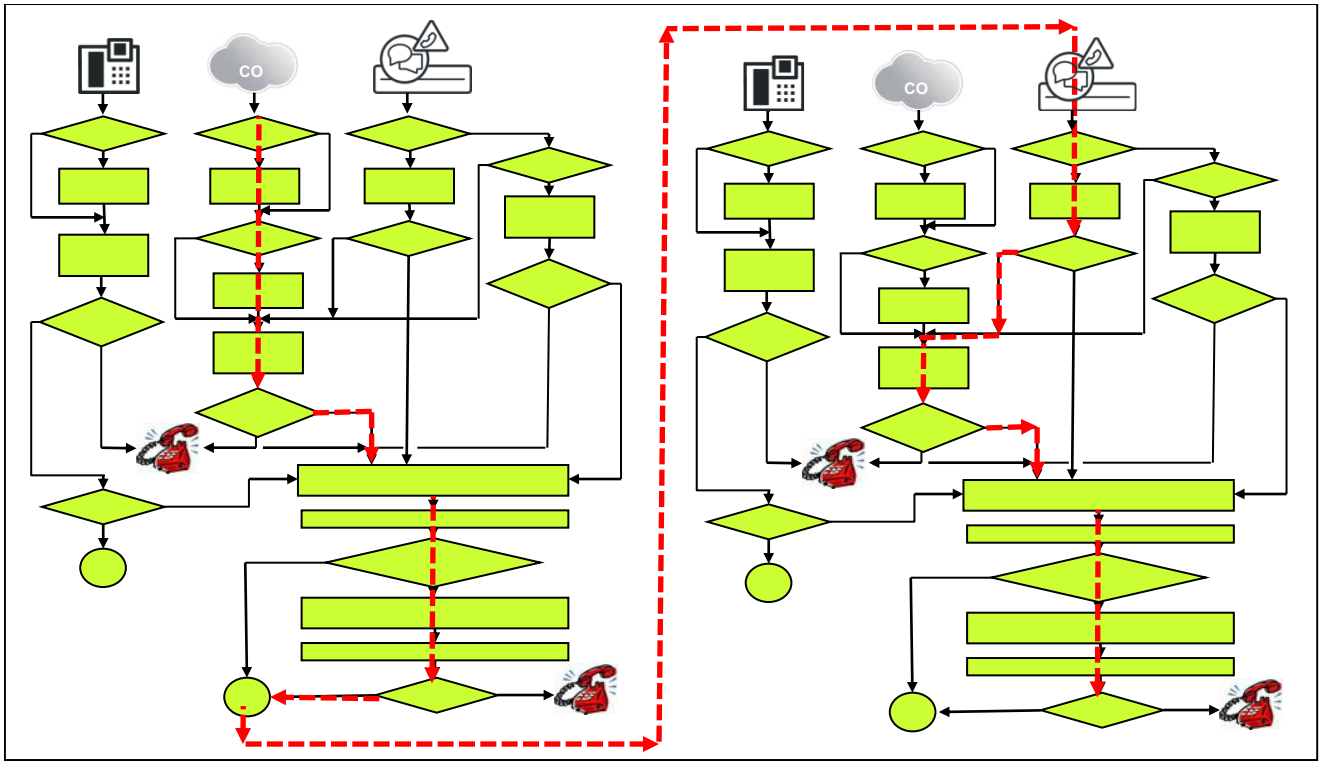
Configuration of Node 2, Setup in the LCR via Dedicated Gateway

In node 2, all public numbers that do not belong to their own node are routed to node 1 (default dialing, e.g., 0CZ)

12.3.4.8 ISDN trunk calls subscriber C

Networked System as a Subsystem





Example: Incoming call with destination number with TON = subscriber

Special Features of this Configuration

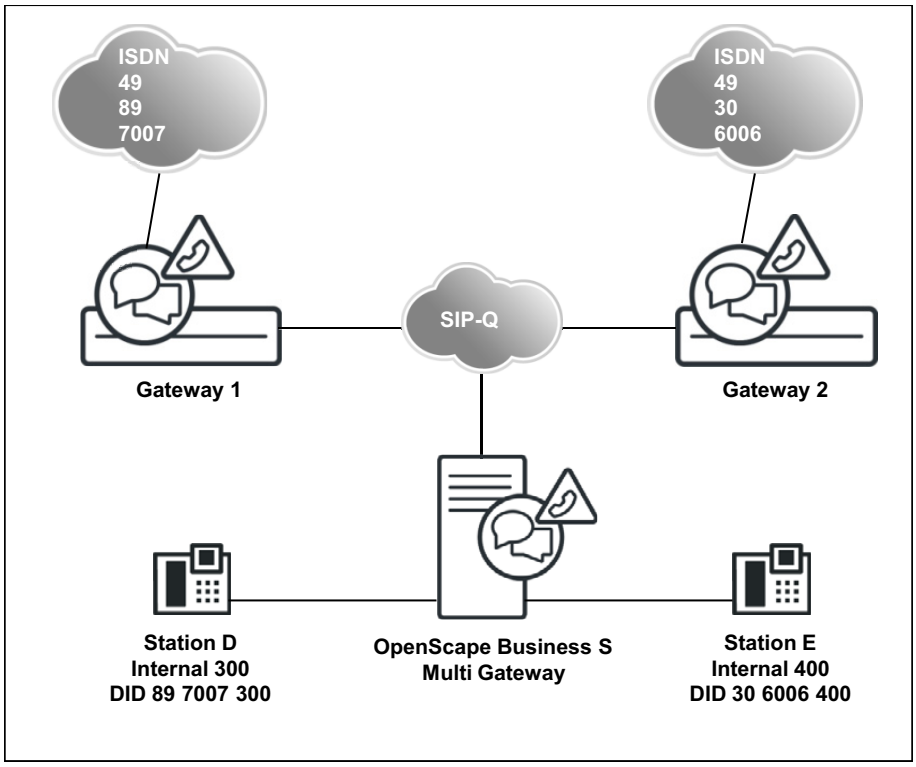
- Node 1 must be set up as described in the previous scenario.
  The addressing of node 2 occurs with the public telephone number in both cases, regardless of whether the origin of the connection is located in node 1 (subscriber of system 1) or in the public network.

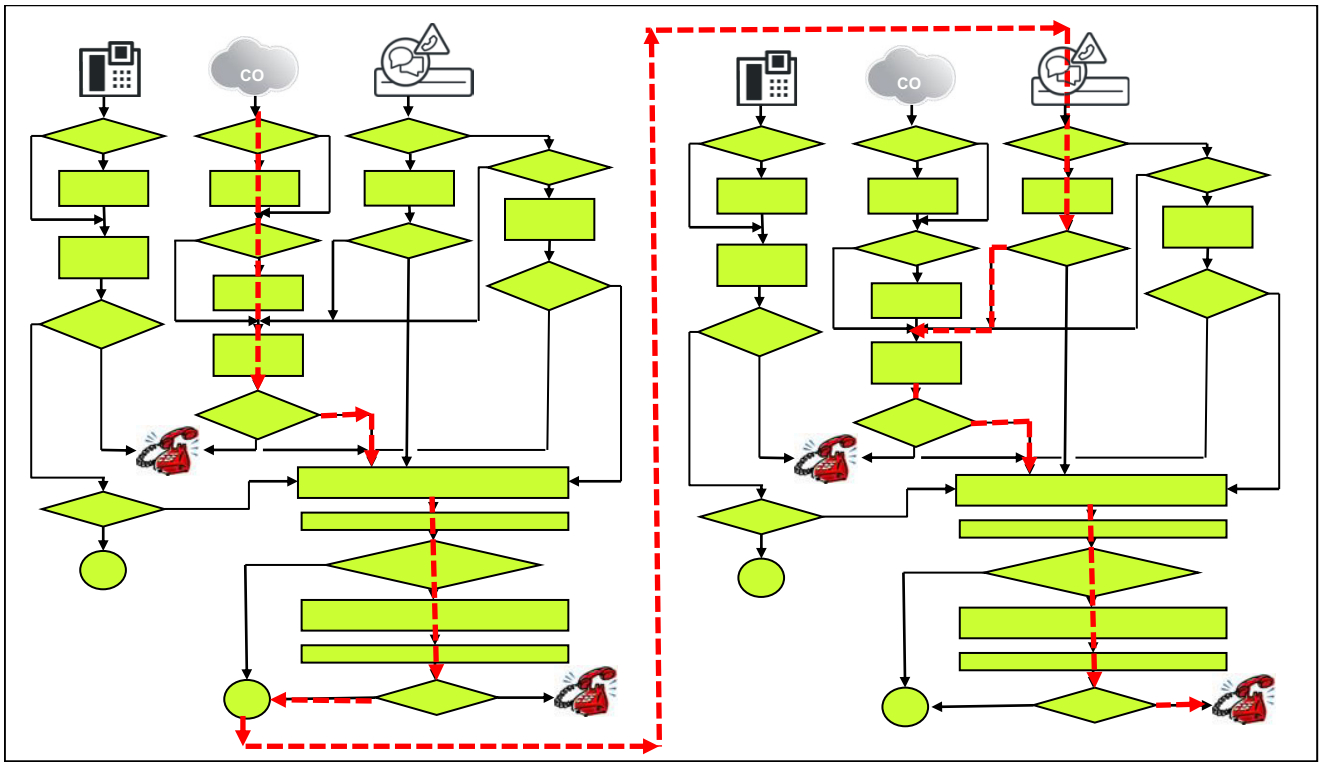
INFO: The dial plan entries must be configured precisely so that ALL numbers involved really belong to the subnode (internetwork). This may require a larger number of entries in a dial plan with peculiarities, e.g., when a shared trunk connection or an MSN configuration is involved.

- Node 2 must likewise be set up as described in the previous scenario.

12.3.4.9 ISDN Trunk Gateway 1 Calls Subscriber D

Networked system in a multi-gateway configuration





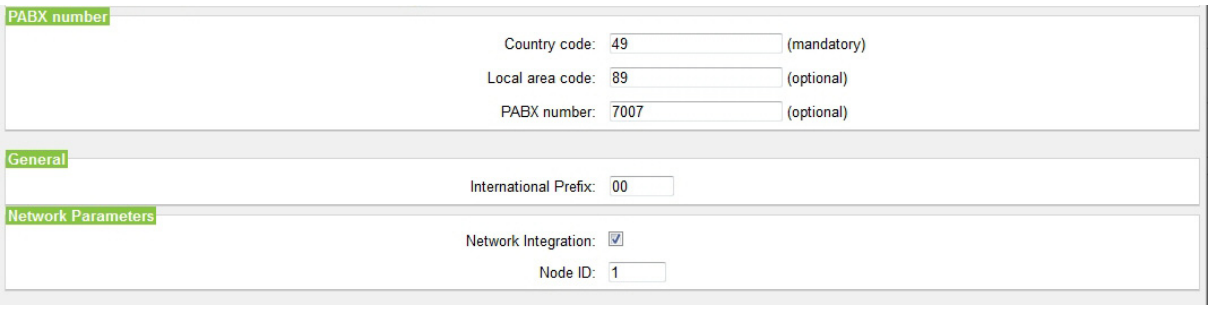
Example: Incoming call with destination number with TON = subscriber

Configuration

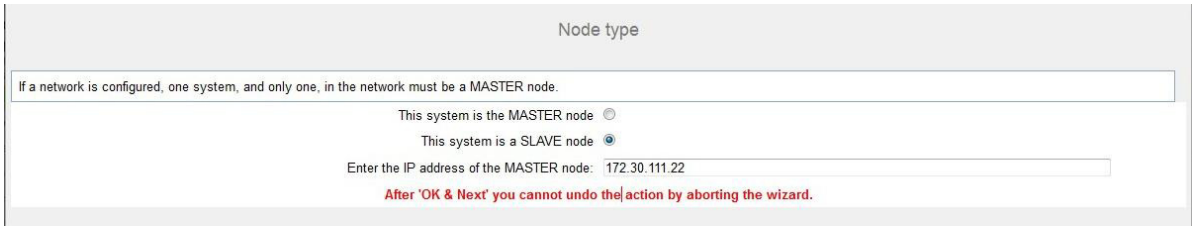
Special features in this scenario:

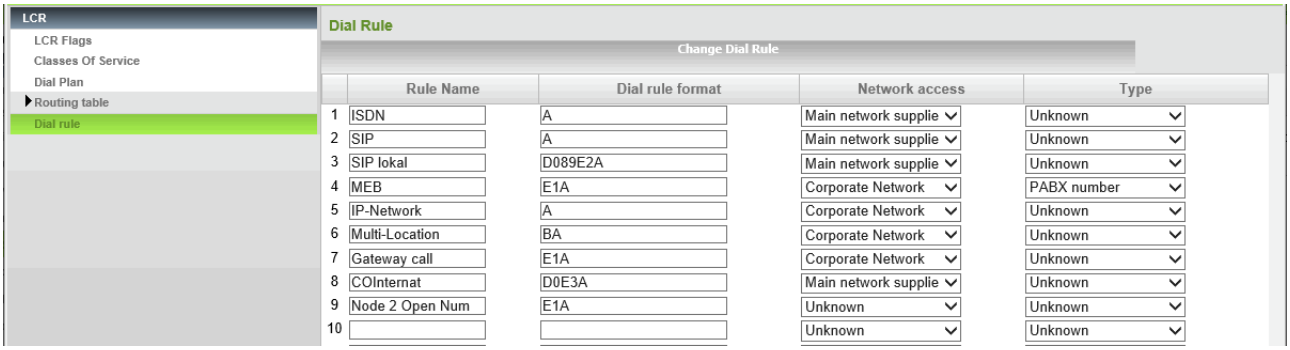
- Gateway 1 is basically set up as in the previous scenario (gateway 1), i.e., through the basic installation first and then by running the Network wizard. The essential difference here is that the gateways are set up as slaves, and the OpenScape Business S is set up set as the master (performance, bandwidth licensing).
- In this example, only the essential differences to the previous scenario are indicated.

Basic installation for gateway 1



Network wizard for gateway 1





In the OpenScape Business S, the destination number is already entered as a DID in the "national" format.

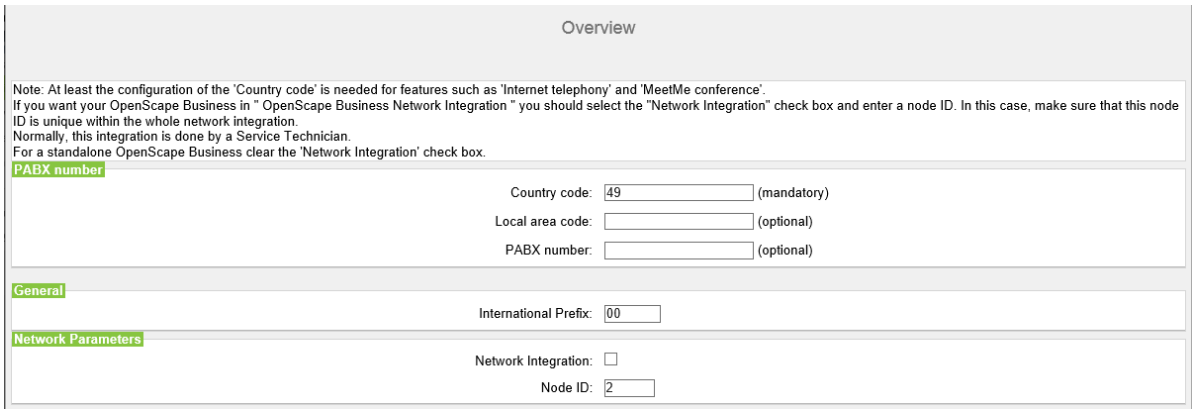
"BA" (Broaden All) is significant only in the gateway.

"BA" is only needed when the original destination number TON unknown has been received, i.e., contains only the "short DID" = extension portion.

Configuring the Multi-Gateway, OpenScape Business S

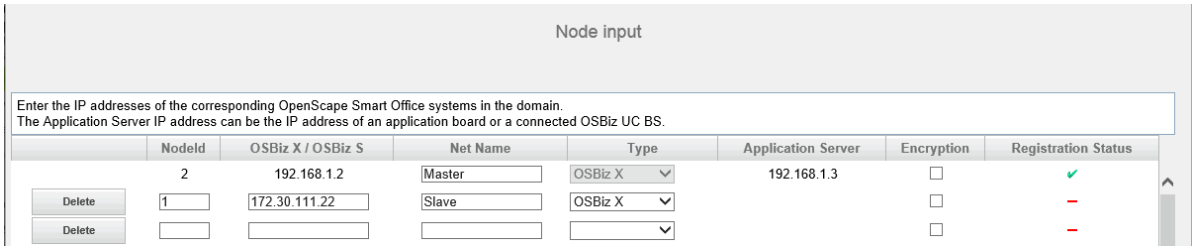
- After completing the basic installation first, the Network wizard is run.
- The following is set up for each subscriber of OpenScape Business S:
  - Internal number in short format (e.g., 300)
  - DID phone number in national format (e.g., 89 7007 300)
  - Associated gateway node ID

Basic installation of OpenScape Business S, multi-gateway



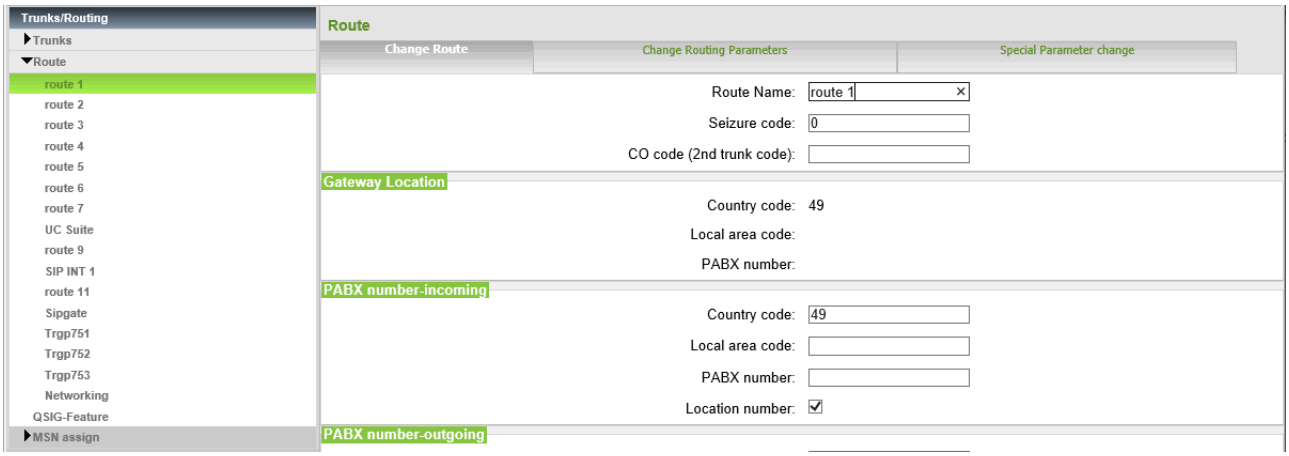
INFO: Only the country code needs to be entered in the system data; the rest of the complete call number is in DID entry of the subscriber.

Network wizard of OpenScape Business S, multi-gateway



Select multi-gateway in the network configuration.

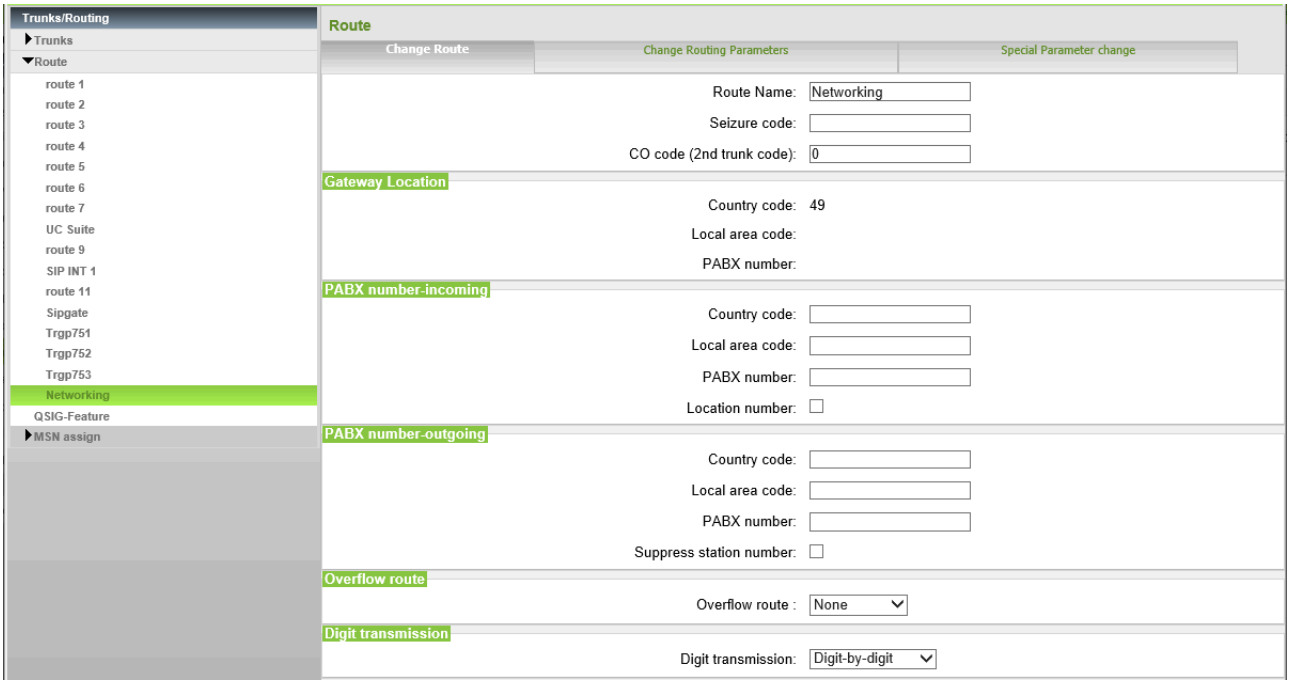
Routes of the OpenScape Business S, multi-gateway



The country code was already entered in the wizard.

Routing parameters: Route type CO (Central Office)

This route is assigned the route type "CO".

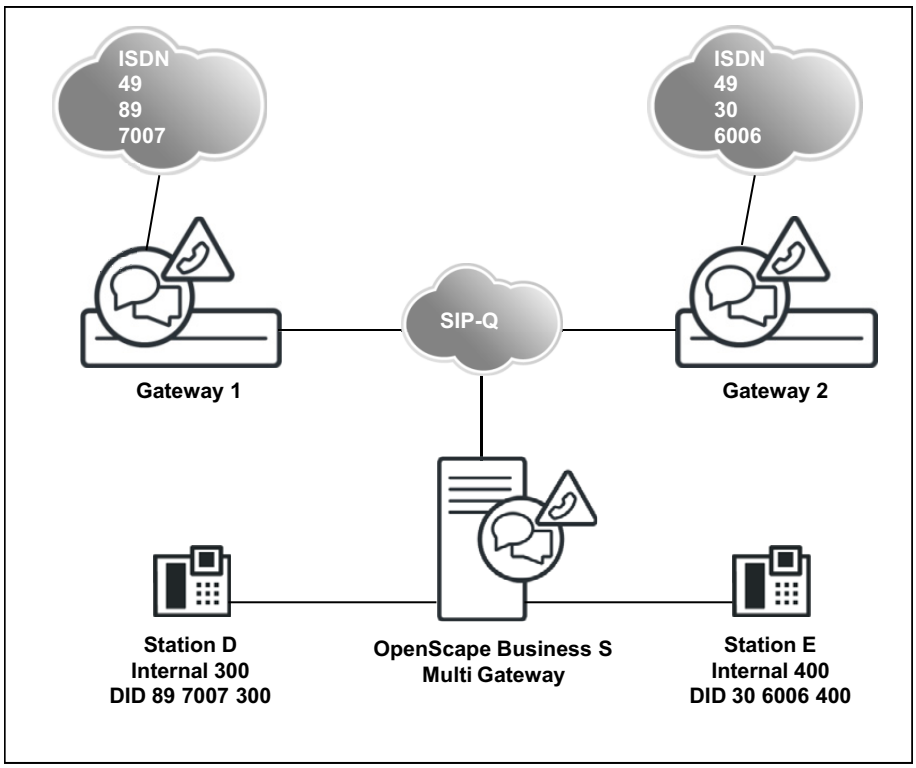


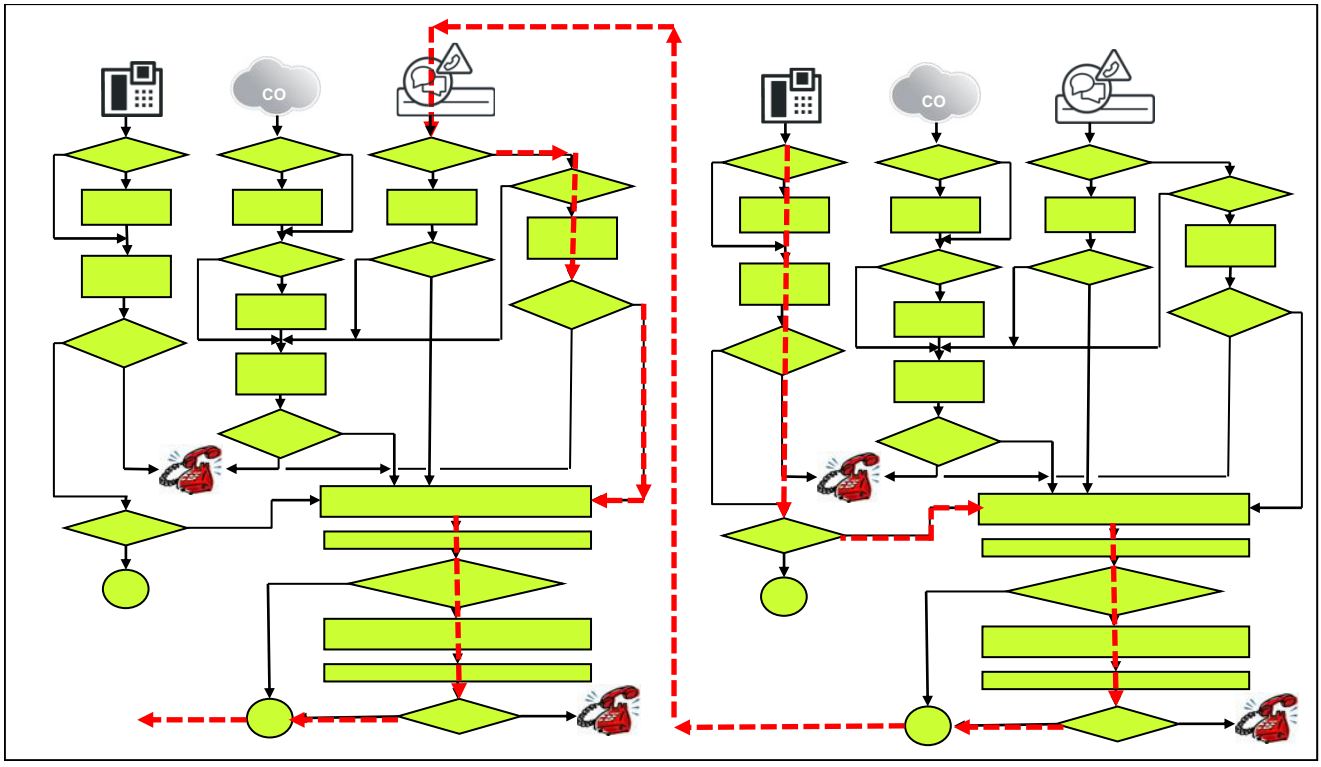
Routing parameters: call number type outgoing = National, Route type PABX

This route is assigned the route type "PABX", and the "No. and type, outgoing" must be set up with the **Local area code**.

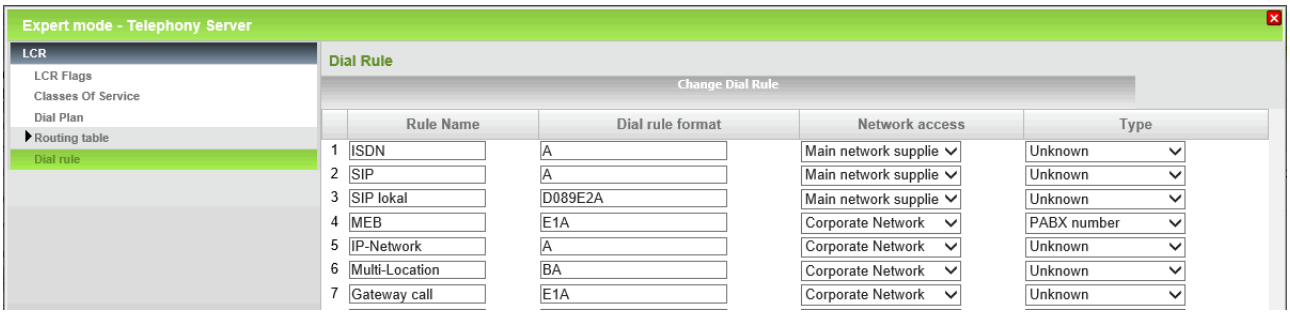
12.3.4.10 Subscriber D calls external station via the CO

Networked system in multi-gateway configuration

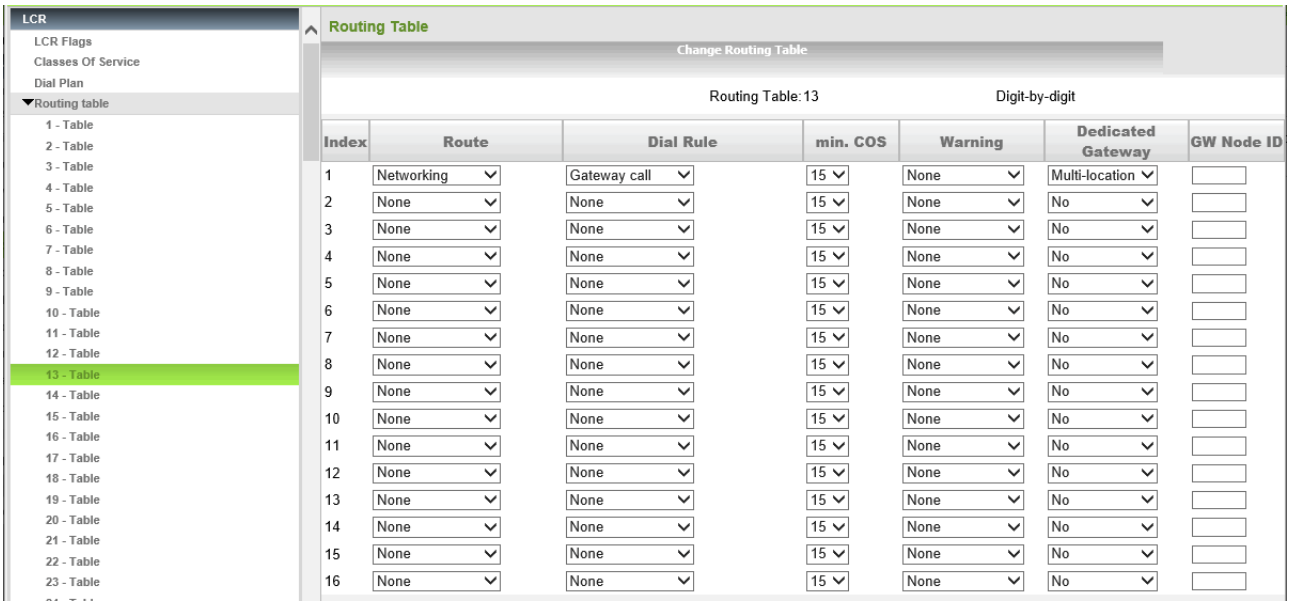

ISDN
49
89
7007
ISDN
49
30
6006
SIP-Q
Gateway 1
Gateway 2
Station D
Internal 300
DID 89 7007 300
OpenScape Business S
Multi Gateway
Station E
Internal 400
DID 30 6006 400


CO
CO

Configuration of the OpenScape Business S, multi-gateway



Routing of OpenScape Business S, multi-gateway, to the gateways



The setup of gateway 1 occurs as in the previous example. This also applies to gateway 2.

12.4 Emergency Calls

The communication system and the phones connected offer different options for making emergency calls. The administrator can configure a hotline or hotline after timeout or an emergency service.

Even if the activation period has not yet started or the communication system is in the failover period, emergency calls can always be made from the first two active telephones.

Prerequisites

The emergency call center is reached by dialing the CO access code (e.g., 0) and the emergency number (e.g., 112). The destination number for emergency calls must therefore be dialed from applications together with the leading CO access code.

Basic Sequence

Emergency calls are initiated by a subscriber of the communication system by dialing the CO access code and the emergency number. The emergency number is passed by the communication system on to the respective provider (PSTN or ITSP).

Case 1: Dialing the emergency call over the PSTN line

The emergency call is issued in the local network to which the communication system connection is assigned. The following must be observed here: All subscribers who are not in the same location as the communication system (e.g., Mobility users, CallMe users (teleworkers) or users with remote WAN-linked phones) should dial the emergency call via a cell phone or another land-line phone to issue the emergency call in the local area network of their site.

Case 2: Dialing the emergency call via an ITSP

Not all ITSPs support emergency calls. In this case, the LCR configuration should be used to ensure that emergency calls are routed via the PSTN.

Case 3: Special agreement with ITSP or PSTN providers

In cases where all subscribers of the communication system are not located at one site, but are nonetheless permanently assigned to a single site without a PSTN of its own, a customized procedure for emergency signaling can be agreed upon in cooperation with the Provider. For example, depending on the caller ID of the caller, the emergency call can be routed by the provider to the appropriate local network as agreed. These agreements are made on an individual basis and not subject to any policy.

Case 4: Emergency calls with Mobile Logon (IP Mobility)

Mobile Logon (IP Mobility) means that subscribers can change their phones and take their phone numbers with them.

Emergency calls work in this case, so long as the phones are logged in at the locations of the gateways. All subscribers who are not at the site of the gateway (e.g., Mobility users, CallMe users, home workers and users with remote WAN-linked phones) should dial the emergency call via a cell phone or another land-line phone to issue the emergency call in the local area network of their site.

INFO: For multi-gateway scenarios in which the Mobile Logon feature is used, special requirements apply. The appropriate configuration is described in the section "Emergency Calls in combination with Mobile Logon".

12.4.1 Hotline after Timeout / Hotline

You can activate the Hotline function for every station. You can thus define whether the connection to the hotline destination should be established as soon as you lift the handset (hotline) or after a short delay (off-hook alarm after timeout).

Hotline after timeout

If the subscriber selects any digit during the predefined time (hotline timeout), **no** connection to the hotline destination is established.

The hotline timeout is configured centrally by the administrator and can be activated and deactivated individually for each station.

Hotline

When the hotline is activated, the subscriber has **no** way to enter a call number. On picking up the receiver, the subscriber always reaches the predefined internal or external hotline destination automatically.

If hotline destination is set for call forwarding or call forwarding-no answer (CFNA), the calling station will always be forwarded.

System-Specific Information

The administrator can configure six hotline destinations and the length of the hotline timeout (0-99 seconds). If the administrator specifies the value 0 for the hotline timeout, the hotline destination is called immediately.

Dependencies

Topic	Dependency
Do Not Disturb	A caller hears the busy tone if Do Not Disturb (DND) is active at the destination called.

12.4.2 Trunk Release for Emergency Call

If an emergency call is made, and no CO trunk is free, a forced disconnect occurs. The emergency caller is automatically assigned the free trunk.

Trunk release works for ISDN and ITSP trunks.

If all trunks are busy, subscribers can execute an automatic or manual trunk release.

- Automatic: The Least Cost Routing (LCR) feature is active, and there is an emergency number stored in the LCR.
- Manual: the "Release trunk" feature is always active for the Attendant Console and is executed via keys or codes.

System-Specific Information

The administrator can configure as many emergency numbers as required.

To ensure that automatic trunk release occurs when all lines are busy, the emergency number must be saved in the LCR dial plan and the *Expert Mode* emergency flag must be set for it.

12.4.3 For U.S. and Canada only: E911 Emergency Call Service

The enhanced E911 emergency service transmits geographical information on the caller (stored address) in addition to the phone number when an emergency call is dispatched.

The receiving station for the emergency call does not require human intervention to determine the site of the caller.

In the USA, this feature is only activated when the emergency number 911 is dialed.

Every station number must be assigned a valid DID number with LIN (location identification number) by the administrator for the E911 emergency service. Subscriber lines that are physically close to one another are given the same LIN. The emergency call center has a database that contains all LINs and uses the transmitted LIN to identify the name and address of the party placing the emergency call.

Dependencies

Topic	Dependency
CLIP	LIN is activated by default for the U.S. However, if CLIP (Calling Line Identification Presentation) is activated for the USA, LIN is automatically disabled.

12.4.4 Emergency Calls in Combination with Mobile Logon

If you use the Mobile Logon feature in a multi-gateway internetwork, switching to another phone may also change the physical location. Consequently, special measures are required for the routing of emergency calls.

Description of the Algorithm for Dialing an Emergency Number

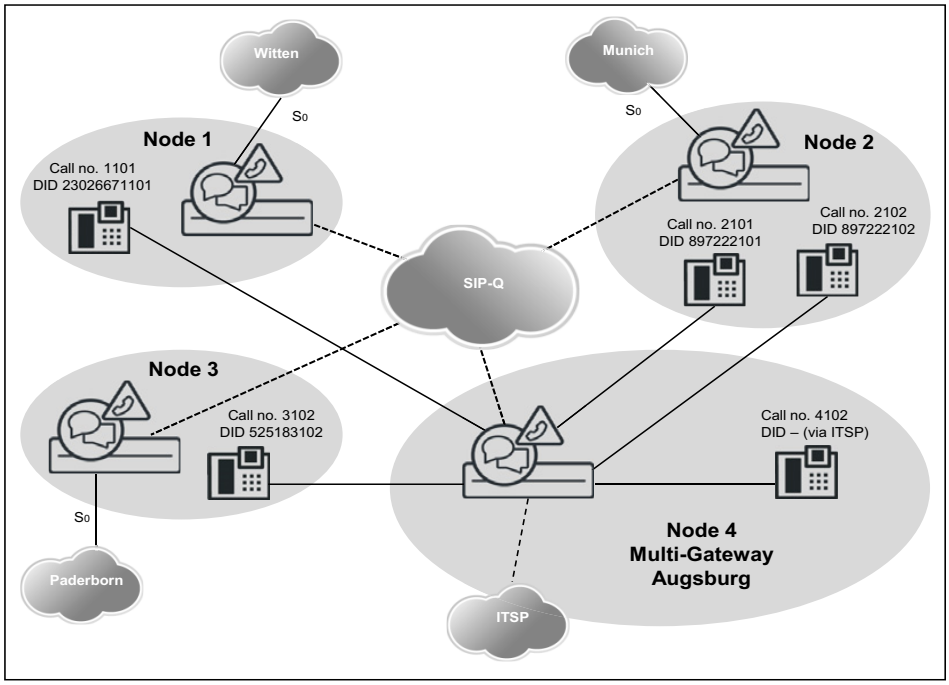
When a subscriber dials an emergency number (ID in the LCR), an algorithm checks whether or not an emergency number has been configured for the telephone. This is then used to produce a derived call number, which is used to route the call via the correct gateway in the internetwork.

Every number marked as an emergency number in the dial plan also features a reference to an entry in the route table. Every entry in the route table that is associated with an emergency number must be assigned a "low" class of service

(COS). A low class of service means that every subscriber is authorized to call an emergency number.

12.4.4.1 Configuring the Emergency Scenario

The configuration of the emergency scenario shows which steps must be performed to set up emergency calling for a multi-gateway internetwork.



Mobile Logon is supported only within a node, i.e., location changes - and thus the special requirements for emergency calls - are only relevant for phones operated on the multi-gateway node (4). In general, all affected phones are logged in at node 4, but are physically located at different sites.

- In all affected phones, one entry is required for emergency calling (connection portion of the canonical phone number of the location node + seizure code for emergency route)
- The LCR entry (node_4local) in the following table is only required if phones are physically present at node 4 (multi-gateway). It is also preceded by the location number which, however, is incomplete here (only country code). The prerequisite for this is an ITSP access to node 4, which supports emergency calls into the local network.

Handling of Emergency Numbers

- On dialing at the telephone, an LCR rule marked with an emergency flag (e.g., 0C11x) is taken.
- The emergency number that is stored in the phone (and transmitted to the system at logon) is compared with the location data of the system (country code, area code, PABX number).
  If different, a "long" emergency number is formed:

  - Removal of the access code: 0112 -> 112
  - Insertion of <LDAP seizure code><international prefix><programmed emergency number>: e.g., 112 -> 0 00 49897220 112
- The "long" emergency number is routed through the LCR, either directly to the local CO (central office) using specific LCR rules or via tie lines to the respective partner node and from there into the CO.

> ***INFO:*** Since the complete location number of the local node is not entered precisely in the telephone, a suitable LCR rule must also be entered for the local emergency call at the multi-gateway location.

Setting up the Location Data for Node 4

Node 4	Gateway Node
G.-Location Country	49
G.-Location Local Network	
G.-Location System	
International Prefix	00
National Prefix	0
LDAP seizure code	0

Routing parameters

Route	No. and type, outgoing	RNR type
Networking	National	Int/DID

Networking Route	
CO code (2nd. trunk code)	0

Node 4, telephones

Location Witten	
Call Number	1101
Emergency Number	4923026670

Location Munich	
Call Number	2101
Emergency Number	49897220

Location Paderborn	
Call Number	3102
Emergency Number	49525180

Location Augsburg	
Call Number	4102
Emergency Number	490

Overview of Entries Relevant for Emergency Calls in the LCR for Node 4

Dial Plan			Route table			Dial Rule		
Name	**Dialed digits**	**Emergency operation**	**Route**	**Dedicated Gateway**	**Gateway ID**	**Dial Rule**	**Procedure**	**Type**
Emergency calls [1)]	0C112	X	Networking	Multi-Gateway	1	E1A	Corp. Network	Unknown
Emergency calls [1)]	0C0110	X						
CO	0CZ							
Emergency_calls_to1	0C00492302667-0-11X	X	Networking	Mandatory	1	E3A	Corp. Network	Unknown
Emergency_calls_to2	0C004989722-0-11X	X			2			
Emergency_calls_to3	0C004952518-0-11X	X			3			
Emergency_calls_4local [2)]	0C0049-0-11X	X	ITSP	no		E4A	Main network supplier	Unknown

[1)] With the above rules in this example, only the emergency situation will be detected, but no routing will occur. The derived "long" emergency number is used to route the emergency call.

[2)] Since stations are physically connected at the multi-gateway location, a separate LCR rule must be entered for the local emergency call access (via the ITSP route).

12.4.5 E112 Emergency Call Service for Europe

The enhanced E112 emergency service transmits geographical information of the caller (stored address) in addition to the phone number when an emergency call is dispatched.

The geographical information is transmitted in a standardized XML document. The definition of the contents of this document depends on the country and ITSP. Thus you have to enter only the required subset of data you received from your ITSP (e.g. in Switzerland only the NAM field is used).

The feature is activated through configuration of emergency numbers in LCR and defining appropriate location information.

12.5 Call Admission Control

Using the Call Admission Control (CAC) feature, the used bandwidth can be restricted by limiting the number of calls.

The communication system offers three ways to influence the required bandwidth:

- Limiting the number of simultaneous calls via an ITSP
- Restricting the bandwidth requirements for gateway calls
- Limiting the number of calls in network scenarios

12.5.1 Limiting the Number of Simultaneous Calls via an ITSP

The maximum number of calls to the ITSP can be restricted by configuring the available upload bandwidth. By reducing the number of calls, the bandwidth requirements can be reduced further.

The settings for this can be made in the **Network/Internet** and **Central Telephony** wizards.

The number of possible calls via an ITSP can be viewed in **Expert mode** under **Telephony** > **Voice Gateway** > **SIP Parameters**.

12.5.2 Restricting the bandwidth requirements for gateway calls

By configuring the codecs allowed for Gateway calls, the bandwidth requirements can be influenced.

If only compressed codecs are set, the bandwidth requirement is lower. When using mixed codecs the prioritization of the uncompressed codecs can be reduced so that they are used less frequently.

The corresponding settings for this are made in **Expert mode** under **Telephony** > **Voice Gateway** > **Edit Codec Parameters**.

12.5.3 Limiting the Number of Calls in Networking Scenarios

The communication system offers two options for controlling bandwidth in networking scenarios.

Limitation by restricting the number of lines to other network nodes

By assigning a specific number of lines to other network nodes, an upper limit can be set on the number of simultaneous calls possible from and to these nodes.

Limitation of bandwidth through specific codec selection

The available bandwidth can be defined by configuring the codecs used from and to the partner (destination IP address).

The corresponding settings for this are made in **Expert mode** under **Telephony** > **Voice Gateway** > **Add Destination Codec Parameters**.

12.6 Tenant system

From an organizational point of view, the total capacity of the communication system can be split across a maximum of six subsystems. This makes it possible for several companies to share one communication system.

The tenant system feature is implemented using existing features. This means that it is not necessary for users to explicitly configure subsystems.

Users can control allowed and denied connections between individual stations and trunks via traffic restriction groups (CON groups).

Features in tenant service include:

- Intercept
- PABX number
- Caller list
- Override
- DISA
- Speaker call
- Call detail recording
- Hotline destinations
- Text messages, advisory messages
- Internal calls
- Internal Directory
- Customer Database Printout
- Night service
- Park slot
- Traffic Restriction Groups
- Voicemail
- Toll restriction

The communication system can be used as a tenant system, which allows it to be used simultaneously by several customers. All features have the same functionality for all users.

However, certain resources must be divided among the tenants (customers). They can be assigned to one, several, or all tenants. The resources to be divided are:

- Station
- Routes
- Attendant Console
- Intercept station
- Announcement devices, voicemail
- Traffic Restriction Groups
- Door Opener
- DISA trunks

Traffic restriction groups determine the ability of tenants to access each other.

Separate hotline destinations can be configured for each tenant.

Dependencies

Topic	Dependencies
CDRC	Only one CDRC exists for all tenants.
Internal calls	Internal calls are possible between stations in "different" tenant systems if allowed by the traffic restriction groups.
LCR	Prime Line can be configured only for the entire system.
Customer Database Printout	The database can only be printed for the entire system.
Internal Directory	The internal directory displays the names of all stations and speed-dialing numbers in the system.
Attendant	It is not possible to transfer undialed trunks.
Intercept	An intercept can be configured only for the entire system.

12.6.1 System Speed Dialing in Tenant Systems

System speed dialing in tenant systems enables the selection of specific speed-dialing destinations, depending on the internal traffic restriction (ITR) groups. To do this, a range of speed-dialing destinations can be assigned to the appropriate traffic restriction groups using the WBM.

Dependencies

Topic	Dependencies
External station numbers	Speed-dial destinations can contain external station numbers only.
	The external station number must include the trunk group or seizure code.
SSD names	You can assign a name to each speed-dialing destination.
Entrance Telephone (Door Opener)	The entrance telephone cannot dial speed-dial numbers.
ITR groups	You cannot assign more than one speed-dial number range for the same ITR group.

13 Attendants

OpenScape Business provides attendant functions for every use case (e.g., AutoAttendants, phone- and PC-based attendants).

Overview of Available Attendants

	Can be used for	Hardware	License
AutoAttendants			
Company AutoAttendant (UC Smart)	UC Smart	OpenScape Business X OpenScape Business S	Required
Company AutoAttendant (UC Suite)	UC Suite	OpenScape Business X3/X5/X8 with UC Booster Card or UC Booster Server OpenScape Business S	Required
IVM		Xpressions Compact board	No license required
Phone-based attendants			
OpenStage Attendant			
PC-based Attendants			
OpenScape Business Attendant	UC Smart	PC and phone, UP_{0E}	Required
- OpenScape Business BLF	UC Smart	IP-based	
myAttendant	UC Suite	OpenScape Business X3/X5/X8 with UC Booster Card or UC Booster Server OpenScape Business S	Required

13.1 AutoAttendant

The AutoAttendant, together with the voicemail, provides an integrated automated Attendant service and a message store, e.g., for the company headquarters. The AutoAttendant plays a greeting to callers. During or after this announcement, the caller can be routed to an extension or mailbox automatically or by entering digits.

A wide range of functions for specific switching are available for this purpose, together with the corresponding prompts, e.g., "Press 1 for service, 2 for Sales, etc". After entering the desired digit, the caller is then automatically connected with the Sales or Service staff.

The Company AutoAttendant is not assigned to any internal call number, but to a central instance. Multiple Company AutoAttendants or mailboxes can thus be assigned to one extension. This makes it possible for the user to individually redirect to the appropriate Company AutoAttendant. Depending on the

redirection, the caller hears either the announcement of the personal mailbox or the central company announcement. It is, however, also possible to play back individual announcements via the Company AutoAttendant, regardless of the personal mailbox.

Function Overview

- Intercept after announcement to a configured destination
- Status-based announcements - depending on the status of the extension (free or busy), different announcements can be played.
- Different day/night announcements (switching occurs either manually or automatically)
- Central calendar control via the automatic night service
- Suffix-dialing of any call number up to a configured length (can be deactivated)
- Speed dialing (= direct dialing external location) to configured destinations (any call number or mailbox)
  A total of 4 lists with a total of 10 destinations and one intercept destination are possible. The active list is determined by the selected greeting.
- Suffix-dialing of any call number up to a configured length. Suffix-dialing can also be disabled to prevent toll fraud.
- Multistep AutoAttendant
  AutoAttendant mailboxes can be configured as speed dial destinations (Manual 1 to 4, day/night). This allows for a concatenation of mailboxes.
  In this case, the Company AutoAttendant acts in the same manner as for call forwarding, i.e., the call is forwarded from one concatenated mailbox to the next, and each time the respective announcement is played. In total, up to 100 AutoAttendant mailboxes are available.
- Speed dialing
  Announcements can be disabled to guarantee fast switching.
- Announcement Prior to Answer with Parallel Signaling (without Speed Dialing)
  While the greeting is being played to the caller, the call is also simultaneously signaled to the subscriber acoustically (and visually). If the subscriber picks up the call, the announcement is interrupted, and the subscriber is connected to the caller. If the subscriber does not pick up the call, the announcement is played in a loop until the caller hangs up or is routed through the call management.
- Busy tone detection
- Forwarding of fax calls (automatic fax tone recognition) to a preconfigured Fax destination.
- Automatic recall
  In the case of a recall (except for fax calls), the caller is forwarded to the connected mailbox, if such a mailbox is available and message recording has been enabled.

NOTICE: I order to enable an automatic intercept from the voicemail system to the attendant console, the attendant code must be entered internally (default 9, USA 0).

NOTICE: AutoAttendant mailboxes can only be administered from a telephone (TUI). This is why the password for the AutoAttendant mailbox should differ from the password for the personal mailbox of the phone!

Use Cases

- Example 1: **Independent standby or emergency services announcements**
  Outside business hours, the customer is redirected to the AutoAttendant (e.g., via the night service). The AutoAttendant connects to the respective on-duty service technician on request and offers the option of leaving a message in a central mailbox. In this case, one announcement enables redirection to the various mobile phone numbers of the service technician.
- Example 2: **Different Sunday services for medical practices**
  It is now no longer necessary to record the currently applicable Sunday service on the answering machine and to replace the AB cartridge. The customer configures as many AutoAttendants as the number of available representatives. The AutoAttendants are recorded once and activated each weekend with a redirection (night service) to the appropriate AutoAttendant. Here the situation is reversed: several different announcements lead to the same mailbox.

13.1.1 Company AutoAttendant (UC Smart)

The Company AutoAttendant (UC Smart) is the Attendant Console of the UC solution UC Smart. It can be used as a personal AutoAttendent and as a central AutoAttendant. The initial setup is performed via the WBM, after which it can subsequently be controlled and configured over the telephone.

The Company AutoAttendant (UC Smart) can be operated in two modes:

- **Personal AutoAttendant**
  The personal AutoAttendant is assigned to a subscriber or group and responds to the call number of the originally called, redirecting subscriber or group (e.g., `12345678-100`).
  The personal AutoAttendant is reached via the "voicemail" hunt group (default call number: 351). Operation occurs via SmartVM ports (EVM ports) of type "PhoneMail", which must all be assigned to this hunt group.
  Parallel operation with UC Suite is not possible.
- **Central AutoAttendant**
  The central AutoAttendant is used as a central attendant console and responds to its own call number (e.g., `12345678-0`). Regardless of whether

a direct call to the AutoAttendant or a diverted call is involved, the behavior is always the same.
The central AutoAttendant is reached via one or more of its own hunt groups (default call number: 352). Operation occurs via SmartVM ports (EVM ports) of type "Standard", which can be assigned to one or more hunt groups (max. 100).
By default, a Company AutoAttendant (group index 3) is configured with 2 SmartVM ports. The names and types of ports can be changed with the **Central Telephony > SmartVM** wizard (see also *UC Smart - Voicemail Box / SmartVM - Configuring the Voicemail Box / SmartVM*).
The speed dial list and the greetings upload be changed in Expert mode under **Telephony > Auxiliary Equipment > SmartVM** (see also *Voicemail Box / SmartVM - Configuring the Voicemail Box / SmartVM*). Additional (max. 99) Company AutoAttendants (UC Smart) can be likewise set up and activated.
Parallel operation with UC Suite is possible.

The Company AutoAttendant (UC Smart) requires a license (Company AutoAttendant license). If no license is present, the "rules" of the Company AutoAttendant are ignored, and calls are forwarded to the central intercept position.

13.1.2 Company AutoAttendant (UC Suite)

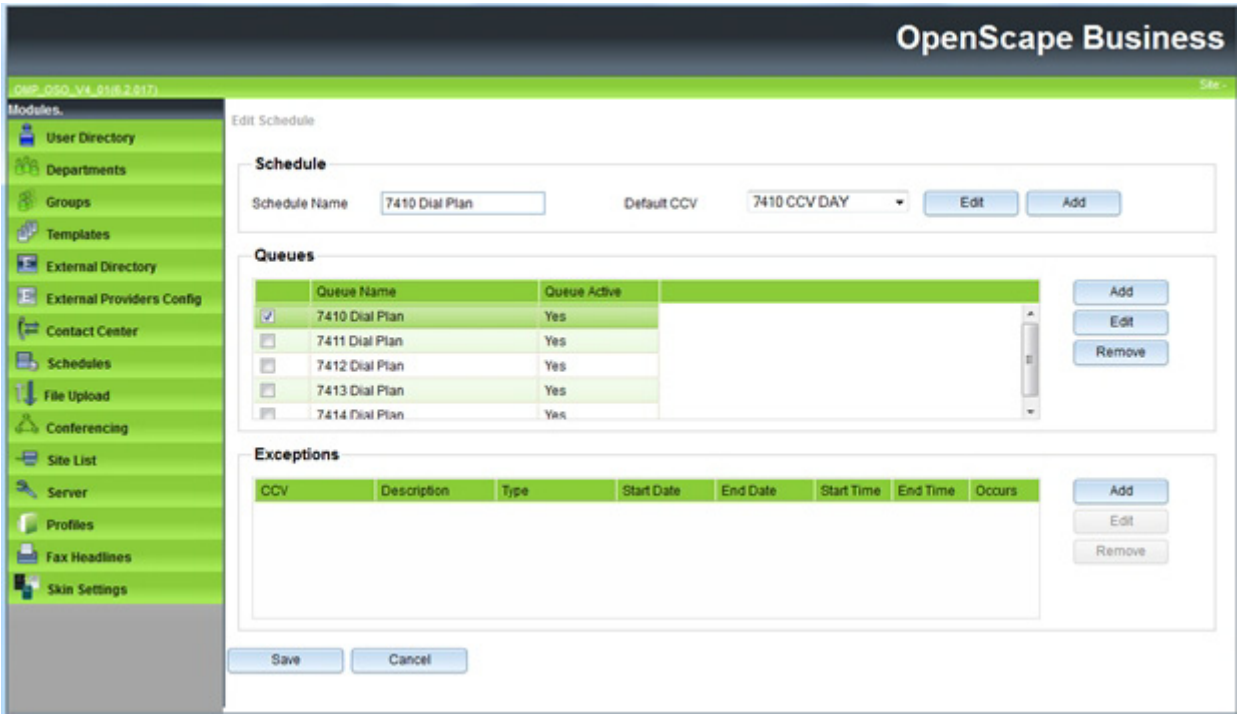
The central Company AutoAttendant (UC Suite) is an attendant console which can only be configured by the administrator. To facilitate the installation and setup, there are five templates that can be customized by the administrator.

The administrator can configure the Company AutoAttendant (UC Suite) on the basis of rules and schedules. Schedules also make it possible to offer advanced selection options such as dialing by name, for example.

13.1.2.1 Schedules

This schedule and the rules contained in it (Call Control Vectors or CCVs) define how incoming calls are to be handled on specific dates and at specific times.

For example, on work days, separate rules may be defined for the morning shift (from 6:00 to 14:00 hours), the afternoon shift (14:00 to 22:00 hours) and the night shift (from 22:00 to 06:00 hours). Similarly, a weekend rule can defined for the weekends. For each of these rules, you can define whether an announcement is to be played, for example, and/or the destination to which the calls are to be forwarded.



A schedule, in turn, must have at least one rule (called a Call Control Vector or CCV) assigned to it. The rules determine how incoming calls are to be handled during the time period to which the schedule applies. Rules apply only to calls and not to faxes and e-mails.

Rules are created with the graphical rule editor (CCV Editor) by combining predefined CCV objects and can be saved under a user-defined name upon completion.

Saved rules can be assigned to one or more schedules as a default rule (default CCV) or an exception rule (exception CCV). They can be opened, edited and saved again at any time by using the rule editor.

After a schedule has been assigned a default rule (default CCV), this schedule can be saved under a user-defined name. A schedule with an assigned default rule applies to a queue 24 hours a day, 365 days a year. If different rules are to applied at certain times (breaks, weekends, holidays, vacations, etc.), these can be assigned to the schedule as exception rules (Exception CCV). This means that you can define how incoming calls are to be handled during the holiday schedule, for example. Holiday schedules have precedence over the other schedules and rules.

Rule Editor (CCV Editor)

The Rule Editor is used to create rules from predefined CCV objects. The arrangement of the CCV objects and their properties determine how incoming calls are to be handled.

The following predefined CCV objects are available:

INFO: For all of the named CCV objects, the two general properties listed below also apply:

Description: Optional entry to describe the CCV object, e.g., Greeting.

Process digit: specification of the digit(s) required without blanks, commas or other characters. The specification refers to the preceding CCV object. If 9 was specified there under Accepted Digits, then 9 must also be entered here.

- **Play Message**
  Causes the desired message to be played. Any audio file present in the UC Suite can be selected. In addition, a new audio file can be imported into the UC Suite or a new announcement can be recorded and then imported as an audio file into the UC Suite.
  The playback of the announcement seizes one respective Media Stream channel.
  Properties:
  - **File Name**: Selection of an announcement (audio file in WAV format)
  - **Interrupt Digits**: specification of a key or key combination on the dial pad with which callers can stop the playback of an announcement.
  - **File Manager**: Using this button, it is possible to directly upload an audio file in wav format or create a new voice file with the recording device.
- **Disconnect Caller**
  Causes the call to be disconnected.
  After this CCV object, no further CCV object may be inserted.
- **Go to CCV**
  Causes a loop to another CCV object
  Property:
  - **Target CCV**: Selection of the CCV object
- **Process after digits**
  Causes the next CCV object(s) to be executed, depending on the digits specified there (process digit).
  Properties:
  - **File Name**: Selection of one or more announcements (audio file in WAV format)
  - **Playlist**: List of selected announcements (audio file in WAV format) in the order in which they are played
  - **Digits Timeout**: Time, in seconds, for which the communication system waits for the input of digits.
    If the required digits are not entered fully within the specified time, the message (announcement) is played again.
  - **Link To**: List of digits with destination.
    The digits and destinations can be added, edited and removed.

– **File Manager**: Using this button, it is possible to directly upload an audio file in wav format or create a new voice file with the recording device.

The contents of the Playlist are presented in the Rule Editor by a tool tip on hovering with the mouse pointer over the CCV object.

- **Single Step Transfer**

  This function depends on the **Normal Attendant Console SST** setting (WBM, **Expert mode**: **Applications > OpenScape Business UC Suite > Server > General Settings**):

  – **Normal Attendant Console SST** enabled (default setting; not for U.S.): Causes the call to be transferred, regardless of whether the destination is free, busy or unavailable.

  INFO: For stations with call waiting rejection enabled, the call is switched through only if the destination station is free. No call waiting on busy occurs.

  – **Normal Attendant Console SST** disabled (default setting, only for U.S.): Causes the call to be transferred if the destination is free.
  If the destination is busy and call waiting rejection is disabled, or if the destination is unavailable, an announcement is played back to the caller. The caller can then optionally choose to leave a message in the voicemail box of the called subscriber or select the call number of another destination.
  If the destination is busy and call waiting rejection is enabled, the call is not switched through.

  After this CCV object, no further CCV object may be inserted.
  Property:

  – **Target Extension**: specification of the internal call number or external DID extension with the number of the CO trunk. Blanks, commas and other characters are not allowed.

  The call number of the target extension is displayed in the CCV object.

  INFO: After Single-Step-Transfer, the system disconnects the call after ringing for 5 minutes.

- **Record In Mailbox**

  Causes the call to be sent to the desired voicemail box of a subscriber or a voicemail group
  After this CCV object, no further CCV object may be inserted.
  Property:

  – **User Mailbox**: specifies the station number of the voicemail box of a subscriber or voicemail group

  The station number and the name of the voicemail box or voicemail group are shown in the Rule Editor by a tool tip on hovering with the mouse pointer over the CCV object.

- **Supervised Transfer(also called screened transfer)**
  Causes the call to be transferred to an internal destination. During the transfer, Music on Hold (MOH of UC Suite) is played back to the caller.
  In contrast to the single-step transfer CCV object, two further CCV objects must be inserted here. This is because we now need to define how the communication system should behave if the call destination is busy or does not answer the call. Usually, an announcement is played to the caller in such cases.
  Properties:
  - **Target Extension**: Specification of the internal phone number.
    Only internal call numbers are supported in the own node. Forwarding to external destinations, virtual stations, additional AutoAttendants, UCD (incl. Contact Center), Mobility users as well as external CallMe destinations is not allowed! For these scenarios, the SST (single-step transfer) should be used.
  - **Ring Time Out (SEC.)**: Time, in seconds, within which the call must be accepted.
    If the call is not answered within the specified time, it is returned to the communication system, and the next CCV object is used.

    INFO: The time specified here must be shorter than the time configured for call forwarding (the default setting for call forwarding = 15 seconds). See *Administrator Documentation, Functions at the Telephone*.

  - **Pull back call if destination device is forwarded / deflected**: Option (only applicable for internal call number.)
    If this option is enabled, the call destination is first checked, and if a forwarding destination or deflection has been set for it, the call is returned to communication system, and the next CCV object is used.
  - **Check Presence status when transferring call**: Option
    If this option is enabled, the presence status of the call destination is checked, and if this status is any presence status other than Office, the call is returned to communication system, and the next CCV object is used.
- **Dial By Name**
  Causes the caller to be prompted to enter the first three letters of the desired subscriber's last name via the dial pad.
  If a unique subscriber name with the entered initial letters is found, a connection is established.
  If there are several subscriber names with the entered initial letters, these subscriber names are announced to the caller (max. 10 subscribers). If a subscriber has no recorded name announcement, the call number is announced instead. After selecting the desired subscriber, a connection is made.
  If none of the subscribers match the entered initial letters, the caller receives a corresponding message.

INFO: The keys on the dialpad respond to the first press of a key. With each key pressed, the system tries to determine whether there are subscriber last names with the letter assigned to that key.

Example: Let us assume the internal phone book has five last names with the initial letters t, u and v: Taylor, Taler, Ullrich, Vasquez and Volterra. To establish a connection with the subscriber Taylor, following keys must be pressed: 8 2 9

After this CCV object, no further CCV object may be inserted.
Properties:

– **Method**: Selection of **Transfer To Extension** or **Record In Mailbox**.
Depending on the method selected, a connection to the desired extension or its voicemail box is established. Note that only internal extensions for which the first and last names of the subscriber are entered in the internal directory are supported here.

- **Dial By Extension**
Causes the caller to be prompted to enter the station number (extension) of the desired subscriber via the dial pad.
If the caller dials the station number of a virtual station, the caller is prompted to enter another station number. A connection is then established. If the desired subscriber does not respond, the call is accepted by his or her voicemail box.
After this CCV object, no further CCV object may be inserted.
Properties:

  – **Method**: Selection of **Transfer To Extension** or **Record In Mailbox**.
  Depending on the method selected, a connection to the desired extension or its voicemail box is established. Note that only internal extensions in the network for which the phone number is entered in the internal directory are supported here.

- **Set language**
Selects the language for each standard announcement based on the phone number of the caller. It should be noted that only standard announcements (i.e., system announcements) and no personal greetings are taken into account here.
For example, it is possible to have German announcements played back to callers with the country code 0049 and French announcements for callers with the country code 0033.
Properties:

  – **Default language**: Drop-down list to select a language.
  The language selected here is used for all phone numbers for which no specific language was defined.

  – **Pattern**: Specifies the phone numbers to which a particular language is to be assigned.
  The following placeholders can be used * = any digit, ? = any digit.

- **Language**: Drop-down list to select the language to be assigned to the relevant phone numbers (matching **Pattern**).

A language can be assigned to any number of different phone numbers (matching **Pattern**).

- **CLI Routing**

  Causes the forwarding of a call to one or more sequential CCV objects based on the caller's number.

  For example, it is possible to first have a German announcement played back to callers with the country code 0049 (CCV object **Play Message**) and then have the call forwarded to an internal phone (CCV object **Single Step Transfer**).

  Properties:

  - **Standard**: Drop-down list to select the CCV object.
    The CCV object selected here is used for all phone numbers for which no specific destination was defined.
  - **Pattern**: Specifies the phone numbers to which a specific CCV object is to be assigned as the destination.
    The following placeholders can be used * = any digit, ? = any digit.
  - **Description**
    Provides an explanation.
    For the **Pattern** 0049 (= country code for Germany), for example, Germany can be entered.
    The text entered here will appear in the Rule Editor.
  - **Target**: Drop-down list to select the CCV object that is to be assigned as a destination to the related phone numbers (matching **Pattern**).

  A CCV object can be assigned as a destination to any number of different phone numbers (matching **Pattern**).

- **Branch on variable**

  Causes the forwarding of a call to one or more sequential CCV objects based on a given condition.

  You can thus define, for example, that an announcement (such as "Please call again later ...") should be played back to callers as soon as there are more than 20 calls in a queue.

  Properties:

  - **Variable**: Selection of **Calls** or **Available agents**.
    Depending on the selected variable, the number of calls waiting in a queue or the number of available agents (including agents in wrap up time) is used as the defined condition. In the associated drop-down list, the condition (**less than**, **greater than**, **less than or equal to**, **equal to or greater than**, **equal to**) must be selected, and the comparison value must then be entered in the corresponding input field.
  - **True branch**: Drop-down list to select the CCV object that is to be used as a destination when the condition is satisfied.
  - **False branch**: Drop-down list to select the CCV object that is to be used as a destination when the condition is not satisfied.

  The number of available agents in a queue is affected by the following status changes of the agents:

  - Login of an agent into the queue using "Anmelden/Login": --> +1

- Logout of an agent from the queue using "Abmeldung/Logout": --> -1
- Agent in the status "Break":-->-1
- Agent in the status "Available after Break":--> +1

The number of available agents in a queue is **not** affected by the following status changes of the agents:

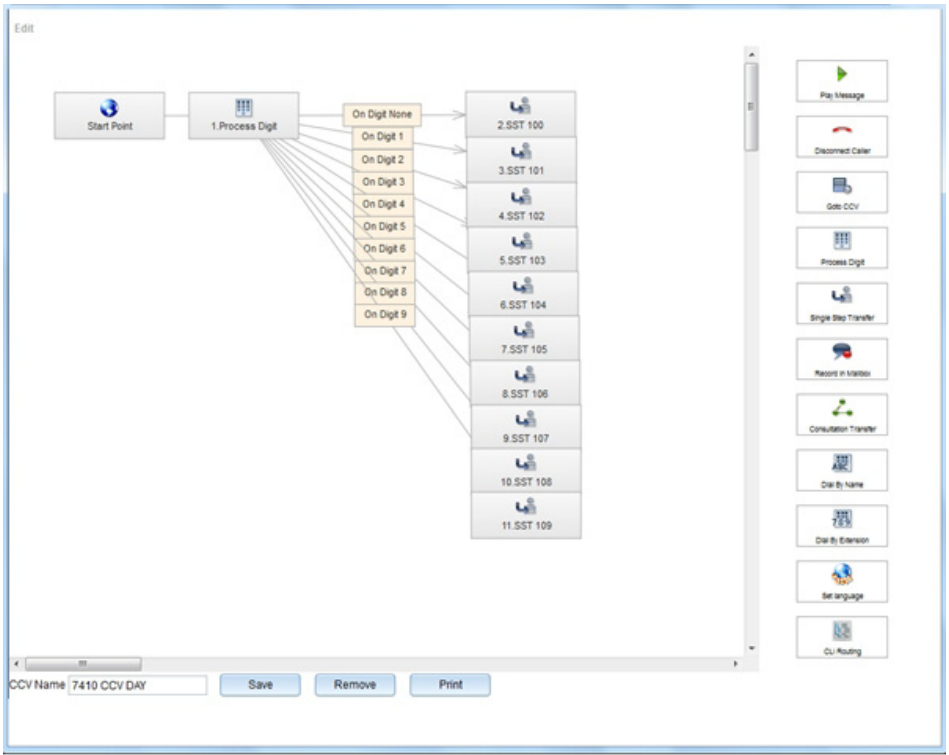
- Agent in the status "Ringing"
- Agent in the status 'Talking'
- Agent in the status "Wrap up"
- Agent in the status "Missed Call"
- Agent in the status "Overdue"

13.1.2.2 Templates

The following templates are predefined, standardized templates for the Company AutoAttendant (UC Suite), but can be changed as desired and adapted to specific needs.

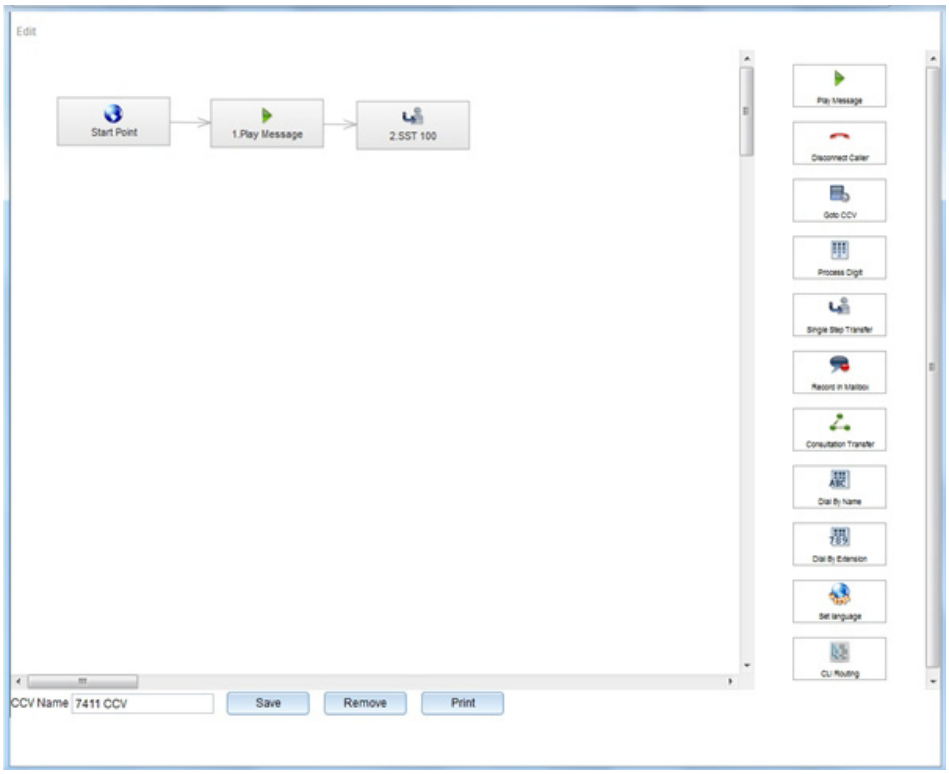
Template 1 - 7410 CCV: Call with Switching (without Voicemail)

An announcement is played for the caller. The caller is then prompted to press a button (digit) and is connected to a subscriber. If the caller does not press any button, the call is switched to to the intercept position (default 100).



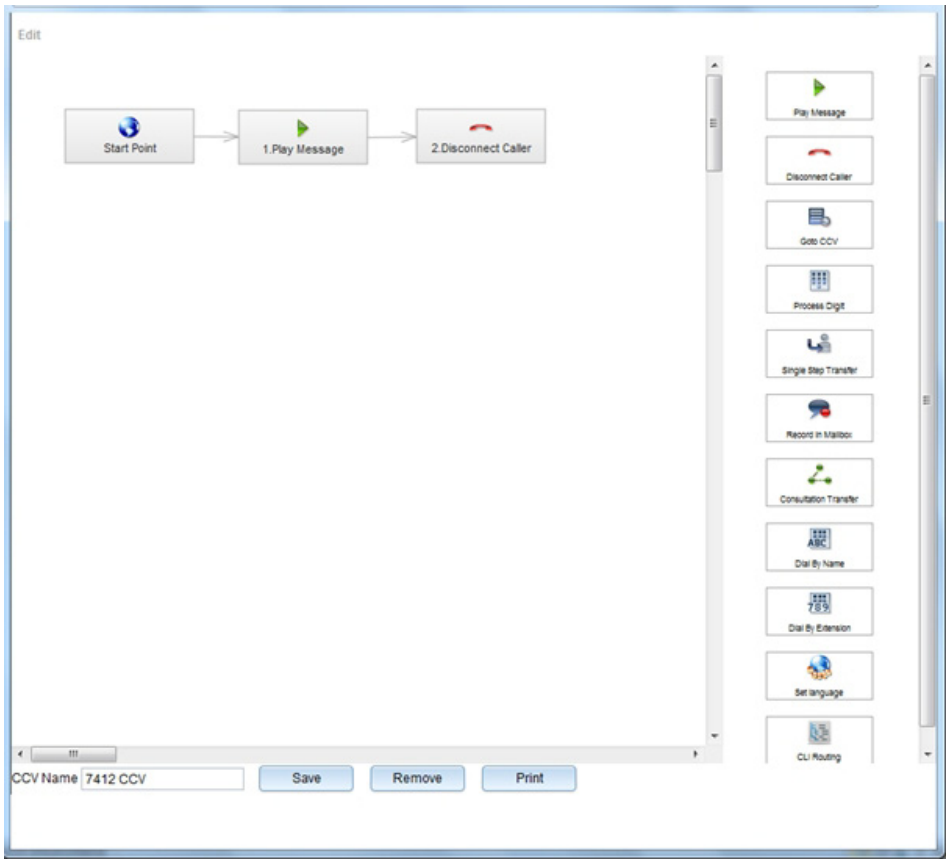
Template 2 - 7411 CCV: Announcement before Answering

An announcement is played for the caller. The call is then switched to the intercept position 100.



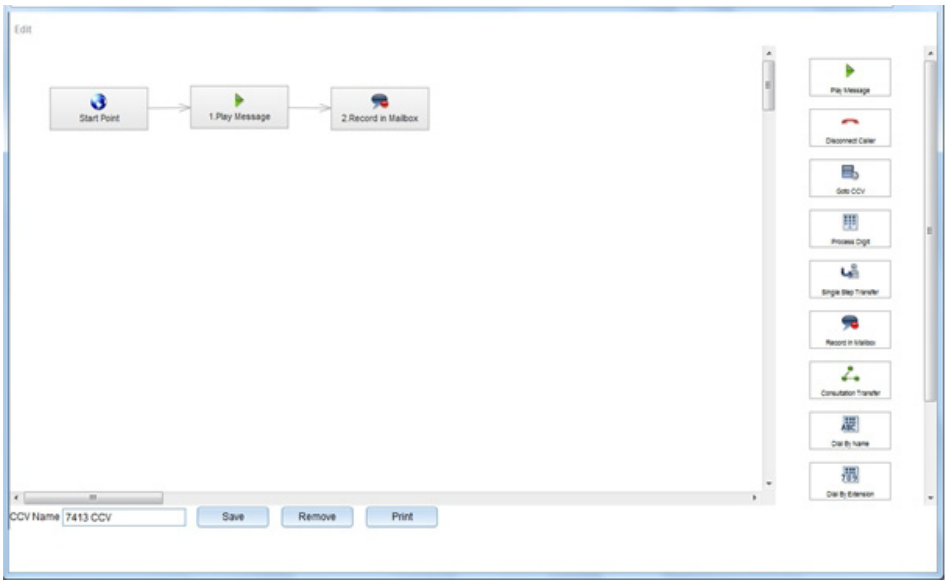
Template 3 - 7412 CCV: Call Outside Business Hours

An announcement is played for an incoming call outside business hours. The call is then disconnected.



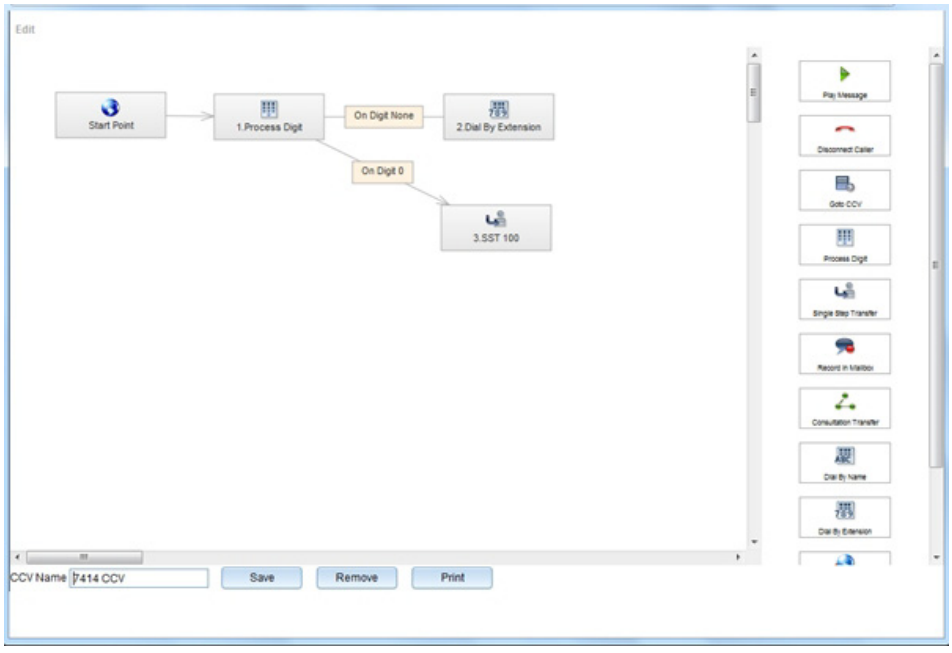
Template 4 - 7413 CCV: Call Outside Business Hours with Call Forwarding to Voicemail

An announcement is played for an incoming call outside business hours. The caller is then prompted to optionally record and leave a message in a voicemail box.



Template 5 -7414 CCV: Dial by Extension U.S. Feature

An announcement is played for the caller. Is the caller then does not enter any further digits, the call is routed to the CCV Dial by Extension. If the caller presses digit 1, the call is switched to the intercept position (default 100).



13.1.3 Xpressions Compact

Xpressions Compact provides an integrated AutoAttendant solution for your communication system. Up to 500 mailboxes are available with a recording capacity of 100 hours.

The AutoAttendant mailbox includes not only the mailbox for the Attendant Console, but also the option of recording messages. Incoming calls can be forwarded to:

- any extension
- a subscriber or guest mailbox
- an information mailbox
- some other user-specified destination, including external destinations
- a pre-defined destination depending on the number (10 destinations are available; no greeting is played in this case)
- an Attendant Console

Xpressions Compact features:

- Call forwarding to a mailbox
- Distribution lists for voice messages (20 lists are possible, with 499 destinations each)
- Message broadcasting
- Message Waiting Indicator
- Voice to E-mail
- Live Recording
- Notification call (SMS and pager possible)
- Forwarding messages by choice of name
- Forwarding of fax calls
- Statistics for Attendant mailboxes
- Central voice mailbox
- Access protection (3 to 8 digit password)

More Information

For more detailed information, refer to the Xpressions Compact Administrator Documentation

13.2 OpenStage Attendant

Attendant functions can be performed using a specially configured OpenStage telephone. The OpenStage Attendant is also an intercept position.

OpenStage Attendant is the destination for all incoming non-DID calls and calls for which no users could be reached (intercept calls) via the call allocation criteria. The attendant then routes these calls to the correct destination.

The following OpenStage phones can act as an Attendant:

- OpenStage 30
- OpenStage 40
- OpenStage 60
- OpenStage 80

Key layout

On OpenStage telephones configured as attendant consoles, the programmable function keys are assigned as follows:

- Night service
- Directory (phone book)
- Queued calls
- Override
- Hold
- External 1
- External 2 (not for OpenStage 40)
- Empty unassigned key (not for OpenStage 40)

13.3 OpenScape Business Attendant

The OpenScape Business Attendant provides switching functions as well as the connection of a phone book for OpenScape Business. In a network, the OpenScape Business Attendant can be expanded to show network-wide BLF and presence information.

Main attendant functions:

- Manage waiting or accepted calls
- Data of the active call
- Parked, held calls
- Call List
- Journal for answered, missed and outbound calls
- Personal VoiceMail

Directory (phonebook) application:

- Outlook contacts
- LDAP (connection via OpenDirectory Service)
- Personal directory

BLF status:

- Free, Busy, Called, Forwarded

Presence visibility:

- Office, Meeting, Sick, Break, Out of the Office, Vacation, Lunch, Gone Home
- Change the presence status for users within your own node (currently not possible for users from other nodes)

Two different "styles" are available for customizing the OpenScape Business Attendant user interface.

You can connect a maximum of eight OpenScape Business Attendants per communication system (a maximum of eight licenses per OpenScape Business X1/X3/X5/X8 and Business OpenScape Business S).

OpenScape Business Attendant is licensed via the WBM.

Technical Requirements

- Standard Windows PC
- Possible use of a Terminal Server when using HFA telephones (see *Prerequisites for UC Suite PC Clients*for the related prerequisites)
- USB interface or LAN interface, depending on the telephone used
- Screen with a resolution of min. 1024x768, optional second screen to display the second BLF
- Video card with 16-bit color depth (min. 256 colors)
- Internet access for support or updates

Operating System

- Microsoft Windows 10 / 8.1 / 8 / 7 (both 32-bit or 64-bit are possible)
- Microsoft Windows Vista (32 bit)
- Microsoft Windows Server 2015 (32 bit / 64 bit) as Microsoft Terminal Server
- Microsoft Windows Server 2012 (32 bit / 64 bit) as Microsoft Terminal Server
- Microsoft Windows Server 2008 R2 (64 bit) as Microsoft Terminal Server

Support for OpenScape Business Attendant for Microsoft Windows XP and Microsoft Windows Server 2003 will end at the same time as the end of support for these products by Microsoft. The product will still be supported, but will no longer be tested in detail.

Supported Phones

- Openstage 40/60/80 HFA
- openStage 30T/40T/60T/80T

Some of the older devices (e.g., optiPoint 410/420/500) are still supported. Please refer to the relevant release notes to see which devices have been tested and released.

Plug-and-Play Installation

The initial setup of the OpenScape Business Attendant is wizard-based. The wizard automatically opens all required configuration dialogs.

e.g.:

- Query the terminal type

- Query and check system access
- Query and check internetwork, if any
- Automatic integration of the BLF.

13.3.1 OpenScape Business BLF

The Busy Lamp Field OpenScape Business BLF is a separate application for displaying busy states. Optional functions include displaying and setting the presence status, and setting up the connection for the associated phone.

Main functions:

- OpenScape Business BLF is scalable and customizable
  - 10 to 350 BLF fields (user buttons), depending on the screen resolution
- Phone functions
  - Dial
  - Call answer
  - Disconnect
- Set the presence status (for own station)
- Directory (system directory)
- Call Journal

One OpenScape Business BLF license plus one UC Smart User license or UC Suite User license are required to operate each OpenScape Business BLF.

Technical Requirements

- Standard Windows PC
- Microsoft Windows 10 / 8.1 / 8 / 7 (both 32-bit or 64-bit are possible)
- Microsoft Windows Vista (32 bit)
- Microsoft Windows Server 2015 (32 bit / 64 bit) as Microsoft Terminal Server
- Microsoft Windows Server 2012 (32 bit / 64 bit) as Microsoft Terminal Server
- Microsoft Windows Server 2008 R2 (64 bit) as Microsoft Terminal Server
- Screen with a resolution of min. 1024x768
- Video card with 16-bit color depth (min. 256 colors)
- LAN interface
- Standard mouse and keyboard
- Internet access for support or updates

13.3.2 Configuration Examples for OpenScape Business Attendant, OpenScape Business BLF

In the following sections you will find configuration examples for the general configuration of OpenScape Business Attendant, OpenScape Business BLF.

13.4 myAttendant

A wide range of Attendant functions are available to you via myAttendant. Subscribers can be easily managed here via user buttons. In addition, messaging functions (voicemail, faxes, instant messages, SMS, and e-mails) are available via the Message Center.

A maximum of 20 myAttendants can be connected per communication system (per node). The maximum configuration of the internetwork is equal to the total capacities of the networked communication systems. The presence and phone status are shown for all subscribers in the network. The Message Center of myAttendant shows the subscribers of the own communication system.

Main Attendant Functions

- Manage waiting or accepted calls
- The data of the active call is displayed
- Parked calls on hold are displayed
- Caller list
- Journal for open, scheduled, internal, external, answered, missed and outbound calls
- Directory (phonebook) application
  - LDAP (e.g., ODS)
  - Personal directory / Outlook contacts
  - Internal directory, for all interconnected stations in the network.
- Busy Lamp Field status of all internal subscribers of the own system as well as all stations of the network
  - Phone status: Free, Busy, Called, Forwarded, Do Not Disturb
  - Presence status (Office, CallMe, Meeting, Sick, Break, Out of the Office, Vacation, Lunch, Gone Home (netwide)
- There are three interface styles to choose from.
- A maximum of 20 myAttendants can be connected per communication system (up to 20 licenses per OpenScape Business X3/X5/X8 and OpenScape Business S). The licensing of myAttendant occurs via the WBM.

Technical Requirements (see the Sales Information for Details)

- Standard Windows PC
- Microsoft Windows 10 / 8.1 / 8 / 7 (both 32-bit or 64-bit are possible)
- Microsoft Windows Vista (32 bit)
- Terminal server usage possible

Additional Software

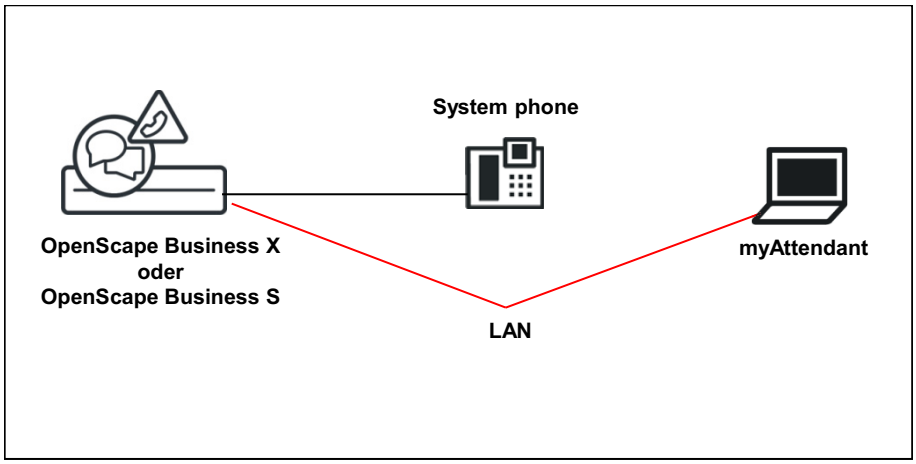
- Latest Oracle Java version (see **Service Center > Software**)

Supported Phones

- Openstage 40/60/80 HFA

- OpenScape Desk Phone IP 35G/55G HFA
- OpenScape Desk Phone IP 35G Eco HFA
- OpenScape Desk Phone CP 200/400/600 HFA
- SIP phones with RFC 3725 support, e.g., OpenScape Desk Phone IP 35G/55G SIP, OpenScape Desk Phone CP 200/400/600 SIP
- OpenStage 30T/40T/60T/80T

Simple plug and play installation; the first steps for the installation are sent to the user by the system (if his or her e-mail address has been configured).



13.4.1 Subscriber Management

Subscriber management is performed in myAttendant via user buttons, the internal directory, and the external directory.

User Buttons

The user buttons are located on the **Default** tab and are a part of the main window of myAttendant.

There are 90 user buttons available on a user buttons tab. The user buttons are sorted in alphabetical order by default. Internal and external subscribers (users) can be assigned to user buttons.

You can configure multiple tabs for user buttons and select the names for these user buttons freely.

13.4.2 Message Center

All voicemails, faxes, instant messages as well as SMS messages and e-mails are recorded and managed via the **Message Center** of myAttendant.

Messages can also be managed for other subscribers, provided these subscribers have granted the appropriate permission for this.

The Subscriber List window, contains a list of all communication system subscribers with their presence/absence status. Your own status is displayed first in a drop-down message overview. The other subscribers follow in alphabetical order.

Depending on what is selected in the message overview, message details are displayed, including a table of message-specific information that can be selected for further processing.

The various message types can be processed as follows:

- **Voice Messages (i.e., voicemails)** can be played back, deleted and forwarded,
- **LAN Messages** can be read, edited and deleted,
- **Fax messages** can be forwarded.

LAN Messages

LAN messages can be created only by myAttendant users. They serve as a kind of "bulletin board" for the subscriber, on which he or she enters notes (about individual subscribers). These messages can be viewed, edited or deleted, but cannot be sent to other subscribers.

13.5 Intercept Position

The communication system diverts external calls that cannot be assigned to a station or answered to a set intercept position to ensure that no calls are lost. As an administrator, you can configure the intercept criteria.

The intercept position can be an individual station, a group or an announcement device:

- Intercept position (Attendant Console)
- Stations
- Hunt group
- Group call
- External announcement device

A UCD group may not be selected as an intercept position.

If an intercept position is configured in the system, intercepted calls are forwarded to this intercept position. If no intercept position is configured, intercepted calls are signaled at the first IP station.

If an internal station is set up as an intercept position, the default key assignment is assigned to it automatically. In addition, the intercept position can be authorized for the Override feature.

As an administrator, you can assign one (two-digit) attendant code each to the intercept position for internal and external, under which the intercept position can be directly reached.

The intercept applies system-wide, i.e., identically for all subscribers in tenant systems. See also "Central Intercept Position in the Internetwork" in the section on Networking.

Intercept criteria

As an administrator, you can specify in which situations the Intercept feature is used via intercept criteria. The following intercept criteria are possible:

- On RNA (ring no answer)
  The call follows the entries in the call management (e.g., for a configured call forwarding). If no subscriber accepts the call, it is routed to the intercept position.
- On busy, if no additional forwarding is possible.
  The system first checks if call waiting is possible. If call waiting is not possible, the call follows the entries in Call Management (e.g., the call forwarding instruction configured). If no subscriber accepts the call, it is routed to the intercept position. Intercept on busy is only performed for first calls, not for forwarded or outgoing connections. A recall of an external station is not immediately intercepted when the destination station is busy; instead, call waiting is activated.
- On Invalid (misdialing)
  If the dialed station number is not configured or is inactive.
- On Incomplete
  If the Dialed station number is too short. Incomplete dialing is not evaluated if a central intercept position is used.
- On unanswered recall
  If an external call is not answered following an unscreened transfer (transfer before answer) and if the automatic recall to the original destination is also not answered, then an intercept is initiated after a preset time.
- On rejection
  If the call was rejected by an internal subscriber, the call follows the entries in the call management (e.g., for a configured call forwarding). If no subscriber accepts the call, it is routed to the intercept position.
- On missing phone number
  As for On Invalid.
- On chained call forwarding
  If a forwarded call encounters another forwarding instruction at the call forwarding destination, and the number of chained forwarding instructions allowed is exceeded, an intercept occurs. The number of chained forwarding instructions depends on the entries in the call forwarding. A maximum of 3 are allowed.
- On lock code
  If a subscriber at a telephone with an activated lock code dials a seizure code, an intercept occurs. A separate intercept is defined by the administrator for this purpose.
- On announcement (only with UC Suite)
  If a subscriber dials the (two-digit) attendant code while listening to a voicemail announcement or the AutoAttendant, an intercept occurs. A separate intercept is defined by the administrator for this purpose.

Dependencies

Topic	Dependency
Data calls	Data calls are disconnected, not intercepted.
Hunt group	Intercepts cannot extend beyond a hunt group; the call is forwarded to the first hunt group station and remains in the hunt group.
Default key assignment	The default key assignment has also the **View number of calls** key. This can be assigned to only 6 telephones. If the limit has been reached, no more default key assignments are made. The assigned default keys are not canceled when a device is no longer defined as an intercept position.
S_0 trunks	On S_0 lines, an evaluation takes place only when no day/night intercept position has been set up.
Night service	In order to reach the same destination from both the DID trunks and the MSI trunks while the Night service is active, the entry for Night Station number under Intercept > Attendant must be identical to the **Night Number** in **Ringing assignment per Line**.

14 Multimedia Contact Center

The Contact Center is a powerful solution for the optimal distribution and handling of incoming calls, faxes and e-mails. Intelligent, skills-based routing ensures that callers are always connected to the most qualified agent, regardless of the contact medium. A number of convenient functions for handling and wrapping up calls, faxes and e-mails are offered to the Contact Center agents via the myAgent application. myReports provides a number of report templates for analyzing the Contact Center operations.

The Multimedia Contact Center is fully integrated in the UC Suite software. It includes all required software components. The Contact Center functions themselves are released through licenses.

The Contact Center uses the resources of the communication system such as queues for incoming calls and unified communications functions to record and play back announcements.

The central software component of the Contact Center controls all routing functions for incoming calls, faxes, and e-mails and also controls the LAN-connected PC workplaces of agents and wallboard displays.

On the PC workplaces of agents, the myAgent application is installed. The myReports application can be optionally installed to generate and send reports. The required software can be downloaded directly from the download area of the communication system and installed on the client PC.

The WBM is used to set up the Contact Center basic functions, schedules, distribution rules as well as the agents. The settings for the daily operation of the Contact Center such as the assignment of agents to queues, for example, can also be made directly via myAgent.

If the Contact Center is unavailable due to problems (such as a system crash, dropped connection, etc.), a fallback solution can be implemented via the UCD feature of the communication system. Distribution rules for emergencies must be taken into account when setting up UCD groups within the framework of the initial setup of the Contact Center.

INFO: Information on the UC Suite and the unified communications features can be found in the UC Suite chapter.

14.1 Contact Center Clients

A number of convenient functions for handling and wrapping up calls, faxes and e-mails are offered to the Contact Center agents via the myAgent application. The myReports application can be used to generate reports on the calls, queues, agents, performance, GOS (Grade of Service) and wrapup codes of the Contact Center. More than 100 predefined report templates are available.

14.1.1 myAgent

Convenient functions for handling and wrapping up calls, faxes and e-mails are available to all agents via myAgent.

myAgent provides the following features:

- Processing of
  - Make Call
  - Faxes
  - E-mails
- Callback function for agents
- Displaying and changing the agent status
- Displaying and changing the presence status of internal subscribers of the communication system
- Real-time presentation of queues
- Recording of calls, if activated in the communication system
- Request for assistance through
  - Silent monitoring of calls (depending on country)
  - Overriding calls
  - Instant Messaging
- Integration of the internal directory, external directory and the external offline directory (LDAP) for searches by name
- Creation of reports based on predefined report templates

Depending on the authorization level assigned to an agent, either a set of standard functions (agent) or advanced functions (Supervisor or Administrator) are available to the agents in myAgent (see *Administrator Documentation, Multimedia Contact Center*).

The assignment of agents to queues occurs using the myAgent application. Only an agent with the authorization level of a Supervisor or an Administrator can make this assignment. The following properties, which affect the distribution of calls, faxes and e-mails in a queue, can be assigned here to the agents (agent assignment (binding)):

- **Primary Agent** or **Overflow Agent**
  Calls are distributed uniformly to primary agents. An overflow agent receives a call only when the number of calls exceeds a defined number ow when a call has exceeded a specified waiting period.
- **Overflow after seconds in queue**
  Calls that exceed this waiting period and received by an overflow agent.
- **Overflow after calls in queue**
  Calls that exceed the maximum number are received by an overflow agent.
- **Skill Level**
  Skill levels control the distribution of calls to agents in call queues. Agents with higher skill levels are given precedence when calls are distributed. In cases where all agents have the same skill level the longest idle agent receives the call.

- **Enable agent callback**
  Agent callback enables a caller in the queue to leave a voicemail for agents. As soon as an appropriate agent becomes free, that agent receives a call, hears the voicemail left by the caller, and can then call back that caller.
- **Wrapup time**
  The wrapup time enables agents to finish any tasks, e.g., administrative tasks, that may be required after completing a call and before receiving the next call.

The **agent binding list** shows agents with the authorization level of a Supervisor or Administrator which agents are assigned to which queues. Agents with the agent authorization level can only see the queues to which they are assigned.

14.1.2 Prerequisites for myAgent

In order to use myAgent, the client PC of the subscriber must be equipped with the appropriate hardware and software configurations.

INFO: Please make sure that you refer to the current notes in the `ReadMe first` file, which is located in the storage directory of the install files.

Telephones

myAgent can be used in combination with the following telephones:

- OpenStage HFA
- OpenScape Desk Phone IP 35G/55G HFA
- OpenScape Desk Phone IP 35G Eco HFA
- OpenScape Desk Phone CP 200/400/600 HFA
- OpenStage T
- OpenScape Personal Edition HFA
- OpenStage S5/M3/SL4 (OpenScape Business Cordless)

Older devices (such as optiPoint 410/420/500 and Gigaset M2/SL3/S4) are supported. Optiset E devices cannot be operated. myAgent cannot be used with SIP stations, Mobility stations, virtual stations, groups or MULAP stations. Details on the tested and released telephones can be found in the Release Notice.

Operating Systems

myAgent can be used in combination with the following operating systems:

- Microsoft Windows 10 / 8.1 / 8 / 7 (both 32-bit or 64-bit are possible)
- Microsoft Windows Vista (32 bit)

INFO: The used operating system always requires the latest version of all available updates (Service Packs and patches).

Support for myReports for Microsoft Windows XP and Microsoft Windows Server 2003 will end at the same time as the end of support for these products by Microsoft. The product will still be supported, but will no longer be tested in detail.

Additional Software

- Latest Oracle Java version (see **Service Center > Software**)
- Adobe Reader 9 or later (for reports in PDF format)

Minimum Hardware Requirements

- 2 GHz CPU
- RAM: 2 GB
- 100 Mbps LAN
- XGA (1024x768) screen resolution, myPortal for Outlook: SVGA (800x600) screen resolution

Microsoft Terminal Server, Citrix XenApp Server

myAgent can be used in Microsoft Terminal Server and Citrix Server environments under the following preconditions:

> ***INFO:*** Terminal Server and Citrix Server environments, including hosted services and virtual environments are the responsibility of the customer.

> ***INFO:*** Citrix server environments can decode some regional characters (e.g., German umlauts) correctly.

Operating systems:

- Microsoft Windows Server 2015 (32 bit / 64 bit) as Microsoft Terminal Server
- Microsoft Windows Server 2012 (32 bit / 64 bit) as Microsoft Terminal Server
- Microsoft Windows Server 2008 R2 (64 bit) as Microsoft Terminal Server
- Microsoft Windows Server 2008 R2 (64 bit) with Citrix XenApp 6.5 Server (Desktop Mode)

Support for myAgent for Microsoft Windows XP and Microsoft Windows Server 2003 will end at the same time as the end of support for these products by Microsoft. The product will still be supported, but will no longer be tested in detail.

Hardware Prerequisites: The number of installable clients depends on the server performance and on the amount of available memory. If the server is also being used for other applications, their memory requirements must also be taken into account.

More information on the configuration of Citrix XenApp Server can be found under:

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

Installation Files

The following options are available for providing installation files to users:

- The administrator downloads the installation files from the **Service Center** and makes them available to users via a network drive, for example.

Please refer to the notes in the `ReadMe first` file, which is located in the storage directory of the install files.

> ***INFO:*** The automatic distribution of the MSI file via a deployment service with Microsoft Windows Server is not supported.

14.1.3 myReports

Agents with the Supervisor or Administrator authorization level can use myReports to generate reports about agents and their activities, calls, queues, performance, GOS (Grade of Service) and wrap-up codes.

myReports offers the following features:

- More than 100 predefined report templates sorted by subject area (report groups) for the creation of reports
- Schedules for the scheduled generation of reports
- Immediate or scheduled sending of reports by e-mail
- Scheduled export of reports
- Output formats for report previews, sent e-mails and exported reports: Excel, PDF, and Word
- Report preview to check a report to be created in the desired output format.

User Roles

myReports has its own user management, which controls access to the functions of myReports through user roles. A distinction is made here between the myReports users (standard user) and the myReports administrator.

The current user role is set when you log into myReports.

The differences between the roles are summarized in the following table.

myReports: Activity	User Role	
	myReports User	myReports Administrator
Reports		

myReports: Activity		User Role	
		myReports User	myReports Administrator
	Preview report	X	X
	Send report immediately by e-mail	X	X
	Add report template	X	X
	Delete added report template	X	X
	Define new report template		X
	Update predefined report templates		X
Schedules			
	Add a schedule	X	X
	Display details of a schedule	X	X
	Edit schedule	X	X
	Delete schedule	X	X
Configuration			
	Change language of user interface	X	X
	Change color of user interface	X	X
	Configure e-mail template	X[1]	X
	Change server address	X	X
	Change administrator password		X
	Configure e-mail account to send reports by e-mail		X
	Configure prefixes for external phone numbers		X
	Enable/disable data protection		X
	Configure the storage location for the export of scheduled reports		X
	language, selecting		X[2]
	Set up default language		X[2]

1 The administrator password must be entered to configure the e-mail template
2 In order to configure languages and set the default language, you will need to log in as a myReports administrator with a special password.

14.1.4 Prerequisites for myReports

In order to use myReports, the client PC of the subscriber must be equipped with the appropriate hardware and software configurations.

> ***INFO:*** Please make sure that you refer to the notes in the `ReadMe first` file, which is located in the storage directory of the install files.

Operating Systems

myReports can be used in combination with the following operating systems:

- Microsoft Windows 10 / 8.1 / 8 / 7 (both 32-bit or 64-bit are possible)
- Microsoft Windows Vista (32 bit)

> ***INFO:*** The used operating system always requires the latest version of all available updates (Service Packs and patches).

Support for myReports for Microsoft Windows XP and Microsoft Windows Server 2003 will end at the same time as the end of support for these products by Microsoft. The product will still be supported, but will no longer be tested in detail.

Additional Software

- Latest Oracle Java version (see **Service Center > Software**)
- Adobe Reader 9 or later (for reports in PDF format)
- Microsoft Excel 16 / 2013 / 2010 / 2007 (for reports in Excel format)
- Microsoft Word 16 / 2013 / 2010 / 2007 (for reports in Word format)

Minimum Hardware Requirements

- 2 GHz CPU
- RAM: 2 GB
- 100 Mbps LAN (1 Gbps LAN recommended)
- XGA (1024x768) screen resolution, myPortal for Outlook: SVGA (800x600) screen resolution

Multi-user PCs

Under Microsoft Windows 7 and Microsoft Windows Vista with multi-user PCs, every local user can use myReports with his or her own custom settings, provided the first local user has installed the client with local administration rights. Only the first local user with local administration rights can perform updates via the AutoUpdate.

Microsoft Terminal Server, Citrix XenApp Server

myReports can be used in Microsoft Terminal Server and Citrix Server environments under the following preconditions:

> ***INFO:*** Terminal Server and Citrix Server environments, including hosted services and virtual environments are the responsibility of the customer.

INFO: Citrix server environments can decode some regional characters (e.g., German umlauts) correctly.

Operating systems:

- Microsoft Windows Server 2015 (32 bit / 64 bit) as Microsoft Terminal Server
- Microsoft Windows Server 2012 (32 bit / 64 bit) as Microsoft Terminal Server
- Microsoft Windows Server 2008 R2 (64 bit) as Microsoft Terminal Server
- Microsoft Windows Server 2008 R2 (64 bit) with Citrix XenApp 6.5 Server (Desktop Mode)

Hardware Prerequisites: The number of installable clients depends on the server performance and on the amount of available memory. If the server is also being used for other applications, their memory requirements must also be taken into account.

More information on the configuration of Citrix XenApp Server can be found under:

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

Installation Files

The following options are available for providing installation files to users:

- The administrator downloads the installation files from the **Service Center** and makes them available to users via a network drive, for example.

Please refer to the notes in the `ReadMe first` file, which is located in the storage directory of the install files.

INFO: The automatic distribution of the MSI file via a deployment service with Microsoft Windows Server is not supported.

14.1.5 Notes on Using myAgent and UC Suite Clients Simultaneously

When myAgent and other UC Suite clients are used simultaneously via one UC Suite user account, the possibility of mutual interactions cannot be excluded.

The term myPortal is used generically in this section to represent myPortal for Desktop, myPortal for Outlook, myPortal to go and myPortal for OpenStage.

Examples of mutual interactions:

- Changing the presence status via myPortal
  The examples apply to the default **Voicemail** setting for all call forwarding destinations.

  - myAgent: Agent is logged on.
    myPortal: The automatic reset of the presence status to Office is disabled.
    Changing the presence status via myPortal causes the agent to be immediately logged out of the queue(s). After the agent logs off via myAgent, the presence status in myPortal is reset to **Office**.
    A change in the agent status via myAgent (e.g., to **Break**) is registered by myPortal, but this does not apply to **Log in**, **Log out** and **Wrap up**.
  - myAgent: Agent is logged on.
    myPortal: The automatic reset of the presence status to Office is enabled.
    If the agent changes his or her status via myAgent to **Break**, he or she will be automatically available again after the break time has expired.
    A change of the presence status via myPortal to **Break** causes the agent to be immediately logged out of the queue(s).
  - myAgent: Agent is logged on.
    A change of the presence status via myPortal to **Do Not Disturb** causes the agent to be immediately logged out of the queue(s).

- Outbound Calls via myPortal
  The presence status of the subscriber is visible via myAgent.
  The calls appear only in the journal of myPortal. No transfer to the statistics of the Contact Center occurs, since these are not Contact Center calls.
- Incoming calls to the station number of the agent
  The presence status of the subscriber is visible via myAgent.
  The calls appear only in the journal of myPortal. No transfer to the statistics of the Contact Center occurs, since these are not Contact Center calls.
- Recording a call
  The recording of calls via myPortal is not registered by myAgent. myAgent offers this function even if the recording of a call is already occurring via myPortal.

14.2 Agents

The agents (stations) of a queue comprise a workgroup and are typically deployed for technical hotlines, for example, or in order processing, order acceptance, CRM, etc. The incoming calls, faxes and e-mails are distributed uniformly to the available agents for a queue.

In order to use a station of the communication system as an agent, this station must first be configured accordingly. The rights of the individual agents are defined by selecting their respective authorization levels (Agent, Supervisor or Administrator). An agent with the authorization level of a Supervisor or Administrator has elevated privileges (see *Administrator Documentation, Multimedia Contact Center*).

An agent can be defined as a permanently available agent. Such agents remain available for calls, faxes and e-mails even when they do not accept a call, fax or e-mail.

14.2.1 Agent Functions Independent of the Authorization Level

When a user is configured as an agent, the rights of the agent are defined by selecting the appropriate class of service for that agent (i.e., the authorization level as an Agent, Supervisor or Administrator). An agent with the authorization level of a Supervisor or Administrator has elevated privileges.

The differences between the authorization levels are summarized in the following table.

myAgent: Activity	Authorization level (class of service)		
	Agent	Supervisor	Administrator
Assign an agent to a queue	–	X	X
Move an agent to another queue	–	X	X
Remove an agent from the queue	–	X	X
Change the status of an agent	–	X	X
Display / hide the agent binding list	Assigned queues	All queues	All queues
Edit an agent assignment	–	X	X
Display list of Contact Center calls	Assigned queues	All queues	All queues
Activate myAgent screen pop automatically for alarms	–	X	X
Activate alarm tone	–	X	X
Display wallboard	Assigned queues	All queues	All queues
Display the Grade of Service graph	Assigned queues	All queues	All queues
Display the Average Times graph	Assigned queues	All queues	All queues
Move call to first position in a queue	–	X	X
Record a call	Current call	All calls	All calls
Save recording of call as WAV file or send as WAV file by e-mail	–	X	X
Save fax as a TIFF file or send by e-mail	–	X	X
Save e-mail as EML file or send as EML file by e-mail.	–	X	X
Call monitoring (country dependent)	–	X	X
How to Override a Call	–	X	X

myAgent: Activity	Authorization level (class of service)		
	Agent	Supervisor	Administrator
Accept a request for assistance	–	X	X
Create reports	–	X	X
Open WBM	–	X	X

14.2.2 Preferred Agents

Every caller (e.g., every calling customer) can be assigned one or more preferred agents of a queue. In such cases, the communication system first tries to switch the caller and his callback requests through to a preferred agent. If multiple preferred agents have been specified, a priority (sequence) can be defined to determine the order in which these agents are connected.

If no preferred agent is available, the call is forwarded to any available agent.

14.2.3 Agents in multiple queues

An agent can be assigned to multiple queues with different skill levels. In such cases, the function of the agent as a primary agent or an overflow agent must be defined.

14.2.4 Contact Center Breaks

In order to allow every agent the chance to take a defined break, Contact Center breaks of different lengths can be defined (e.g., for lunch or a cigarette break). Contact Center breaks are available system-wide and can be selected by an agent via myAgent as required.

14.2.5 Agent Login/Logout via Telephone

Login/Logout into the Contact Center is supported also via phone without the need to run myAgent in order to use the Contact Center functions. If an agent has been logged in via phone only voice calls can be processed. PopUp Window and WrapUp Code entry are not supported in this case. This applies also if myAgent is active and agent logs into the Contact Center using the phone. Full functionality of myAgent can be regained if the agent logs out via the phone and then logs in via myAgent.

Prerequisites and Constrains

- OpenScape Business Contact Center functions via telephone only work for agents for which a myAgent license is assigned within OpenScape Business
- All functions are only supported on such phones, which are released for use with OpenScape Business Contact Center
- In case that login via phone is successful and the associated myAgent client is not active, only Voice Calls are routed to the agent
- In case that login via phone is successful and the associated myAgent client is active, Email / Fax and Callback Calls are not be presented to agent if he logs in via phone. In this case screen-pops and wrap up work as usual but only voice calls will be delivered to the agent. To get full functionality, agent has first to logout via phone mode and login afterwards via myAgen

Login to Contact Center via Telephone

When the agents log into OpenScape Business Contact Center via the telephone, independent from myAgent client and Contact Center is active:

- The UCD functions for login are used at the phone
- The login function can either be executed via feature code or by a programmed key
- Agent is logged into all queues, to which he is assigned within the Contact Center configuration
- Telephone display informs agent about the login status
- Only UCD queue information (e.g. calls in queue information) is displayed on demand

The agent can use the following functions:

- Logon / Logoff (with UCD Agent ID)
- Wrap Up
- Available/Unavailable
- Display of calls within UCD Queue to which the UCD Agents ID has been assigned

> ***INFO:*** UCD Night Service must not be used by the agent.

In case that Contact Center fails during agent is logged on, the agent stays logged on into UCD and voice calls are routed as configured within the UCD routing. In case that agent was not logged in he can log into UCD via telephone.

Logout of Contact Center via Telephone

When the agents log out of OpenScape Business Contact Center via the telephone, independent from myAgent client and Contact Center is active:

- The UCD functions for logout are used at the phone
- The logiout function can either be executed via feature code or by a programmed key

- Agent is logged out of all queues, to which he is assigned within the Contact Center configuration
- Telephone display informs agent about the logout status
- No other Contact Center / UCD information (e.g. calls in queue information) is displayed

Set agent available/unavailable via Telephone

When an agent sets his status to available / unavailable for contacts routing of OpenScape Business Contact Center via telephone independent from myAgent client and Contact Center is active:

- Telephone display informs agent about the login status
- In case that myAgent is not active only voice calls shall be routed to the agent

Set/Reset Working after call (Wrap Up) via Telephone

When an agent sets his status to "Working after call" (Wrap Up) via telephone independent from myAgent client and Contact Center is active, it does not route any calls to the agent until the agent's specific Wrap up time, which is configured within OpenScape Business Contact Center, is expired or agent has reset Wrap Up via telephone.

Status Mapping

Agent status change via phone is mapped as follows to myAgent agent status:

Phone Device				myAgent		
Feature Code	**Feature Code**	**Description**	**Phone Display Text**	**Status**	**Addi-tional Text**	**Remark**
*401	UCD Agent ID	Log on UCD agents	Available	Available	-	Agent is set as available in all assigned queues
#401	–	UCD - agent log off	Not Available	Not avail-able	-	Agent is set as not available from all assigned queues
*402	–	UCD - agent available	Available	-	-	Available (end of Work Time)
#402	–	UCD - agent not avail-able	Not Available	Work Time	count-down from 999.999 seconds	-

Phone Device				myAgent		
Feature Code	**Feature Code**	**Description**	**Phone Display Text**	**Status**	**Addi-tional Text**	**Remark**
*403	–	UCD work on	Wrap up	Work Time	count-down of config-ured work-time	Work time must be finished before it can started again. No work time cumulating like in myAgent. After work time is elapsed agent is set available automatically.
#403	–	UCD work off	Available	Available	-	-
*404	night ser-vice target	UCD night service on	–	Not sup-ported	-	UCD Night Ser-vice must not be used
#404	–	UCD night service off	–	Not sup-ported	-	UCD Night Ser-vice must not be used
*405	–	UCD - calls in queue	-	-	-	Only the queue to which the UCD agent ID has been assigned is shown, regard-less if the agent is assigned to multiple queues within the Con-tact Center

14.3 Queues and Schedules

Queues are the basis of the Contact Center. Calls, faxes and e-mails for a queue can be handled, depending on the skill levels of agents, the priorities and waiting periods. Announcements can be played for waiting callers. A schedule is used to define how incoming calls are to be handled on certain days and at specific times.

14.3.1 Queues

As a rule, call distribution occurs by sending any incoming call, fax or e-mail for a queue to the specific station in the group (i.e., the agent) whose last call lies furthest in the past. It is also possible to define other distribution rules (based on

the different skill levels of agents, for example). If all agents are busy, any additional calls, faxes and e-mails are placed in the queue and then distributed to the next free agent based on their priority and the waiting time.

Schedules and the rules contained in them (i.e., the CCVs or call control vectors) can be used to define how a call to a queue at a specific time and on a specific date is to be handled. The rules define which announcement is to be played back to callers, for example, or where a call is to be forwarded.

Faxes, e-mails and agent callbacks are assigned to queues directly, independently of schedules.

When assigning agents to queues, different properties, which affect the distribution of calls in a queue, can be assigned to agents (e.g., Primary Agent or Overflow Agent and Skill Level). Agents can be assigned to queues

- via the WBM by an administrator with the **Advanced** profile.
- via the application myAgent by an agent with the Supervisor or Administrator authorization level.

If an agent is assigned to multiple queues, the queue priority can be used to define whether calls for a queue with higher priority should be forwarded to this agent with precedence over calls for other queues.

The following main settings can be made for queues via the WBM:

- Activating, deactivating and deleting queues
  Note: After the deletion of a queue, no reports for past time periods can be generated. Queues that are no longer required should be deactivated.
- Configuring queue alarms
  You have the following options:
  - Queue Alarm Count (alarm threshold value): If the number of calls waiting in the queue exceeds the number specified here, the queue symbol for the agent changes from green to orange. Agents with the Supervisor or Administrator authorization level can set whether they should be warned with an alarm tone and whether myAgent should be automatically brought to the foreground with a screen pop.
  - Queue Alarm Time (alarm threshold value): If the waiting time for a queued call exceeds the time specified here, the corresponding item in the list of Contact Center calls for the agents changes to red. Agents with the Supervisor or Administrator authorization level can set whether they should be warned with an alarm tone and whether myAgent should be automatically brought to the foreground with a screen pop.
- Defining timeouts for missed calls, faxes and e-mails
  If a phone call, fax or e-mail is not accepted by the agent at the end of the time specified here, the call, fax or e-mail will be forwarded to the next available agent.
- Defining an abandoned call threshold
  The time specified here determines whether or not an abandoned call is included in the statistics (i.e., in a report). Calls abandoned after the specified time has elapsed are included in the statistics.

- Configuring queue depth
  Control of the maximum number of active and waiting calls in a specific queue. The Contact Center indicates to the system that the defined threshold of the queue size is reached. As a result the system rejects every new incoming call for the appropriate queue before the call is connected with the system, until the number of calls falls below the threshold.
  The maximum queue size is determined by following parameters:
  - Maximum number of waiting positions within the queue. (WLS = Waiting Loop Size)
  - Maximum number of active and waiting calls of the queue.(Queue Depth Size).
- Setting up inbound fax pilots
  If configured, station numbers can be selected for incoming Fax messages. Faxes to these phone numbers will then be added to the queue and treated as incoming calls.
- Setting up an inbound e-mail service
  Multiple e-mail addresses can be set up for a queue. E-mails sent to these addresses are placed in the queue and treated like incoming calls.
- Setting up a return e-mail address
  E-mail address of the queue, which is displayed to the recipient when an e-mail is sent by an agent.
- Activating intelligent call routing
  An incoming call is forwarded to the agent with whom the caller was last connected, provided no preferred agent was defined for that caller.

14.3.2 Schedules

For each queue, a schedule can be defined with rules (Call Control Vectors or CCVs) to determine how incoming calls are to be handled on specific dates and at specific times.

For example, on work days, separate rules may be defined for the morning shift (from 6:00 to 14:00 hours), the afternoon shift (14:00 to 22:00 hours) and the night shift (from 22:00 to 06:00 hours). Similarly, a weekend rule can defined for the weekends. For each of these rules, you can define whether an announcement is to be played, for example, and/or the destination to which the calls are to be forwarded.

Schedules are the core of the Contact Center configuration. Without the definition of at least one schedule, the configuration of a Contact Center cannot be completed successfully. Every queue must be assigned at least one schedule. This may also be the same schedule in every case.

A schedule, in turn, must have at least one rule (called a Call Control Vector or CCV) assigned to it. The rules determine how incoming calls for a queue are to be handled during the time period to which the schedule applies. Rules apply only to calls and not to faxes and e-mails.

Rules are created with the graphical rule editor (CCV Editor) by combining predefined CCV objects and can be saved under a user-defined name upon completion.

Saved rules can be assigned to one or more schedules as a default rule (default CCV) or an exception rule (exception CCV). They can be opened, edited and saved again at any time by using the rule editor.

After a schedule has been assigned a default rule (default CCV), this schedule can be saved under a user-defined name. A schedule with an assigned default rule applies to a queue 24 hours a day, 365 days a year. If different rules are to applied at certain times (breaks, weekends, holidays, vacations, etc.), these can be assigned to the schedule as exception rules (Exception CCV). This means that you can define how incoming calls are to be handled during the holiday schedule, for example. Holiday schedules have precedence over the other schedules and rules of a queue.

Rule Editor (CCV Editor)

The Rule Editor is used to create rules from predefined CCV objects. The arrangement of the CCV objects and their properties determine how incoming calls are to be handled.

The following predefined CCV objects are available:

INFO: For all of the named CCV objects, the two general properties listed below also apply:

Description: Optional entry to describe the CCV object, e.g., Greeting.

Process digit: specification of the digit(s) required without blanks, commas or other characters. The specification refers to the preceding CCV object. If 9 was specified there under Accepted Digits, then 9 must also be entered here.

- **Play Message**
  Causes the desired message to be played. Any audio file present in the UC Suite can be selected. In addition, a new audio file can be imported into the UC Suite or a new announcement can be recorded and then imported as an audio file into the UC Suite.
  The playback of the announcement seizes one respective Media Stream channel.
  Properties:
  - **File Name**: Selection of an announcement (audio file in WAV format)
  - **Interrupt Digits**: specification of a key or key combination on the dial pad with which callers can stop the playback of an announcement.
  - **File Manager**: Using this button, it is possible to directly upload an audio file in wav format or create a new voice file with the recording device.
- **Music on Hold**
  Causes Music on Hold (MOH of the communication system) to be played for external calls for an adjustable period of time
  Property:

  - **Time Value**: Time, in seconds, for which the Music on Hold is to be played.
- **Disconnect Caller**
  Causes the call to be disconnected.
  After this CCV object, no further CCV object may be inserted.
- **Play Queue Position**
  Causes information on the current queue position of the caller to be played.
- **Go to CCV**
  Causes a loop to another CCV object
  Property:
  - **Target CCV**: Selection of the CCV object
- **Record Callback**
  Enables a caller in a queue to enable an agent callback (record a voicemail). Instead of the actual caller, the agent callback remains in the queue. For agents with the **Enable agent callback** feature, the agent callback appears in the list of Contact Center calls.
  After this CCV object, no further CCV object may be inserted.
  Properties:
  - **Type**: Selection of **Simple Callback** or **Extensive Callback**.
    In contrast to simple callbacks, extensive callbacks offer callers additional options and information (e.g., the option to confirm or change the phone number that is to be called back and the option to confirm the voicemail).
  - **Maximum message length**: Time, in seconds, that is available to a caller when recording a voicemail.
- **Process after digits**
  Causes the next CCV object(s) to be executed, depending on the digits specified there (process digit).
  Properties:
  - **File Name**: Selection of one or more announcements (audio file in WAV format)
  - **Playlist**: List of selected announcements (audio file in WAV format) in the order in which they are played
  - **Digits Timeout**: Time, in seconds, for which the communication system waits for the input of digits.
    If the required digits are not entered fully within the specified time, the message (announcement) is played again.
  - **Link To**: List of digits with destination.
    The digits and destinations can be added, edited and removed.
  - **File Manager**: Using this button, it is possible to directly upload an audio file in wav format or create a new voice file with the recording device.

  The contents of the Playlist are presented in the Rule Editor by a tool tip on hovering with the mouse pointer over the CCV object.
- **Single-step transfer**
  This function depends on the **Normal Attendant Console SST** setting (WBM, **Expert mode**: **Applications > OpenScape Business UC Suite > Server > General Settings**):

– **Normal Attendant Console SST** enabled (default setting; not for U.S.): Causes the call to be transferred, regardless of whether the destination is free, busy or unavailable.

> ***INFO:*** For stations with call waiting rejection enabled, the call is switched through only if the destination station is free. No call waiting on busy occurs.

– **Normal Attendant Console SST** disabled (default setting, only for U.S.): Causes the call to be transferred if the destination is free.
If the destination is busy and call waiting rejection is disabled, or if the destination is unavailable, an announcement is played back to the caller. The caller can then optionally choose to leave a message in the voicemail box of the called subscriber or select the call number of another destination.
If the destination is busy and call waiting rejection is enabled, the call is not switched through.

After this CCV object, no further CCV object may be inserted.
Property:

– **Target Extension**: specification of the internal call number or external DID extension with the number of the CO trunk. Blanks, commas and other characters are not allowed.

The call number of the target extension is displayed in the CCV object.

> ***INFO:*** After Single-Step-Transfer, the system disconnects the call after ringing for 5 minutes.

- **Transfer To Queue**
  Causes the call to be transferred to a queue.
  After this CCV object, no further CCV object may be inserted.
  Property:
  – **Queue**: Selection of the queue
- **Record In Mailbox**
  Causes the call to be sent to the desired voicemail box of a subscriber or a voicemail group
  After this CCV object, no further CCV object may be inserted.
  Property:
  – **User Mailbox**: specifies the station number of the voicemail box of a subscriber or voicemail group
  The station number and the name of the voicemail box or voicemail group are shown in the Rule Editor by a tool tip on hovering with the mouse pointer over the CCV object.
- **Supervised Transfer(also called screened transfer)**
  Causes the call to be transferred to an internal destination. During the transfer, Music on Hold (MOH of UC Suite) is played back to the caller.
  In contrast to the single-step transfer CCV object, two further CCV objects must be inserted here. This is because we now need to define how the communication system should behave if the call destination is busy or does

not answer the call. Usually, an announcement is played to the caller in such cases.
Properties:

– **Target Extension**: Specification of the internal phone number.
Only internal call numbers are supported in the own node. Forwarding to external destinations, virtual stations, additional AutoAttendants, UCD (incl. Contact Center), Mobility users as well as external CallMe destinations is not allowed! For these scenarios, the SST (single-step transfer) should be used.

– **Ring Timeout**: Time, in seconds, within which the call must be accepted.
If the call is not answered within the specified time, it is returned to the communication system, and the next CCV object is used.

INFO: The time specified here must be shorter than the time configured for call forwarding (the default setting for call forwarding = 15 seconds). See *Administrator Documentation, Functions at the Telephone*.

– **Pull back call if destination device is forwarded / deflected**: Option (only applicable for internal call number.)
If this option is enabled, the call destination is first checked, and if a forwarding destination or deflection has been set for it, the call is returned to communication system, and the next CCV object is used.

– **Check Presence status when transferring call**: Option
If this option is enabled, the presence status of the call destination is checked, and if this status is any presence status other than Office, the call is returned to communication system, and the next CCV object is used.

• **Dial By Name**
Causes the caller to be prompted to enter the first three letters of the desired subscriber's last name via the dial pad.
If a unique subscriber name with the entered initial letters is found, a connection is established.
If there are several subscriber names with the entered initial letters, these subscriber names are announced to the caller (max. 10 subscribers). If a subscriber has no recorded name announcement, the call number is announced instead. After selecting the desired subscriber, a connection is made.
If none of the subscribers match the entered initial letters, the caller receives a corresponding message.

INFO: The keys on the dialpad respond to the first press of a key. With each key pressed, the system tries to determine whether there are subscriber last names with the letter assigned to that key.

Example: Let us assume the internal phone book has five last names with the initial letters t, u and v: Taylor, Taler, Ullrich,

Vasquez and Volterra. To establish a connection with the subscriber Taylor, following keys must be pressed: 8 2 9

After this CCV object, no further CCV object may be inserted.
Properties:

– **Method**: Selection of **Transfer To Extension** or **Record In Mailbox**.
Depending on the method selected, a connection to the desired extension or its voicemail box is established. Note that only internal extensions for which the first and last names of the subscriber are entered in the internal directory are supported here.

- **Dial By Extension**
Causes the caller to be prompted to enter the station number (extension) of the desired subscriber via the dial pad.
If the caller dials the station number of a virtual station, the caller is prompted to enter another station number. A connection is then established. If the desired subscriber does not respond, the call is accepted by his or her voicemail box.
After this CCV object, no further CCV object may be inserted.
Properties:
  – **Method**: Selection of **Transfer To Extension** or **Record In Mailbox**.
  Depending on the method selected, a connection to the desired extension or its voicemail box is established. Note that only internal extensions in the network for which the phone number is entered in the internal directory are supported here.
- **Set language**
Selects the language for each standard announcement based on the phone number of the caller. It should be noted that only standard announcements (i.e., system announcements) and no personal greetings are taken into account here.
For example, it is possible to have German announcements played back to callers with the country code 0049 and French announcements for callers with the country code 0033.
Properties:
  – **Default language**: Drop-down list to select a language.
  The language selected here is used for all phone numbers for which no specific language was defined.
  – **Pattern**: Specifies the phone numbers to which a particular language is to be assigned.
  The following placeholders can be used * = any digit, ? = any digit.
  – **Language**: Drop-down list to select the language to be assigned to the relevant phone numbers (matching **Pattern**).
A language can be assigned to any number of different phone numbers (matching **Pattern**).
- **CLI Routing**
Causes the forwarding of a call to one or more sequential CCV objects based on the caller's number.
For example, it is possible to first have a German announcement played back to callers with the country code 0049 (CCV object **Play Message**) and then

have the call forwarded to an internal phone (CCV object **Single Step Transfer**).
Properties:

– **Standard**: Drop-down list to select the CCV object.
The CCV object selected here is used for all phone numbers for which no specific destination was defined.
– **Pattern**: Specifies the phone numbers to which a specific CCV object is to be assigned as the destination.
The following placeholders can be used * = any digit, ? = any digit.
– **Description**
Provides an explanation.
For the **Pattern** 0049 (= country code for Germany), for example, Germany can be entered.
The text entered here will appear in the Rule Editor.
– **Target**: Drop-down list to select the CCV object that is to be assigned as a destination to the related phone numbers (matching **Pattern**).

A CCV object can be assigned as a destination to any number of different phone numbers (matching **Pattern**).

• **Branch on variable**
Causes the forwarding of a call to one or more sequential CCV objects based on a given condition.
You can thus define, for example, that an announcement (such as "Please call again later ...") should be played back to callers as soon as there are more than 20 calls in a queue.
Properties:

– **Variable**: Selection of **Calls** or **Available agents**.
Depending on the selected variable, the number of calls waiting in a queue or the number of available agents (including agents in wrap up time) is used as the defined condition. In the associated drop-down list, the condition (**less than**, **greater than**, **less than or equal to**, **equal to or greater than**, **equal to**) must be selected, and the comparison value must then be entered in the corresponding input field.
– **True branch**: Drop-down list to select the CCV object that is to be used as a destination when the condition is satisfied.
– **False branch**: Drop-down list to select the CCV object that is to be used as a destination when the condition is not satisfied.

The number of available agents in a queue is affected by the following status changes of the agents:

– Login of an agent into the queue using "Anmelden/Login": --> +1
– Logout of an agent from the queue using "Abmeldung/Logout": --> -1
– Agent in the status "Break":-->-1
– Agent in the status "Available after Break":--> +1

The number of available agents in a queue is **not** affected by the following status changes of the agents:

– Agent in the status "Ringing"
– Agent in the status 'Talking'
– Agent in the status "Wrap up"

  - Agent in the status "Missed Call"
  - Agent in the status "Overdue"
- **Branch on data**
  Causes the forwarding of a call to one or more sequential CCV objects based on a given condition.
  You can thus define, for example, that an announcement (such as "Please call again later ...") should be played back to callers as soon as there are more than 20 calls in a queue.
  Properties:
  - **Variable**: Selection of **LDAP data1 (xmpp)** or **LDAP data2 (pager)**. The data query is done via LDAP either directly to an LDAP capable database or indirectly via the Directory Service (ODS) to an SQL / ODBC database. The query results are assigned via the UC Suite LDAP field mapping to the appropriate criterias of the Contact Center. In the associated drop-down list, the condition (**less than**, **greater than**, **less than or equal to**, **equal to or greater than**, **equal to**) must be selected, and the comparison value must then be entered in the corresponding input field. It is necessary to map the keywords "pager" and "info".
  - **Timeout**: The time in seconds before a timeout occurs.
  - **Timeout branch**: Drop-down list to select the CCV object that is to be used as a destination when timeout occurs.
  - **True branch**: Drop-down list to select the CCV object that is to be used as a destination when the condition is satisfied.
  - **False branch**: Drop-down list to select the CCV object that is to be used as a destination when the condition is not satisfied.
  - **Description**: Provides an explanation.

14.3.3 Wrap up

Wrapup reasons can be used to assign incoming calls to specific categories (orders, complaints, service, etc.). The assignment is made by an agent after completing the call (during the wrap-up time) by entering the appropriate wrapup reason using myAgent.

Wrapup reasons can be defined individually for each queue.

A distinction is made here between:

- Simple Wrapup
  One or more wrapup reasons can be defined for queues with the wrapup mode "Simple Wrapup".
  Example: The two wrapup reasons "hardware problem" and "software problem" were defined for a queue. Every call is assigned one of these wrapup reasons by an agent during the wrapup time. This makes it possible to subsequently create a report with an overview of all calls related to the subject of hardware problems, for example.

- Multiple Wrapup
  For queues with the wrapup mode "Multiple Wrapup", one or more wrapup reasons can be defined and then classified into groups and subgroups.
  Example: A Hardware group with the wrapup reasons Motherboard and Power Supply and a Software group with the wrapup reasons Operating System and Drivers were defined for a queue. Every call is assigned one of these wrapup reasons by an agent during the wrapup time. This makes it possible to subsequently create a report with an overview of all calls related to hardware problems or also all calls related specifically to motherboard hardware problems.

14.3.4 Grade of Service

The Grade of Service can be used to assess the response rate of the queue. This is achieved by comparing the waiting time for callers in the queue with target values, which can be specified individually for each queue.

The target values for the Grade Of Service (GoS) can be defined freely, depending on the acceptable waiting time for callers in a queue. For each call to an appropriate queue, the service level is determined after the call and committed to the database. The Grade of Service can be evaluated by agents with the authorization level of a Supervisor or Administrator by using the myAgent application.

14.3.5 Wallboard

Queue details can be retrieved and displayed using myAgent. The display contains a table with statistical information on queues in real time for the current 24-hour period. The display can then be presented on a large LCD monitor, for example, or via a beamer (wallboard).

Agents with the agent authorization level receive information on the queues to which they are assigned. Agents with the Supervisor or Administrator authorization level receive information on all queues.

A separate station should be set up for a wallboard display. A Station license (IP User or TDM User) and a myAgent license are required for this.

14.3.6 Agent Callback

If the waiting time in the queue is too long for a caller, and the associated schedule includes the CCV object **Record Callback**, the caller can leave a callback request. This callback request retains the original position of the caller in the queue and is delivered to the agent in the form of a voicemail. After listening to the voice message, the agent can call back the caller via a screen pop.

If a preferred agent has been set for a caller, an attempt is first made to route the callback requests of that caller to the preferred agent. If the preferred agent is not available, the callback request is forwarded to any available agent.

14.4 VIP service

For each queue, you can individually define whether certain callers (with a VIP status) or callers which match configurable call number patterns should be given preferential treatment and thus allowed to reach a free agent faster.

If all agents of a queue are busy, VIP callers are preferentially connected to the next available agent.

14.4.1 VIP Caller Priority

The VIP Caller Priority can be defined individually for each queue in order to specify whether callers (customers, for example) included in the VIP Call List should be given preferential treatment.

The values for the VIP Caller Priority can be defined freely, depending on the waiting time for callers in a queue. This determines the level of preference for VIP callers as opposed to normal callers.

When a VIP caller activates an agent callback (by recording a voicemail with a callback request), the agent callback is retained in the queue instead of the VIP caller. but without the VIP Caller Priority.

VIP callers must be registered in the VIP call list directory (see *VIP Call List*).

14.4.2 VIP Call List

Callers who have already been registered in the communication system (external directory) can be added to the VIP call list. Multiple selection can be done or the "**Select All**" function can be used. In addition, call number patterns can be entered. A call number pattern consists of a specific sequence of digits and a wildcard (placeholder). It can thus be used to transfer all employees of a company to the VIP call list, for example.

For each queue, the VIP caller priority can be used to define whether

- the callers included in the VIP call list and
- the callers who match the call number pattern contained in the VIP call list should be given preferential treatment.

It is not possible to enter call number patterns in the canonical call number format. The use of shortcut characters for country codes (for example +49 instead 0049) is likewise not possible. Call number patterns must always be specified without the CO access code.

Examples of call number patterns:

- 089 7577* (089 = area code for Munich, 7577 = PABX number of a company, * = wildcard for any number). By entering this call number pattern in the VIP call list, all callers from Munich, whose telephone number begins with 7577, are given priority.
- 0039* (0039 = country code for Italy, * = wildcard for any number). By entering this call number pattern in the VIP call list, all callers from Italy are given priority.

The following characters can be used as wildcards (placeholders) in a call number pattern:

- * = wildcard for any number
- ? = wildcard for any digit

14.5 Fallback solution

If the Contact Center is unavailable due to problems (crash, connection down, etc.) the "Uniform Call Distribution (UCD)" feature of the communication system is automatically used. This feature thus serves as the fallback solution for the Contact Center.

In the event of a failure in the Contact Center, incoming calls are distributed according to the fallback solution. The distribution of faxes and e-mails is not possible.

Depending on requirements, one of the fallback solutions described below can be configured.

Default Fallback Solution

In this case, the fallback solution is based on the UCD IDs (agent IDs) of the agents:

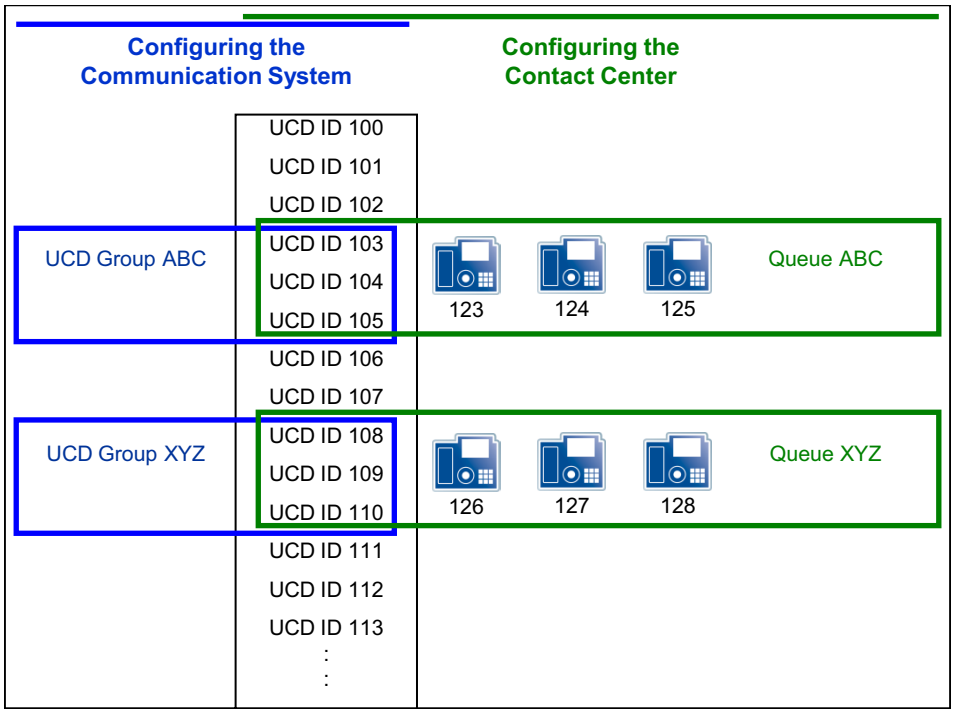
- Agents are assigned to the UCD groups of the communication system based on UCD IDs. The UCD ID determines to which UCD group this agent is assigned in the event of a failure at the Contact Center.

To ensure that the default fallback solution works properly, every queue must be assigned the Contact Center agents with the UCD IDs that were assigned to the appropriate UCD groups.

In the event of a failure in the Contact Center, incoming calls are distributed to the logged in agents via the different UCD groups.

Example:

- UCD IDs 103, 104 and 105 are assigned to UCD group ABC. UCD IDs 108, 109 and 110 are assigned to UCD group XYZ.
- The stations 123, 124 and 125 are configured as agents with the UCD IDs 103, 104 and 105. The stations 126, 127 and 128 are configured as agents with the UCD IDs 108, 109 and 110.
- When assigning agents to queues, the stations 123, 124 and 125 must be assigned to the queue ABC, and the stations 126, 127 and 128 to the queue XYZ.



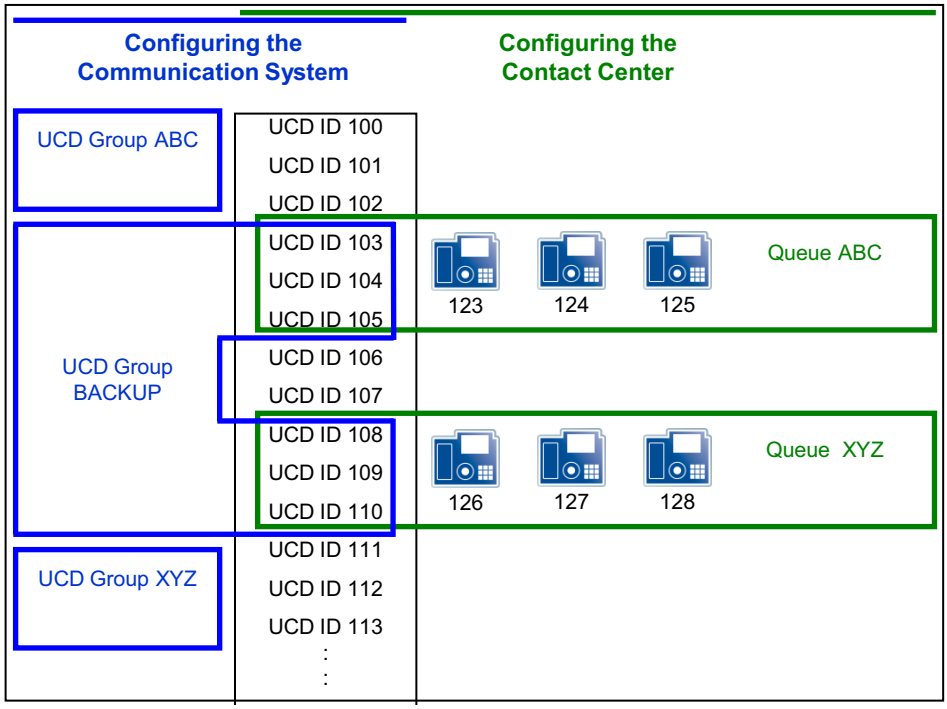
Basic fallback solution

In this case, all agents of the Contact Center are assigned using their UCD IDs to only the Backup UCD group. By assigning the appropriate agents, these UCD IDs are then also used in the queues of the Contact Center. This ensures that in the event of a failure in the Contact Center, the agents do not have to manually log in at their phones with a different ID. This Backup UCD group is defined as a second call forwarding destination for all UCD groups of the communication system.

If the Contact Center fails, the incoming calls are then distributed to all agents of the backup UCD group.

Example:

- No UCD IDs were assigned to the UCD groups ABC and XYZ. UCD IDs 103 to 105 and 108 to 110 were assigned to the UCD group BACKUP.
- The stations 123, 124 and 125 are configured as agents with the UCD IDs 103, 104 and 105. The stations 126, 127 and 128 are configured as agents with the UCD IDs 108, 109 and 110.
- When assigning agents to queues, the stations 123, 124 and 125 are assigned to the queue ABC, and the stations 126, 127 and 128 to the queue XYZ.



Custom fallback solution

In this case, the customized configuration of the Contact Center is mapped via multiple UCD groups.

If the Contact Center fails, similar behavior is thus achieved by the fallback solution.

For details on configuring call distribution via the "Uniform Call Distribution (UCD)" feature of the communication system, see *UCD (Uniform Call Distribution)*.

The main advantage of the of the custom fallback solution, by contrast, lies in its accurate mapping of the Contact Center operations.

The disadvantage of the custom fallback solution is the high configuration effort involved. Furthermore, to achieve similar call distribution behavior, all changes made to the Contact Center configuration also need to be mapped to the fallback solution.

The main advantage of the default and basic fallback solution is the easy configuration.

14.6 Configuring the Contact Center

When configuring the Contact Center, the UCD groups must be defined first. The queues of the Contact Center are essentially workgroups that are based on the UCD groups of the communication system. The actual configuration of the Contact Center (schedules, queues, etc.) can then be performed.

Before configuring the Contact Center, the standard processes for call distribution in normal and emergency modes must be coordinated with the customer.

> ***INFO:*** The configuration of the Contact Center should only occur after the setup of the communication system and the UC suite have been fully completed.

If changes are made to the configuration of the UCD groups, then the UC Suite must be subsequently restarted via the Service Center of the WBM.

The following licenses are a prerequisite for the operation of a Contact Center:

- An appropriate number of licenses for agents (myAgent)
- Contact Center Fax License (for receiving and sending faxes), if necessary
- Contact Center E-mail License (for receiving and sending e-mails), if necessary

14.6.1 Example of a Contact Center Configuration

The operating principle of the Contact Center with OpenScape Business is presented here with the aid of an example. The structure and configuration of the example are based on a fictional customer scenario with standard Contact Center functions.

Sample Scenario for a Contact Center

Company XYZ operates a Contact Center with the following station numbers (queues):

- Station number 440 for the Service Department
- Station number 444 for the Sales department
- Station number 456 for free calls (Hotline). Callers receive an announcement and can then reach the Service or Sales Department by selecting the appropriate digit.

The Contact Center consists of six employees (agents), of which three work for the Service Department and three for Sales.

The queues for the Service and Sales Departments should be directly reachable during normal business hours from 09:00 to 17:00 hours. Both queues have a fax box and an e-mail address.

If all agents are busy or not available, callers are to be notified accordingly and have music played back to them. Is no agent becomes free after a certain period of time, a caller can leave a callback request or and reach the Attendant by dialing a specific number. If no digit is dialed, the caller should be automatically placed back in the queue.

During closed hours, callers are to hear an announcement enabling them to record a voicemail with a callback request (agent callback).

During the lunch break from 12:00 to 13:00 hours, an announcement is to be activated for the Service and Sales Departments to offer callers the option of recording a message with a callback request.

Fallback solution via Backup UCD group: If the Contact Center is unavailable due to problems (such as a system crash, dropped connection, etc.), the system should automatically switch to the "Uniform Call Distribution UCD" feature of the communication system as a fallback solution. This requires all of the Contact Center agents to be assigned to a single backup UCD group. For all UCD groups of the communication system, this Backup UCD group should be defined as a call forwarding destination. If the Contact Center fails, the incoming calls will then distributed to the agents of the Backup UCD group.

Configuring the Sample Scenario

The following actions must be performed for this sample scenario:

- Configure UCD groups
  The queues of the Contact Center are essentially workgroups that are based on the UCD groups of the communication system. The UCD groups must be defined before the actual configuration of the Contact Center.
  For this example of the Contact Center of company XYZ, three UCD groups (Service, Sales and Hotline) are to be configured.
- Configure the fallback solution
  For this example, a Backup UCD group is to be configured and defined as a call forwarding destination for all UCD groups of the communication system.
- Configure subscribers as agents
  For this example, six subscribers must be configured as agents.
- Record individual announcements
  For this example, various announcements are to be recorded. This includes an announcement for situations when no agent is available, for example, or an announcement to inform callers about possible options (using **Process after digits**).
- Load individual announcements
  For this example, the recorded announcements are to be loaded into the communication system.
- Define schedules
  For each time interval within a schedule, rules (Call Control Vectors or CCVs) can be defined to determine how incoming calls are to be handled on specific days and at specific times.
  In the example, a standard schedule XYZ is to be defined with a rule for the times outside business hours and with exceptions for business hours and the lunch break. In addition, a second schedule (Standard Schedule Hotline) to be defined with a rule for free calls (Hotline).

Schedule	Rule (CCV)	
Standard Schedule XYZ	Out of the Office	Times outside business hours
	Open	Business hours 08:00 to 11:59 hours = Open1
		Business hours 13:00 to 17:00 hours = Open2
	Lunch Break	Lunch 12:00 to 12:59 hours
Standard Schedule Hotline	Hotline	24 Hours

- Adding three queues
  In this example, one queue is to be configured for the Service Department and one for Sales. A further queue (hotline) is to be configured for free calls.
- Assign agents to queues
  For this example, three agents are to be assigned to the Service queue and three to the Sales queue.

More details on the configuration of all Contact Center functions can be found under the *Configuration Procedure*.

14.6.2 Configuration Procedure

This section contains an overview of the actions to be performed when configuring the Contact Center.

- Configure UCD groups
  The queues of the Contact Center are essentially workgroups that are based on the UCD groups of the communication system. The UCD groups must be defined before the actual configuration of the Contact Center.
- Configure a fallback solution
  If the Contact Center is unavailable due to problems (crash, connection down, etc.) the "Uniform Call Distribution (UCD)" feature of the communication system is automatically used. This feature thus serves as the fallback solution for the Contact Center (see *Fallback solution*).
- Configure subscribers as agents
- Record individual announcements for the Contact Center
- Load individual announcements for the Contact Center
- Add schedules
- Add queues
- Define target values for the Grade of Service
- Define the VIP caller priority
- Edit the VIP call list
- Define preferred agents
- Add Contact Center breaks
- Add wrap-up codes

- Assigning agents to queues

14.7 Notes on Using the Contact Center

This section contains information about some special aspects and possible restrictions to be observed when using the Contact Center.

14.7.1 Restrictions on Operating the Contact Center

The operation of the Contact Center is subject to certain conditions. In addition, there are some restrictions on the use of system features by agents.

Conditions for the Operation of the Contact Center

The following conditions for the operation of the Contact Center must be taken into account:

- Trunks
  The Contact Center does not support analog trunks (MSI). All external connections of the Contact Center must be made via ISDN or IP telephony. It should be noted that the integration of IP telephony is only possible through certified Internet Telephony Service Providers (ITSPs).
- Networking
  In a networked scenario, all agents must be connected to the communication system in which the Contact Center is configured.
- Agent telephones
  Agents can use all system telephones (IP phones (HFA) such as OpenStage 40, for example, or $U_{P0/E}$ phones such as OpenStage 40 T) and DECT telephones. Note that only the DECT telephones that are currently released for operation with OpenScape Business Cordless may be used.
  It is not possible to use analog, ISDN and SIP telephones here.
  Agents are not allowed to be members of a group (Group Call, Hunt Group) or a MULAP. This restriction also applies to system features used in combination with MULAPs, i.e., Team Configuration (Team Group), Executive/Secretary (Top Group) and Mobility Entry.
- myAgent
  myAgent should not be used simultaneously with other UC clients, since mutual interference with the presence status cannot be excluded (see *Notes on Using myAgent and UC Suite Clients Simultaneously*). During normal operation of the Contact Center, agents use only myAgent to change their status (logged in, logged out, available, etc.).
- Connecting applications via the CSTA interface
  It is possible to connect applications via the CSTA interface, provided the following conditions are met:

- The application should not produce any significant additional load on the CSTA interface.
  Consequently, the connection of unified communications or call distribution solutions, CTI power dialers or even CTI solutions with many intensively used individual CTI clients is not allowed.
- The application must not control any agent telephones via the CSTA interface or set up any call forwarding for the agent telephones.
  Consequently, the connection of CTI applications for agents, rule assistants or personal assistants is not allowed.

The connection of TAPI 120/170 has been basically approved. For the load of the communication system, the same conditions as for the connection of other applications via the CSTA interface apply. In connection with the Contact Center, TAPI 120/170 should preferably be used to connect CRM (Customer Relationship Management) or ERP (Enterprise Resource Planning) systems, provided they support TAPI.

Restrictions on Using System Features

The following system features are not available to agents or are subject to restrictions. These features are, however, not mandatory for agents, since the allocation of calls is handled automatically by the Contact Center. The allocation depends on the set rules and the availability of agents.

- Locked Features
  The activation of system features via myAgent and the associated agent telephone is not supported for the available agents of the Contact Center. Agents can activate system features only via myAgent.
  The following system features are therefore not supported in conjunction with myAgent:
  - Call waiting
  - Second call
  - Parking
  - Group Call
  - Do Not Disturb (for logged in agents)
  - Intrusion on an agent call (exception: agents with the authorization level of a Supervisor or Administrator)
  - Features that affect call routing and active call connections
- Features that affect call routing
  The following features could potentially change the call routing in the contact center and should therefore not be executed by agents.
  - Call forwarding
    If a logged in agent activates call forwarding, a logout occurs.
    Call forwarding is disabled as soon as an agent logs into a queue.
  - Do Not Disturb
    If a logged in agent activates Do Not Disturb via a UC client, an automatic logout occurs.
    Do not Disturb is disabled as soon as an agent logs into a queue.

  - Relocate
    Relocating a telephone changes the logical assignment of the station numbers. The new station number assignment is only transmitted after restarting the Contact Center.
  - Night service
    When setting up a night service in the communication system, it must be ensured that the configurations of the Contact Center-related parameters (agents, queues, etc.) for the day and night service are identical.
- Features that affect reports
  Executing the following features from an agent telephone can lead to a distortion of the information in reports:
  - Call pickup of Contact Center calls by non-agents
  - Call transfers (e.g., via the Direct Station Select (DSS) key) of Contact Center calls to non-agents
  - Conferencing
  - Toggle/Connect
  - Parking

  INFO: The "Consultation Hold" feature is transparent for the presentation of Contact Center calls in reports and can be used by agents, regardless of the consultation destination.

- Roles and functions not relevant for agents
  The following functions are not relevant, since the "Call Waiting" feature (also called "camp on") is blocked for agents.
  - Attendant Console
  - Hotline destination

14.8 Notes on the Use of DECT Phones

DECT telephones can be used as phones for contact center agents. However, the differences in the operating procedure as compared to corded phones must be taken into account.

Prerequisites for the Use of DECT Phones

- Only the DECT telephones that are currently released for operation with HiPath Cordless Office and OpenScape Business Cordless may be used.
- The area within which the contact center agents move about must provide a complete wireless coverage.
- The number of base stations must be such that enough B-channels are available for the DECT telephones of the contact center agents.
- As far as possible, a contact center agent should not leave the wireless range while logged into a queue of the contact center.

Differences in the Operating Procedure as Compared to Corded Phones

- Logging into a queue of the contact center is only possible through myAgent.
- No messages such as **Available** or **Break**, for example, appear in the display of the DECT telephone.
- The control of a DECT telephone via myAgent (e.g., via the **Telephony** area of the myAgent main window or the screen pop of the incoming myAgent call) is not possible.
- Incoming calls can only be accepted via the DECT telephone.
- Outbound calls must be initiated via the DECT telephone.

Aspects to be considered when using DECT phones:

- Search time
  For an incoming call, the time required to find the DECT telephone may take several seconds (at worst up to 20 seconds) before a call is signaled on the DECT telephone. During the search time, the caller hears the ringing tone.
  The contact center evaluates this time as "pickup time". The actual pickup time by a contact center agent thus consists of the search time and the alert time (i.e., time until the call is answered).
  If a contact center agent leaves the wireless range with his or her DECT telephone, this may result in longer search times.
- DECT telephone cannot be found
  If a contact center call exceeds the prescribed time for a call to be answered by the agent (e.g., because the contact center agent is out of range), the agent is automatically logged out of the queue or queues involved. Logging in again is only possible through myAgent.

14.9 Reports

Reports are used to determine the current status of the Contact Center and to analyze the strengths and weaknesses of its associated components. This makes it possible to optimize the Contact Center configuration, for example, and to thus use the Contact Center resources more efficiently. The Contact Center provides users with real-time reports as well as historical reports.

Real-time Reports

Real-time reports are continuously updated. They provide important information such as details on agent utilization, the grade of service, abandon rates and average processing times. Using these continually updated and filterable caller lists, the progress of a customer contact can be examined in stages. In addition, the activities of all agents can be reviewed. This information can be used for training purposes, for example, and for contact analysis and wrap-up activities.

Agents with the authorization level of a Supervisor or Administrator can be acoustically and visually informed when definable operating parameters are exceeded. Appropriate thresholds for each queue can be defined individually.

Historical Reports

By selecting data elements and user-specific report parameters, historical reports can be set up quickly and retrieved in graphic or tabular form.

Using the myAgent application, more than 20 predefined report templates can be used for standard reports.

The optionally available myReports application expands the options for creating historical reports with over 100 predefined report templates. The report generation can be individually scheduled, and the prepared reports can be automatically sent at scheduled times in standard export formats to predefined e-mail addresses or stored at a location configured by the myReports administrator.

INFO: Reports based on the call history stored in the communication system. The maximum retention period for the call history is 365 days (default setting). An administrator with the **Expert** profile can set the retention period for the call history on a system-wide basis.

Example: The retention period was set to 100 days. This means that only data that is up to 100 days old can be used for the preparation of reports.

Data Protection

If the myReports administrator enabled data protection when configuring myReports, the last four digits of the phone numbers (CLI column) will be replaced by **** in all relevant reports.

If the subscriber has flagged his or her private number, mobile number, external number 1 and/or external number 2 as invisible, these phone numbers will not be displayed in all relevant reports.

14.9.1 Predefined Report Templates

myReports provides more than 100 predefined report templates for creating reports.

These templates are classified by subject area and assigned to the following report groups:

- **Agent Activity**
- **Agents**
- **CLI**
- **Call History**
- **Calls**
- **Fax / E-Mail**
- **Other**
- **Performance**
- **Queues**

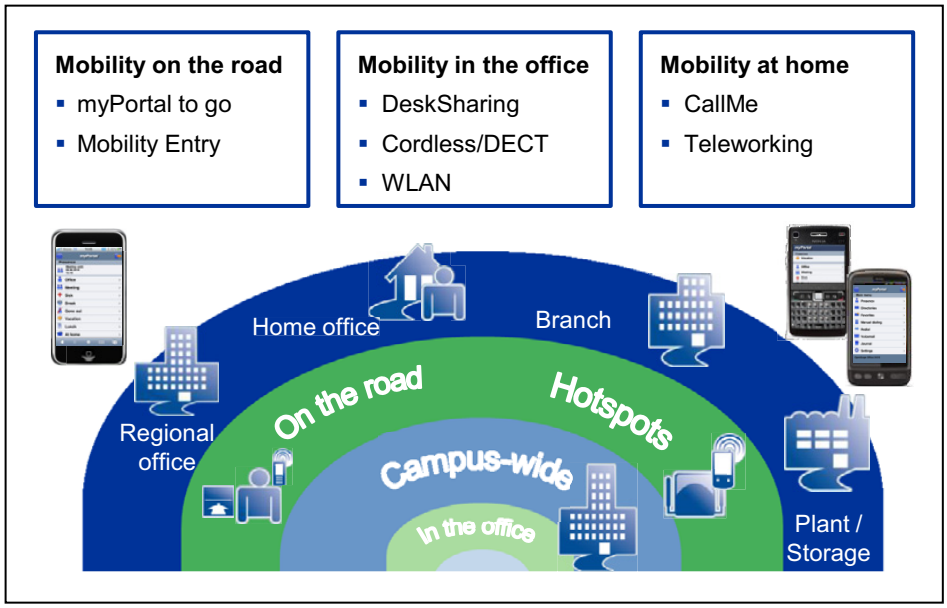
- **User Presence Status**
- **Wrap-up Codes**

15 Mobility

OpenScape Business provides integrated mobility solutions for any business. This typically includes the integration of mobile phones/smartphones, the usage of Cordless/DECT and WLAN phones, etc., down to Desk Sharing and teleworking. Mobility includes Mobility on the road, Mobility in the office and Mobility at home.

15.1 Integrated Mobility Solution

The mobility solutions integrated in the communication system provide efficient communication everywhere and with a wide variety of endpoints.



15.2 Mobility on the Road

Mobility on the road is achieved through the integration of mobile phones via myPortal to go or Mobility Entry. The One Number Service enables a subscriber to be reached through a single phone number worldwide. Furthermore, with dual-mode telephony, additional cost savings can be achieved if the subscriber is within range of a WLAN.

Mobility on the road is the combination of:

- Office phone and smartphone (myPortal to go)
  - Availability under one number (One Number Service)
  - Control of features via the web client
  - UC features such as control of the presence status

- Office phone and mobile phone (Mobility Entry)
  - Availability under one number (One Number Service)
  - Control of features via DTMF codes

In addition to the combination of mobile phone and office phone, it is also possible to configure a mobile phone alone (i.e., without a parallel office phone) to be reached under a land-line number.

Full functionality is achieved with system telephones (HFA). SIP phones can be used with restrictions.

15.2.1 myPortal to go

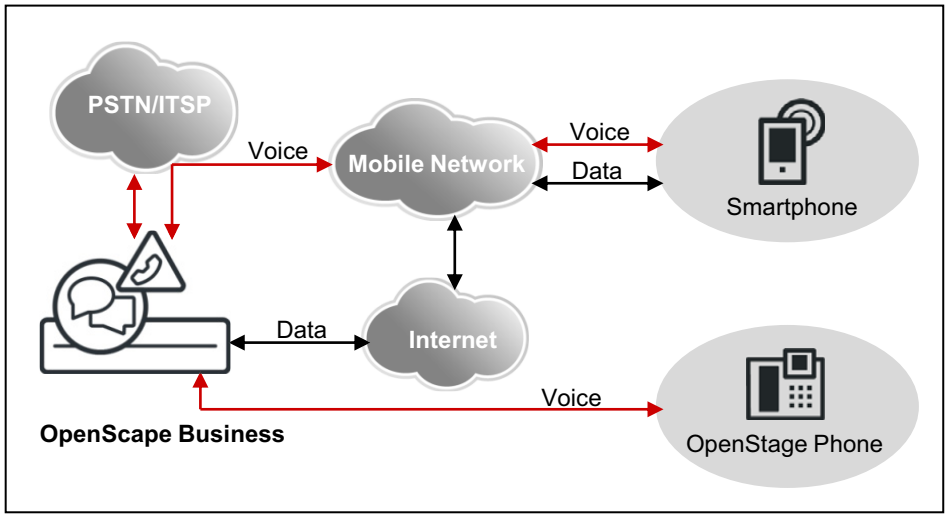
myPortal to go is a powerful unified communications application for smartphones and tablet PCs which provides access to the unified communications features of the communication system. Besides convenient dialing aids via phone directories and favorites, and information on the presence status of colleagues, it can, for example, also be used to access voicemails.

myPortal to go is available in three variants:

- As a Mobile UC App for the Android operating system (version 4.0 or higher)
- As a Mobile UC App for the Apple iOS operating system (version 6 or higher)
- as a Web Edition for mobile web browsers with HTML5 support, e.g., for the Windows Phone (version 8.0 or higher) or BlackBerry (version 10 or higher) operating systems:
  `http://<IP address of the communication system>:8801`
  `https://<IP address of the communication system>:8802`
  For security reasons it is recommended that only https be used. This requires port forwarding to be set up in the router from external TCP/443 to internal TCP/8802.

> ***INFO:*** Please note that by using myPortal to go Web Edition with Desk phone operating mode, telephony is not possible from the client. You can place calls but payload will go through the desk phone which is connected.

myPortal to go can be used both on pure GSM mobile phones as well as dual-mode phones. In order to use myPortal to go, a mobile phone contract with data option (flat rate recommended) is required.



Apart from a few exceptions (e.g., access to contact details in the mobile phone), the scope of features is identical in all variants.

myPortal to go supports the following features:

- Presence status
- Status-based call forwarding
- CallMe service (only with UC Suite)
- Directories
- Favorites List
- Journal
- Search by phone number and name
- Call Functions
- One Number Service (ONS)
- Voicemail
- Text messages

CTI Features During a Call:

- Consultation
- Toggle/Connect
- Attendant
- Conferencing
- Disconnect

myPortal to go can be used with both the UC solutions, UC Smart and UC Suite. Depending on the UC solution and the licenses assigned to you, the scope of the available features may vary slightly.

myPortal to go supports the following operating modes:

- Mobility:
  Unrestricted access to the telephony and UC features, regardless of location (including One Number Service).

- Desk phone:
  Use of UC features and as a convenient dialing aid for the office phone (without One Number Service).

Other features can be used with the UC clients (e.g., myPortal Smart or myPortal for Desktop)

myPortal go establishes an encrypted connection (https) to the OpenScape Business UC Server. If the connection is interrupted (offline mode), you can still select and dial cached entries from the journal and the favorites list via GSM and perform GSM dialing manually.

INFO: For supporting mobility, myPortal to go has to be firstly registered as VoIP (HFA) user so that the OSBiz System side relevant port to become active.

Dialing mode of myPortal to go

Smartphone users can choose between different dialing modes for outbound calls, depending on which operating mode is set as the intended use.

- Call through (only in the Mobility mode)
- Preferred callback (only in the Mobility mode)
- Associated dialing (only in the Mobility mode)
  myPortal to go controls the connection setup for the desk phone at the workplace. If a SIP phone or a SIP softclient is controlled via associated dialing, some CTI features such as consultation holds and conferencing are not available.

15.2.1.1 Prerequisites for myPortal to go

In order to use myPortal to go, the smartphone must be equipped with the appropriate hardware and software.

The following requirements apply:

- For myPortal to go as Mobile UC App: Android operating system (version 4.4 or higher) or Apple iOS (version 6 or higher)
- For myPortal to go as Web Edition: Mobile web browser with HTML5 support, e.g., for the Windows Phone (version 8.1 or higher) or BlackBerry (version 10 or higher) operating systems. Web browsers without TLS 1.2 support are not supported anymore.
  To enable access, port forwarding must be set up in the router from external TCP/443 to internal TCP/8802 (https) or internal TCP/8801 (http). For security reasons it is recommended that only https be used.
- Touch screen (recommended for ease of use)
- Display resolution for smartphones: at least 240 pixels * 320 pixels (recommended: 320 pixels * 480 pixels or higher)
- Display resolution for tablet PCs: at least 800 pixels * 480 pixels (recommended: 1024 pixels * 600 pixels or higher)

- Internet access
- Support for the simultaneous transmission of voice and data through mobile phones and the mobile network
- 3G data connection, for example, EDGE, UMTS, HSDPA (recommended for smooth service). GPRS can lead to slow page rendering.
  Alternatively: a pure WLAN connection with a SIP client for telephony.
- Flat rate data plan (recommended for cost reasons), since data volumes of several 100 MB per month may be involved, depending on usage.

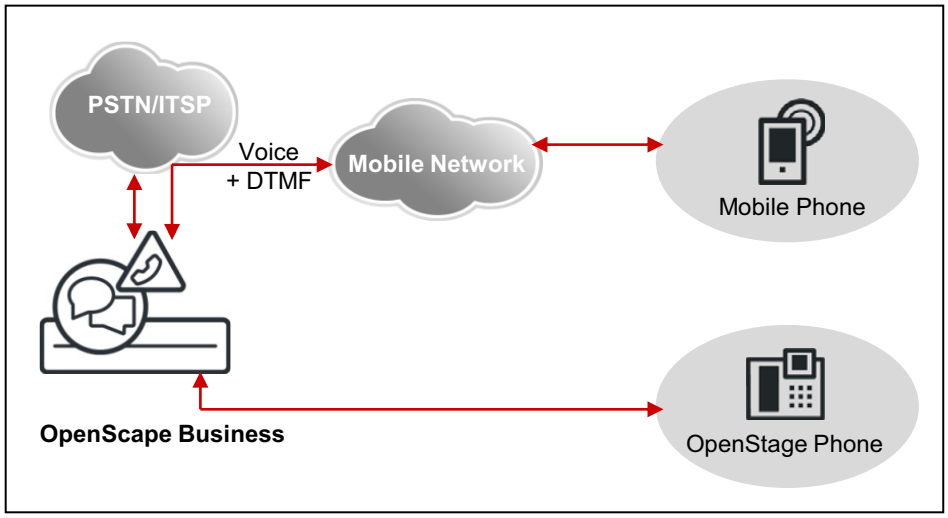
The mobile UC app can be downloaded free of charge from the Google Play Store or the Apple App Store.

Depending on which device and operating system is used, the ease of use or function may be affected. Support is only provided if a reported problem with a reference device can be reproduced. For more information on reference devices, browsers and operating systems, refer to the Release Notes and the Experts wiki at `http://wiki.unify.com/wiki/myPortal_to_go`.

15.2.2 Mobility Entry

Mobility Entry enables the integration of mobile phones. This provides subscribers with access to certain system features via mobile phones.

Mobility Entry enables subscribers to control voice connections using DTMF after dialing into the system.



Dialing Methods for Mobility Entry

Mobile phone users can choose between different dialing methods for outbound calls.

Mobility Entry offers the following dialing methods:

- Callback
- Call Through

If a mobile phone subscriber at the communication system calls a special DID number with a callback, the call is automatically terminated before the connection is established, and a callback is executed immediately. After the callback, no further authorization is necessary. The mobile phone subscriber can conduct internal and external calls and also use all Mobility features via the communications system.

The prerequisites for a callback are as follows:

- The external number of the calling telephone must be registered and configured at the communication system. If not, the call is disconnected, and no callback is executed.
- The DISA direct inward dialing number has been configured.
- The external number of the mobile phone subscriber is transmitted to the communication system (CLIP information).

Features in a Dormant State

- Dial a number
- Program or delete call forwarding
- Activate or deactivate Do Not Disturb
- Send message
- Reset all services
- Activate or deactivate station number suppression (CLIR)

Features in the Call State

- Consultation
- Alternate (Toggle/Connect)
- Conferencing
- Disconnect and return to held call
- Activate callback
- Enabling DTMF suffix dialing

The signaling of features is handled via system codes (e.g., *1 to program call forwarding).

INFO: For Mobility Entry users, the station flag **Disa Class of service** must be enabled.

A maximum of 16 DTMF code receiver resources are available with OpenScape Business X, i.e., a maximum of 16 subscribers (analog, Mobility, etc.) can simultaneously reserve DTMF code receivers. Subscribers for whom the **DTMF-based feature activation** flag is set reserve one code receiver each for the duration of the call.

With OpenScape Business S, the control of features using DTMF codes is supported if the DTMF digits are transmitted as per RFC 2833. If an external Session Border Controller (SBC) is used in the network, no DTMF detection is possible.

INFO: Mobility entry must be only configured at nodes with direct CO access.

Related Topics

- One Number Service (ONS)
- Comparison between Mobile Clients and Mobility Entry
- Dependencies for Mobile Clients and Mobility Entry

15.2.3 Comparison between Mobile Clients and Mobility Entry

The mobile clients myPortal Mobile, myPortal to go and Mobility Entry support different features.

Feature	myPortal to go	Mobility Entry
General functions		
Mobile phone contract with data option	Yes (flat rate recommended)	no
Parallel call signaling on system telephone and mobile phone (twinning)	yes	yes
Transfer of caller number to the mobile phone (if the network transmits external phone numbers as CLIP; CLIP no screening)	yes	yes
One Number Service (if the network transmits external numbers as CLIP, CLIP no Screening))	yes	yes
Do not Disturb / Disablable call forwarding	no	yes
Station number suppression, enablable/disablable	no	yes
Automatic identification of registered stations	yes	yes
Operation without the Office phone (as a virtual station)	yes	yes
Can be used with OpenScape Business S	yes	yes
Presence status, Journal, voicemail box		
Change own presence status	yes	no
View presence status of other subscribers	yes	no
Journal	New, All, Missed, Answered, Inbound, Voicemail	no
Shared voicemail box; can also be checked on the go	yes	yes
Display received voicemail	Display new, retrieved and saved voicemails	no
Dial		
Access to contacts in mobile phone	yes	yes

Feature	myPortal to go	Mobility Entry
Access to contacts in the communication system	External directory (UC Suite), internal directory, personal contacts and system directory	no
Favorites	yes	no
Manual dialing	yes	yes
Redialing	yes	no
Dialing method	Callback, Call Through, Associated Dialing	Callback, Call Through
During the call		
Consultation	yes (not with SIP phone)	yes
Alternate (Toggle/Connect)	yes (not with SIP phone)	yes
Attendant	yes (not with SIP phone)	yes
Conferencing	yes (not with SIP phone)	yes
Callback on free and busy	no	yes
Call pickup from mobile phone to system telephone	yes	yes
Busy indicator also for calls at the mobile phone (with One Number Service)	yes	yes

Related Topics

- Mobility Entry

15.2.4 Dependencies for Mobile Clients and Mobility Entry

myPortal to go and Mobility Entry have dependencies on other features (e.g., DISA).

Dependency	myPortal to go	Mobility Entry
Mobility Callback DID	For the Mobile Callback dialing mode, the Mobility Callback DID must be configured.	
External destination phone number	Dialing external destination phone numbers by the mobile subscriber is controlled by the system because of the LCR configuration. Dialing can therefore be performed via the ISDN fixed network, analog fixed network or via ITSP.	
Activate CLIP No Screening	You cannot display a caller's number on the mobile station unless it was supplied unverified by the network provider.	
Mobile subscriber CLIP	The CLIP of the mobile subscriber must be transmitted to the communication system. This must be made available by the network provider.	
LCR Administration	As some network providers (fixed-network or ITSP) do not accept destination numbers with a separate international prefix, the system must delete this prefix from these destination numbers. This can be performed in least cost routing (LCR).	

Dependency	myPortal to go	Mobility Entry
B channels / External connections	The number of B channels depends on the connection duration or the number of mobile stations. Every incoming external call to a mobile subscriber requires two voice channels in the system. If there are not enough voice channels available, it may not be possible to reach a mobile subscriber, and the mobile subscriber may not be able to initiate any calls with the One Number Service.	
Emergency Numbers	When a mobile user dials an emergency number via the communication system, the location of his or her mobile phone cannot be identified. It is therefore advisable to dial an emergency number directly.	
Dialing internal station numbers	When dialing internal phone numbers in international format (e.g., 0004989100) at the mobile station, the location number of the communication system must be configured. Otherwise, internal destinations are routed via the exchange, which can result in costs.	
Directory maintenance	To ensure that the called party can be reached when dialing from directories in all dialing modes, all external phone numbers should be entered in canonical format (e.g., +49 89 100).	-
Firewall	A data channel is set up to the integrated web server of the communication system. Consequently, port forwarding to port 8801 (http) and port 8802 (https) must be configured in the firewall. However, it is recommended not to configure any port forwarding for port 8803 (https) in order to access UC Smart Assistant.	-
Data connection	It is advisable to sign a mobile phone contract with a flat-rate data plan. Users of volume rates should disable the "Auto Refresh" option in the settings of myPortal to go.	-
Parallel connections	For some features, a simultaneous voice and data connection is required. This must be supported by both the mobile network providers and the mobile devices.	-
Connection setup from the communication system to mobile stations via	All feature types	All line types that support DTMF transmission.

Related Topics

- Mobility Entry

15.2.5 One Number Service (ONS)

The One Number Service (ONS) effectively makes mobile phones operate as fixed network extensions. This means that subscribers can be reached under one

phone number world-wide and can identify themselves only by their respective fixed network numbers.

Setting up a team configuration enables the One Number Service with a single phone number for the workplace (system telephone) and the mobile phone. The caller dials the system phone's number (fixed network). Outgoing calls from mobile phones are signaled to the called party with the fixed network number. Another advantage of the One Number Service is the busy indicator for the mobile subscriber.

Related Topics

- Mobility Entry

15.2.6 Dual-Mode Telephony

Dual-mode mobile phones support both GSM/UMTS networks and WLAN networks. Registration at the communication system is possible over a WLAN either as SIP station or as system client (i.e. HFA station).

If the dual-mode mobile phone is in the WLAN range, it is automatically called as system client (HFA station) or SIP station. If it is outside the WLAN range, the dual-mode mobile phone is called via GSM/UMTS (i.e., mobile phone integration functionality is available).

Automatic forwarding to the GSM phone number only works if the associated HFA or SIP station is entered in the system as a mobile phone station (mobile phone integration). This means that if the HFA or SIP station is registered, it is called as HFA or SIP station, and if it is not registered, it is called via the GSM phone number assigned in the mobile phone integration configuration. CTI call features are not available for SIP clients in myPortal to go. Call control usually occurs within the HFA or SIP clients instead (see also the Release Notice and `http://wiki.unify.com`).

Calls on the company premises occur over the WLAN. As long as calls are made over the WLAN, no call charges are incurred on the mobile phone. Handover and roaming are supported within the WLAN range (if the wireless LAN infrastructure is designed for it), but not from WLAN to GSM, and vice versa.

15.2.7 Configuring myPortal to go and Mobility Entry

myPortal to go (Web Edition) and Mobility Entry are configured with the **Mobile Phone Integration** wizard.

Using the **Mobile Phone Integration** wizard, the administrator can:

- Set up the One Number Service
- Set up myPortal to go (Web Edition)
- Set up Mobility Entry

- Set up dual-mode phones

The mobile phone integration of GSM phones occurs via virtual stations. Features are transferred to the mobile station in this way. Every station with a corresponding license (mobility user) can be assigned a maximum of one mobile station

Operating Modes of Mobile Phones

The following operating modes are implemented for mobile phones:

- **GSM Mode**
  Calls to the internal mobile call number are signaled at the GSM mobile phone.
- **WLAN Mode**
  If the WLAN mobile phone is reachable via the WLAN, the call is conducted via the WLAN. If the WLAN is not available, the call is made via GSM.

Twinning

Calls are signaled in parallel at the mobile phone and the system telephone (twinning). To implement twinning, a team configuration must be set up once the configuration of the **Mobile Phone Integration** has been completed. To do this, use the **Team Configuration** wizard and first select the phone number under which the parallel signaling is to occur (e.g., the system telephone). For the use of myPortal to go (Web Edition), the last step is to reconfigure the user name to the team group in the **Mobile Phone Integration** wizard. On the system telephone, a Direct Station Select (DSS) key to the Mobility stations can be programmed for the seamless (i.e., uninterrupted) transfer of mobile phone calls. Full functionality is achieved with system telephones (HFA). SIP phones can be used but are subject to certain restrictions, e.g., they do not support MULAP keys.

Related Topics

- Configuring Team Configurations / Team Groups and Executive/Secretary Functions / Top Groups using Wizards

15.3 Mobility in the office

Mobility in the office is achieved via Desk Sharing, Cordless Phones and WLAN phones. For Desk Sharing, IP Mobility (Mobile Logon and Flex Call) offers features for mobile users who want to use the phone at a different workplace just like their own phone.

15.3.1 Desk Sharing

With Desk Sharing, multiple subscribers can share one system telephone and thus one IP phone (HFA).

With Desk Sharing, subscribers have no fixed workplace and no fixed office telephone. Desk Sharing enables multiple mobile subscribers of the communication system to share an office workplace and/or the phone. The subscriber simply logs in at the workplace phone where he or she happens to be currently working.

After the login, the station number of the logged in subscriber is transferred to the used system telephone. The used system telephone can no longer be reached under its original station number. If the subscriber logs in at another system telephone, his or her station number is transferred to that new system telephone. When the user logs out (Logout), the system phone automatically logs back on with its own non-mobile number.

One of the following steps must be performed at the system phone to activate the feature:

- Enter code for "mobile logon" + number of mobile station + optional password/ PIN

When using phones with different numbers of function keys, the transfer of key layouts may be subject to restrictions.

If Desk Sharing is to be implemented for IP telephones (HFA) in networked nodes, an external DLS (Deployment Service) must be installed. The required expertise for this purpose is assumed.

The following features can be used for Desk Sharing:

- Speaker call (paging)
- Conferencing
- Override
- Toggle/Connect
- Parking
- Consultation
- Transfer
- Call pickup
- Do not disturb
- Call forwarding
- Send message (message waiting)
- Callback
- Station number suppression
- Ringing group on

INFO: For each mobile phone number, an additional Deskshare license is required. This Deskshare license must be activated for the subscriber, and the subscriber must be configured as **mobile**. In addition, the Relocate feature must be enabled.

A system telephone that is used for Desk Sharing does not necessarily require a license. However, if no license is activated and no Desk Sharing subscriber is logged in, not even emergency

calls will be possible from this phone. The system telephone/ subscriber must be configured as **Non-mobile**.

If a system telephone is not to be used for Desk Sharing, it must be configured as **Non-mobile and blocked**.

15.3.2 Integrated Cordless Solution

OpenScape Business Cordless is the integrated cordless solution for operating cordless telephones (DECT phones) via the communication system. The HFA features of OpenScape Business can then be used with the connected DECT phones.

In the integrated cordless solution, the DECT phones are internal, system-specific stations as opposed to separate DECT systems, which are connected via standard interfaces.

The connection of OpenScape Business base stations for the operation of DECT phones can be implemented via:

- For OpenScape Business X1/X3/X5: direct connections to the $U_{P0/E}$ interfaces of the mainboard of the communication system (DECT Light)
- For OpenScape Business X3/X5: connection to the $U_{P0/E}$ interfaces of an SLU8N/SLU8NR board
- For OpenScape Business X5W/X8: connection to the $U_{P0/E}$ interfaces of a Cordless SLC board

The Cordless radio technology corresponds to the DECT (Digital Enhanced Cordless Telecommunications) Standard. The entire radio area administered by the system is made up of base stations, which together form either a complete network of overlapping radio cells or individual radio "islands". The size of a radio cell is dependent on the local/structural factors.

ECO Mode

In ECO mode (economic mode), the transmit power of DECT phones is either reduced by a fixed value (static) or every DECT phone adjusts its transmit power independently to the received signal strength (adaptive). ECO mode can be enabled at the communication system on a system-wide basis for all DECT phones (**Expert Mode > Telephony > Cordless > System-wide**). No configuration is required at the DECT telephones. A manual system restart is needed to activate the feature in case of OpenScape Business X1, X3, X5

- Static adjustment of transmit power
  The DECT phones and base station reduce the transmit power to a set fixed value.
- Adaptive adjustment of transmit power
  The DECT phones transmit with normal or reduced transmit power, depending on the reception field strength. During a handover, the system first switches to the high transmit power and then reduces the transmit power, depending on the reception.

DECT phones

The integrated Cordless solution supports GAP-enabled mobile telephones from third-party manufacturers. The full scope of HFA services can, however, only be used with approved DECT phones.

Configuration

For a description of the configuration, see *Configuring the Integrated Cordless Solution*.

Boards and Base Stations

The descriptions of the boards and base stations can be found in the service documentation (*Integrated Cordless Solution*).

15.3.2.1 Cordless Direct Connections (DECT Light)

In the case of a direct connection (also referred to as DECT Light), the base station is connected directly to a $U_{P0/E}$ interface of the mainboard of the communication system or a $U_{P0/E}$ interface of an SLU8 board (only for OpenScape Business X3/X5).

When connecting base stations to an SLU8 board (only for OpenScape Business X3/X5), the following connectivity requirements apply:

- In total, a maximum of 15 base stations (7 at the mainboard and 8 more at an SLU8 board) can be operated. The maximum number of connectable DECT telephones remains unchanged at 32.
- Only one SLU8 board can be used for the connection of base stations.
- The $U_{P0/E}$ interfaces of the SLU8 board can be used with a mixed combination of base stations and/or telephones.
- Up to 4 simultaneous calls per base station can be conducted with an additionally installed CMA or CMAe module.

TDM User Licenses are required for the DECT phones.

15.3.2.2 Connecting Cordless Boards

When using Cordless boards, the base stations are connected to the $U_{P0/E}$ interfaces of the Cordless boards (SLC modules).

Base stations can be connected to the $U_{P0/E}$ interfaces of the following cordless boards:

- SLC16N with OpenScape Business X5W (wall-mount system only)
- SLCN with OpenScape Business X8

You can install up to four Cordless boards (SLCN) in OpenScape Business X8. All four Cordless boards provide full cordless functionality (roaming and seamless connection handover) because the radio fields on the Cordless boards are

synchronized within the communication system via SLC networking lines (Multi-SLC). Network-wide handover is currently not supported.

If there are not SLCN or SLC16N boards and BS is plugged on $U_{P0/E}$, then in case of an OpenScape Busines network with CMI roaming over the nodes, a CMA or CMAe module is needed on the control board.

15.3.2.3 System Configuration

Depending on the communication system, up to 64 base stations can be connected, and up to 250 DECT phones can be used.

The following table shows the maximum possible system configuration for the integrated cordless solution and indicates in which cases analog trunk access of the communication system is possible.

NOTICE: The base stations BS4 (S30807-U5491-X), BS3/1 (S30807-H5482-X), BS3/3 (S30807-H5485-X) and BS3/S (X30807-X5482-X100) are being phased out and can no longer be ordered. However, they can still be connected to OpenScape Business X communication systems.

In the event of a failure, the current base stations should be used.

INFO: If no CMA is installed, a maximum of two calls can be conducted per base station. In this case, ADPCM conversion is performed directly by the DECT base station,but echo cancellation is not directly supported. In case that echo cancellation is required a CMA/CMAe subboard is needed .

OpenScape Business	Maximum number of simultaneous calls per base station, depending on the $U_{P0/E}$ connection			Clock Module	Max. number of BaseStation BS when connected via 1xU_{P0}	Ports/ Simultaneous calls per BS	Max. number of registred devices	Max. number of simultaneous calls
	SLC16N	SLCN	SLUN					
X1	–	–	–	–	7	1/2	16	14
	–	–	–	CMA	7	1/4	16	16
	–	–	–	CMAe	7	1/4	16	16
X3	–	–	–	–	7	1/2	32	16
(Onboard SLUC)	–	–	–	CMA	7	1/4	32	16
	–	–	1	CMA	15	1/4	32	16
	–	–	–	CMAe	7	1/4	64	28
	–	–	1	CMAe	15	1/4	64	48

OpenScape Business	Maximum number of simultaneous calls per base station, depending on the $U_{P0/E}$ connection			Clock Module	Max. number of BaseStation BS when connected via $1xU_{P0}$	Ports/ Simultaneous calls per BS	Max. number of registred devices	Max. number of simultaneous calls
	SLC16N	SLCN	SLUN					
X5	–	–	–	–	7	1/2	32	16
(Onboard SLUC)	–	–	–	CMA	7	1/4	32	16
	–	–	1	CMA	15	1/4	32	16
	–	–	–	CMAe	7	1/4	64	28
	–	–	1	CMAe	15	1/4	64	48
X5	1	–	–	–	16	3/12	64	*
X8	–	4	–	–	64	3/12	250 (128 per SLCN)	**

15.3.2.4 Cordless/DECT Phones

Inserting the SLC board and entering the DECT system ID will automatically configure 16 handsets. The handset codes (PIN) are allocated and the handsets can be registered. Any additional handsets must be released before they can be used.

If a handset is replaced for servicing, the PIN must be changed before logging on the replacement handset. When a handset is replaced, a new PIN must be assigned to the relevant station in the communication system. This ensures that the handset is automatically logged off. It also improves security by preventing unauthorized parties from misusing the old PIN to log on the mobile handset.

15.3.3 Configuring the Integrated Cordless Solution

The configuration of the integrated Cordless solution includes setting up the base stations and the registration of DECT phones / mobile handsets at the communication system.

The configuration is performed in Expert mode.

The requisite steps for project planning, lighting, installation and cabling, setting up the system physically and inserting the SLC or CMA boards have been completed (see also Service Documentation). The DECT phones are charged. The DECT system ID is known. Information about subscribers, station numbers, names and, if necessary, their allocation to the SLC board is available.

General Process for Configuring the Integrated Cordless Solution

1. Configure the DECT system ID and other Cordless parameters, if necessary
2. Configure Cordless base stations

3. Log on the DECT phone at the Cordless base station
4. If necessary, add more DECT phones as required.

After the DECT phones have been commissioned, the phone numbers and names and other settings of the DECT subscribers can be edited via the WBM with the **Telephones/Subscribers** wizard.

DECT System ID

The DECT system ID is used to distinguish the different DECT systems and thus to identify the radio signals. Specifying the DECT system ID is necessary for synchronizing the registered handsets with the system.

The DECT system ID is an 8-digit hexadecimal string that is supplied on purchasing the DECT system. It is valid throughout the system (even for maintenance and service).

The DECT system ID consists of:

Digit	Meaning
1st. digit	E/ARC (Access Right Code)
2nd. - 5th. digits	EIC (Equipment Installers Code)
6th. - 7th. digits	FPN (Fixed Part Number)
8th. digit	FPS (Fixed Part Subscriber)

15.3.4 Cordless IP

Cordless IP (IP DECT) is the optional Cordless solution that serves as an alternative to the integrated Cordless solution or is used with OpenScape Business S.

The DECT phones at Cordless IP communicate via the BSIP base station with the communication system like SIP phones. Consequently, only SIP features can be used with Cordless IP. For more information on Cordless IP, refer to the documentation for HiPath Cordless IP.

For all SIP subscribers who are logged on at a Cordless IP, the station parameter **autom. connection, CSTA** must be disabled. Otherwise, this could cause calls between SIP subscribers to not be set up via DECT IP.

15.3.5 WLAN Phones and Access Points

WLAN phones and dual-mode telephones enable mobile communications. These phones can be integrated in already existing WLAN infrastructures. With WLAN Access Points, you can build wireless networks and use the same infrastructure for voice and data services. It is only recommended that only high-performance WLAN Access Points (e.g., from Enterasys) be used.

15.3.5.1 WLAN Requirements

When using a WLAN, it is important to ensure that the basic requirements for Voice-over-WLAN are satisfied. To implement the wireless portion of the network, a site survey may need to be conducted.

Decision-making aids:

- Smaller installations with up to three APs can be effectively assessed during a site visit or by studying the floor plans. It is not generally necessary to perform a site survey in this scenario.
- Site surveys should always be performed for installations with more than four APs. This applies specially to installations extending across multiple buildings or floors within buildings.
- A site survey is required irrespective of the number of APs in scenarios involving an RF-intensive environment or if you want the solution to operate alongside preexisting WLAN systems.

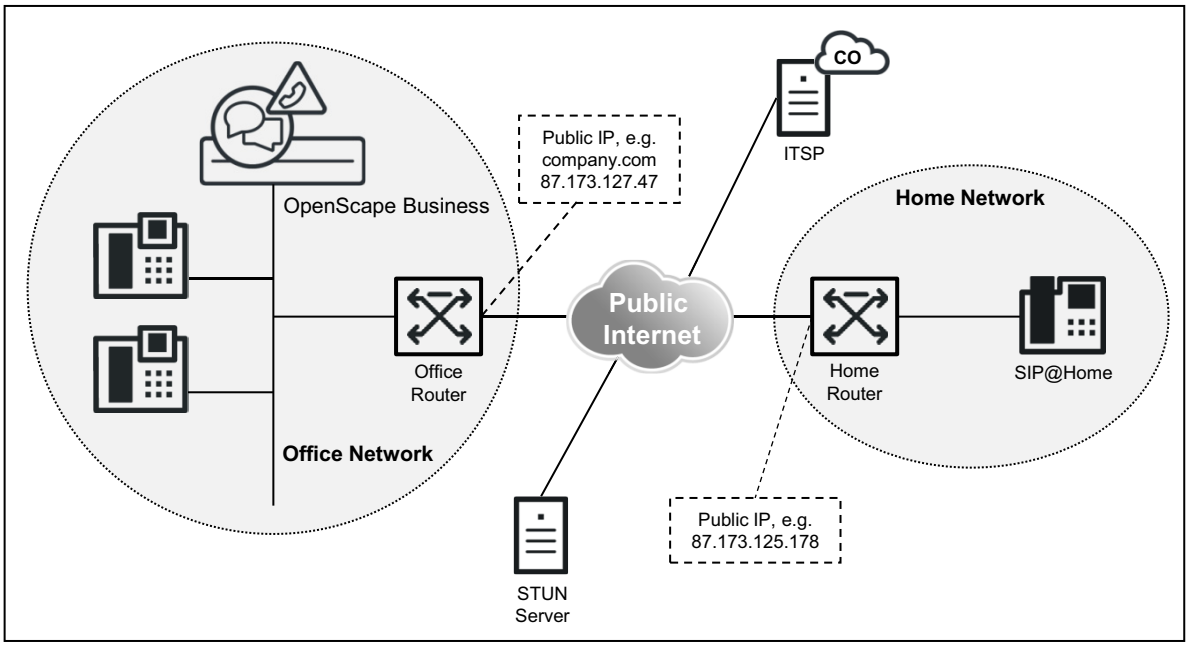
15.4 Mobility at Home

Mobility at Home is achieved through teleworking. This is done by integrating non-local phones (such as a home phone or mobile phone) in the OpenScape Business communication network.

The following types of teleworking stations are available:

- VPN stations
  OpenScape Business has a built-in VPN functionality. A total of 10 teleworkers can be simultaneously active via VPN. This may involve a home PC or a mobile phone with an Android or iOS operating system. The VPN connection is established between the native VPN client of the PC or of the mobile phone and the OpenVPN server of OpenScape Business.
  Users of UC Suite can specify their home phone number from home via their UC client and then use their private phone as an office phone (CallMe).
- Device@Home: SIP@Home stations or System Device@Home stations
  STUN-enabled SIP phones (e.g., Yealink T19) (SIP Device@Home stations) or HFA phones (System Device@Home stations) can register themselves at the communication system over the Internet by using the internal SBC function of OpenScape Business. To do this, the feature must be enabled in the station data for each SIP phone or HFA phones via the WBM.
  A STUN server must be additionally specified in the WBM only if no ITSP is being used or if the used ITSP does not offer any STUN server.
  SIP Device@Home does not support the transmission of video signals.

Figure: Device@Home (SIP Device@Home or System Device@Home) components



15.4.1 Configuring a VPN

In order to connect subscribers to the communication system via the integrated VPN functionality, certain configurations must be performed at both OpenScape Business and the VPN stations.

Configuring OpenScape Business

For the VPN configuration of the communication system, see ***Security > Virtual Private Network VPN > Connecting Teleworkers via a VPN***.

Configuring VPN Stations (VPN Clients)

To configure the VPN client, see *VPN Clients*.

15.4.2 Configuration for SIP Device@Home

In order to set up connections from a STUN-enabled SIP phone to OpenScape Business over the Internet, certain configurations must be performed at OpenScape Business, the office Internet router and the SIP telephone.

Configuring OpenScape Business

In order to enable a SIP station to register at the communication system over the Internet, the integrated SBC function must be activated for the SIP station (see).

The integrated SBC function detects the public IP address of the communication system and the port used with the aid of the STUN protocol. If the communication system is connected to an ITSP that offers a STUN server, no further configuration must be performed on the communication system. However, if either no ITSP is used or if the used ITSP does not offer any STUN server, then a STUN server must be configured in the system (see).

Configuring the Office Internet Router

In order to enable SIP phones to reach the communication system over the Internet, port forwarding for the external SIP port must be set up in the Office Internet router. To prevent SIP attacks from the Internet, a SIP port other than the default must be used as an external SIP port.

The transport protocol is set at the SIP phone.

Table: Configure Port Forwarding in the Office Router

Transport protocol	Internal SIP port	External SIP port	Comment
UDP	5070	Entering 5090, for example.	For port forwarding, the external and internal SIP ports must not be the same. A port with a different value than the internal default SIP port 5070 can thus be entered as an external SIP port. UDP is therefore recommended.
TCP	5070 Switching to 5080, for example	Entering 5080 (= internal SIP port), for example	For port forwarding, the external and internal SIP ports must be the same. To use an external SIP port other than the default 5070, the internal SIP port must be changed. This requires a reconfiguration of all IP components that use SIP. TCP is therefore **not** recommended.
TLS	5071	Entering 5071 (= internal SIP-TLS port)	For port forwarding, the external and internal SIP-TLS port must be the same. Since the internal SIP-TLS port already differs from the default SIP-TLS port, 5071 can also be entered as the external SIP-TLS port. TLS is therefore recommended.

INFO: In an upgraded system no change regarding SIP ports is performed automatically. After upgrade the ports are:

SIP_EXT = 5060

SIP_TLS_SUB_EXT = 5062

These values must be changed manually by the administrator if Device@Home is used in a migrated system.

For TLS, valid certificates must be enabled in the communication system. TLS connections for SIP stations are supported at the LAN interface of the communication system, but not at the WAN interface. SRTP payload with SDES signaling is not supported.

If the Office Internet router is connected to the Internet without a fixed IP address, then DynDNS must be configured at the Office Internet router so that SIP stations can reach the communication system over the Internet. The current IP address is registered via the DynDNS account at regular intervals. With free DynDNS accounts, which expire at regular intervals, this may temporarily lead to disruptions.

Configuring SIP Phones

As an example for the configuration you can find some tested SIP phones that support STUN, please refer to the Unify Experts wiki on the Internet. You will find the values that need to be entered at the SIP phone there.

Configuring the Home Internet Router

No special configuration is needed on the home Internet router.

The home Internet router must meet the following requirements:

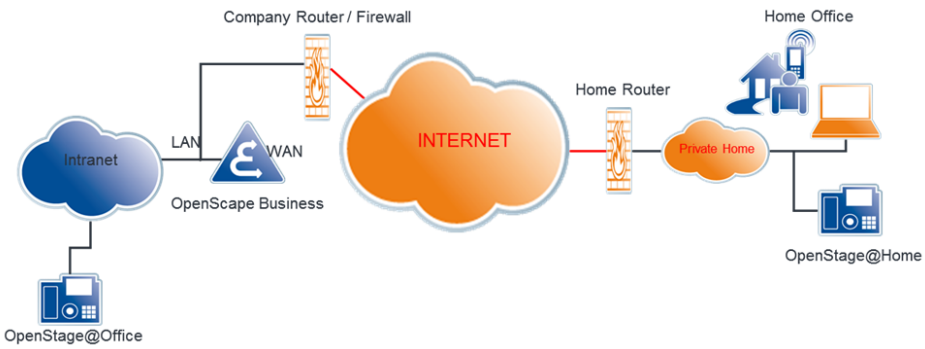
- The router must provide VoIP functionality with NAT enabled (not a symmetric NAT).
- The ALG function must be disabled in the router.

The Internet connection must provide enough bandwidth for the transmission of the call. For asymmetric DSL connections, in particular, the availability of sufficient upload bandwidth must be ensured.

15.4.3 Configuration for System Device@Home

In order to set up connections from a System Device phone to OpenScape Business over the Internet, certain configurations must be performed at OpenScape Business, the office Internet router and the System Device phone.

Figure: Example of System Device@Home use case



Configuring OpenScape Business

In order to enable a System Device@Home station to register at the communication system over the Internet, the integrated SBC function must be activated for the System Device@Home station (see *How to Enable or Disable System Device@Home*).

The integrated SBC function detects the public IP address of the communication system and the port used with the aid of the STUN protocol. If the communication system is connected to an ITSP that offers a STUN server, no further configuration must be performed on the communication system. However, if either no ITSP is used or if the used ITSP does not offer any STUN server, then a STUN server must be made known to the communication system (see How to Specify a STUN Server for System Device@Home).

Configuring the Office Internet Router

In order to enable System Device@Home stations to reach the communication system over the Internet, port forwarding for the System Device port must be set up in the Office Internet router. To be able to register from the Internet, the office router/ firewall must be configured with a port forwarding rule:

- external port TCP/4060 to internal port TCP/4062(HFA), for non-TLS
  external port TCP/4061 to internal port TCP/4063(HFA), for TLS

  NOTICE: During migration from V2R1 to a higher version, the office internet router should also reconfigured according to this rule.

- RTP port range in OpenScape Business X:30274-30529RTP port range in OpenScape Business S: 30528-30887 (default values)
- TCP/8802 (HTTPS) (required for Unified Communications client (e.g myPortal to Go, my Portal to Go Web, or VoIP for myPortal to Go configured as System Device@Home)

The transport protocol is set at the System Device@Home station.

If the Office Internet router is connected to the Internet without a fixed IP address, then DynDNS must be configured at the Office Internet router so that System Device@Home stations can reach the communication system over the Internet. The current IP address is registered via the DynDNS account at regular intervals. With free DynDNS accounts, which expire at regular intervals, this may temporarily lead to disruptions.

Configuring the Home Internet Router

No special configuration is needed on the home Internet router.

The home Internet router must meet the following requirements:

- The router must provide VoIP functionality with NAT enabled (not a symmetric NAT).
- The ALG function must be disabled in the router.

The Internet connection must provide enough bandwidth for the transmission of the call. For asymmetric DSL connections, in particular, the availability of sufficient upload bandwidth must be ensured.

Configuring the HFA Phone

The Gateway must be configured with the DNS name (e.g. mycompany.net) so that the phone can reach the system over the Internet. An internal phone number must be added for the subscriber. The device's password must also be set.

Restrictions

- It is not possible to configure XML applications at OpenStage
- Automatic phone software updates (triggered via DLI) are not supported. Only manual software update can be performed or by using an external DLS server. The phones must be updated to the latest firmware contained in the OpenSCape Business software before configuring them for System Device@Home and installing them.

OpenScape Business RTPproxy limitations

Call scenarios with payload routing via the OpenScape Business RTPproxy share common resources. As a result, the following limitations apply:

- A limited number of channels (i.e. parallel active calls), can be shared amongst all call scenarios:
  60 channels in OpenScape Business X
  180 channels in OpenScape Business S

  INFO: The available channels are used in the following cases:
  - System Device@Home
  - SIP Device@Home
  - ITSP connections
  - Circuit user connections

- Internet connection bandwidth limitations

16 Security

Security involves protecting the communication system and the stored and transmitted data against unauthorized access. This can be achieved through access protection for the IP network (firewall) and encrypted transmissions (SSL VPN, for example).

Security Checklist

The aspect of secure communications has been taken into account in the default settings of the communication system. During the initial setup, the functions and settings may need to be adapted to the specific situation of the customer, and additional provisions may have to be made in the customer environment. In order to raise the awareness of security risks and to implement suitable measures to counteract them, a security checklist is provided in the product documentation. It is urgently recommended that this checklist be discussed with the customer during the initial setup and that all implemented measures be carefully documented.

16.1 Firewall

A firewall is a system of software and hardware components that restricts access to different networks in order to implement a security concept.

Firewalls are installed at the interfaces between individual networks and control the data flow between the sub-segments to prevent unwanted data traffic and only allow the desired traffic. Firewall are most frequently used to control traffic between a local network (LAN) and the Internet.

In any corporate network, a firewall isolates the internal LAN from the Internet.

The communication system provides integrated security functions. Different functionality is offered by OpenScape Business X and OpenScape Business S for this purpose.

OpenScape Business X provides the following features:

- Port Firewall / NAT (firewall between WAN port and LAN)
- Application Firewall (firewall for access to the communication system)

OpenScape Business S uses the Linux firewall.

16.1.1 Port Handling

Port handling is used for activating ports (port mapping, port forwarding) in the firewall of the integrated router of the OpenScape Business X.

NOTICE: You should open ports only if it is absolutely necessary for a particular application!

Ports or services are required for communication via the protocols TCP and UDP because they allow multiple applications to exchange data simultaneously over a single connection.

The term firewall is generally understood as a port firewall (i.e., the blocking of individual services, or ports). The port firewall affects only the WAN port of OpenScape Business.

With OpenScape Business S, a port firewall can be enabled on the LAN port under Linux. With OpenScape Business X, the firewall on the WAN port is enabled in order to protect the internal network (LAN ports) against attacks from the Internet. If any specific ports/services need to be accessible from the Internet, they must be explicitly released (see Opening Ports). All ports/services for the functionality of OpenScape Business X are automatically released on the LAN port (into the internal network).

OpenScape Business S has only one LAN port (into the internal customer network) and is protected from the Internet by other components/routers in the customer network. In addition, the Server-internal Linux firewall is enabled. To provide the required OpenScape Business functionality, specific ports/services must be opened (to allow the phones to communicate with OpenScape Business S, for example). This is done automatically, but the administrator can disable individual services.

Port Numbers

Port numbers can accept values between 0 and 65535 which is how they are assigned to the different applications. The ports between 0 and 1023 are referred to as 'well-known ports' and are permanently assigned by the IANA (Internet Assigned Numbers Authority). A list of these ports can be found under http://www.iana.org/assignments/port-numbers.

16.1.1.1 Opening Ports

If the system sets up the Internet access (via the WAN port), then, by default, the only communication allowed is from within the internal network (i.e., from the corporate network or the communication system itself) to the Internet and the associated response packets. Requests initiated from the Internet are blocked. This security setting can be bypassed by opening the port selectively to operate a Web server on the network, for example.

NOTICE: If the communication system is used as an Internet router, port 5060 must be closed (default setting). For Internet

telephony via an ITSP, the communication system opens the relevant ports and keeps them open.

Port 5060 must likewise be closed If an external router or firewall is being used. The communication system is responsible for opening this port (if required).

16.1.1.2 Port Management

Port Management can be used to change some of the ports used by the communication system itself. This enables the network communication to be customized for each customer network even if the ports are already being used elsewhere.

If changes are to be made at the port administration, these changes must generally be made in all components (phones, systems, etc.) simultaneously in order to retain functionality.

16.1.2 NAT

NAT (network address translation) is a procedure for replacing one IP address in a data packet with another. The clients in an internal network use private IP addresses. As private IP addresses are not forwarded in a public network, you can use NAT to map the private IP addresses to a public IP address. This gives internal clients access to the public network while masking the structure of the internal network with its private IP addresses and keeping it separate from the public network (for example, the Internet). NAT and NAT rules are needed for the opening of ports.

Address translation is performed at the gateway between an internal and a public network. NAT can run on an Internet router, a server or another specialized device. An Internet router can use NAT, for instance, to connect the internal network to the Internet.

The internal network appears on the Internet with only a single public IP address, which is assigned to the Internet router by the Internet Service Provider (ISP). All access attempts made from the internal network are routed via this official IP address with different port numbers. The Internet router replaces the private IP addresses with the official IP address assigned by the ISP. In the case of incoming data packets, the official IP address is replaced by the private IP addresses. The relevant port numbers are important for allocation. Only specially enabled private IP addresses can be reached directly from the Internet.

NAT rules

You can use NAT rules to define if private (local) IP addresses should be reached directly from the Internet. Individual NAT rules can be defined for this or the default NAT rules already set can be used for the services FTP Server, HTTP Server, etc. A total of 20 NAT rules can be defined. In order to use a NAT rule, the

local address data of the client PC that will provide these services for the Internet must be entered, and the NAT rule must be activated. Multiple NAT rules can be configured together with the help of a NAT table editor. You can delete NAT rules that are no longer needed.

Ports

At startup, servers usually require the operating system to provide specific ports in order to accept connections. Typical examples include an HTTP server on port 80, an FTP server port 21, etc. Clients normally request the operating system for a random port in order to set up connections.

16.1.3 Application Firewall

The Application Firewall is used to restrict access to specific services such as FTP or LDAP. It is disabled by default and can be enabled by defining appropriate rules.

The following services can either be blocked or restricted to specific IP addresses or IP address ranges by the Application Firewall in OpenScape Business X:

Service	Ports
FTP	21, 40000 - 40040
ssh (locked by default)	22
LDAP	389
HTTPS	443
Postgres	5432
Manager E	7000
CSTA	7001 (FP), 7004 (FP), 8800 (CSP)
Observer	8808

Only the listed services can be blocked via a selection menu in Expert mode.

Telephone features such as SIP, HFA, etc. cannot be blocked using the Application Firewall.

A service can be selected multiple times; each time, different IP restrictions can be specified.

NOTICE: The activation/deactivation or modification of firewall parameters may severely restrict the functionality of the board (LAN-based administration may no longer be possible, for example).

16.1.4 Services Administration (OpenScape Business S)

The Linux-internal firewall is enabled by default, which prevents access to OpenScape Business S. The communication system does, however, also provide services (e.g., the telephony service) that require open ports (services). After the installation of OpenScape Business S, these required ports/services must therefore be opened in the firewall. If services such as SNMP are not to be used, they can be disabled in the Linux firewall.

NOTICE: Note that the blocking of services that are used by OpenScape Business S can lead to a degradation and/or failure in the functionality of the communication system.

16.2 Signaling and Payload Encryption (SPE)

SPE is a security feature for the transmission of signaling and payload data between IP system phones and the communication system. The feature is based on an asymmetrical encryption mechanism in which public and private keys are used.

Encryption of signaling and payload data:

- Signaling encryption: The signal transmission between the gateway and clients is encrypted with a 128-bit key. The TLS protocol with AES encryption is used for the transmission.
- Payload encryption: The payload or voice data is transmitted using the Secure Real-time Transport Protocol (SRTP). They are likewise encrypted with a 128-bit key (AES). SRTP is also used for IP networking. The procedure for exchanging the key for SRTP is known as Multimedia Internet Keying (MIKEY).

For SPE, the individual system telephones and communication systems involved must be able to uniquely identify one another. This is achieved through certificates, which also provide the public keys.

The keys and certificates are distributed by the DLS server; however, they can also be distributed manually.

INFO: WL2 and SIP phones cannot be used in conjunction with SPE.

An encrypted connection only exists for direct connections between two system telephones or for conferences.

SRTCP Encryption

SRTCP (Secure Real-time Transport Control Protocol) is an extension of the SRTP protocol and implements the security of control data. The extension

consists of three additional fields: an SRTCP index, an encryption flag and an authentication tag.

SPE conformity

Family	Protocol / Interface	Signalling Encryption								Payload Encryption				
		Column1	HFA Subscriber	SIP Subscriber	TDM Subscriber	Analog Subscriber	SIP-Q Trunking	ISDN CO	FAX (T38, G711)	Column2	HFA Subscriber2	SIP Subscriber2	TDM Subscriber2	Analog Subscriber2	IP-Q Trunking (GW)
OpenScape Office MX/LX															
	HFA		s	nv	t	t	s	t	t		y	n	y	y	y
	SIP-UA		t*	t*	nv	nv	t*	nv	nv		n	n	n	n	n
	SIP-Trunking/ITSP		t*	nv	nv	nv	t*	nv	nv		n	n	n	n	n
	SIP-Q Homogenous		s	t*	t	t	s	t	t*		y	n	y	y	y
	Media Server / Conference		t	nv	nv	nv	t	nv	nv		n	n	n	n	n
Openscape Business X3/X5/X8															
	HFA		s	nv	t	t	s	t	t		y	n	y	y	y
	SIP-UA		t*	t*	nv	nv	t*	nv	nv		n	n	n	n	n
	SIP-Trunking/ITSP		t*	nv	nv	nv	t*	nv	nv		n	n	n	n	n
	SIP-Q Homogenous		s	t*	t	t	s	t	t*		y	n	y	y	y
	SIP-Q Heterogenous - H4k		s	t*	t	t	s	t	t*		y	n	y	y	y
	SIP-Q Heterogenous - OSV		s	t*	t	t	s	t	t*		y	n	y	y	y
	Media Server / Conference		t	nv	nv	nv	t	nv	nv		n	n	n	n	n
	MEB / VSL		t	nv	nv	nv	t	nv	nv		n	n	n	n	n

Legend:

nv	No VoIP security
t	Default: TLS on the VoIP side; no end-to-end secure payload
s	Signaling and Payload Encryption (SPE)
*	No End-to-end Signaling Encryption (TLS)
*	
	Payload encryption
y	Secure Payload (SRTP)
n	Non-Secure Payload (RTP)

16.3 Virtual Private Network (VPN)

A virtual private network (VPN) is a PC network used to transport private data in a public network (such as the Internet). It therefore transfers data securely over an insecure network. Data is transmitted in encrypted format.

VPN offers you:

- Secure connection via an unprotected medium (Internet)
- Protection of confidential data against manipulation
- Reliable integration of external partners in the corporate network
- Access to corporate information for field service

Overview of a VPN

To ensure secure communications, VPN works as follows: A tunnel is created between the communication peers. In this instance, tunnel configuration is subject to authentication and authorization. The actual data is encrypted following tunnel configuration.

A VPN can be set up between (at least) two computers or networks (tunnel endpoints).

Two types of networking exist:

- Site-to-Site VPN
  This type of networking performs encryption between two VPN gateways; data is transferred unencrypted within the LANs.
- End-to-Site VPN
  Remote access VPN (remote access by mobile teleworkers)

System-Specific Information

The VPN parameters are principally administered via the VPN wizard.

Note that the connection to the communication system must be a secure SSL connection using OpenSwan or OpenSSL.

Dependencies

Topic	Dependency
DynDNS	The VPN endpoints must be reachable via a domain name or a fixed IP address. If this is not the case, DynDNS can be used.
DynDNS	If you change an IP address in VPN, the communication system updates the host-name-specific data (IP address) in DynDNS.
DNS	Every VPN partner can resolve the host name/IP address via the standard DNS protocol. All DNS names (such as host name) must be fully qualified domain names (FQDN). Connections via IPSec tunnels are not possible while the IP address is being updated via DNS.

16.3.1 Requirements for VPN

To ensure the quality of the voice and data transmissions, the networks being used must satisfy certain requirements. Due to encryption, in particular, more bandwidth than for other networks must be planned.

In the following examples and in the tables, the encryption mode "ESP Tunnel Mode with Authentication" is used as a basis. This mode offers the highest security for site-to-site VPNs.

Structure of an encrypted voice packet:

Protocol	Bytes	
ESP Trailer	12	
ESP Padding	varies (y)	encrypted
ESP Padding Header	2	encrypted
Voice Payload	varies (x)	encrypted
RTP	12	encrypted
UDP	8	encrypted
IP (original)	20	encrypted
ESP header	8 + iv	
IP (tunnel)	20	
802.1Q VLAN Tagging	4	
MAC (incl. Preamble, FCS)	26	
Total	**112 + iv + x + y**	

Length of the ESP Header

The length of the ESP header depends on the encryption algorithm used.

Required for Cipher Block Chaining. The ESP header contains an initialization vector (IV). The length of the IV is identical to the length of the cipher block.

Padding

Padding is required, since the encryption algorithm is based on cipher block chaining. This means that the entire encrypted portion of the packet (original IP/ UDP/ RTP header + voice payload+ESP header padding) must correspond to an integral multiple of the cipher block length.

Block length of the encryption algorithm:

Encryption Algorithm	Block length	Length of the initialization vector
AES	16 bytes (128 bit)	16 bytes (128 bit)
3DES	8 bytes (64 bit)	8 bytes (64 bit)

Calculation of the required padding bytes for voice packets:

(42 + x + y) (bytes) = N x (0 or 16 (bytes)) (N integer)

Bandwidth calculation for the AES encryption algorithm:

Codec	Packet parameters	Frame size (ms)	Payload (bytes)	Padding (Bytes)	Ethernet packet length (bytes)	Payload / Packet overhead ration	Ethernet load (incl.) header (kbps)
G.711	20	20	160	6	294	75%	117.6
G.711	30	30	240	6	372	50%	99.2
G.711	40	40	320	6	454	38%	90.8
G.711	60	60	480	6	614	25%	81.9
G.729A	1	20	20	2	150	600%	60.0
G.729A	2	40	40	6	182	300%	36.4
G.729A	3	60	60	2	198	200%	26.4

Bandwidth calculation for the DES/3DES encryption algorithm:

Codec	Packet parameters	Frame size (ms)	Payload (bytes)	Padding (Bytes)	Ethernet packet length (bytes)	Payload / Packet overhead ration	Ethernet load (incl.) header (kbps)
G.711	20	20	160	6	286	75%	114.4
G.711	30	30	240	6	366	50%	97.6
G.711	40	40	320	6	446	38%	89.2
G.711	60	60	480	6	606	25%	80.8
G.729A	1	20	20	2	142	600%	56.8
G.729A	2	40	40	14	166	300%	33.2
G.729A	3	60	60	10	182	200%	24.3

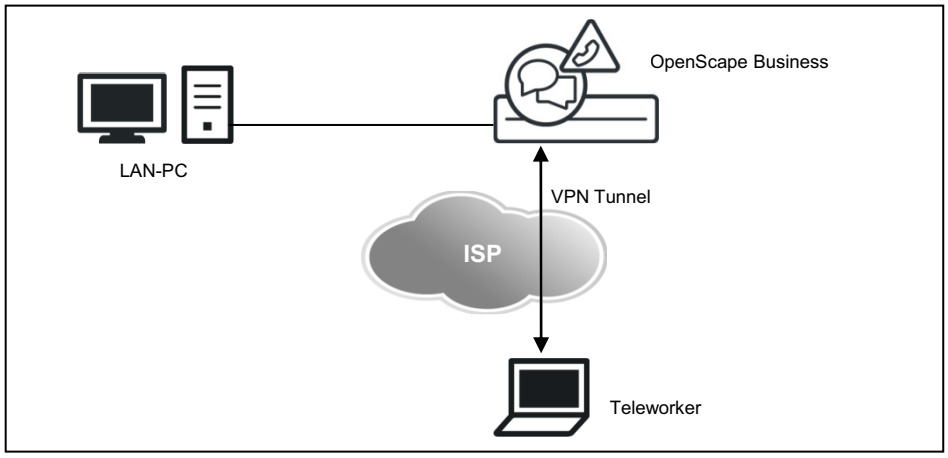
Bandwidth for T.38 Fax

Encryption Algorithm	Frame size (ms)	Payload y (bytes)	Padding x (bytes)	Ethernet packet length (bytes)	Payload packet (overhead in percent)	Ethernet load (incl.) header (kbps)
DES / 3DES	30	169	1	278	64%	74.1
AES	30	169	9	294	74%	78.3

16.3.2 Connecting Teleworkers via a VPN

Teleworkers can be connected to the communication system via a secure VPN connection.

Stand-alone System with Integration of Teleworkers via a VPN



The communication system provides integrated VPN functionality (configured using a wizard). Per communication system, up to 10 teleworkers can be simultaneously active via a VPN connection.

The following VPN clients have been released for OpenScape Business:

- NCP VPN Client
- Shrew Soft VPN Client
- Android VPN Client
- iOS VPN Client
- Mac OS-X VPN Client

Exporting the Teleworker Data

The teleworker data can be exported as a ZIP file (unencrypted). For each supported VPN client, the ZIP file contains a separate text file with the teleworker data. This is an `.ini` file for the NCP VPN client, a `.vpn` file for the Shrew Soft VPN Client and a `.networkConnect` file for the OS X VPN client. These text files can be imported at the VPN client.

> ***INFO:*** Umlauts or accents in the text files with the teleworker data are ignored. Blanks are replaced by underscores.

Status Display of VPN Connections

A status display of all VPN connections can be found in the **VPN** wizard. A detailed overview of all VPN connections can be found in the **Service Center** under **Diagnostics > Status > VPN Status**.

VPN with OpenScape Business S

With OpenScape Business S, the VPN is terminated via an external router. The description of external applications is not part of this documentation.

16.3.3 Networking Communication Systems via a VPN

Several OpenScape Business communication systems can be networked together securely using a site-to-site VPN network.

Networking via VPN

You can optionally configure all the data required for networking multiple systems on one communication system, encrypt and export this topology data and then import it on all other systems. This enables a fast and consistent configuration on all systems in the internetwork.

The distinction between the own system and the foreign systems occurs through the detection of the own DynDNS name or (when using fixed IP addresses) through the own Internet address.

- Exporting topology data from a system
  - All data about the topology of the VPN network is written to an encrypted XML file and provided as a ZIP export file for import into another system.
- Importing topology data into a system
  - All data about the topology of the VPN network can be imported from the ZIP file (with the encrypted XML file) and applied to this system.

The key (password) for export is freely selectable and must be communicated to any other administrator who may want to import these settings.

Status Display of VPN Connections

A status display of all VPN connections can be found in the **VPN** wizard. A detailed overview of all VPN connections can be found in the **Service Center** under **Diagnostics > Status > VPN Status**.

16.3.4 VPN - Security Mechanisms

In VPN, the encryption of data occurs via different security mechanisms such as IPSec tunneling, Security Associations and authentication methods (peer-to-peer, digital signatures).

IPSec Tunnels

IPSec is used to encrypt data and can generally be implemented with and without tunnels. IPSec is an option for implementing VPN. You can encrypt the entire IP packet here with the IP header: this occurs in tunnel mode.

Tunnels must always be configured for both VPN peers.

IPSec supports the automatic key management system, Internet Key Exchange (IKE). This is a standard that is integrated in IPSec.

Security Associations SA

A security association (SA) is an agreement between two communicating units in computer networks. It describes how the two parties will use security services to communicate securely with each other.

VPN connections always require three security associations (SA), negotiated in two phases:

- Phase 1 - Generating the IKE SA
  One for the initial mutual authentication and for exchanging the session keys (IKE-SA)
- Phase 2 - Negotiating the payload SAs
  One for each direction in the connection for payload traffic once established (payload SAs)

IKE SA

The IKE protocol has essentially two different tasks. Start by creating a protocol used exclusively by the IKE protocol (IKE-SA). The existing IKE-SA is then used for secure negotiation of all further SAs (payload SA) for the transmission of payload data. IKE therefore operates in the two consecutive phases:

When setting up a call between VPN partners, various parameters must be negotiated (such as how often a key is regenerated or which encryption procedures are used). These parameters are stored and administered in IKE SAs.

Payload SA

IKE phase 2 is used to negotiate all security parameters for the payload SAs between the VPN partners.

You always have to configure two SAs for transmission and receipt.

The following steps are essentially performed:

- Negotiating the algorithms for encryption and authentication
- Negotiating the security protocols used (ESP and AH)
- Negotiating the security protocol operating mode
- Negotiating the SA lifetime
- Defining the key material

Authentication

Peer-to-peer communication in VPN. The following two types of authentication are possible for VPN peers:

- Pre-shared keys
  Pre-shared keys are also mostly used for VPN. A key pair is configured for both VPN partners for this. These keys form a "hash value" which is verified by the relevant partners for authentication purposes.

- Digital signatures
  Every VPN partner is assigned a certificate. For successful authentication, the VPN peers at both tunnel endpoints must check the digital signature of their peer against a trusted CA.

System-Specific Information

The VPN parameters are principally administered via the wizard.

Note that the administrator connection must run via a secure connection with SSL.

- Security Associations SA
  The communication system supports Oakley groups 1, 2, and 5.
- IPSec
  The communication system uses IPSec tunnel mode with ESP (Encapsulating Security Payload). ESP is an IPSec protocol that guarantees packet encryption, packet integrity as well as packet authenticity
- Payload SA
  The communication system supports the encryption algorithms DES, 3DES, and AES
  Of all the MAC algorithms (MAC=Message Authentication Code) for authenticating data origin and data integrity, HMAC-SHA1, HMAC-SHA2, and HMAC-MD5 are supported.
- Recommended operating modes
  - IKE in "Main Mode" with Perfect Forward Secrecy
  - Hash function with SHA-2
  - Authentication with certificates (RSA)
  - Encryption with AES (up to 256 bits)
  - Support for dynamic public IP addresses via virtual IP addresses or DynDNS updating mechanisms for teleworker PCs

16.3.5 VPN - Certificates

A certificate binds a specific public key to a specific VPN client. In this case, the client can be both a client of the communication system and a teleworker. The unique combination of public key and VPN client provides the basis for authentication.

Certificates and certificate authority

Certificates are digitally signed and generated by a certificate authority (CA). IPSec accepts a certificate if it is issued by a trusted certificate authority.

In a simple VPN environment, the definition of an individual certificate authority may be sufficient; this CA operates as a trusted master certificate authority for the entire VPN and uses its self-signed CA certification for identification at all VPN clients.

Every VPN client needs one of the certificates issued by this CA.

Certificates based on the X.509 standard (the most widely used standard today) include the following main elements:

- information about the identity of the certificate owner
- the public key of the certificate owner,
- information about the CA that signed the certificate (a serial number, the validity period, information about the identity of the CA, and the digital signature of the CA)

Lightweight CA

A Lightweight CA function helps with certification in environments where the customer is not already using a PKI. A Lightweight CA offers the following options:

- creating public/private key pairs
- signing and generating corresponding certificates
- saving key pairs with associated certificates in files

In cryptographic terms, a PKI (public key infrastructure) is a system for generating, distributing, and verifying digital certificates.

Certificate revocation lists (CRL)

A critical situation occurs when a certificate has become known (or if this is suspected), and this certificate is hence no longer trustworthy for the peer authentication. In this case, the certificate authority must revoke the certificate and the revocation must be signaled to all peers as soon as possible. A remote peer's attempt to authenticate its identity using a revoked certificate is denied.

Basically, a CRL is a list of all revoked certificates. CRLs always have to be generated by the CA where the certificates originate.

A CRL contains the following main elements:

- a list of all revoked certificates; the certificates are identified by serial numbers
- the publication date for the next CRL updated (specifies the time to live for the CRL)
- information about the CA that generated the certificate (information on the identity of the CA and the digital signature of the CA)

The administrator must manually update and distribute the CRLs at regular intervals.

System-Specific Information

Authentication is performed on the basis of cryptographic algorithms with public keys. The communication system supports RSA as the algorithm for cryptography with public keys. The communication system only supports certificates that correspond to the X.509 standard.

The communication system always operates as a VPN client for authentication.

- Lightweight CA
  The communication system offers restricted CA functionality (Lightweight CA). The administrator provides the key material for a system by manually importing private/public key pairs and certificates via the SSL-secured administration connection for all communication partners involved.

- CRL
  CRLs (certificate revocation lists) are used to revoke certificates. The CRL is imported into the communication system by the administrator via an SSL-protected connection.

16.3.6 VPN Clients

Teleworkers can establish a secure VPN connection to the corporate network using a VPN tunnel over the Internet. To do this, a VPN client must be installed on their device (PC, tablet PC, smartphone). All data transmitted between the VPN client, the corporate firewall and the VPN server of the communication system is encrypted.

The following VPN clients are supported:

- **NCP VPN Client**
  NCP clients can be used in any VPN environments with IPSec. This is significant if access is required from a remote PC to VPN gateways of different manufacturers or if a central VPN gateway from a third-party vendor is already installed in the company network. In the case of a branch office network, the NCP Secure Enterprise Gateway can be used with other VPN gateways on the basis of IPSec connections.
  The NCP client is not free, but it offers the benefits of a graphical user interface and a status indicator for the connection.
- **Shrew Soft VPN Client**
  The Shrew Soft VPN Client is a free VPN client with a graphical user interface that supports version 2.1.5 and hybrid authentication.
  The Shrew Soft VPN client includes, among other things, ISAKMP, Xauth and RSA support, AES, Blowfish and 3DES encryption protocols, and numerous other features that are usually found only in professional solutions.
- **iOS and Android VPN Client**
  The L2TP/IPSec VPN client is integrated in the iOS or Android operating system.
  The L2TP/IPSec VPN clients use the IP address range `10.254.253.x`. If IP addresses from this range are already being used in the customer network, the IP address range needs to be changed in the WBM (e.g., from `10.254.253.1` to `10.254.252.1`) via **Expert mode > Maintenance > Application Diagnostics > IPSec Test: IPSec Test Routines > Set IP Address for L2TP**.
- **Mac OS-X VPN Client**
  The Mac OS X VPN client is integrated in the MAC OS X operating system.

System-Specific Information

- The teleworker data of a VPN client can be exported as a ZIP file (unencrypted). For each supported VPN client, the ZIP file contains a separate text file with the teleworker data. This is an `.ini` file for the NCP VPN client, a `.vpn` file for the Shrew Soft VPN Client and a `.networkConnect` file for the OS X VPN client. These text files can be imported at the VPN client.

- LAN infrastructure with multiple subnets
  If VPN is to be used for a LAN infrastructure with multiple subnets, it is necessary to create rules for these subnets. These rules cannot be created via wizards, but must be configured in Expert mode.
- Tunnel in Tunnel
  It is not possible create a second VPN tunnel through an already existing VPN tunnel.

16.3.6.1 NCP VPN Client Settings

VPN connections via the NCP VPN client require the following settings if the configuration is to be performed manually. You can export a text file with the configured VPN client data (`ncp_vpn.ini`) from your communication system and import it into the VPN client. This ensures that the respective configuration settings are populated automatically.

Basic Settings

- Profile name
  freely selectable; use of meaningful names recommended
- Connection type
  VPN to IPSec peer
- Connection medium
  In accordance with the Internet connection used
  e.g., LAN (over IP) or xDSL (PPPoE)

Dialing into network

No configuration required.

HTTP Login

No configuration required.

Modem

No configuration required.

Line Management

- Call setup
  automatic or manual
  Timeout = 0

  INFO: This ensures the connection is not cleared due to idle time!

- Prioritizing Voice over IP (VoIP)
  Set check mark
- EAP Authentication
  No configuration required

- HTTP authentication
  No configuration required

IPSec Settings

- Gateway = IP address or DNS name of the communication system
  The communication system can be reached via the Internet under this IP address or DNS name.
  Designation in the VPN wizard: **IP Address/DynDNS Name**
- IKE Policy = Unattended Mode
- IPSec Policy = Unattended Mode
- Exchange Mode = Main Mode
- PFS Group = DH Group 2 (1024 bits)
- Validity / Duration
  - IKE Policy: 000:00:07:00 (7 minutes)
  - IPSec Policy: 000:00:08:00 (8 minutes)
- Editor
  No configuration required

Advanced IPSec Options

No configuration required

Identity

- Type = IP address
  ID = IP address of the teleworker PC (see also: Assigning IP addresses)
  Use Pre-shared key
  Set check mark
  Shared Secret = This is the password for the VPN connection
  Designation in the VPN wizard: **PreShared Secret**
- Extended Authentication (XAUTH)
  not used, no configuration required

IP address assignment

- Assign IP address manually
  IP address = IP address of the teleworker PC
  Designation in the VPN wizard: **IP Address/DynDNS Name**
- DNS / WINS
  Set check mark
- DNS server = IP address of the communication system
  Designation in the VPN wizard: **Local IP Subnet Address (LAN)**

VPN - IP Networks

No configuration required.

Certificate check

No configuration required

Link Firewall

- Activate Stateful Inspection:
  for existing connection
- Allow only communication in the tunnel:
  Set check mark

16.3.7 VPN Services

You can manage services via the Configured Services function. Configured services become active services only on activation.

16.3.8 VPN tunnel

Tunnel is the term used to describe the transportation of encrypted data packets to a defined endpoint. Active tunnels become configured tunnels when the configuration is enabled. A maximum of 256 tunnels can be set up per gateway.

16.3.9 VPN rules

Rules define how IP packets are to be handled. The rule action *Pass* means that the IP packet is to be transported further (passed through). The rule action *Deny* means that the IP packet will not be transported further (i.e., will be ignored). You can also select whether or not the IP packet will use an encrypted VPN tunnel.

The communication system can manage 640 rules, of which 6 rules are preset (default rules) and 634 are free for allocation.

16.3.10 PKI Server

The PKI server designates a server that can issue, distribute and verify digital certificates. The certificates issued within a PKI (Public Key Infrastructure) are used to protect communications.

When using certificates (digital signatures), an attempt is made to download the CRL via the PKI URL configured by the PKI server.

16.4 Certificate Handling

Certificate handling (for Secure Sockets Layer, SSL) promotes the reliable administration of the communication system. The data cannot be read or manipulated by unauthorized parties. Certificates are used for authorization. You can generate and administer certificates.

Administrative access is encrypted over HTTPS using the TLS 1.2 protocol. Certificates are used to authenticate the communication system. By default, a self-signed certificate is used. A customer-specific certificate can be used to enhance security.

SSL supports the following security services:

- Authenticity (the communication partner is who he says he is)
- Trustworthiness (the data cannot be read by a third party)
- Integrity (the data was received in the same condition as it was sent)

These security services demand prior agreement on the security mechanism used and the exchange of cryptographic keys. These two tasks are performed in the course of connection setup.

SSL uses certificates and keys to guarantee secure data transmission.

CRL (Certificate Revocation List)

Certificate Revocation Lists (CRL) are files containing a list of blocked certificates, their serial number, and their blocking data. A CRL list also contains the name of the party who issued the certificate revocation list and the next authentication time.

CDP (CRL Distribution Point)

The CRL Distribution Point (CDP) is the directory (location) where the current versions of the CRLs are located (for example, http://sectestcal.microsoft.com/ErtEnvoll/SecTestCAL.crl).

System-Specific Information

Client/server communication in SSL-based administration.

The server uses the certificates generated or imported by the WBM for authentication at the client. Such certificates can be imported into the browser as trusted certificates to avoid warning messages in the browser when connecting to the SSL server.

INFO: The SSL certificate generation can also be used for SPE.

16.5 Web Security

The web access filter can be found under Web Security. It allows you to manage client permissions as well as the admin log which keeps track of any access or change to the communication system.

16.5.1 Connections to the Web Server

The connections of the clients (e.g., myPortal to go) to the internal web server of the communication system can be either encrypted (HTTPS) or unencrypted (HTTP).

NOTICE: Unencrypted connections to the web server may allow unauthorized access to sensitive data! For security reasons, it is strongly recommended that only an encrypted connection (HTTPS) be used when working with myPortal to go (Web Edition) over the Internet.

Only an encrypted connection to the web server is available for myPortal to go (App Edition).

myPortal for OpenStage (XML), the unencrypted connection (HTTP) must be first unlocked.

16.5.2 Admin Log (also called Admin Protocol)

The Admin log enables you to track what changes were made to the communication system and by whom and when.

16.6 SQL Security

OpenScape Business stores system configuration data, call data records, user account credentials, UC data etc. in an internal SQL database. Access to the database is protected by login credentials.

Up to SW version V2R2 the used login credentials are protected by a password, which could not be changed by an OpenScape Business administrator. From V2R2 on the password can be changed.The password is machine generated and is not shown to the administrator. For compatibility within multinode scenarios running old SW versions, it possible to change back a modified password to the “old” value.The SQL access password configuration can be found under SQL Security. The SQL access password configuration can be used both in network and single node environments. The handling for specific single node or multinode scenarios is described with the subsequent chapters.

16.6.1 Single node

SW Upgrade from V2R1 or older

After a SW upgrade from V2R1 the OLD SQL database password is active.The SQL password has to be changed within the new software version by the system administrator using the Administration Portal (WBM).

Setup of new system

When the date is set up in the system for the first time, a new SQL password will be generated. Only the first time the date and time is set, is when the SQL password is changed automatically.

Setup of a reloaded "single node" system

After each system reload the OLD SQL database password is active within the system.The SQL password has to be changed within the new software version by the system administrator using the Administration Portal (WBM).

16.6.2 Multinode

The single node system is configured and integrated in the network in the known manner. After system setup the new slave node synchronizes its SQL password with the master node. No action is required to adapt the SQL password within the slave node.

Reload of a V2R2 or higher node within V2R2 or higher Network

After a reload of a network node within the network, the node has to re-configured and integrated again into the network.

Reload of the Master Node

In case of a master node the SQL password has to be changed by the system administrator using the Administration Portal (WBM). All slave nodes synchronize their SQL password with the new one within the master node. No action is required to change the SQL password within the slave nodes.

Reload of the Slave Node

In case of a slave node no action is required as the slave node synchronizes its SQL password with the master node.

New V2R2 or higher slave node within V2R1 Network (not recommended scenario)

The single node system is configured and integrated in the network in the known manner. After system setup the new slave node detects that the master node uses the old SQL password and uses the old SQL password as well. No further action is required to adapt the SQL password within the slave node.

INFO: It is strictly recommended to upgrade the whole network to the latest software version.

New V2R2 or higher master node within V2R1 Network (not recommended scenario)

The master node system is configured and integrated in the network in the known manner. After system setup the new master node uses the old SQL password. The system administrator may not change the old password, as the V2R1 slaves are not able to synchronize with a new SQL password in the master node. In this case the node would not work together within the network.In case that system administrator has change the SQL password by hazard he has to switch back to the “default” password within the master node configuration.

INFO: It is strictly recommended to upgrade the whole network to the latest software version.

16.7 SIP Attack Protection

The so-called SIP attacks represent a new form of attacks on communications systems via IP telephony. Such attacks may occur either from the LAN or via the Internet (through badly configured routers). Protection against SIP attacks is provided through password-protected SIP access.

The following rules should be applicable for any SIP subscriber access:

- Active authentication
- A qualified password that
  - is between 8 and 20 characters in length
  - includes one or more uppercase letters (A to Z)
  - includes one or more lowercase letters (A to Z)
  - includes one or more digits (0 to 9),
  - includes one or more special characters (e.g.: %),
  - does not have more than 3 repeated characters
- Definition of a SIP station ID that differs from the station number.

When a new SIP station is set up, authentication is activated by default, and a random password is generated. Since this random password is not known, it must be changed by the administrator.

The relevant settings in the communication system are made using the "Central Telephony" wizard or Manager E.

During system startup, the password list is checked, and a n entry is made in the EventLog (Event Viewer) if a SIP station is configured without a password.

INFO: If the communication system is used as an Internet router, port 5060 must be closed (default setting). For Internet telephony via an ITSP, the communication system opens the relevant ports and keeps them open.

Port 5060 must likewise be closed If an external router or firewall is being used. The communication system is responsible for opening this port (if required).

17 Networking OpenScape Business

OpenScape Business communication systems can be networked with one another and additionally with the communication systems OpenScape 4000 (HiPath 4000) and OpenScape Voice as well. In a homogeneous OpenScape Business network, subscribers can now use features such as the presence status, voicemail, conferencing and much more in exactly the same way as was originally possible with only a single OpenScape Business communication system.

Possible Networks:

- Pure voice network of OpenScape Business X
- OpenScape Business X and S OpenScape Business networking (optionally with UC Suite or UC Smart).
- OpenScape Business X with OpenScape 4000 (UC functionality in OpenScape Business only under certain conditions)
- OpenScape Business X with OpenScape Voice (without UC functionality in OpenScape Business)
- Connecting External Auxiliary Equipment to OpenScape Business via SIP Interconnection.
- Networking via ISDN
- OpenScape Business internetwork with central ITSP trunk connection

The communication systems are prepared for networking with the **Networking Configuration** wizard. In this wizard, it must be specified whether a master or slave node is involved. In addition, 16 lines are automatically assigned to route 16 (networking).

All networks that use unified communications features (such as UC Smart or UC Suite, for example) must be based on a closed numbering plan. Networks without unified communications features can be based on an open or closed numbering plan. In order to respond flexibly to future extension requests from customers, it is recommended to always use closed numbering for any newly created internetwork.

> ***INFO:*** Configuring an IP network is a complex task and should only be performed by experienced service technicians.

It is not possible to set up a pure OpenScape Business X1 internetwork, since an X1 system cannot be a master system, and there always needs to be a master system in the internetwork.

A network of OpenScape Business with the following systems is not supported:

- HiPath 3000 SIP-Q; only TDM networking based on S0/S2M with CorNet NQ is supported; see *Networking via ISDN*,
- HiPath 5000 RSM
- OpenScape Office MX
- OpenScape Office LX

The migration from a HiPath 3000 (including HiPath 5000 RSM) to OpenScape Business is described in the section on *Migration*.

17.1 Network Plan

Before configuring an internetwork, a network plan should first be created after consulting with the customer.

The network plan should include the following data:

- Node ID (node number) and the associated IP addresses
- Dial plan

17.1.1 Homogeneous and Heterogeneous Networks

In general, a distinction is made in networking between homogeneous (where all components belong to a single systems family) and heterogeneous networks (with different systems).

Homogeneous (Native) Network

A homogeneous (native) network consists of components of the OpenScape Business systems family.

Heterogeneous (Hybrid) Network

A heterogeneous (hybrid) network consists of components of the OpenScape Business systems family and an OpenScape 4000 or an OpenScape Voice, for example.

Overview of all OpenScape Business Nodes in the Network

All OpenScape Business nodes in an internetwork can be displayed via the **Network** entry in the navigation bar of the WBM. In addition, all the OpenScape Business stations of the internetwork can be displayed sorted by node.

The following information can be displayed:

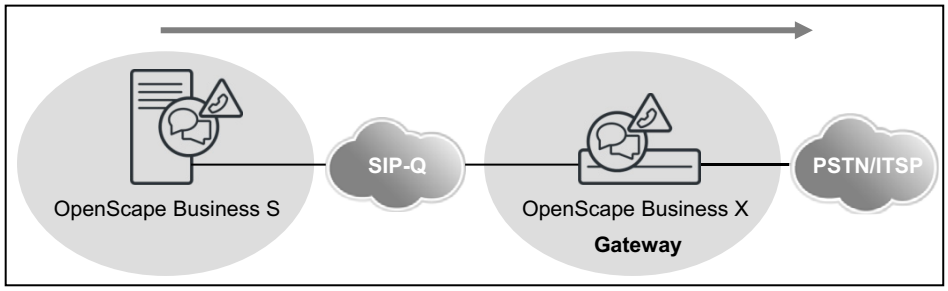
- **Node ID**: Node ID
- **M** / **S**: Identification to indicate whether the node is a Master or Slave
- **Network name**: name of the node
- **Type**: type of the node (**OSBiz X**: hardware model, **OSBiz S**: softswitch)
- **OSBiz X / OSBiz S**: IP address of the node, clickable (opens the WBM of the node)
- **Application Server**: IP address of the UC server (UC Booster Card or UC Booster Server)
- **Registration status**: status of the registration
- **Active**: Displays whether the node is active or not

17.1.2 Single and Multi-Gateway

In homogeneous OpenScape Business networks, a distinction is made between a single network and multi-gateway network, depending on whether only a single gateway or multiple gateways are used.

Single Gateway

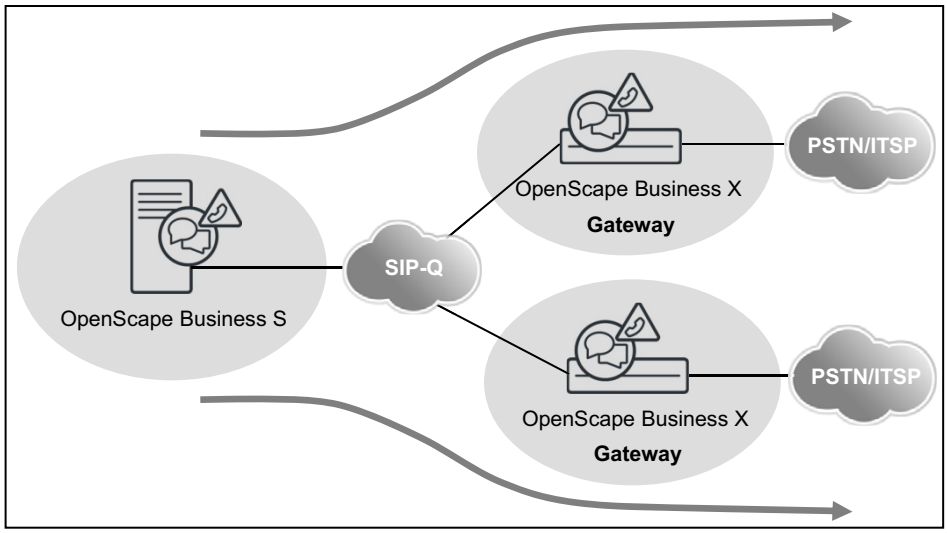
In the case of a single-gateway network, calls from and to the server are routed via a single gateway. All IP stations that are registered at the server use this single gateway.



- Supported if there are one or more OpenScape Business S systems in the network.
- The IP stations are connected to different communication systems.
- OpenScape Business X is used as a gateway.

Multi-Gateway

In the case of a multi-gateway network, calls are routed via several different OpenScape Business gateways.



- There is only one PSTN Provider and one CO station number per gateway.
- The stations of the different locations are registered at a central system (OpenScape Business S).

- Every station of the OpenScape Business S is assigned a specific gateway (OpenScape Business X).
- There must only be a single OpenScape Business S in the network.
- OpenScape Business and OpenScape Business S are in the same time zone and in the same country (same country code).
- There is only one CO access code netwide.
- ISDN and analog stations, for example, can be locally set up on the gateways.

17.2 Network-wide Features

Network-wide voice features are essentially determined by the SIP-Q networking protocol. Network-wide UC features are determined by the networking of the UC solution (UC Suite or UC Smart) and their UC clients.

17.2.1 Network-wide Features of the UC Solutions

The following table provides you with an overview of the network-wide features of both the UC solutions, UC Smart and UC Suite.

UC interworking using both OpenScape 4000 and OpenScape Voice is not possible. In an OpenScape Business internetwork, either UC Smart or UC Suite should be used. Mixed UC solutions are not supported.

Network-wide UC features	UC Smart		UC Suite	
	myPortal Smart	myPortal to go	myPortal for Desktop / Outlook	myPortal to go
Network-wide visibility of the Presence status (presence management)	x	x	x	x
Change of own presence status via the client	x	x	x	x
Change of own presence status via the TUI	x	x	x	x
Status-based call forwarding	x	x	x	Via destinations defined in myPortal
Network-wide status display in Favorites	x	x	x	x
Network-wide status display in directories	x	x	x	x

Network-wide UC features	UC Smart		UC Suite	
	myPortal Smart	myPortal to go	myPortal for Desktop / Outlook	myPortal to go
Network-wide status display in the Journal	-	-	x	-
Enable CallMe service	-	-	x	x
Calendar integration (Outlook)	-	-	x	-
Calendar integration (iCal) (only with myPortal for Desktop)	-	-	x	-
Network-wide display of the call status (free, busy, ringing state)	x	x	x	x
Creation of network-wide groups	x	x	x	-
Compact display of favorites	x	-	x	-
Personal directory	Local	Local	Local	Local
Internal directory	Local	Local	Local	Local
External directory	-	-	x	x
Searching in directories on a network-wide basis	x	x	x	x
Access to speed-dial destinations defined in the system (SSD)	Local	Local	-	Local
Import/Manage personal contacts (CSV/XML)	x	-	x	-
Access to Outlook Contacts	x	-	x	-
Import personal contacts (Mac OS) (myPortal for Desktop)	-	-	x	-
Integration of external directory server via LDAP	-	-	x	-
All calls	x	x	x	x
Open calls	x	x	x	-
Missed calls	x	x	x	x
Answered calls	x	x	x	x
Scheduled calls	-	-	x	-
Fax journal	-	-	x	-
Manual dialing	x	x	x	x
Desktop dialer (click to call)	x	-	x	-
Forwarding	x	x	x	x

Network-wide UC features	UC Smart		UC Suite	
	myPortal Smart	myPortal to go	myPortal for Desktop / Outlook	myPortal to go
Place call on hold	x	x	x	x
Record calls (voice recording)	-	-	x	-
Send e-mail	x	x	x	x
Send SMS	-	x	-	x
Popups	x	-	x	-
AdHoc conference	x	x	x	x
Scheduled conferences	-	-	x	-
Permanent and open conferences (drag & drop conference)	x	-	x	-
Web Collaboration Integration	x	-	x	-
Voicemail box (visual voicemail)	x	x	x	x
Listen to voicemail via telephone	x	x	x	x
Listen to voicemail via PC sound card	-	-	x	-
How to Send a Voice Message as an E-mail	x	x	x	-
Fax (for Windows operating systems)	-	-	x	-
Instant messaging (chat) network-wide	x	-	x	-

17.2.2 Network-wide Voice Features

For networking via the SIP-Q protocol, the following voice features are supported for OpenScape Business and other communication systems.

Feature	SIP-Q (IP Network)
Basic call	Yes
Callback on busy	Yes
Callback on RNA	Yes
Override	Yes
Call waiting	Yes

Feature	SIP-Q (IP Network)
Second call	Yes
Calling Line Identification Presentation (CLIP)	Yes
Calling Line Identification Restriction (CLIR)	Yes
Connected Line ID Presentation (COLP)	Yes
Connected Line ID Restriction (COLR)	Yes
Calling / Connected Name Identification Presentation (CNIP)	Yes
Calling / Connected Name Identification Restriction (CNIR)	Yes
Do Not Disturb	Yes
Call forwarding	Yes
Call Forwarding on Busy	Yes
Call Forwarding on RNA	Yes
Call Deflection	Yes
Advice of Charge at Call Setup	no
Advice of Charge during Call	Yes
Advice of Charge at the end of the call	Yes
Path optimization	Yes
Rerouting	no
Message Waiting Indication / Info	Yes
Trace call	Yes
Hold	Yes
Toggle/Connect	Yes
Transfer	Yes
Conferencing	Yes
Automatic Recall	Yes
Calling for Help	Yes
Intercept	Yes
Private Numbering Plan (PNP)	no
Call pickup	no
Hunt Group	Yes
SPE (except for conferencing and applications)	Yes

17.3 Licensing an Internetwork

For a networked communication system, central licensing can be selected.

All licenses of the individual systems are combined into a network-wide license at the license server. In the internetwork, the licenses can be assigned freely to the individual nodes using the WBM.

For more information, see *Licensing Multiple Communication Systems (Internetwork)*.

17.4 Networking Requirements

To ensure the quality of the voice transmission, the IP networks being used and the communication system must meet certain requirements. The voice quality and voice communication reliability always depend on the network technology in use.

Network Parameters, LAN and WAN Requirements

Parameters	Minimum requirement	Notes
Delay (one way)	50 ms	Higher values degrade the voice quality.
Round Trip Delay	100 ms	Higher values degrade the voice quality.
Jitter	20 ms	Higher values degrade the voice quality.
Packet Loss	3%	For fax or modem transmissions using G.711, the packet loss should not exceed 0.05% (in the event that no T.38 is possible).
Consecutive Packet Loss	3 with G.711	Higher values degrade the voice quality.

Recommendation for Calculating Bandwidth

- A bandwidth of at least 256 kbps (in both the sending and receiving direction) is required on the internetwork.
- The bandwidth calculation should be based on a maximum of 50% for the voice portion with respect to the total bandwidth. In other words, in the case of a 1 Mbit WAN, for example, a maximum of 500 kbps should be calculated for voice. With the G.711 codec, for example, that would be a maximum of 5 IP trunks.
- Regardless thereof, the network properties with respect to QoS, delay, packet loss, etc., must also be taken into account.

17.4.1 LAN Networking Requirements

To ensure the quality of the voice and data transmissions, the IP networks being used and the communication system must meet certain requirements for the LAN.

LAN requirements

The data network must be of the Ethernet type:

- The recommended cable is at least a Cat.5 cable (screened/unscreened multi-element cables characterized for up to 100 MHz for horizontal and building backbone cables as per EN 50288).
- Support for QoS: IEEE. 802.1p, DiffServ (RFC 2474).
- All active LAN ports must support 100 / 1000 MBit/sec. and full duplex communications.

Every communication system must be connected via a switch or a dedicated port of a router. Hubs and repeaters are not supported.

Payload Connections with RTP (Real-time Transport Protocol) in a LAN Environment

The required bandwidth for voice transmissions in an IP network can be calculated with the help of the following table:

Codec type	Packet parameters	Sample Rate (ms)	Payload (bytes)	Ethernet packet length (bytes)	Payload packet (overhead in percent)	Ethernet load (incl. header) (kbps)
G.711	20	20	160	230	44%	92
G.711	30	30	240	310	29%	82.7
G.711	40	40	320	390	22%	78
G.711	60	60	480	550	15%	73.3
G.729A	1	20	20	90	350%	36
G.729A	2	40	40	110	175%	22
G.729A	3	60	60	130	117%	17.3
RTCP		5000		280		0.4

The load in the LAN applies to both the sending and receiving direction.

The calculation includes VLAN tagging in accordance IEEE 802 1q. Without VLAN tagging, the packet length is shorter by 4 bytes.

The overhead is calculated as follows:

Protocol	Bytes
RTP Header	12
UDP Header	8
IP Header	20
802.1Q VLAN Tagging	4
MAC (incl. Preamble, FCS)	26
Total	70

Payload transport in a T.38 LAN environment:

	Sample Rate (ms)	Payload (bytes)	Ethernet packet length (bytes)	Payload packet (overhead in percent)	Ethernet load (incl. header) (kbps)
T.38	30	169	227	34%	60.5

Payload Connections with SRTP (Real-time Transport Protocol) in a LAN Environment:

Codec type	Sample Rate (ms)	Payload (bytes)	Ethernet packet length (bytes)	SRTP Ethernet packet length (kbps)	RTP Ethernet packet length (kbps)	Additional bandwidth for SRTP (%)
G.711	20	160	244	97.6	92	6.1
G.711	30	240	324	86.4	82.4	4.5
G.711	40	320	404	80.8	78	3.6
G.711	60	480	564	75.2	73.3	2.5
G.729A	20	20	104	41.6	36	15.6
G.729A	40	40	124	24.8	22	12.7
G.729A	60	60	144	19.2	17.3	10.8

17.4.2 Dial Plan in the Network

The dial plan is an important prerequisite for networking. The complexity of the internetwork configuration depends on the dial plan. OpenScape Business generally supports open and closed numbering in an internetwork. It should be noted, however, that the full scope of UC features can only be used only with closed numbering.

Closed numbering

In the case of closed numbering, a station in the internetwork is uniquely identified by the station number. Each station in the internetwork can reach another station by directly dialing its station number.

The advantage of closed numbering is that you do not have to dial a node number to reach another station in another networked communication system.

Table: Examples of closed numbering

	Node 1	Node 2	Node 3	Node 4
Phone Numbers	100	200	300	400
	101	201	301	401
	102	202	302	402
	103	203	303	403
	104	204	304	404

Open numbering

In open numbering, a station is uniquely identified by the node number and the station number. Users of different communication systems (nodes) in the internetwork can thus have the same station number.

With open numbering, the station's node number must always be dialed in addition to the phone number. Phone number ranges can be used more than once for this, and multiple phone numbers can be used.

The following UC features are not supported with open numbering:

- UC Smart
- UC Suite
- network-wide CSP (CSTA Service Provider)
- DSS server
- CMD (CSTA Message Dispatcher)
- BLF server for presence status

Table: Examples of Open Numbering

	Node 1	Node 2	Node 3	Node 4
Node number (PABX number)	95	96	97	98
Phone Numbers	100	100	100	100
	101	101	101	101
	102	102	102	102
	103	103	103	103
	104	104	104	104

17.4.2.1 Dialing Public Phone Numbers in the Network

Regardless of whether a closed or open numbering system is being used, it makes sense to dial both node and network-internal destinations using public phone numbers (e.g., as a UC client that dials contacts in the fully-qualified format from directories).

17.5 Path Optimization (Path Replacement)

Path optimization (also called path replacement) helps to avoid the dual seizure of IP trunks for networked communication systems.

When multiple OpenScape Business systems are networked, the following problem could occur, for example: First, let us assume that subscriber A calls subscriber B who, in turn, has forwarded all calls to subscriber C. Subscribers A and C are in the same network node, but subscriber B is on a different network

node. Consequently, the call with call forwarding initially seizes two trunks between the two network nodes. To avoid this dual seizure, path optimization must be enabled.

> ***INFO:*** The system flag for the path optimization must be enabled for all networked OpenScape Business systems.

The path optimization is performed:

- Within the OpenScape Business network segment
- After the connection setup (not in the ringing phase!)
- After transfer scenarios
- After call forwarding and CFNA (call forwarding-no answer)

The path optimization is not performed:

- When a ringing group or group call is involved
- For conferences
- If some other feature is enabled when executing the path optimization, the optimization is aborted.
- For inhomogeneous networking, the external systems are configured via the SIP interconnection. In this case, regardless of the configuration of the flag, no path replacement is possible (e.g., OpenScape 4000, OpenScape Voice, external SIP servers).

17.6 Networking Scenarios

There are several scenarios how OpenScape Business systems can be networked with one another and with other communication systems.

- Networking Multiple OpenScape Business X Systems
- Networking OpenScape Business X and OpenScape Business S (Single Gateway)
- Networking OpenScape Business X and OpenScape Business S (Multi-Gateway)
- Networking of OpenScape Business S in a Hosting Environment
- Networking OpenScape Business X and OpenScape Voice
- Networking OpenScape Business X and OpenScape Voice
- Connecting External Auxiliary Equipment to OpenScape Business via SIP Interconnection
- Open Numbering in OpenScape Business X Networks
- Networking via ISDN
- OpenScape Business internetwork with central ITSP trunk connection

Call charge details can only be retrieved per network node, but not across nodes.

17.6.1 Dependencies and Restrictions

It is important to note some dependencies and constraints on the possible networking scenarios.

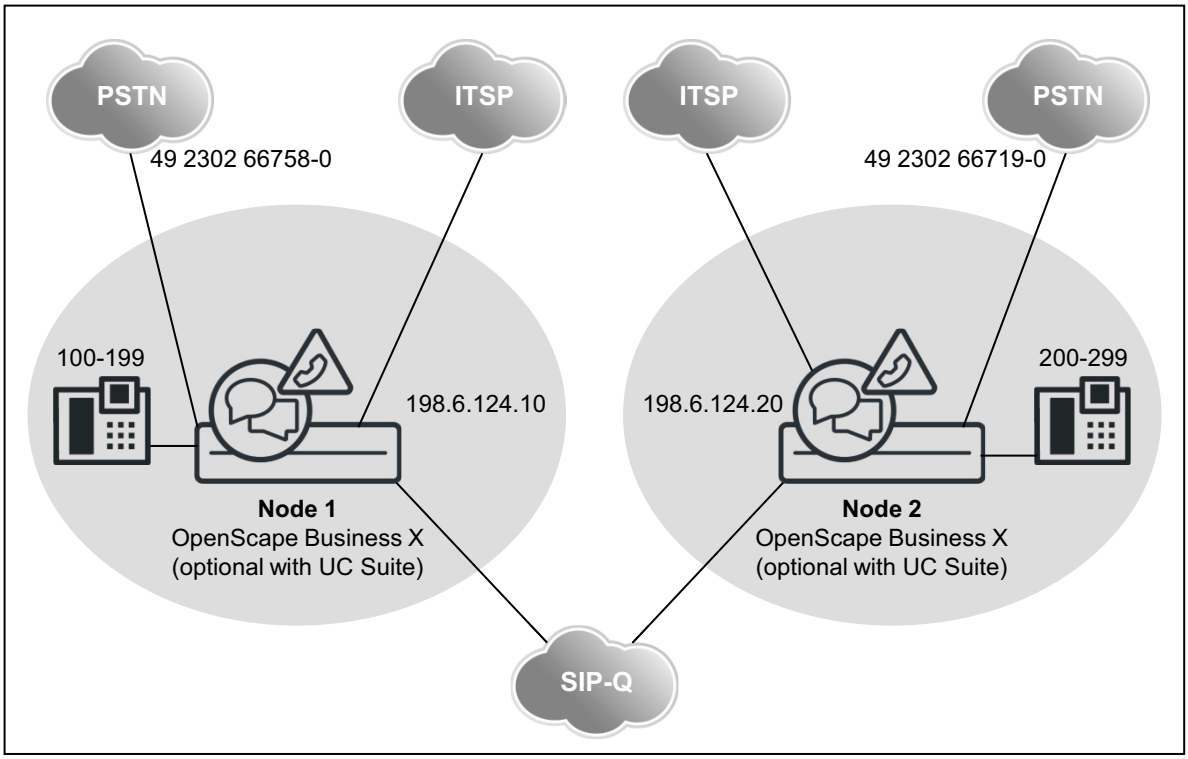
Dependencies and Restrictions

- Every system in the internetwork is assigned its own time zone. Consequently, all stations in a system have the same time zone.
- OpenScape Business S multi-gateway networks have only been released within a country (same time zone, same CO access code).
- As a general rule, all OpenScape Business internetworks are configured using wizards. OpenScape Voice and OpenScape 4000 in the internetwork are configured per node in Expert mode.
- The Presence Manager (DSS server functionality = network-wide display of busy states at DSS keys + call pickup) is available in OpenScape Business networks.
- SIP-Q trunks with route 16 (last route) are used to configure homogeneous OpenScape Business communication systems via the **Networking Configuration** wizard. External SIP trunks (SIP interconnections) are used for networking OpenScape 4000, OpenScape Voice or other communication systems; the configuration is performed in Expert mode.
- If the system is configured as a slave or master using the **Networking Configuration** wizard, a check is performed to determine whether lines are assigned to "Networking" route. If not, 16 lines are automatically assigned to the "Networking" route. If the system is removed from the internetwork, these assignments are retained.
- In each node, only ONE voicemail system can be used. As a general rule, different voicemail systems are allowed in an OpenScape Business internetwork:
  - If the UC Suite is used, any other voicemail systems present in the internetwork must be disabled by the administrator.
  - A HiPath 3000 internetwork with different voicemail systems can be migrated 1:1 to OpenScape Business.
- For technical reasons, OSBiz X1 systems can not be set up as masters. Since a master system is required in each OSBiz network, at least one system must be larger than X1.

> ***INFO:*** The relevant sales limits may differ from these details (and the following details in the individual scenarios). Please read the notes in the Sales Information.

17.6.2 Networking Multiple OpenScape Business X Systems

Up to 32 OpenScape Business X communication systems can be networked with each other.



Network Data

- With UC solution (UC Smart or UC Suite): Only closed numbering possible
- Without UC solution: Closed or open numbering possible
- Configuration via WBM (wizards) when using closed numbering
- UC Suite functionality based on UC Booster Server or UC Booster Card
- Up to 32 networked systems and 1500 users without UC solution
- Up to 8 networked systems and 1500 users with UC solution

Network-wide Features

UC networking	Closed numbering	Open numbering
Maximum number of nodes	8 with UC solution and 32 without UC solution	
Maximum number of stations in a single communication system	Depending on OpenScape Business X	
Maximum number of stations in the network	1500	

UC networking	Closed numbering	Open numbering
UC Booster Card	UC Smart: 51 - 150 stations (0 - 50 stations without UC Booster Card) UC Suite: 0 - 150 stations	Not supported
UC Booster Server	UC Smart: from 150 stations UC Suite: from 150 stations	Not supported

Administration	Closed numbering	Open numbering
WBM	Network-wide administration using wizards	Network-wide administration in Expert mode
Manager E	Network-wide administration for special tasks	Network-wide administration for special tasks
UC Suite Administration (for UC Booster Server and UC Booster Card)	Network-wide administration using wizards	Not supported
Mass data import via CSV files (call numbers, DID numbers, names)	Separately for each node in the internetwork	

Licensing	Closed numbering	Open numbering
Licensing structure	A networking license is required for each node	

Configuration

This configuration (with closed numbering and UC Suite) shows the steps required to set up networking with the help of an example.

Prerequisites:

- A network plan is available. The network plan was used to ensure that every internal call number in the internetwork is only used once for closed numbering. Different station number lengths are allowed. Only DID station numbers may occur more than once (e.g., the CO station numbers 49 2302 66758 100 and 49 2302 66719 100 have the same DID No. 100).

  INFO: The station numbers may need to be adapted. An open numbering scheme is not implemented!

- The IP network has been configured, and all nodes can be mutually pinged successfully
- All nodes have been upgraded to the same software version

Call forwarding across nodes: For incoming calls over IP trunks, which have already been forwarded, no further forwardings to the voicemail box are executed. This is because no unique assignment to the voicemail box can otherwise be made

If cross-node deputy rules (referral extensions) are required, this must be set up via the profiles of the OpenScape Business stations or ringing groups. The corresponding cross-node calls are not signaled as forwarded in this case, but as

DSS (direct station selection) calls. Call forwardings of the deputy are therefore forwarded to the voicemail box

Table: Setting up the Location Data for Node 1

Node 1		
G.-Location Country		49
G.-Location Local Network		2302
G.-Location System		66758
International Prefix		00
National Prefix		0
Routes		
ISDN	Trunk code	0
Networking	2nd trunk code	0
Routing parameters		
Route	No. and type, outgoing	RNR type
Networking	Unknown	Int/DID
ISDN	(No change in entry)	DID

The station numbers of all stations outside node 1 are automatically entered in the routing tables. This includes the internal station numbers as well as the DID station numbers, which differ from the respective internal station numbers.

Table: Overview of Entries in the LCR for Node 1

Dial Plan		**Routing table**			**Dial Rule**		
Name	**Dialed digits**	**Route**	**Dedicated Gateway**	**Gateway ID**	**Dial Rule**	**Procedure**	**Type**
Node 2 Internat	0C0049230266719-Z	Networking	Mandatory	2	D49230266719E3A	Corp. Network	International
Node 2 NAT	0C0230266719-Z						
Node 2 Stn.	0C66719-Z						
CO	0CZ	ISDN	No		A	Main network supplier	Unknown
Various	-Z	Networking	No		A	Corp. Network	Unknown

Table: Setting up the Location Data for Node 2

Node 2	
G.-Location Country	49
G.-Location Local Network	2302
G.-Location System	66719
International Prefix	00

Node 2		
National Prefix		0
Routes		
ISDN	Trunk code	0
Networking	2nd trunk code	0
Routing parameters		
Route	No. and type, outgoing	RNR type
Networking	Unknown	Int/DID
ISDN	(No change in entry)	DID

The station numbers of all stations outside node 2 are automatically entered in the routing tables. This includes the internal station numbers as well as the DID station numbers, which differ from the respective internal station numbers.

Table: Overview of Entries in the LCR for Node 2

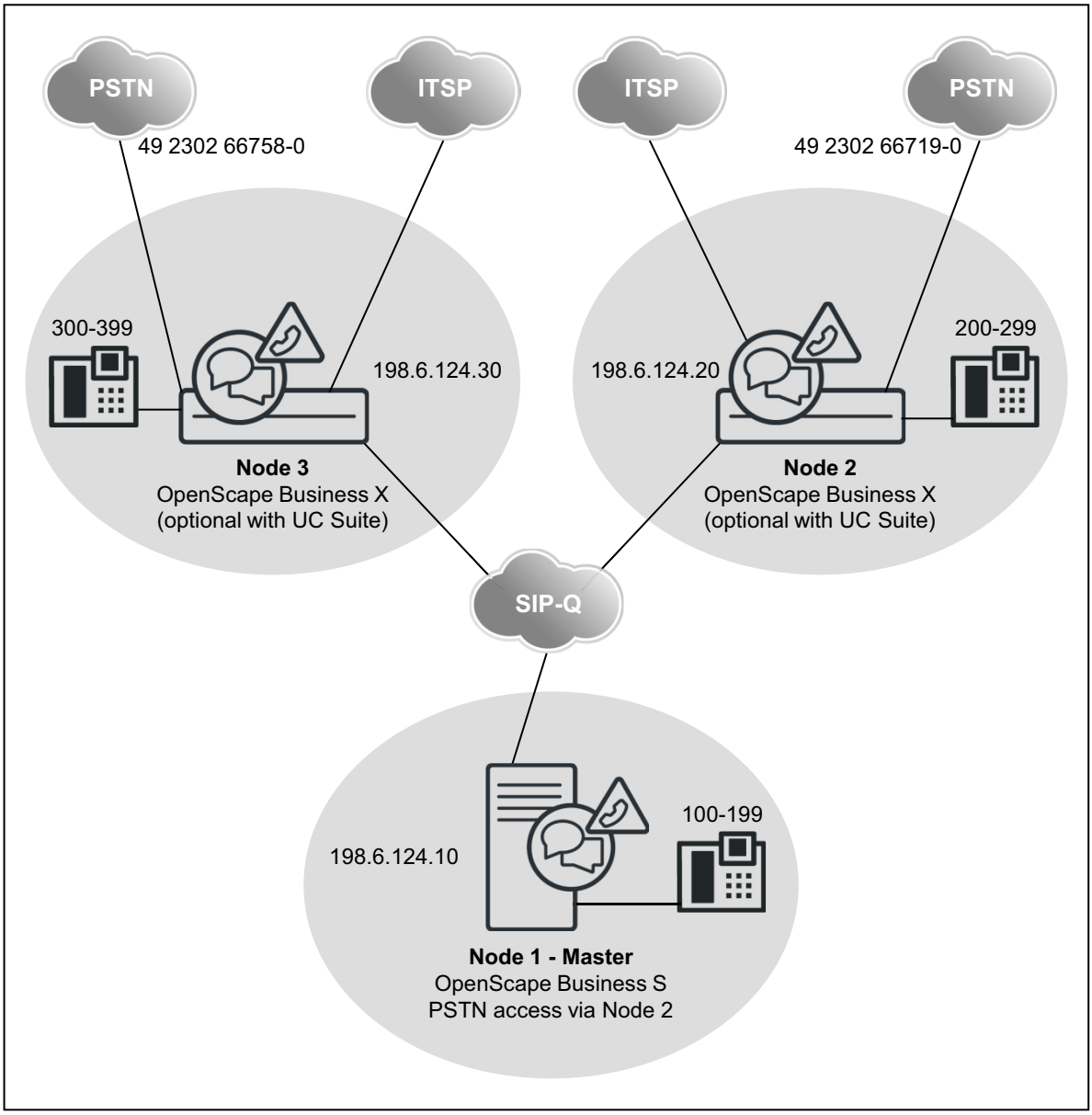
Dial Plan		Routing table			Dial Rule		
Name	**Dialed digits**	**Route**	**Dedicated Gateway**	**Gateway ID**	**Dial Rule**	**Procedure**	**Type**
Node 1 Internat	0C0049230266758-Z	Networking	Mandatory	1	D49230266758E3A	Corp. Network	International
Node 1 NAT	0C0230266758-Z						
Node 1 Stn.	0C66758-Z						
CO	0CZ	ISDN	No		A	Main network supplier	Unknown
Various	-Z	Networking	No		A	Corp. Network	Unknown

Procedure to Set up Networking:

1. Configure the basic installation for node 1 (master)
2. Configuring Networking for Node 1
3. Configure the basic installation for node 2 (slave)
4. Configuring Networking for Node 2
5. Verify the networking function for the master
6. Check routes and routing parameters (master)
7. Check routes and routing parameters (Trk. Grp. 16) (master)
8. Configure LCR for networking (master)
9. Check routes and routing parameters (Slave)
10. Configure LCR for networking (slave)

17.6.3 Networking OpenScape Business X and OpenScape Business S (Single Gateway)

Up to 32 OpenScape Business X/S communication systems can be networked with each other. Multiple OpenScape Business S systems are allowed in an internetwork. Single Gateway means that all IP stations registered at OpenScape Business S only use ONE gateway to the PSTN or ITSP.



Network Data

- Closed numbering

- Network-wide voice and UC functionality with UC Suite configuration via WBM (wizards)
- The UC functionality is implemented either through the UC Booster Server or via the UC Booster Card
- Several OpenScape Business S in one internetwork are allowed.
- Up to 32 networked systems and 1500 users without UC solution
- Up to 8 networked systems and 1500 users with UC solution

Network-wide Features

UC networking	Closed numbering	Open numbering
Maximum number of nodes	8 with UC solution and 32 without UC solution	
Maximum number of stations in a single communication system	Depending on OpenScape Business X	
Maximum number of stations in the network	1500	

UC networking	Closed numbering	Open numbering
UC Booster Card	UC Smart: 51 - 150 stations (0 - 50 stations without UC Booster Card) UC Suite: 0 - 150 stations	Not supported
UC Booster Server	UC Smart: from 150 stations UC Suite: from 150 stations	Not supported

Administration	Closed numbering	Open numbering
WBM	Network-wide administration using wizards	Not supported
Manager E	Network-wide administration for special tasks (not for OpenScape Business S)	Not supported
UC Suite Administration (for UC Booster Server and UC Booster Card)	Network-wide administration using wizards	Not supported
Mass data import via CSV files (call numbers, DID numbers, names)	Separately for each node in the internetwork	Not supported

Licensing	Closed numbering	Open numbering
Licensing structure	A networking license is required for each node	Not supported

Configuration

This configuration (with closed numbering and UC Suite) shows the steps required to set up networking with the help of an example.

Prerequisites:

- A network plan is available. The network plan was used to ensure that every internal call number in the internetwork is only used once for closed numbering. Different station number lengths are allowed. Only DID station numbers may occur more than once (e.g., the CO station numbers 49 2302 66758 100 and 49 2302 66719 100 have the same DID No. 100).
- The IP network has been configured, and all nodes can be mutually pinged successfully

Call forwarding across nodes: For incoming calls over IP trunks, which have already been forwarded, no further forwardings to the voicemail box are executed. This is because no unique assignment to the voicemail box can otherwise be made

If cross-node deputy rules (referral extensions) are required, this must be set up via the profiles of the OpenScape Business stations or ringing groups. The corresponding cross-node calls are not signaled as forwarded in this case, but as DSS (direct station selection) calls. Call forwardings of the deputy are therefore forwarded to the voicemail box.

In an internetwork in which the activation period is being used, the CLA of OpenScape Business S must always as be used as the central CLA!

Due to the different amounts of the upper limits, two different activation period files are required for OpenScape Business and OpenScape Business S. The activation period file for OpenScape Business S includes the OpenScape Business base in addition to the S base for networking scenarios.

In this scenario, whenever an OpenScape Business requests a license from a CLA of the OpenScape Business S during the activation period, the limits of the OpenScape Business S are used.

By contrast, if the CLA of the OpenScape Business were to be used instead, NO activation period would be granted to any requesting OpenScape Business S, since no basis for OpenScape Business S is included in this file.

Table: Setting up the Location Data for Node 1, OpenScape Business S

Node 1		
G.-Location Country		49
G.-Location Local Network		2302
G.-Location System		66719
International Prefix		00
National Prefix		0
Routes		
Trk. Grp 1	Trunk code	0
Networking	2nd trunk code	0
Routing parameters		
Route	No. and type, outgoing	RNR type
Networking	Unknown	Int/DID
ISDN	(No change in entry)	DID

The station numbers of all stations outside node 1 are automatically entered in the routing tables. This includes the internal station numbers as well as the DID station numbers, which differ from the respective internal station numbers.

Table: Overview of Entries in the LCR for Node 1

Dial Plan		Routing table			Dial Rule		
Name	**Dialed digits**	**Route**	**Dedicated Gateway**	**Gateway ID**	**Dial Rule**	**Procedure**	**Type**
Node 2 Internat	0C0049230266719-2Z	Networking	Mandatory	2	D49230266719E3A	Corp. Network	International
Node 2 NAT	0C0230266719-2Z						
Node 2 Stn.	0C66719-2Z						
Node 3 Internat	0C0049230266758-3Z	Networking	Mandatory	3	D49230266758E3A	Corp. Network	International
Node 3 NAT	0C0230266758-3Z						
Node 3 Stn.	0C66758-3Z						
CO	0CZ	Networking	Mandatory	2	E1A	Main network supplier	Unknown
Various	-Z	Networking	No		A	Corp. Network	Unknown

Table: Setting up the Location Data for Node 2, OpenScape Business

Node 2		
G.-Location Country		49
G.-Location Local Network		2302
G.-Location System		66719
International Prefix		00
National Prefix		0
Routes		
ISDN	Trunk code	0
Networking	2nd trunk code	0
Routing parameters		
Route	No. and type, outgoing	RNR type
Networking	Unknown	Int/DID
ISDN	(No change in entry)	DID

The station numbers of all stations outside node 2 are automatically entered in the routing tables. This includes the internal station numbers as well as the DID station numbers, which differ from the respective internal station numbers.

Table: Overview of Entries in the LCR for Node 2

Dial Plan		Routing table			Dial Rule		
Name	**Dialed digits**	**Route**	**Dedicated Gateway**	**Gateway ID**	**Dial Rule**	**Procedure**	**Type**
Node 1 Internat	0C0049230266719-1Z	Networking	Mandatory	1	D49230266719E3A	Corp. Network	International
Node 1 NAT	0C0230266719-1Z						
Node 1 Stn.	0C66719-1Z						
Node 3 Internat	0C0049230266758-3Z	Networking	Mandatory	3	D49230266758E3A	Corp. Network	International
Node 3 NAT	0C0230266758-3Z						
Node 3 Stn.	0C66758-3Z						
CO	0CZ	ISDN	No		A	Main network supplier	Unknown
Various	-Z	Networking	No		A	Corp. Network	Unknown

Table: Setting up the Location Data for Node 3, OpenScape Business

Node 3		
G.-Location Country		49
G.-Location Local Network		2302
G.-Location System		66758
International Prefix		00
National Prefix		0
Routes		
ISDN	Trunk code	0
Networking	2nd trunk code	0
Routing parameters		
Route	No. and type, outgoing	RNR type
Networking	Unknown	Int/DID
ISDN	(No change in entry)	DID

The station numbers of all stations outside node 3 are automatically entered in the routing tables. This includes the internal station numbers as well as the DID station numbers, which differ from the respective internal station numbers.

Table: Overview of Entries in the LCR for Node 3

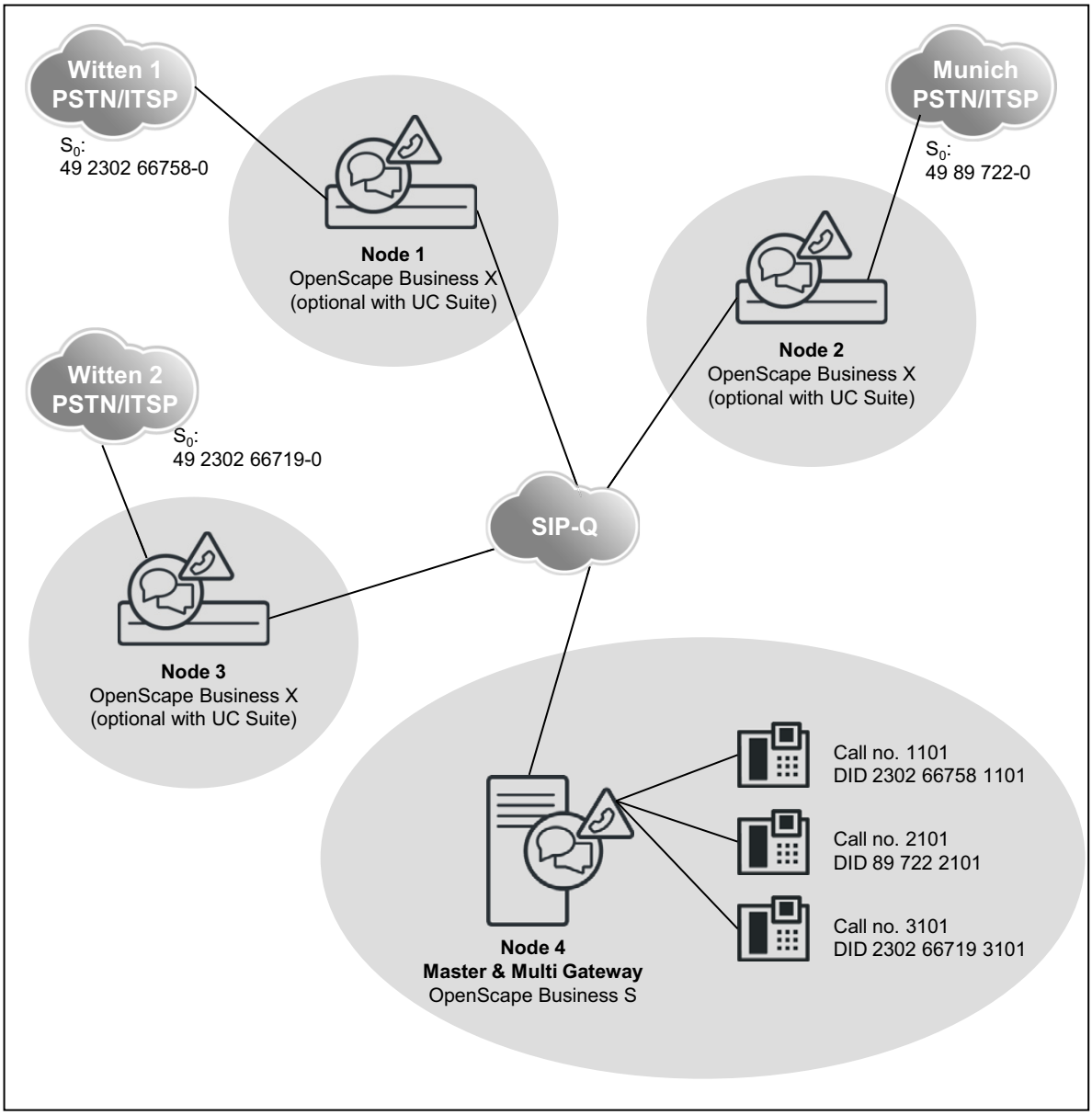
Dial Plan		Routing table			Dial Rule		
Name	**Dialed digits**	**Route**	**Dedicated Gateway**	**Gateway ID**	**Dial Rule**	**Procedure**	**Type**
Node 1 Internat	0C0049230266719-1Z	Networking	Mandatory	1	D49230266719E3A	Corp. Network	International
Node 1 NAT	0C0230266719-1Z						
Node 1 Stn.	0C66719-1Z						
Node 2 Internat	0C0049230266719-2Z	Networking	Mandatory	2	D49230266719E3A	Corp. Network	International
Node 2 NAT	0C0230266719-2Z						
Node 2 Stn.	0C66719-2Z						
CO	0CZ	ISDN	No		A	Main network supplier	Unknown
Various	-Z	Networking	No		A	Corp. Network	Unknown

Procedure to Set up Networking:

1. Configure the basic installation for node 1 (master)
2. Configuring Networking for Node 1
3. Configure the basic installation for node 2 (slave)
4. Configuring Networking for Node 2
5. Configure the basic installation for node 3 (slave)
6. Configure networking for node 3 (slave)
7. Verify the networking function for the master
8. Configure LCR for networking (node 1, master)
9. Configure LCR for networking (node 2)
10. Configure routes and routing parameters (node 3)
11. Configure routes and routing parameters (Trk. Grp. 16) (Node 3)
12. Configure LCR for networking (node 3)

17.6.4 Networking OpenScape Business X and OpenScape Business S (Multi-Gateway)

Up to 32 OpenScape Business X and OpenScape Business S communication systems can be networked with one another. Multi-gateway means that every IP station registered at OpenScape Business S is assigned to exactly one specific gateway.



Network Data

- Closed numbering
- Network-wide voice and UC functionality with UC Suite configuration via WBM (wizards)
- The UC functionality is implemented either through the UC Booster Server or via the UC Booster Card
- Only one OpenScape Business S in the internetwork is allowed.
- All systems must have the same country code
- All systems must be located in the same time zone
- Only one CO access code (e.g., 0) must exist for the entire network.
- Up to 32 networked systems and 1500 users without UC solution

- Up to 8 networked systems and 1500 users with UC solution

Network-wide Features

UC networking	Closed numbering	Open numbering
Maximum number of nodes	8 with UC solution and 32 without UC solution	
Maximum number of stations in a single communication system	Depending on OpenScape Business X	
Maximum number of stations in the network	1500	

UC networking	Closed numbering	Open numbering
UC Booster Card	UC Smart: 51 - 150 stations (0 - 50 stations without UC Booster Card) UC Suite: 0 - 150 stations	Not supported
UC Booster Server	UC Smart: from 150 stations UC Suite: from 150 stations	Not supported

Administration	Closed numbering	Open numbering
WBM	Network-wide administration using wizards	Not supported
Manager E	Network-wide administration for special tasks (not for OpenScape Business S)	Not supported
UC Suite Administration (for UC Booster Server and UC Booster Card	Network-wide administration using wizards	Not supported
Mass data import via CSV files (call numbers, DID numbers, names)	Separately for each node in the internetwork	Not supported

Licensing	Closed numbering	Open numbering
Licensing structure	A networking license is required for each node	Not supported

Configuration

This configuration (with closed numbering and UC Suite) shows the steps required to set up a multi-gateway network with the help of an example.

Prerequisites:

- A network plan is available. The network plan was used to ensure that every internal call number in the internetwork is only used once for closed numbering. Different station number lengths are allowed. Only DID station numbers may occur more than once
- The IP network has been configured, and all nodes can be mutually pinged successfully
- All nodes have been upgraded to the same software version

Call forwarding across nodes: For incoming calls over IP trunks, which have already been forwarded, no further forwardings to the voicemail box are executed. This is because no unique assignment to the voicemail box can otherwise be made

If cross-node deputy rules (referral extensions) are required, this must be set up via the profiles of the OpenScape Business stations or ringing groups. The corresponding cross-node calls are not signaled as forwarded in this case, but as DSS (direct station selection) calls. Call forwardings of the deputy are therefore forwarded to the voicemail box

Table: Setting up the Location Data for Node 1

Node 1		
G.-Location Country		49
G.-Location Local Network		2302
G.-Location System		66758
International Prefix		00
National Prefix		0
Routes		
ISDN	Trunk code	0
Networking	2nd trunk code	0
Routing parameters		
Route	No. and type, outgoing	RNR type
Networking	Unknown	Int/DID
ISDN	(No change in entry)	DID

The station numbers of all stations outside node 1 are automatically entered in the routing tables. This includes the internal station numbers as well as the DID station numbers, which differ from the respective internal station numbers.

Table: Overview of Entries in the LCR for Node 1

Dial Plan		**Routing table**			**Dial Rule**		
Name	**Dialed digits**	**Route**	**Dedicated Gateway**	**Gateway ID**	**Dial Rule**	**Procedure**	**Type**
Node 2 Internat	0C004989722-Z	Networking	Mandatory	2	D4989722E3A	Corp. Network	International
Node 2 NAT	0C089722-Z						
Node 2 Stn.	0C722-Z						
Node 3 Internat	0C00492302667 19-Z	Networking	Mandatory	3	D492302667 19E3A	Corp. Network	International
Node 3 NAT	0C0230266719-Z						
Node 3 Stn.	0C66719-Z						

Dial Plan		Routing table			Dial Rule		
Name	**Dialed digits**	**Route**	**Dedicated Gateway**	**Gateway ID**	**Dial Rule**	**Procedure**	**Type**
Node 4 Internat	0C00492302667 58-Z	Networking	NO		D230266758 E3A	Corp. Network	National
Node 4 NAT	0C0230266758-Z						
Node 4 Stn.	0C66758-Z						
Various	-Z	Networking	No		BA	Corp. Network	Unknown
CO International	0C0049-Z	ISDN	No		D0E3A	Main network supplier	Unknown
CO	0CZ	ISDN	No		A	Main network supplier	Unknown

Table: Setting up the Location Data for Node 2

Node 2		
G.-Location Country		49
G.-Location Local Network		89
G.-Location System		722
International Prefix		00
National Prefix		0
Routes		
ISDN	Trunk code	0
Networking	2nd trunk code	0
Routing parameters		
Route	No. and type, outgoing	RNR type
Networking	Unknown	Int/DID
ISDN	(No change in entry)	DID

The station numbers of all stations outside node 2 are automatically entered in the routing tables. This includes the internal station numbers as well as the DID station numbers, which differ from the respective internal station numbers.

Table: Overview of Entries in the LCR for Node 2

Dial Plan		Routing table			Dial Rule		
Name	**Dialed digits**	**Route**	**Dedicated Gateway**	**Gateway ID**	**Dial Rule**	**Procedure**	**Type**
Node 1 Internat	0C00492302667 58-Z	Networking	Mandatory	1	D492302667 E3A	Corp. Network	International
Node 1 NAT	0C0230266758-Z						
Node 1 Stn.	0C66758-Z						

Dial Plan		Routing table			Dial Rule		
Name	**Dialed digits**	**Route**	**Dedicated Gateway**	**Gateway ID**	**Dial Rule**	**Procedure**	**Type**
Node 3 Internat	0C0049230266719-Z	Networking	Mandatory	3	D49230266719E3A	Corp. Network	International
Node 3 NAT	0C0230266719-Z						
Node 3 Stn.	0C66719-Z						
Node 4 Internat	0C004989722-Z	Networking	NO		D89722E3A	Corp. Network	National
Node 4 NAT	0C089722-Z						
Node 4 Stn.	0C722-Z						
Various	-Z	Networking	No		BA	Corp. Network	Unknown
CO International	0C0049-Z	ISDN	No		D0E3A	Main network supplier	Unknown
CO	0CZ	ISDN	No		A	Main network supplier	Unknown

Table: Setting up the Location Data for Node 3

Node 3		
G.-Location Country		49
G.-Location Local Network		2302
G.-Location System		66719
International Prefix		00
National Prefix		0
Routes		
ISDN	Trunk code	0
Networking	2nd trunk code	0
Routing parameters		
Route	No. and type, outgoing	RNR type
Networking	Unknown	Int/DID
ISDN	(No change in entry)	DID

The station numbers of all stations outside node 3 are automatically entered in the routing tables. This includes the internal station numbers as well as the DID station numbers, which differ from the respective internal station numbers.

Table: Overview of Entries in the LCR for Node 3

Dial Plan		Routing table			Dial Rule		
Name	**Dialed digits**	**Route**	**Dedicated Gateway**	**Gateway ID**	**Dial Rule**	**Procedure**	**Type**
Node 1 Internat	0C00492302667 58-Z	Networking	Mandatory	1	D492302667 58E3A	Corp. Network	International
Node 1 NAT	0C0230266758-Z						
Node 1 Stn.	0C66758-Z						
Node 2 Internat	0C004989722-Z	Networking	Mandatory	2	D4989722E3 A	Corp. Network	International
Node 2 NAT	0C089722-Z						
Node 2 Stn.	0C722-Z						
Node 4 Internat	0C00498923026 6719-Z	Networking	No		D230266719 E3A	Corp. Network	National
Node 4 NAT	0C0230266719-Z						
Node 4 Stn.	0C66719-Z						
Various	-Z	Networking	No		BA	Corp. Network	Unknown
CO International	0C0049-Z	ISDN	No		D0E3A	Main network supplier	Unknown
CO	0CZ	ISDN	No		A	Main network supplier	Unknown

Setting up the Location Data for Node 4: Associate location data with a dummy CO trunk (Trk. Grp. 1) incl. CO access code = 0 and Type = CO, since node 4 has no direct connection to a Central Office.

Table: Node 4, dummy CO trunk

Node 4		
G.-Location Country		49
G.-Location Local Network		
G.-Location System		
International Prefix		00
National Prefix		0
Routes		
ISDN	Trunk code	0
Networking	2nd trunk code	0
Routing parameters		
Route	No. and type, outgoing	RNR type
Networking	Unknown	Int/DID
ISDN	(No change in entry)	DID

The station numbers of all stations outside node 1 are automatically entered in the routing tables. This includes the internal station numbers as well as the DID station numbers, which differ from the respective internal station numbers.

Table: Node 4, Networking Route

Node 4		
G.-Location Country		
G.-Location Local Network		
G.-Location System		
International Prefix		00
National Prefix		0
Routes		
ISDN	Trunk code	0
Networking	2nd trunk code	0
Routing parameters		
Route	No. and type, outgoing	RNR type
Networking	National	Int/DID
ISDN	(No change in entry)	DID

Table: Overview of Entries in the LCR for Node 4

Dial Plan		**Routing table**			**Dial Rule**		
Name	**Dialed digits**	**Route**	**Dedicated Gateway**	**Gateway ID**	**Dial Rule**	**Procedure**	**Type**
Node 1 Internat	0C00492302667 58-Z	Networking	Mandatory	1	D492302667 58E3A	Corp. Network	International
Node 1 NAT	0C0230266758-Z						
Node 2 Internat	0C004989722-Z	Networking	Mandatory	2	D4989722E3 A	Corp. Network	International
Node 2 NAT	0C089722-Z						
Node 3 Internat	0C00498923026 6719-Z	Networking	Mandatory	3	D492302667 19E3A	Corp. Network	International
Node 3 NAT	0C0230266719-Z						
Various	-Z	Networking	NO		A	Corp. Network	Unknown
CO	0CZ	Networking	MULTI-GATEWAY	1	E1A	Main network supplier	Unknown

Procedure to Set up Networking:

1. Configure the basic installation for node 4 (master)
2. Configure networking for node 4 (master)
3. Configure the basic installation for node 1 (slave)
4. Configure networking for node 1 (slave)
5. Configure the basic installation for node 2 (slave)

6. Configure networking for node 2 (slave)
7. Configure the basic installation for node 3 (slave)
8. Configure networking for node 3 (slave)
9. Verify the networking function for the master
10. Configure a multi-gateway for node 4 (master)
11. Configure routes and routing parameters (node 1, slave)
12. Configure LCR for networking (node 1, slave)
13. Configure routes and routing parameters (node 2, slave)
14. Configure LCR for networking (node 2, slave)
15. Configure routes and routing parameters (node 3, slave)
16. Configure LCR for networking (node 3, slave)
17. Configure routes and routing parameters (node 4, master)
18. Configure LCR for networking (node 4, master)

17.6.5 Networking OpenScape Business in Hosting Environments

In an environment with multiple locations (hosting environment), each site can be assigned a route, and each route can be assigned an ITSP registration. A maximum of 8 ITSP registrations can be managed. One registration per ITSP is possible or even multiple registrations at one ITSP. Each ITSP registration can be assigned an area code, and multiple subscribers can then be assigned to it. The connection between the subscribers at the different sites and the communication system occurs via a VPN or MPLS. If the sites are located in different countries, a separate OpenScape Business S must be used for each country (Scenario 1a). If all sites are located within one country, a single OpenScape Business S can be used (Scenario 1b).

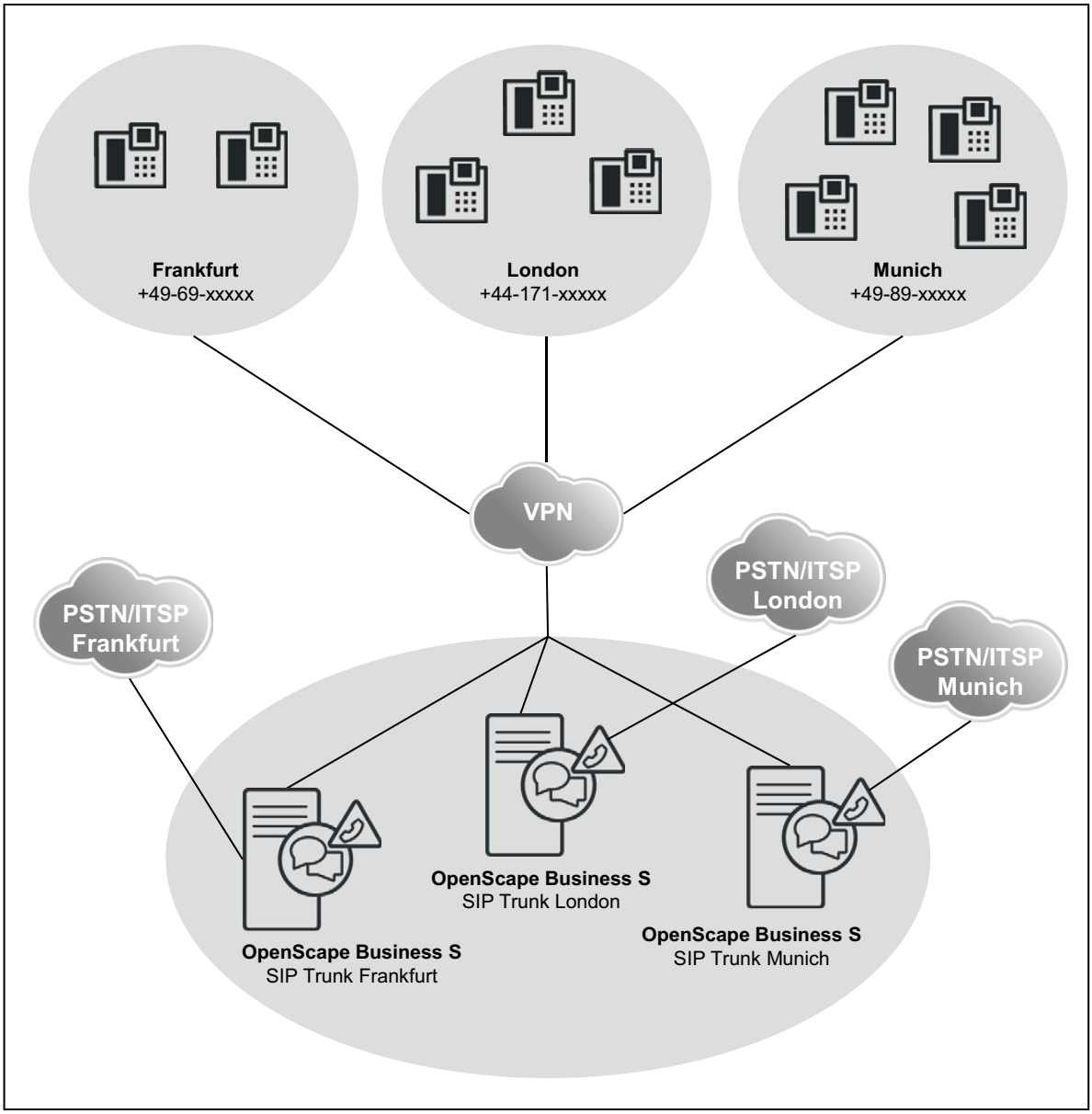
Both scenarios can also be implemented with the OpenScape Business X hardware models (e.g., for smaller configurations). The TDM components can be additionally used at one site.

The following hosting scenarios are described here in general. The following variations can be implemented:

- Use of OpenScape Business S and OpenScape Business X in the Data Center of the customer or at the hoster
- OpenScape Business S on dedicated server hardware or virtualized
- This requires a VPN or MPLS infrastructure, especially for multiple customer sites (no site-specific NAT router for Internet access)
- Up to 8 ITSP per system and country, MSN or DID provider
- Up to 8 site area codes per system and country, assigned to up to 8 customer sites (multi-site)
- Multi-site scenarios combined with classic networking (Voice and UC)
- Multi-site with more than 8 locations feasible in networks (multi-site networked n times)
- Transnational multi-site (multi-site networked n times) feasible in networks

- Networking scenarios with ISDN gateways fully integratable
- The technical prerequisite is the ability to use DID phone numbers for both ISDN providers as well as SIP providers.

Scenario a: Hosting with an OpenScape Business S per Site

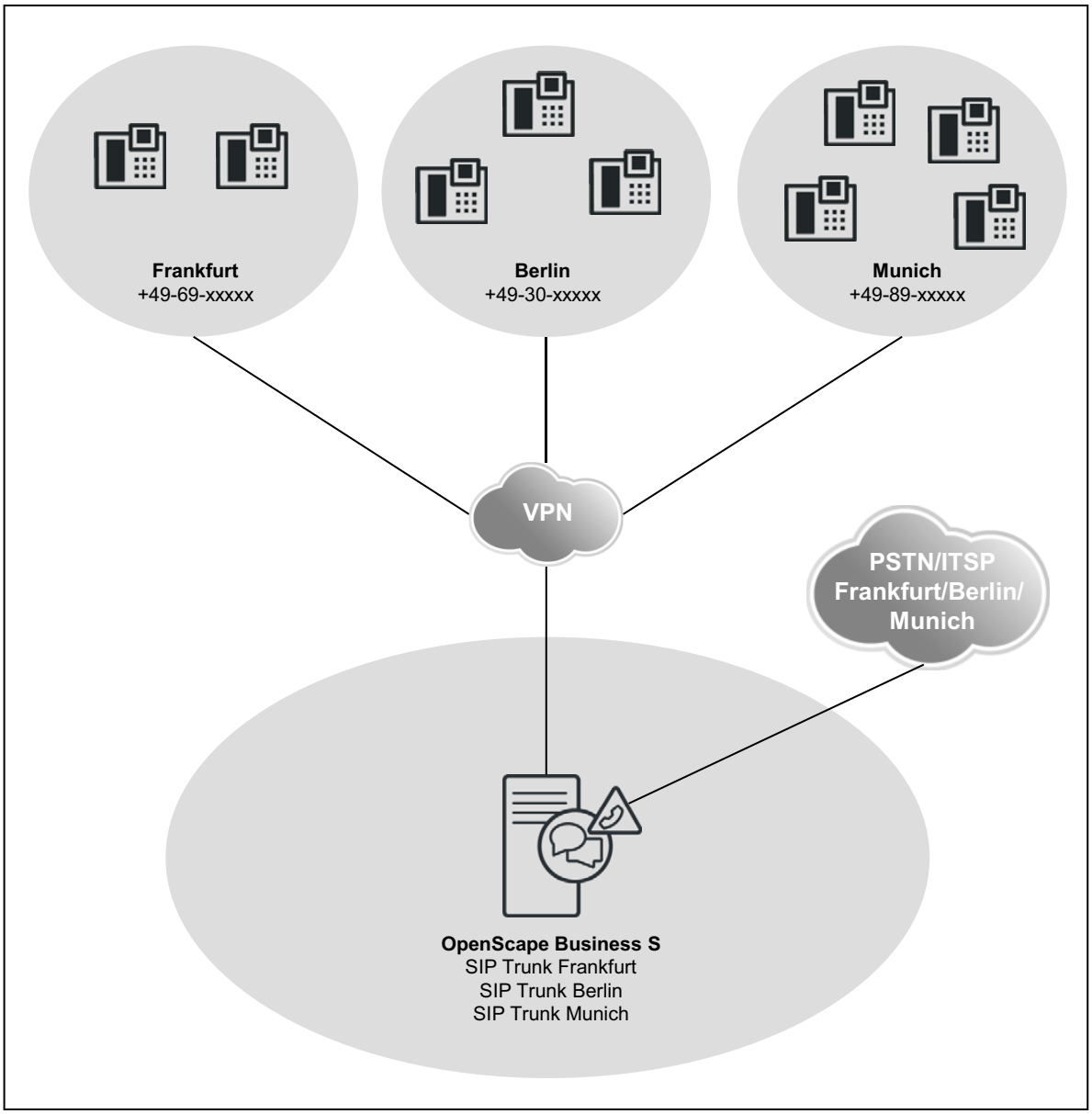


Network Data

- A customer within a VPN or MPLS.
- One OpenScape Business S per site.
- The sites may be distributed within a country or across multiple countries.
- Up to 1000 users and 180 SIP trunks per OpenScape Business S.

- OpenScape Business networking is optional, up to a total of 1500 users. Larger configurations are possible within the framework of project-specific releases.

Scenario b: Hosting with OpenScape Business S for Multiple Sites



Network Data

- A customer within a VPN or MPLS.
- One OpenScape Business S for all sites.
- All sites located within only one country.
- Up to 8 sites with different site prefixes
- Up to 8 SIP providers per OpenScape Business S.

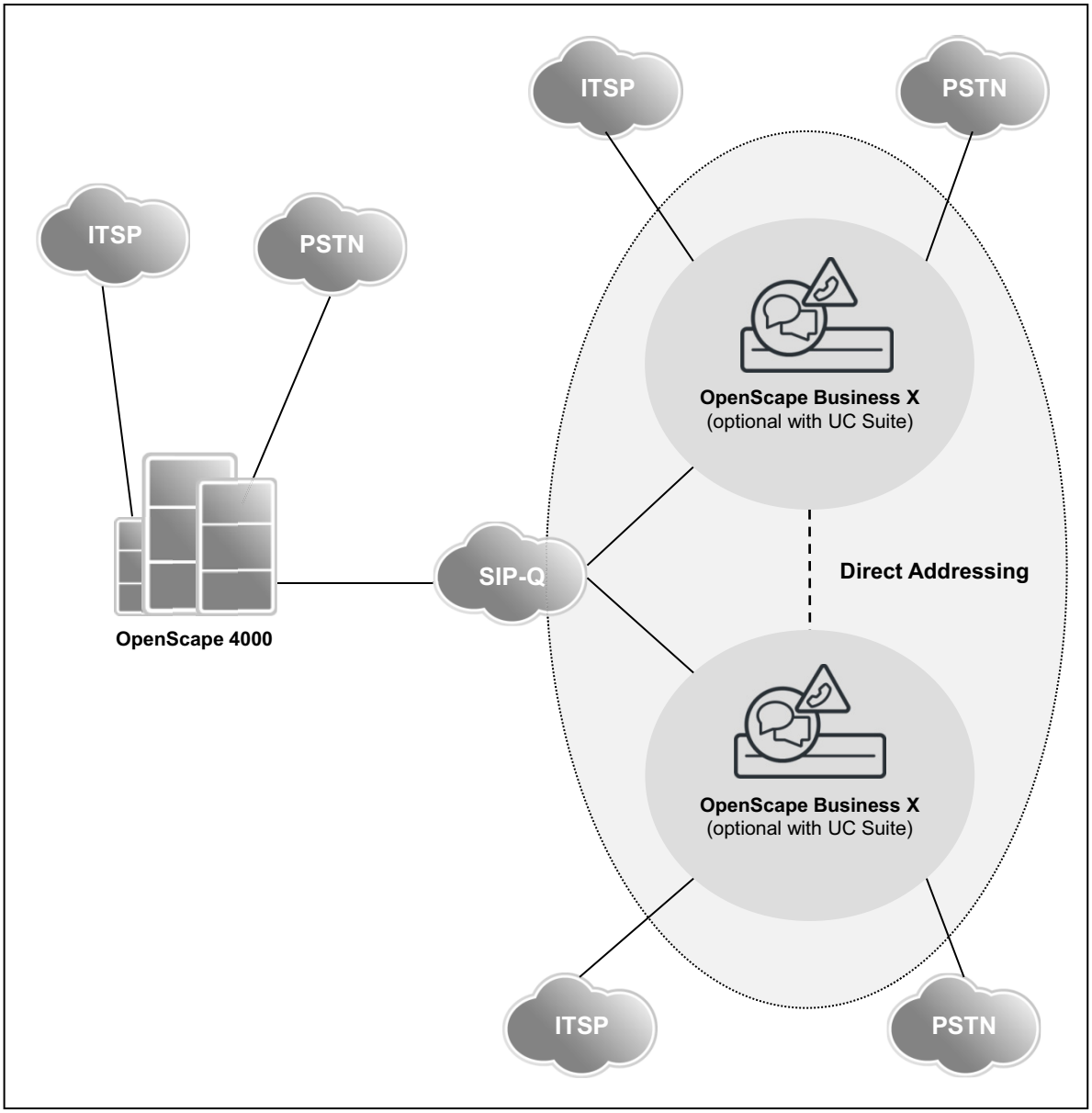
- One SIP provider per site.
- Up to 1000 users and 180 SIP trunks.
- OpenScape Business networking with multiple OpenScape Business S within a VPN is optional (OS Biz S 1 in country 1, OS Biz S 2 in country 2, etc.), up to a total of 1500 users. Larger configurations are possible within the framework of project-specific releases.
- A configuration example can be found at the Unify Experts wiki on the Internet under *ITSP Configuration Guide*,

17.6.6 Networking OpenScape Business X and OpenScape Voice

An internetwork of OpenScape Business X with OpenScape 4000 can take two different forms. First, with direct addressing between the OpenScape Business nodes (Scenario 4a), and second, with the routing of all connections via OpenScape 4000 (Scenario 4b).

INFO: A configuration example for networking with OpenScape Voice can be found in the Unify Experts wiki at `http://wiki.unify.com/wiki/How_to_collection_and_tutorials_for_OpenScape_Business`

Scenario a: Internetwork with OpenScape 4000 and Direct Addressing Between the OpenScape Business X Nodes

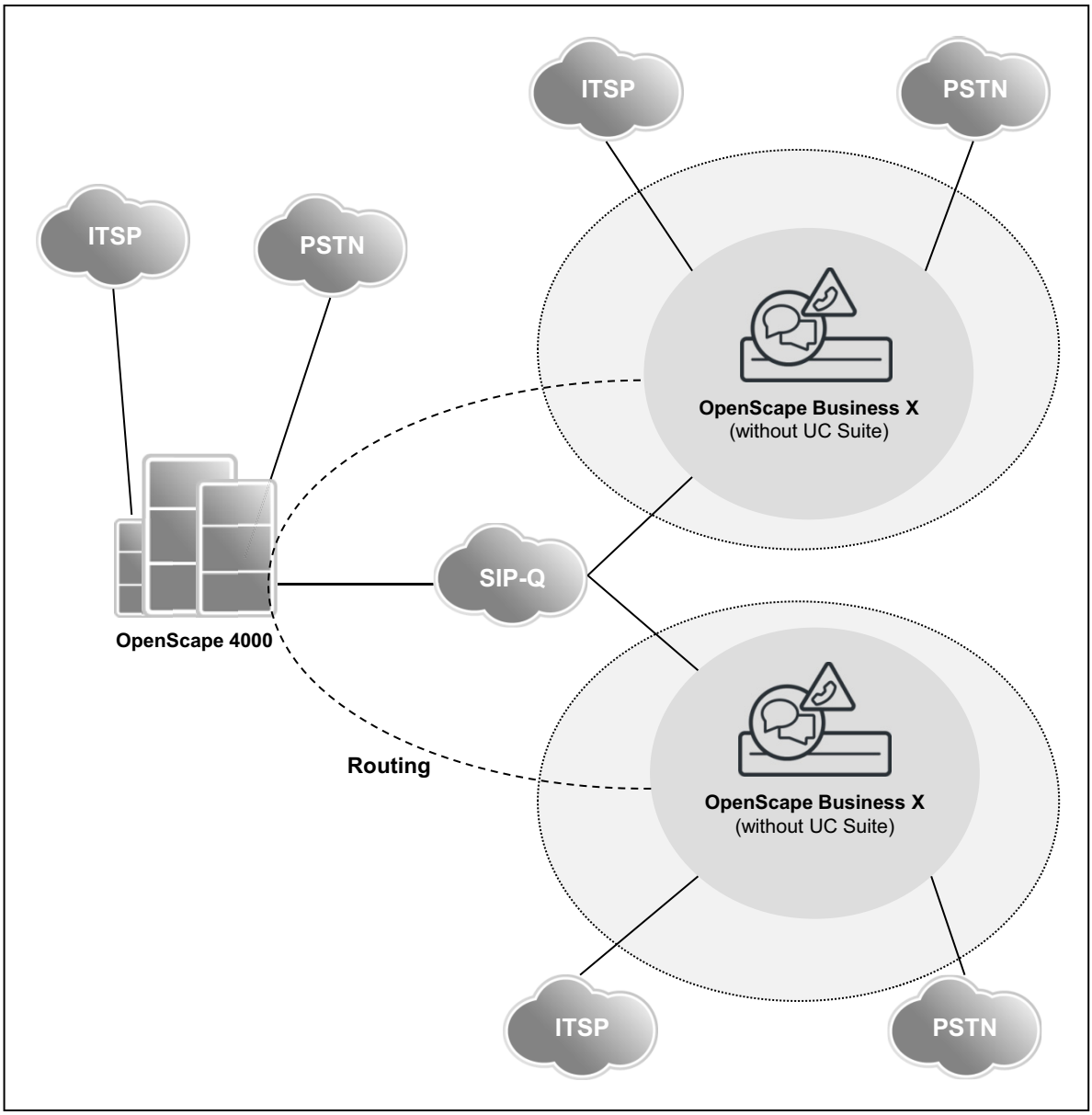


Network Data

- Closed numbering within the OpenScape Business internetwork
- Network-wide voice and UC functionality within the OpenScape Business internetwork
- Configuring the OpenScape Business internetwork with the Networking wizard
- Configuring the OpenScape 4000 network components in Expert mode
- The Small Remote Site (SRS) concept is not supported

- UC functionality via the UC Booster Server or the UC Booster Card is optional.
- OpenScape Business S can be integrated in single or multi-gateway mode.

Scenario b: Internetwork with OpenScape 4000 and Routing of all Connections via OpenScape 4000



Network Data

- Open numbering
- Network-wide voice functionality
- Every call to another node is routed via OpenScape 4000

- No UC solution in OpenScape Business because the internetwork uses open numbering
- The Small Remote Site (SRS) concept is not supported
- The configuration must be done in Expert mode for each node

Network-wide Features

Expansion	Closed numbering within the OpenScape Business internetwork (scenario 4a)	Open numbering (scenario 4b)
Maximum number of nodes	100 (32 released, depending on OpenScape 4000	
Maximum number of stations per system	Depending on the OpenScape Business X model	
Maximum number of stations in the network	1500 for the OpenScape Business network segment	Depending on OpenScape 4000
Voice networking	SIP-Q	

UC networking	Closed Numbering (Scenario 4a)	Open numbering (scenario 4b)
	Network-wide functionality within OpenScape Business	Not supported
UC Booster Card	UC Smart: 51 - 150 stations (0 - 50 stations without UC Booster Card) UC Suite: 0 - 150 stations	Not supported
UC Booster Server	UC Smart: from 150 stations UC Suite: from 150 stations	Not supported
OpenScape Business S	Supported	Not supported

Administration	Closed Numbering (Scenario 4a)	Open numbering (scenario 4b)
	WBM with wizards for OpenScape Business nodes; OpenScape 4000 is administered via the Expert mode of OpenScape Business.	Network-wide administration in Expert mode
WBM	WBM with wizards	WBM with Expert mode
Manager E	Not recommended	Not recommended
UC Suite administration	WBM with wizards for OpenScape Business nodes	Not supported
Mass data import via CSV files (call numbers, DID numbers, names)	Separately for each node in the internetwork	

Licensing	Closed Numbering (Scenario 4a)	Open numbering (scenario 4b)
Licensing structure	A network license is required for each OpenScape Business	

myPortal for Desktop / myPortal for Outlook (UC Suite)	Closed Numbering (Scenario 4a)	Open numbering (scenario 4b)
	Netwide with UC functionality via UC Booster Server, UC Booster Card or OpenScape Business S	Not supported
Instant Messaging	Network-wide, within the OpenScape Business internetwork	Not supported
Voicemail	Subscribers use their local voicemail system; there is no central voicemail for the entire internetwork.	Not supported
Presence Status	Network-wide, within the OpenScape Business internetwork	Not supported
Busy indication	Network-wide, within the OpenScape Business internetwork	Not supported
Internal Directory / Favorites	Network-wide, within the OpenScape Business internetwork	Not supported
External directory	Local, via import of CSV files	Not supported
Search in external directories of other nodes	Not possible	Not supported
External Offline Directory (LDAP)	via LDAP	Not supported

myPortal Smart (UC Smart)	Closed numbering	Open numbering
	Netwide	Not supported
Voicemail	Subscribers use their local voicemail system; there is no central voicemail for the entire internetwork.	Not supported
Presence Status	Local	Not supported
Busy indication	Local	Not supported
Internal Directory / Favorites	Local	Not supported

myAttendant	Closed Numbering (Scenario 4a)	Open numbering (scenario 4b)
	With UC functionality via UC Booster Server, UC Booster Card or OpenScape Business S	Not supported
Instant Messaging	Network-wide, within the OpenScape Business internetwork	Not supported
Voicemail	Subscribers use their local voicemail system; there is no central voicemail for the entire internetwork.	Not supported
Presence Status	Network-wide, within the OpenScape Business internetwork	Not supported
Busy indication	Network-wide, within the OpenScape Business internetwork	Not supported

myAttendant	Closed Numbering (Scenario 4a)	Open numbering (scenario 4b)
Internal Directory / Favorites	Network-wide, within the OpenScape Business internetwork	Not supported
External directory	Local, via import of CSV files	Not supported
Search in external directories of other nodes	Not possible	Not supported
External Offline Directory (LDAP)	via LDAP	Not supported

OpenScape Business Attendant	Closed Numbering (Scenario 4a)	Open numbering (scenario 4b)
	Interface limited to 8-digit phone numbers	Interface limited to 8-digit phone numbers
Presence Status	Network-wide	
Busy indication	Network-wide	
External directory	via LDAP	via LDAP
Central Attendant Console	Network-wide, within the OpenScape Business internetwork	

Company AutoAttendant (UC Suite)	Closed Numbering (Scenario 4a)	Open numbering (scenario 4b)
Company AutoAttendant: after the AutoAttendant answers a call, the caller must dial the number of the station to which he or she wants to be connected.	CCV scripts allow you to dial station numbers from the internal directory within the internetwork.	Not supported
Personal AutoAttendant: after the Auto Attendant answers a call, the caller must dial a single digit to be connected to his or her call destination.	Any station number preconfigured by a UC subscriber is possible	Not supported

Company AutoAttendant (UC Smart)	Closed Numbering (Scenario 4a)	Open numbering (scenario 4b)
Company AutoAttendant (UC Smart)	Local	Local

myAgent	Closed Numbering (Scenario 4a)	Open numbering (scenario 4b)
	With UC functionality via UC Booster Server, UC Booster Card or OpenScape Business S. All agents are registered on ONE node. Incoming CC calls via the local PSTN, ITSP and SIP-Q trunk circuits.	Not supported
Voicemail (Recording, Message Waiting Indication, Check)	Subscribers use their local voicemail system; there is no central voicemail for the entire internetwork.	Not supported
Presence Status	Netwide	Not supported
Busy indication	Netwide	Not supported
Agent status	Local	Not supported
Internal Directory / Favorites	Netwide	Not supported

myAgent	Closed Numbering (Scenario 4a)	Open numbering (scenario 4b)
External directory	Local, via import of CSV files	Not supported
Search in external directories of other nodes	Not possible	Not supported
External Offline Directory (LDAP)	Local	Not supported
Transferring a Call	Local	Not supported
Customer information	Local	Not supported
Reporting	Local	Not supported

External applications	Closed Numbering (Scenario 4a)	Open numbering (scenario 4b)
OpenScape Business TAPI application	See *Application Connectivity*	
External CSTA applications		
Application Launcher		
OpenScape Contact Center	See *Multimedia Contact Center*.	

Telephony	Closed Numbering (Scenario 4a)	Open numbering (scenario 4b)
SIP Provider (ITSP)	Local	Local
PSTN Provider	Local; network nodes without a PSTN provider of their own are reached via SIP-Q or the associated gateway.	
Survivability (redundancy in the event of an internetwork or OpenScape Business S breakdown)	Is supported between OpenScape Business X and OpenScape Business S	Not supported
Dial a public number in the own node	Supported	
Dial a public number in a networked node	Network-wide, within the OpenScape Business internetwork	

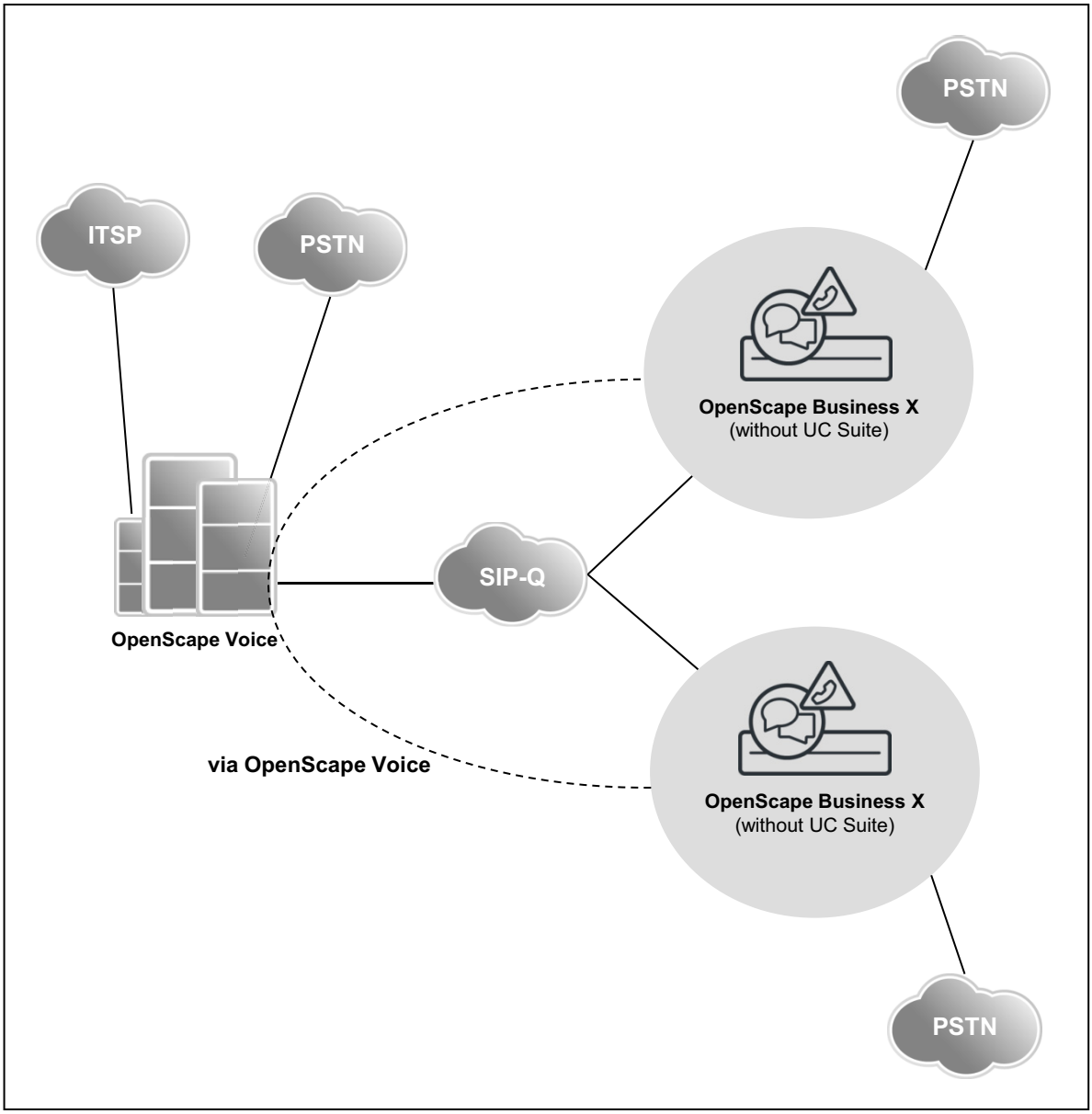
Mobility	Closed Numbering (Scenario 4a)	Open numbering (scenario 4b)
Desk Sharing	Within a node; network-wide, within the OpenScape Business internetwork (with DLS)	Not supported
Mobility with DTMF control of the system	Local (not supported for OpenScape Business S)	Local
myPortal to go (Web Edition), UC Suite	Network-wide presence status and directories (requires a UC Booster Server, UC Booster Card or OpenScape Business S for each node)	Not supported
myPortal to go (Web Edition), UC Smart	Local, not for UC Booster Server, UC Booster Card and OpenScape Business S	Not supported

Other functionalities	Closed Numbering (Scenario 4a)	Open numbering (scenario 4b)
Signaling and Payload Encryption (SPE)	Not supported in OpenScape 4000 / OpenScape Business networks. Not supported for UC connections and conferences	Not supported in OpenScape 4000 / OpenScape Business networks. Not supported for conferences
DSS server	Network-wide, within the OpenScape Business internetwork	Not supported
Call Pickup	Not supported	Not supported

17.6.7 Networking OpenScape Business X and OpenScape Voice

OpenScape Business X can be networked with OpenScape Voice.

INFO: A configuration example for networking with OpenScape Voice can be found in the Unify Experts wiki at `http://wiki.unify.com/wiki/How_to_collection_and_tutorials_for_OpenScape_Business`



Network Data

- OpenScape Business X provides network-wide voice and gateway functionality for OpenScape Voice.
- One or more OpenScape Business X systems can be used as a gateway for digital Central Offices (ISDN, T1, CAS)
- The following devices can be operated at cape Business X gateways: digital / analog / DECT / IP (HFA)
- UC is generally not supported by OpenScape Business X in this networking scenario.
- Each call from one node to another is routed through OpenScape Voice.
- The configuration of each node occurs in Expert mode.

- The OpenScape Voice dial plan is based on E.164, which explains why neither open nor closed numbering is available.

Network-wide Features

Maximum configuration	
Maximum number of nodes	Depending on OpenScape Voice
Maximum number of stations in a single communication system	Depending on OpenScape Business X
Maximum number of stations in the network	Depending on OpenScape Voice

Administration	
WBM	The Networking wizard cannot be used. OpenScape Voice is administered per node via the OpenScape Business expert mode.
Manager E	Not recommended
UC Administration	UC is not relevant in connection with OpenScape Voice
Mass data import via CSV files (call numbers, DID numbers, names)	Separately for each of the nodes in the OpenScape Business internetwork

Licensing	
Licensing structure	Each node individually; a network license is required for each OpenScape Business node

Restrictions and Notes on the Features

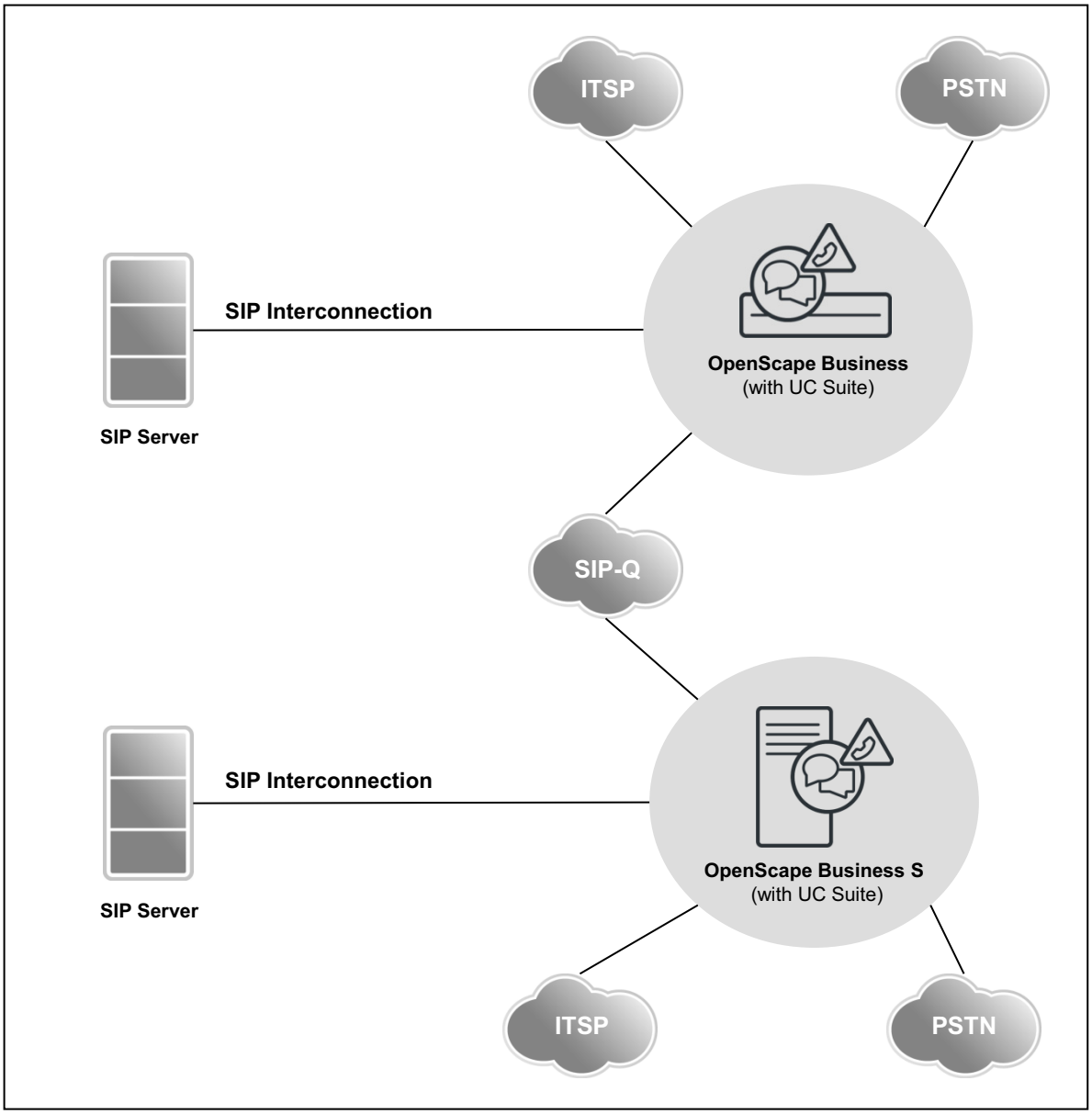
- The connection of analog CO trunks at OpenScape Business gateways is released **only** for Brazil (due to the support for line reversal and backward release of analog CO trunks in Brazilian COs).
- A network of OpenScape Business gateways with one another or with systems other than OpenScape Voice is not supported. The networking of the OpenScape Business gateways with OpenScape Voice must occur through a star-shaped network structure.
- Path replacement (route optimization) via SIP-Q is not supported for the devices connected to an OpenScape Business gateway.
- To avoid poor voice quality on transit line connections, the G.711 voice codec should be used. The G.729 codec is not recommended, since transit line connections can be caused by features such as conferencing and call forwarding. This is because path replacement (i.e., route optimization) is not supported.
- No cross-system support between OpenScape Voice and OpenScape Business gateways is available for features such as call pickup groups, group calls and hunt groups. The groups may include only subscribers of either OpenScape Voice or OpenScape Business, but not both.
- Encryption (SPE) between OpenScape Voice and OpenScape Business gateways is supported. The connection between OpenScape Voice and OpenScape Business must be made by means of the TLS encryption

protocol. SRTP (SDES) is not supported in a network with OpenScape Voice V7R1.

- Networking is supported only with the E.164 numbering plan.
- The following applies to the IP stations (HFA) connected to OpenScape Business gateways: For each active OpenScape Business/OpenScape Voice connection, two B channels per HFA device are required (one B channel per TDM device). The need for these additional DSP resources should be reviewed and taken into consideration.

17.6.8 Connecting External Auxiliary Equipment to OpenScape Business via SIP Interconnection

External auxiliary equipment can be connected to OpenScape Business via SIP Interconnection, e.g., to use applications such as OpenScape Alarm Server, OpenScape 4000, OpenScape Voice or other certified SIP servers.



Prerequisites

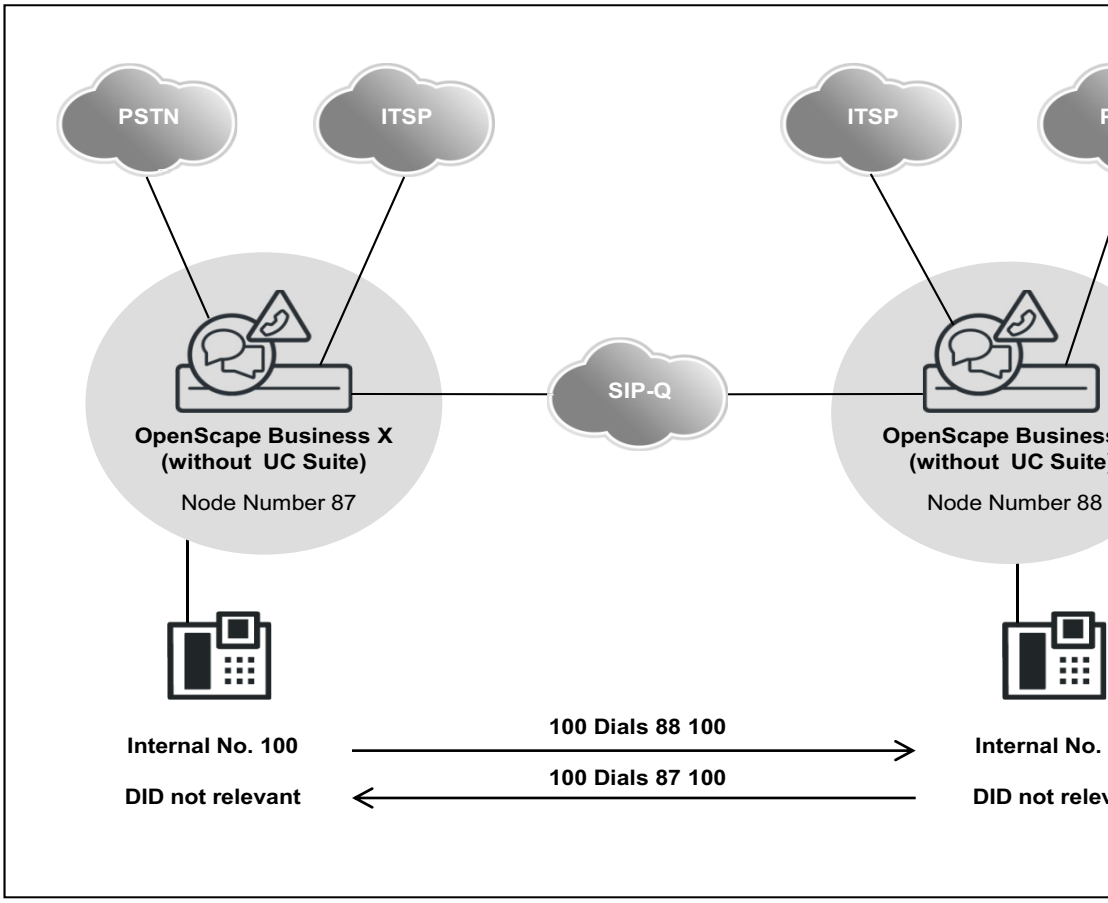
- Only certified applications may be connected, for example, OScAR.
- An external SIP server can be connected via the Native SIP or SIP-Q protocol.
- A maximum of two SIP-Q routes (one is required for UC Suite, if present) and a maximum of 10 Native SIP routes (of which up to 8 Native SIP routes can be used for ITSP) are available.

Additional information can be found in the

- Expert wiki for telephones, communication systems and UC:
  `http://wiki.unify.com`

17.6.9 Open Numbering in OpenScape Business X Networks

A internetwork with open numbering can be set up by networking two (or more) communication systems whose numbering schemes overlap one another (i.e., not unique throughout the internetwork).



Network Data

- Network-wide voice networking via OpenScape Business.
- UC features are not supported.
- Every call within a node occurs with an internal call number.
- Every call to another node occurs with a node number (plus an internal number).
- Each node must be configured in Expert mode. The Networking wizard is disabled once a node number for open numbering has been configured.
- Outside line access to the PSTN or ITSP is possible from each node.

> ***INFO:*** In case of a network-wide extension on UC functionality, it is necessary to change from open to closed numbering in order to adapt the internal numbers. Thus, the open numbering must be disabled, while the node number must be deleted and

subsequently added as a prefix (for example, extended internal number 87100 instead of 100 and 88100 instead of 100).

Differences:

- The selection of participants in their own node is made with the extended internal number.

- The internal number and the DID number may differ if necessary, but the DID numbers must not be changed.

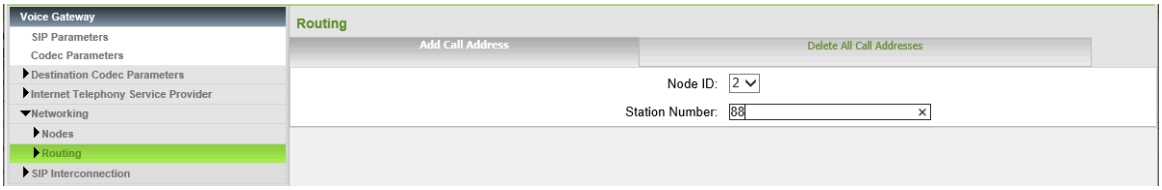
17.6.9.1 How to Configure Open Numbering

Configuring Open Numbering

1. Use the **Open numbering** system flag to enable open numbering for the communication system
2. Enter the number of your own node (e.g., "87")

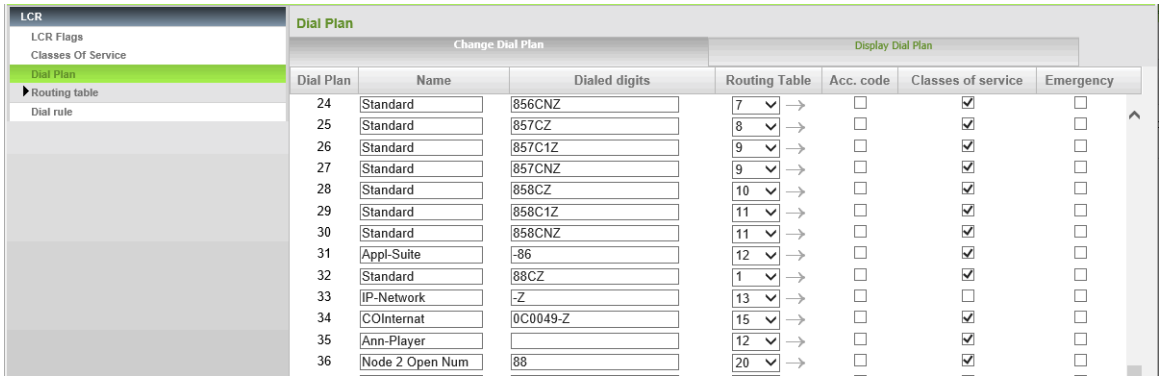
Configuring Nodes (Routing)

1. The destination nodes are addressed via Voice Gateway > Networking > Nodes > Routing (e.g., "88")
2. In an open numbering scheme, the **Networking** wizard cannot be used; this is prevented by the **Open numbering** system flag.

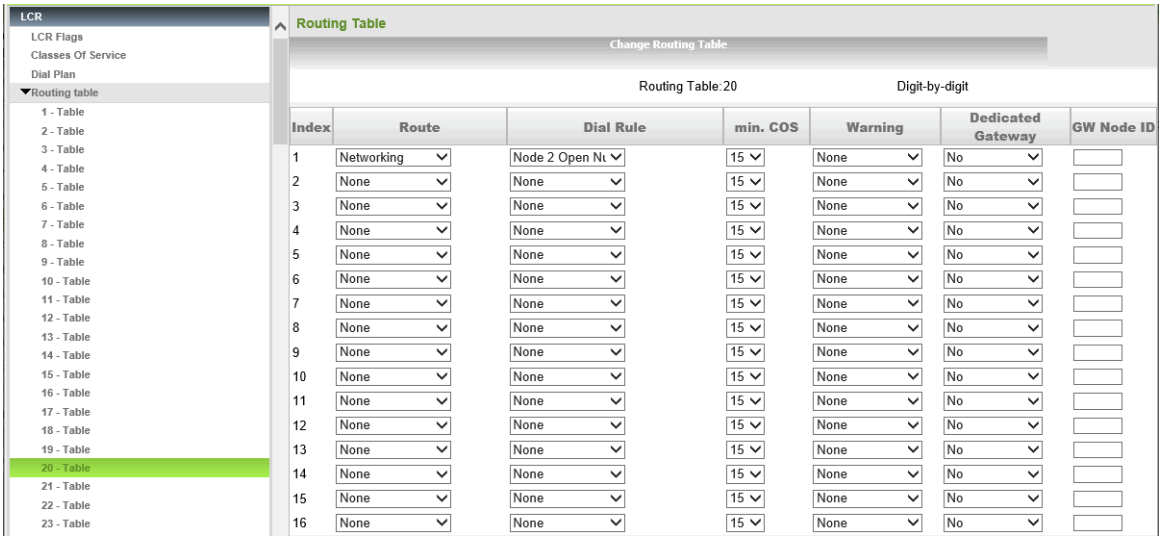


Configure LCR

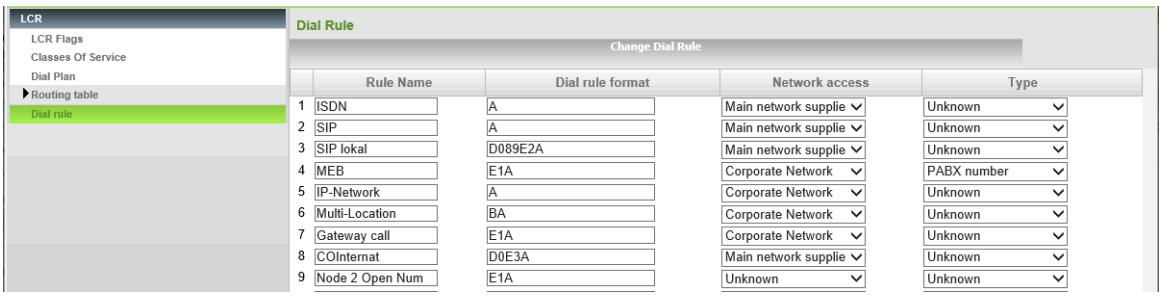
1. Assign the "Node 2 open Num" dial rule to the node number and select the associated routing table.



2. Display the configured route



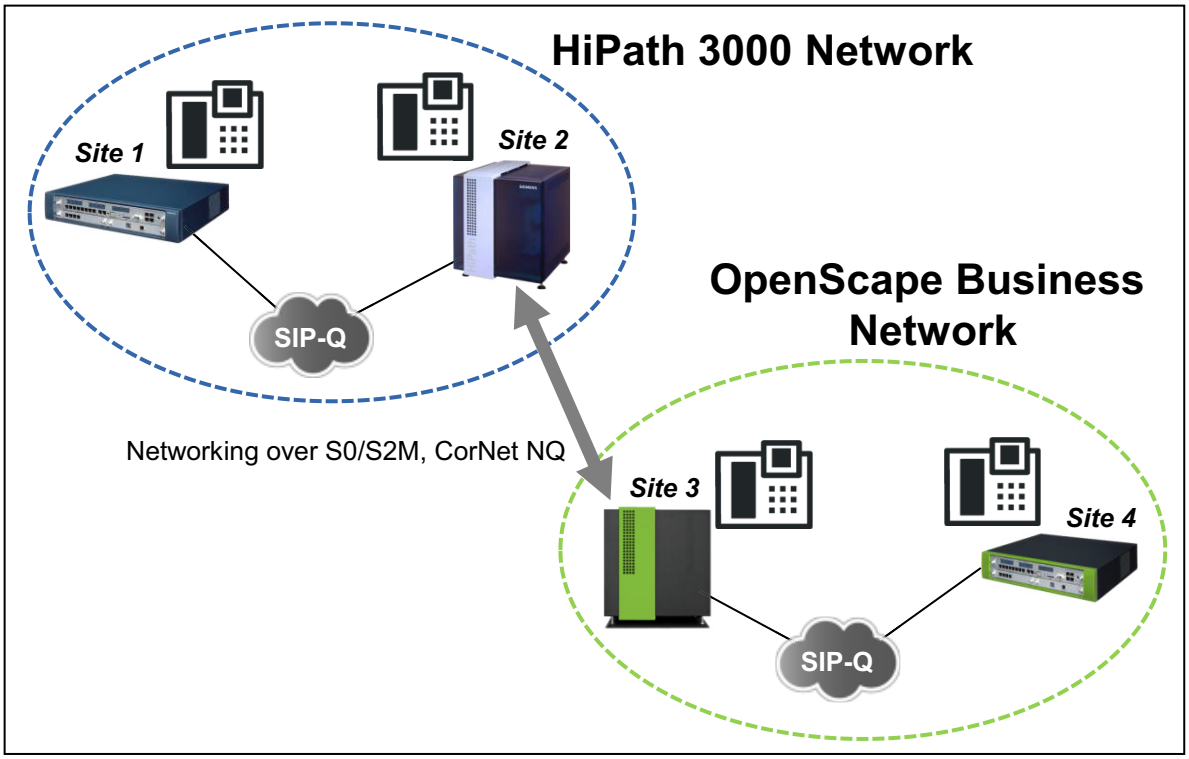
3. Enter the name of the "Networking" route and the dial rule "Node 2 open Num" associated with it.



17.6.10 Networking via ISDN

OpenScape Business systems can be networked with one another as well as with HiPath 3000 and OpenScape 4000 communication systems via digital trunks. Both S_0 as well as S_{2M} lines can be used for the connection.

Networking with HiPath 3000



The existing HiPath 3000 network is (initially) left intact. The expansion of the network occurs with OpenScape Business. HiPath 3000 nodes can be gradually migrated into the OpenScape Business network as required.

Every cross-network call that traverses the HiPath 3000/OpenScape Business is conducted via suitable TDM gateways (S_0 or S_{2M} with CorNet NQ protocol, possibly QSIG as a vendor-independent protocol).

The following constraints apply:

- Separate licensing for HiPath 3000 / OpenScape Business
- Separate administration for HiPath 3000 / OpenScape Business
- Recommendation: closed numbering in the overall network. Open numbering could potentially result in erratic behavior with CLIP and for journal entries / caller lists.
- Recommendation: use only the G.711 codec to ensure good voice quality in the overall network.
- The number of B-channels must be determined by taking the expected call volume into account.
- OpenScape Business requires a Networking license in any case.

Connection of External Systems via QSIG

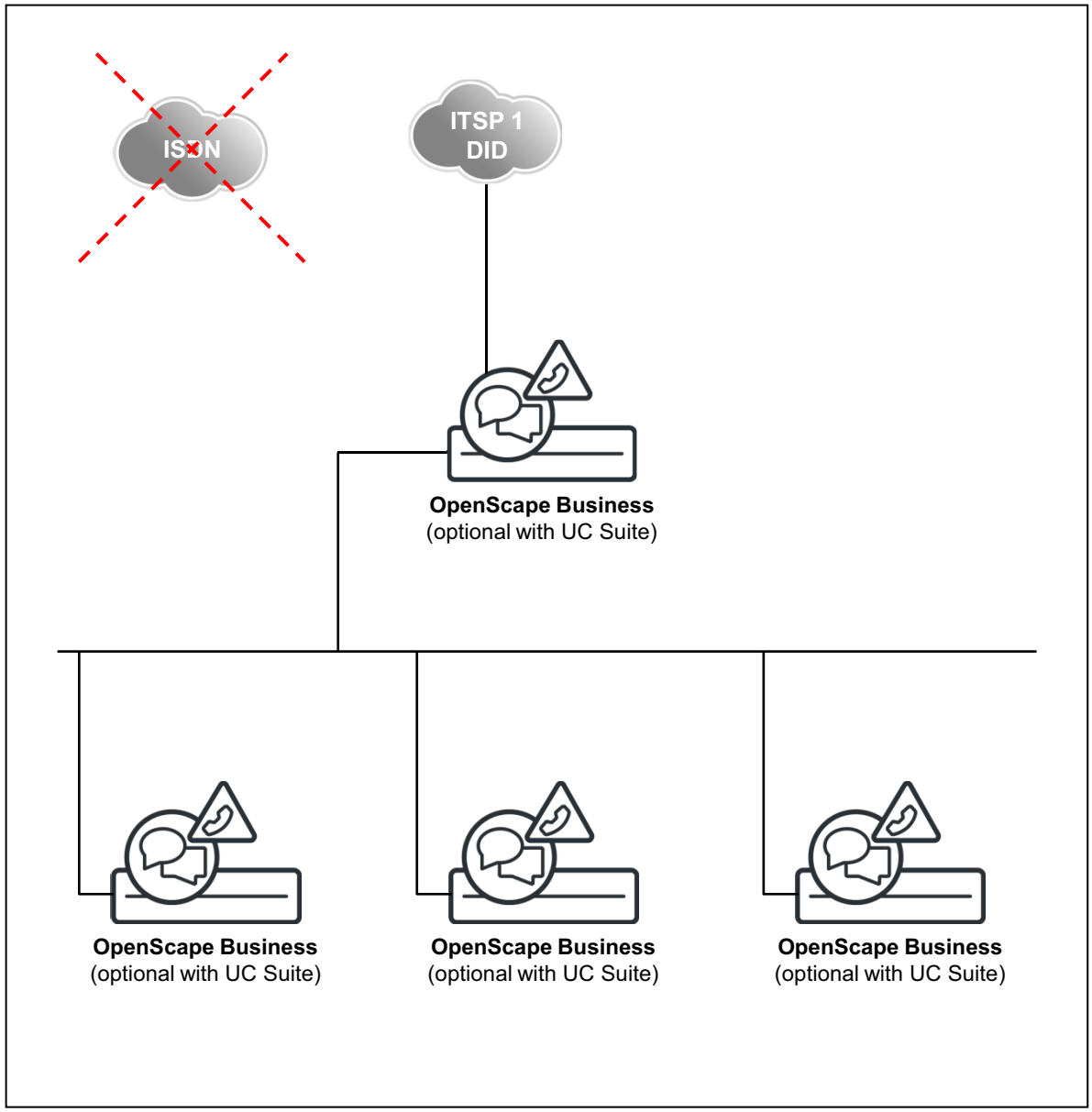
The following must be noted when connecting external systems with the QSIG protocol:

- Check the QSIG variants of the external systems involved for compatibility (QSIG V1, also called QSIG as per the ECMA Standard, and QSIG V2, also called QSIG as per the ISO Standard)
- Compare the feature sets of the relevant systems. This should help to determine to what extent the theoretically expected scope of functionality, i.e., the intersection of both feature sets, corresponds to the customer's wishes.
- Furthermore, to guarantee the expected functionality, an on-site test of the connection is recommended. In particular, interworking with other networking and PBX protocols must be taken into account.

17.6.11 OpenScape Business internetwork with central ITSP trunk connection

A pure OpenScape Business internetwork can be implemented with a central DID-capable ITSP trunk connection instead of ISDN.

Networking with Central DID-capable ITSP Trunk connection



The following must be observed when planning customer networks:

- **One** central ITSP trunk connection for the entire OpenScape Business network.
- Registration at exactly one local network, i.e., all nodes in the network use exactly one Central Office number, e.g., 0049 89 7007-XXXXX.
- For emergency calls, the networked nodes can use their own trunk connections for outbound calls in cases where the central ITSP access fails. Under certain circumstances, a correct caller identification to the outside may not be possible in this case. Emergency calls, for example, may not be delivered correctly. Incoming accessibility via this local connection is also

subject to restrictions. For these reasons, local connections are not recommended, though not prevented technically.

- For the same reason, additional ISDN connections are not recommended (though technically not prevented) at the central node.
- All digit analysis and call routing rules for standalone OpenScape Business systems and networks apply. The station number assignment of the ITSP CO numbers occurs exclusively via the DID configuration of the station in this case (and not via the mapping table; see Configuring an ITSP in section 9.2 and the Unify Experts wiki on the Internet).

17.7 Central Intercept Position in the Internetwork (Not for U.S.)

OpenScape Business allows incoming calls that cannot be assigned to a station or answered to be diverted to a defined intercept position in the internetwork to ensure that no calls are lost.

If the central intercept position in the internetwork is configured using ISDN, then the functionality is identical to the functionality without networking.

In conjunction with an ITSP Central Office, the central intercept position is subject to some restrictions, since every node essentially has its own ITSP:

- The ITSP intercept criteria apply only to each respective node.
- The intercepts "on RNA", "on Device Busy", "on Incomplete", "on Invalid", and "on Unanswered Recall" work.
- The intercept types "on Invalid" and "on Incomplete" do not work with the ITSP.
- Incomplete or invalid telephone numbers are returned to the ITSP with a busy signal.

If a central intercept position is to be used in an internetwork, virtual stations must be configured in each node. These virtual stations are permanently diverted via the internetwork to the myAttendant user.

Example for an ITSP CO: ITSP PABX number is 0211-23456789 + ITSP DID number; the number 0211-23456789-0 is publicly announced as the central number of the communication system.

- Station 100 is myAttendant with its own ITSP DID number 100 and a virtual station 199 with the ITSP DID number "0".
- In the ITSP mapping list of each node, the ITSP DID number "0" is assigned to the own virtual station.
- Under **Incoming Calls/Call Forwarding**, the virtual stations are referred to station 100.
  First destination: own virtual station
  Second destination: station 100 in the destination node
  Call time 5 seconds

For better identification of calls, it is recommended that the virtual stations of all nodes be provided with their call number (DID) and a name (e.g., company) via the myAttendant application (under **Setup**/**myAttendant**/**DIDs**). This enables a

more detailed identification of the caller in the **Active Calls** window of myAttendant.

17.8 Presence Manager

Presence Manager enables the subscriber states "Free", "Busy" and "Ring" to be signaled throughout the network at the LEDs of the HFA telephones. This requires closed numbering and at least one UC Booster Server at the master node of the internetwork or an OpenScape Business S as the master node. A network license is required for each node.

In the idle state, the corresponding LED is off; in the busy state, it is constantly on, and in the ringing state, the LED flashes. In the ringing state, the call involved can be picked by pressing the corresponding button.

Call processing states can only be signaled for a station if the Presence Manager can set a CSTA monitor point on the relevant station.

The keys are configured by the user. When station numbers are programmed on the telephone itself, no distinction is drawn between internal and network-wide numbers.

The Presence Manager is a service and has no user interface. No settings need be made, as all data is automatically obtained through data synchronization.

Groups are not supported by Presence Manager. LED signaling is not performed and call pickup is not possible. MULAPs, however, are not supported by Presence Manager.

Presence Manager does not actively support any SIP and S_0 phones.

17.9 Synchronization Status in the Internetwork

In an internetwork, the synchronization status is displayed in the Admin Portal, and the registration status of each node is indicated by colored buttons. The display of the synchronization status applies to network nodes of the communication system, but not to OpenScape 4000 and OpenScape Voice nodes.

Display of the Synchronization Status

Display	Color	Meaning for the master	Meaning for the slave
Synchronization status (display on the home page of the Admin Portal)	Red	-	The IP address of the master node is configured, but the slave system could not register. The slave tries to register with the master at cyclical intervals.
	Yellow	-	The slave is registered with the master, but the call numbers are not consistent in the internetwork. This may occur after a backup/restore or after the first registration.
	Green	If a node is configured as the master, the status appears as green.	
Registration status of the individual nodes (displayed in the Network>Node View dialog)	Red	The slave is configured, but the system has never registered.	The slave is configured, but the system has never registered.
	Green	The system is registered.	The system is registered.
Alive (displayed in the dialog Network>Node View)	Red	Node-specific view of the internetwork: all nodes that are marked in red cannot be reached. The reasons may be network problems or a failure in the communication system.	
	Green	The (external) node can be reached via the network. The own node is always shown in green.	

17.9.1 Manual Synchronization in the Internetwork

If the automatic synchronization of the configured call numbers and names (internal or DID numbers) has not been completed in the other systems of an internetwork, a manual synchronization can be initiated. This manual synchronization in the internetwork only works in homogeneous networks.

The synchronization process only transfers changes in the configuration.

If the status indicator in the Admin Portal appears as "red", the Synchronization button can be pressed to try and manually synchronize the data with the master.

In cases where already configured systems in the network can no longer make calls, the potential cause for the problem must be found elsewhere. If the Alive status of individual nodes appears as "red", this indicates network problems or other reasons why the node cannot be reached in the network. In such cases, activating the Synchronization button will not improve the situation.

Master

When activated on the master node, the slave nodes are requested to update the phone numbers and names of the system from the master.

Slave

When activated on a slave node, the station numbers and names of the system are updated on the master. At the same time, the slave node is registered again at the master node.

17.10 Survivability

Survivability is a feature within a network of OpenScape Business S systems with OpenScape Business X gateways. If the OpenScape Business S fails or cannot be reached due to network errors, the system telephones (HFA) logged in at the OpenScape Business S can log in at an OpenScape Business X Gateway (standby gateway) instead. The phone numbers of the system telephones are retained after the new login. This provides continuity for basic telephony; however, the features of applications such as myPortal, voicemail and CTI will be temporarily unavailable.

After the OpenScape Business S can be securely accessed again, the system telephones automatically revert to the OpenScape Business S.

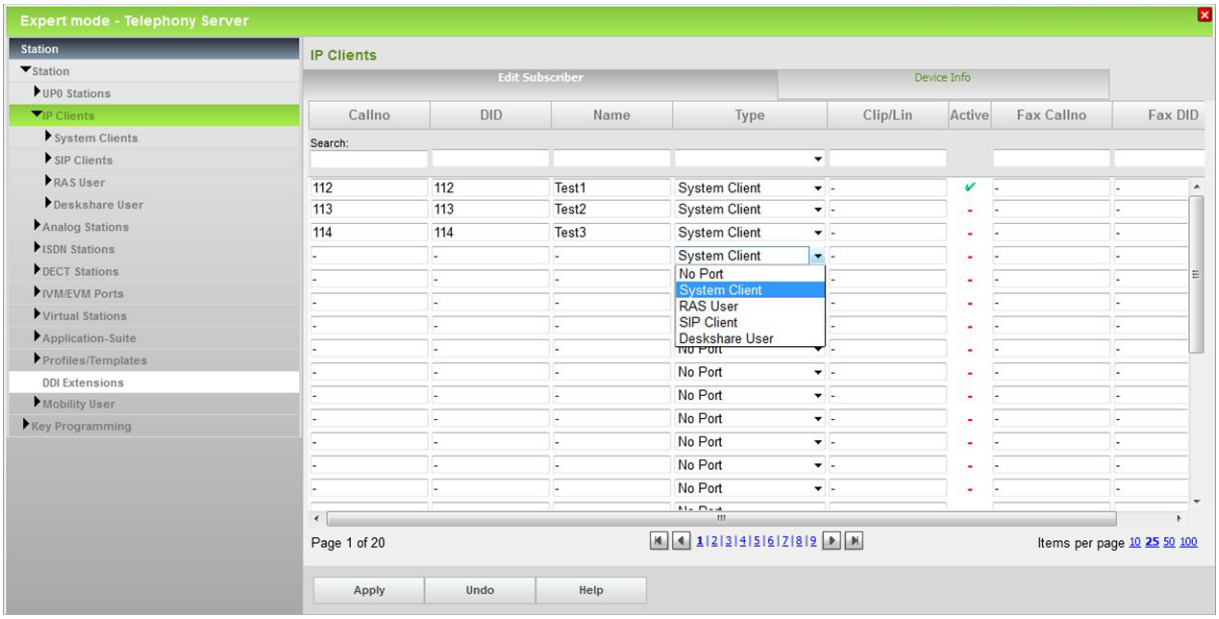
The time for switching to the standby gateway can last up to 30 minutes.

If the OpenScape Business S fails, an attempt is first made to reach it again for a fixed time period (10 minutes; cannot be changed). It is only when this time has expired that the system telephones intended for this purpose are registered at the standby gateway. The current statuses of the registered phones can be viewed in **Expert Mode > Diagnosis Logs**.

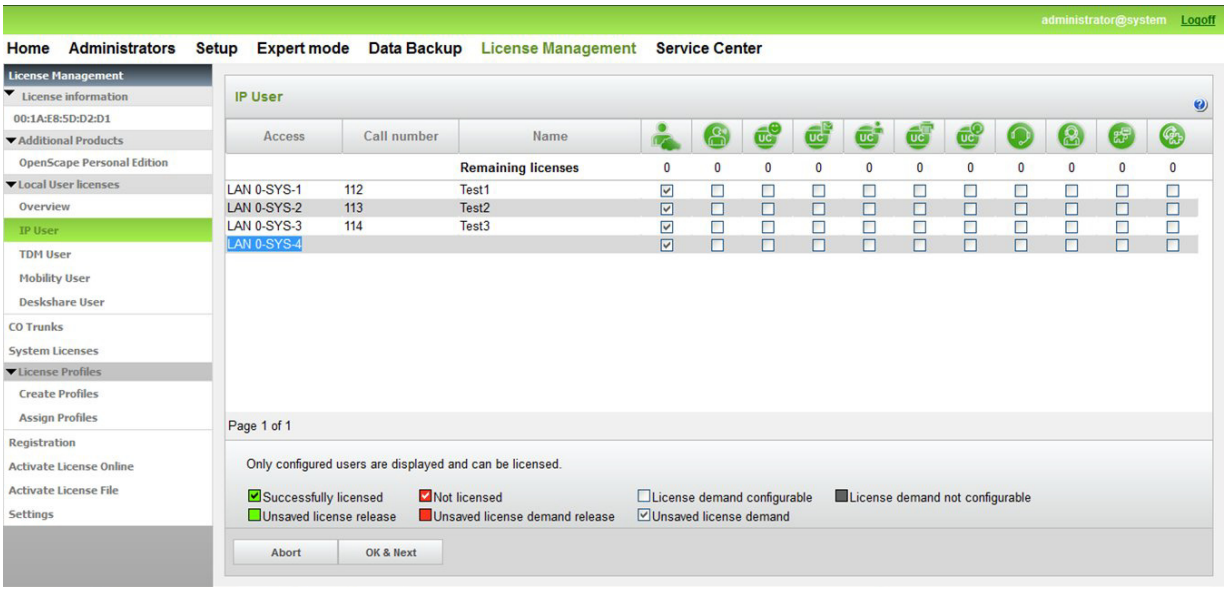
The survivability settings are configured at the system telephones. If the OpenScape Business S fails, the phones will initially try to reach it again several times. A time-out or how often the phone tries to log in again can be configured via the "System Redundancy" setting on the Administration menu of the telephones. The default setting for the timeout is 30 seconds with one retry. After that, the telephones register at the standby gateway. The automatic registration back at the OpenScape Business S must also be configured at the system telephones.

The following prerequisites must be satisfied for survivability:

- A sufficient number of free IP ports must be available at the standby gateway for the system phones connected to the OpenScape Business S that need to be "saved" when a network node fails.
- For these free ports on the standby gateway, stations must be set up without a name and phone number.



- The stations must be configured as system phones (system clients) and have an IP user license. In the event of survivability, the stations can only use telephony features.



17.11 Removing a Node from the Internetwork

If a node is to be removed from the internetwork, it must first be ensured that the node is no longer available in the network configuration. Otherwise, the node will independently attempt to register itself again in the network and master node will try to synchronize data.

Procedure

The deletion of a node occurs via the Networking wizard, where all nodes involved must always be removed.

- Interrupt all paths (routing) to the nodes to be removed
- Administration of the internetwork
- Enter "No network" for the slave node involved in the networking wizard of the slave node.
- Remove the slave node from the registration list in the networking wizard of the master node.

If o node is not removed properly, data will continue to be transferred from one OpenScape Business to another and thus produce inconsistencies in the internal directory, i.e., the users will not appear in the user directory and will therefore be unable to use myPortal for Desktop.

18 Auxiliary Equipment

Auxiliary equipment consists of external devices (such as an announcement device or an entrance telephone with door opener) that are connected to the interfaces of the communication system. Using an IP-enabled camera, the video surveillance solution Gate View can be deployed.

18.1 Analog Announcement Device

An analog announcement device can be connected to an a/b interface to play custom announcements (e.g., for the central AutoAttendant or as a replacement for music on hold).

INFO: Before using announcements or music from other sources, make sure that you do not infringe on any copyrights.

Up to 16 announcement sources (e.g., media servers, announcement players or analog announcement devices) can be configured for each communication system.

The following types of announcement devices can be used:

- Announcement devices that always start at the beginning of the message when activated (such as greeting messages).
- Continuous playback devices (e.g., for music on hold)

The announcement device must behave like a station, i.e., announce itself, play the announcement and switch the call (enter consultation hold, dial and hang up).

Announcements Types

The following types of announcement are available:

- Greeting announcement (announcement prior to answer)
  A greeting announcement can be played to callers prior to answering their calls.
- AutoAttendant
  When the AutoAttendant is enabled, music and/or further announcements can be played to callers if they cannot be switched immediately.
- DTMF DID
  When DTMF direct inward dialing is enabled, an announcement lets callers know that they can use DID to dial another extension. During the announcement, a code receiver detects if the caller uses suffix dialing and then forwards the call to the number dialed.

Alternatives to the A/B Interface (SLA Boards)

- OpenScape Business X8: TMEW2 board
- OpenScape Business X5: Optional STRB Board

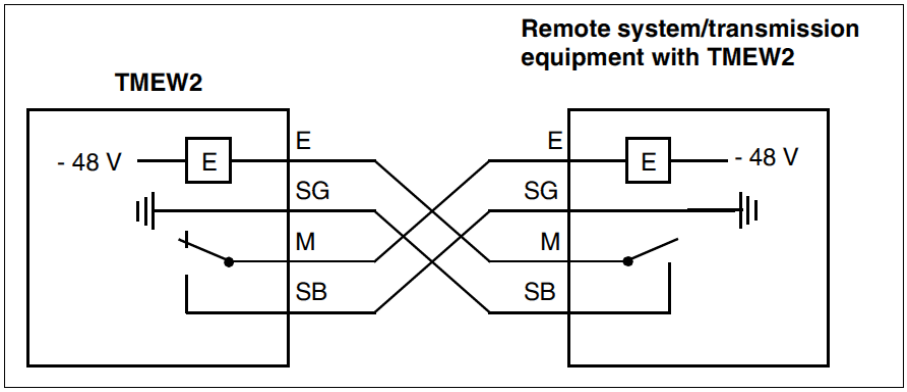
- OpenScape Business X3: Optional STRBR Board

Announcement Delay Time

The announcement delay time is the time (0 - 600 s, configurable) which must elapse before a waiting call is forwarded to an announcement device.

Announcement Device - Genius

The TMEW2 board may be installed on interface type 2 for connecting the Genius announcement device. A description of the TMEW2 board and the assignment of SIVAPAC connectors on the backplane when connecting the Genius announcement device can be found in the Service Documentation, Hardware Installation, Chapter "Boards".



The configuration of the Genius announcement device is performed in Manager E via **System View > Settings > Auxiliary Equipment > Announcement**.

18.2 Entrance Telephone and Door Opener

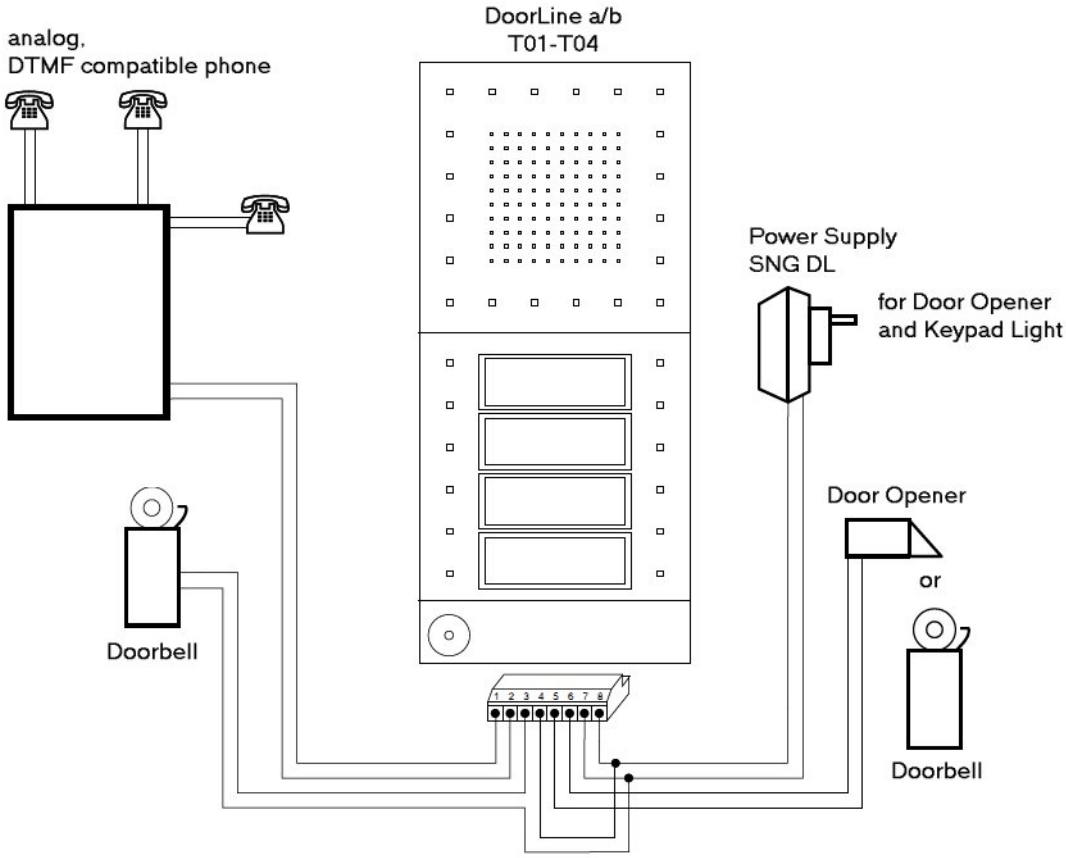
Entrance telephones (ET) are offered in a wide range of options from several different manufacturers today. The available connection options are essential for the operation and functionality of each ET. The Doorline a/b T01-T04, which is similar to other door openers by Behnke, Keil, 2n EntryCom, Auerswald, etc., is described here as an example.

18.2.1 DoorLine a/b T01-T04

The door opener DoorLine a/b T01-T04 is connected to an analog port. Equipped with 1 to 4 bell buttons (depending on model), several independent residential and commercial areas can be reached. The DoorLine a/b T01-T04 can not only be operated from any phone, but also provides the connection for the power supply of the door opener.

Due to the 2-wire a/b technology, the DoorLine a/b T01-T04 can be quickly and easily mounted. To synchronize with the communication system, the dialing

method can be set, and the voice channel can be matched. The door is opened via the code of the Doorline (e.g., #9). A special interface module such as the Doorline M02, M03, M06 and M06/1 is no longer necessary.



INFO: No further setting is required in OpenScape Business for this entrance telephone/door opener. For security reasons, it is recommended that the extension be configured with "no trunk access" or with "outward-restricted" trunk access.

18.2.2 DoorCom Analog

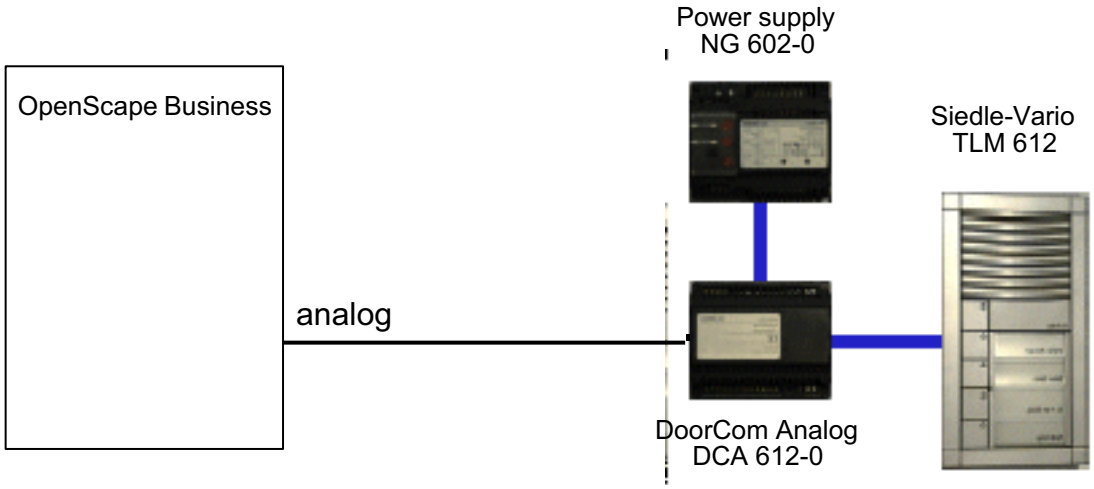
DoorCom® Analog is a universal entrance telephone adapter box for Siedle entrance telephones (such as the Vario TLM 612).

The DoorCom® Analog is connected to an analog port of the communication system. It behaves like an analog telephone with DTMF dialing, DTMF detection and DTMF control. It can be operated with DTMF signals.

DoorCom Analog can function only in combination with the following components:

- DoorCom Analog DCA 612-0

- Siedle-Vario TLM 612 entrance telephone
- Switching remote control interface DCSF 600
  For the voice connection of an internal user to the entrance telephone. Without this module, it is not possible to call back to the entrance telephone, for example, if a call was unintentionally cleared down by the entrance telephone.
- Power supply NG 602-0



Device control features (open doors, select entrance telephone, etc.) can be programmed on the procedure keys of a phone. The programmed DTMF signal sequence is then sent to the entrance telephone/door opener.

INFO: No further setting is required in OpenScape Business for this entrance telephone/door opener. For security reasons, it is recommended that the extension be configured with "no trunk access" or with "outward-restricted" trunk access.

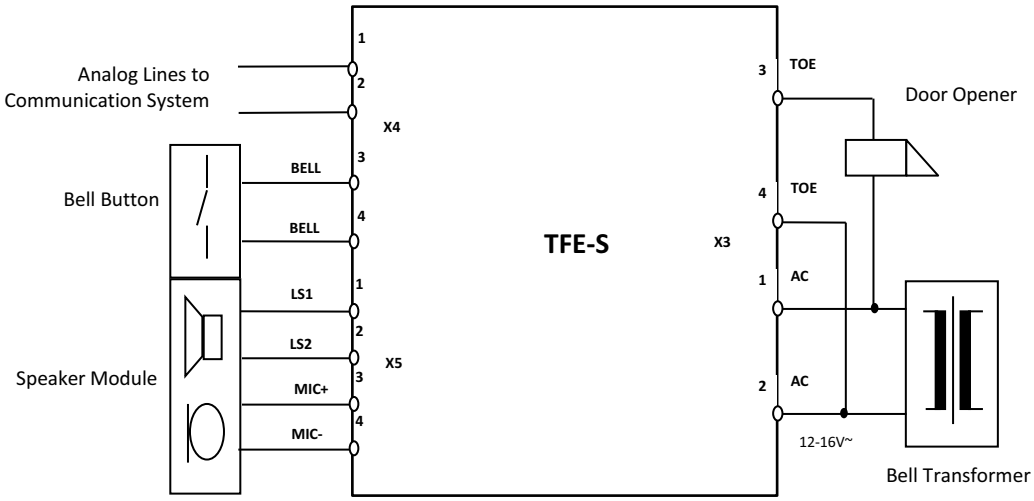
18.2.3 Entrance Telephone with Amplifier (TFE-S)

The TFE-S module (S30122-K7696-T313) connects an analog interface of the communication system with an entrance telephone, a door opener and a doorbell button. Control occurs via the communication system.

This makes it possible to connect to passive entrance telephones, which are comparable with the following types:

- From the company Siedle (TLM511-01, 611-01)
- From the company Rito (5760)
- From the company Grothe (TS6216)

The amplification can be adjusted manually. The TFE-S module requires its own power supply.



Technical Data

Parameters	Value
Power supply	Bell transformer 12V - 16V AC, 50Hz
Current draw	Max. 150 mA
OpenScape Business interface	Analog station
Dimensions	100mm x 160mm (5.7" x 9.1")
Ambient temperature	0°C to + 45°C

Functional description

Doorbell activation is signaled as a call at the phone of any configured station (ring destination). A voice connection to the entrance telephone is set up when the subscriber accepts the call. Additionally, the subscriber can also activate the door opener on his or her phone.

The call is intercepted if the entrance telephone ring destination is not reachable. If the intercept destination is busy, a system search is performed across all system phones.

INFO: The night service is ignored when signaling a door call.

INFO: System speed dialing at the entrance telephone is not possible.

Configuration Options

The following configuration options are available:

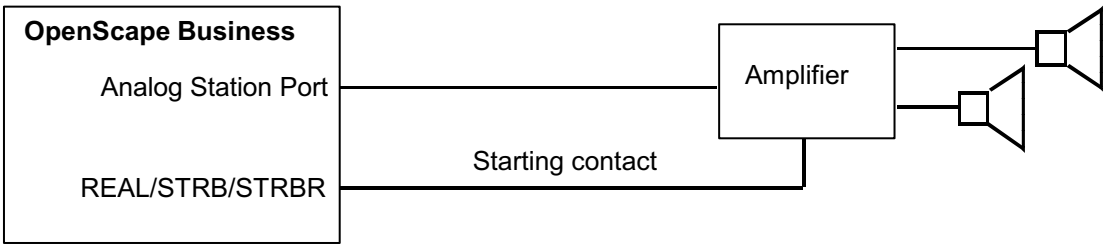
- Door opener:
  The door opener is configured via an a/b (T/R) interface and the entrance telephone must be connected via an adapter. The subscriber can then open the door by simply pressing a button on the phone during the connection with the ring destination.
- DTMF:
  This setting specifies whether the door opener is activated by a DTMF transmitter (DTMF: dual-tone multifrequency), that is, if the ring destination can open the door with DTMF suffix-dialing.
- Call Forwarding (CF):
  This specifies whether the call from the entrance telephone should be forwarded to an external call forwarding destination.

18.2.4 Loudspeakers

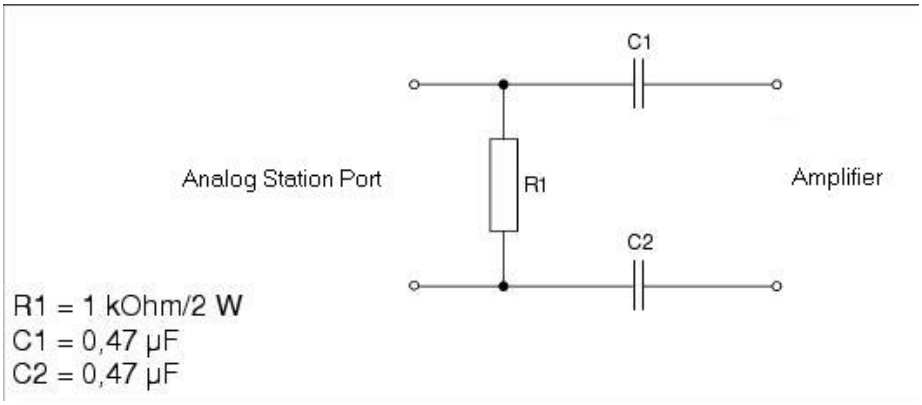
Speakers can be connected to the communication system via an amplifier.

The following options are available for connecting an amplifier, including the loudspeaker:

- **Connection of the amplifier at an analog station interface**
  A level adjustment of the amplifier may be required for this.



Furthermore, an additional loop resistor as in the following circuit may be needed:



- **Connection of the amplifier to the entrance telephone module TFE-S**
  An active amplifier / sound system can be connected via the TFE-S module. The amplifier input is connected to the speaker output of the TFE-S module. Furthermore, a contact of the STRB board may still be required to turn on the amplifier or switch through the input signal (noise suppression).

18.3 Relays

Actuators are control outputs which are activated or deactivated by control signals from the communication system. They cause a change in the state of the connected equipment and support functions for monitoring, alerting, control and regulation. They are mainly used in security and building management systems (e.g., for door openers).

Actuators are contained in optional control relay modules. All control relay modules include four control outputs (actuators).

Possible control relay modules:

- REALS (OpenScape Business X8)
- STRB (OpenScape Business X3W/X5W)
- STRBR (OpenScape Business X3R/X5R)

The detailed description of these boards, including the assignments, can be found in the Service Documentation in the section on "Boards".

Actuators can be controlled in one of the following ways:

- from the phone by entering codes
- from the system phone by pressing a key
- remotely via a CO trunk (DISA) by the station assigned to the relay function
- remotely via the "Associated Services" feature

Actuators can be enabled or disabled using the following functions:

INFO: The control codes can be found the "Expert Mode" section.

- **No function**
  The actuator is either not operational or entered as a common ringer/night bell (under "Settings" - "Incoming calls" - "Call destination lists").
- **Manual on/off**
  The actuator can be activated or deactivated via a key or via the "Activate/deactivate selected switch" code. This function can be assigned to a station, a group or all stations.
- **Auto off on timeout**
  The actuator acts as a time switch and can be activated or deactivated via a key or via the "Activate/deactivate selected switch" code. This function can be assigned to a station, a group or all stations. If a value greater than 0 is entered for the switching time, the actuator is deactivated only when the switching time has elapsed.

- **Door opener**
  The actuator acts as a door opener and can be activated or deactivated via a key or via the "Activate/deactivate selected switch" code. This function can be assigned to a station, a group or all stations. If a value greater than 0 is entered for the switching time, the actuator is deactivated only when the switching time has elapsed. The text "Door opener" appears on the display of all associated telephones. Example for the switching time multiplication factor: 30*100ms = 3 sec
- **Speaker amplifier**
  The actuator is activated when a connection is set up to the entrance telephone/door opener/loudspeaker. It is deactivated as soon as the connection is interrupted. This makes it possible to control an entrance telephone amplifier so that it is only activated when required. An entrance telephone or the loudspeaker port must be allocated to this function.
- **Busy indication**
  The actuator is activated when the associated station leaves the idle state (i.e., goes off-hook or activates the loudspeaker or receives an incoming call). The actuator is deactivated once the associated station re-enters the idle state. The actuator can also be directly activated via a key or via the "Activate/deactivate selected switch" code. In this case, the status of the associated station is ignored and the actuator can only be deactivated via a key or a code. A specific station must be allocated to this function. Example - Door busy indicator: If the Executive is on the phone, the door busy indicator lights up to show that he or she does not want to be disturbed.
- **Music On Hold**
  The actuator is activated if at least one station or a line in the communication system is not in the idle state. In this case, an announcement device or a CD player is activated. The actuator is deactivated if all stations and lines in the communication system are in the idle state. This function can only be assigned to all stations and must only be used once in the communication system. The value for the switching time must be greater than 0 (for example, 600*100ms = 60 sec). The actuator remains active and plays music until the switching time has elapsed or until it is disabled by a control signal.
- **Secondary bell**
  The actuator is activated for the allocated station if that station is being called. The actuator is deactivated when the called party answers or the call is terminated. The actuator is not clocked. A specific station must be allocated to this function. If a value greater than 0 is entered for the switching time, shutdown can be delayed. The switching time is a multiple of 3 seconds.
- **Call charge pulse**
  The actuator is clocked in accordance with the number for the allocated station on the basis of the incoming call charge pulses or call charge signals. A specific station must be allocated to this function. The switching time is 150 ms pulse and 150 ms break and cannot be changed.
- **Station active**
  The actuator is activated when the associated station is active (off-hook or loudspeaker activated). The actuator is deactivated once the associated station re-enters the idle state. A specific station must be allocated to this function.

Actuator Names

Any names (up to 16 characters) can be assigned to the actuators.

18.4 Sensors

Sensors are control inputs and detect a change in the state of the connected device. You can enable or disable functions of the communication system and thus support functions for monitoring, alerting, control and regulation. They are mainly used in security and building management systems (e.g., for temperature control or motion detection).

Sensors are contained in optional control relay modules. All control relay modules include four control inputs.

Possible control relay modules:

- REALS (OpenScape Business X8)
- STRB (OpenScape Business X3W/X5W)
- STRBR (OpenScape Business X3R/X5R)

The detailed description of these boards, including the assignments, can be found in the Service Documentation in the section on "Boards".

Sensors can enable or disable the following functions:

INFO: The control codes can be found the "Expert Mode" section.

- Call signaling on telephones
- Display message on system telephones
- Turning an announcement device on or off
- Answering machine control
- Automatic dialing with a predefined telephone number (internal phone number, group number or external destination call number)
- Activation of the following services for a STN (with code + STN):
  - Actuator on/off
  - Do not disturb
  - Call forwarding on/off
  - Codelock on/off
  - Send message texts
  - Withdraw message texts
  - Night service on/off
  - Ring transfer on/off
- Direct activation of the following services (only with station number):
  - Actuator on/off
  - Use speed dialing system
- Error signaling - The following are possible:

- Output of a programmable error message (sensor name, max. 10 characters: for example, Temp Alarm) on the display of a specific system telephone (no acoustic signaling)
- Display of calls on a specific system telephone with error message during call (destination call number)
- Error entry in error history (entry in error memory = activated)

Destination Call Number

An associated analog port is programmable for the sensors. This port is called by the system once a setup signal has been received. The calling party then overrides this connection. A recorded announcement can be activated via an answering machine connected to this port, which informs the dialed station of the response of the sensor. An analog port programmed in this way cannot be contacted from the outside. If an external call number has been programmed for a sensor, but an analog port has not, the external connection will be established but an audible signal in relation to the response of the sensor is not transmitted. However, if necessary, the called STN can identify the origin of the call on the basis of the call number (CLIP).

Message Texts Box Control Data

Input of the control string with a maximum of 24 characters for the Phonemail system (mailbox call number). If the connection has been established, the control string is transmitted to the recorded announcement port. If a recorded announcement port is not available, the control string is transmitted to the destination.

18.5 OpenStage Gate View

OpenStage Gate View is a user-friendly entry-level security solution that presents real-time video images on your OpenStage telephone, PC or - when on the road - the iPhone.

This enables you to monitor your entrance area and to control and provide secure access to your corporate premises.

The most important operating steps for users of OpenStage Gate View at an OpenStage 60/80, an iPhone or a web client are explained in the *Quick Reference Guide*.

18.5.1 Legal Framework

Video surveillance refers to the monitoring of locations with optical electronic equipment and is also known as "optical room surveillance system". When using video surveillance, the applicable country-specific regulations and laws must be observed.

Country-specific Legal Situation

The legal framework for video surveillance in publicly accessible areas varies among countries. You should therefore check the legal situation in your own country.

Areas monitored through video surveillance may need to be identified by a symbol. A corresponding symbol is usually supplied by the camera manufacturer and may look something like this:

18.5.2 Components

In order to use OpenStage Gate View, the components *Source*, *Processing* and *Appearance* are required. All components are connected through a local area network.

Source

The video source provides the video signal. Cameras from different manufacturers can be used as the source. Depending on the camera type, a video converter may be additionally required.

- IP cameras
- Analog cameras (in combination with composite/IP converter)
- Entrance telephones with integrated camera

The interface for processing the video signal is always an IP video stream.

If a commercial network camera is used as a video source, a LAN with Power over Ethernet (PoE) may be required to connect the camera in some circumstances.

Processing

To process the video signal, the appropriate server software (which is already integrated into the communication system) is required. No additional hardware for processing the video signal is required

Presentation

The presentation can occur on different devices. The following devices are intended for presenting the video signal.

- Devices for OpenStage Family as of Version V2R0.48.0.
  - OpenStage 60/80 HFA

  - Octophon 660/680 HFA
- iPhone
  Using the iPhone App *OpenStage Gate View*, available in the Apple AppStore.
- Web Browsers
  Presentation within the web-based administration software *Video Surveillance System* or as Web Client.

The recording of the video signal at the server can be controlled from some devices.

18.5.3 Function Overview

By using an OpenStage 60/80 HFA telephone, Openstage Gate View makes it possible to offer a powerful combination of the best voice quality, video transmission, and door opener functionality on one device.

Features and benefits

- Video recording on network drive.
- Different displays of multiple video signals on OpenStage telephones, mobile phones (iPhone app) or web clients.
- Simple, password-protected administration via web-based, multilingual interface.
- Flexible licensing concept.
- Integrates into already existing investments (equipment and infrastructure).

Capacity Limits

Depending on the platform on which the server software is running, a different number of cameras and devices can be used for the display.

- Hardware platform:
  - 2 cameras
  - 10 OpenStage telephones
  - 10 iPhones or web clients
- Softswitch / Application Server:
  - 8 cameras
  - 20 OpenStage telephones
  - 10 iPhones or web clients

In addition, the maximum number of usable cameras depends on the licenses procured. In this context, a license corresponds to one camera.

18.5.4 Menu

This section provides an overview of the menu of the administration software and describes how to set up individual features and parameters.

An overview of the menu functions is shown below.

Overview

Displays detailed information about each installed camera with editing options.

Surveillance

Displays the video image for each installed camera.

Recording

Displays details for all recorded video files and also options to play, download or delete them.

Status

Displays information about the hardware and software of the OpenStage Gate View system.

Administration

- **Maintenance**
  Enables the deletion of software and user data.
- **Recording Configuration**
  Enables the configuration of the recording device (recorder) and the recording mode.
- **Door Opener**
  Enables the configuration of an entrance telephone with assignment of camera and telephone.
- **User Management**
  Provides information and settings options for users, profiles and sessions.
- **Cameras**
  - **Installed Cameras**
    Shows all installed cameras as a list.
  - **Add Camera (Auto Discovery)**
    Displays a list of all detected cameras to automatically install a camera.
  - **Add Camera (Manual)**
    Enables the manual installation of a camera.
  - [Name of the camera]:
    Displays detailed information on the selected camera with editing options.
- **Telephones**
  - **Installed Phones**
    Shows all installed phones as a list.
  - **Add Phone (Auto Discovery)**
    Displays a list of all detected phones to automatically install a phone.
  - **Add Phone (Manual)**
    Enables the manual installation of a phone.
  - [Name of the telephone]
    Displays detailed information on the selected phone with editing options.

- **Log**
  - **View Log**
    Displays the current log file with download option.
  - **Download Log**
    Downloads the current log file.

18.5.5 Initial Setup of OpenStage Gate View

In order to set up the camera and display device, some minimal configuration is required at the OpenStage Gate View server. The setup is usually completed within a few minutes. Depending on the LAN infrastructure and the components used, additional installation steps may be required.

- First, a camera and a phone are assigned to the server configuration.
- After this, an OpenStage 60/80 telephone receives the software required to present the video image and is configured to operate the video function.

If the automatic detection of the camera or OpenStage 60/80 telephone fails, you also have the option to manually add these devices to the configuration.

18.5.6 OpenStage Gate View Video Recording

OpenStage Gate View enables you to record a video and review it later at any time and as often as desired.

Storage location

The recordings are stored on a network drive.

If the video recorder is set up, you can just start and stop a recording easily from the OpenStage phone. In addition, a time-controlled recording is possible.

The recordings are stored in files named with following syntax:
`recording-type_date-time_camera-name.file-format`

- recording-type:
  - SCH = scheduled recording
  - MAN = manual recording
  - CYC = cyclic (cyclic recording)
- File format: e.g., mp4 or mpeg

Quality and Quantity of the Recording Data

Recordings can be created in varying quality. Recordings with high quality take up more space than low quality recordings.

Space Usage (%): High Quality: approx. 650 MB for 1 hour; Low Quality: approx. 400 MB for 1 hour.

To limit the space used on storage media for the recording, the percentage of space reserved for recordings can be set in advance.

For cyclic recording, the length of a cycle can be set from 30 to 120 minutes. Depending on the amount of storage space available, several files are created, and the oldest among them are overwritten.

Restrictions

Even when using multiple cameras, only the video image of one camera can be recorded at any given time.

A scheduled recording has priority over a manually started recording and will stop the manual recording if required.

Only recordings in mp4 format can be viewed directly in the browser. Recordings in other video formats must first be downloaded in order to be viewed.

Still images (screenshots) cannot be stored directly, but must be created later from the stored video.

Recordings are only possible with cameras of known brands. No recording is possible when the camera brand **other** is selected.

18.5.7 OpenStage Gate View Entrance Telephone

OpenStage Gate View works with analog entrance telephones (also called door openers). When someone rings at the door, the video image of the door camera automatically appears on the OpenStage phone. You can use the video image on the phone to decide whether the person is to be admitted by pressing a button on the phone.

Setting up the Entrance Telephone in the Communication Platform

In order to use the entrance telephone function in OpenStage Gate View, the entrance telephone must be first set up correctly on the communication platform, depending on which communication platform is used.

- Setup of the entrance telephone as an analog device at a physical analog port of the communication platform. It is not possible to use a Mediatrix/AP1120 device to connect an analog entrance telephone at an IP port here.
- Setup of an entrance telephone button on the OpenStage phone.
- Setup of the password for the entrance telephone function.

Only one entrance telephone can be used together with OpenStage Gate View in each case.

More information on setting up the function in the communication platform can be found in the appropriate service documentation.

18.5.8 OpenStage Gate View User Management

As an administrator, you can enable the customized usage of OpenStage Gate View by optionally setting up further users in addition to the default user **admin**.

With these personal user accounts, you can not only obtain a better overview as an administrator, but also implement more security in the use of OpenStage Gate View:

- Each user has a personal account with a user name and password.
- You can temporarily block users.
- You can enforce password changes.
- You can view the session data of users with their respective IP addresses and the time of last use and can optionally end active sessions.
- Using the log file, you can review past activities of different users.

You can create any number of users, edit user data and remove users from the configuration permanently.

18.5.9 OpenStage Gate View Server Administration

As an administrator, you should keep track of the extensive server data and delete the information that is no longer required.

- You can view both the version number of the installed server software as well as the maximum number of devices and licenses.
- You can optionally delete phone and user data permanently.
- You can view the log data of the OpenStage Gate View server and download it.

18.5.10 OpenStage Gate View Customizations

Most administration tasks have been automated in order to minimize the customized settings that need to be made manually. However, due to the large number of different LAN configurations, it may be necessary to make some individual settings by hand.

- You can add and remove a camera to and from configuration manually.
- You can add and remove a telephone to and from configuration manually.
- At the communication system, you can disable the entire OpenStage Gate View server.

Adding a Camera Manually

Many different camera types have already been stored with the appropriate access data. In such cases, only the camera type needs to be selected, and the IP address adjusted if required.

If you select an Axis camera, a software version of 5.0 or later must be installed on this camera.

If the camera is not included in the list, select **other** and enter the required access parameters, i.e., the camera IP, port, user name and password as a URL. The format usually looks like this:

`http://<user-name>:<password>@<camera-IP>:<port>`

All unlisted cameras should be set up on the camera side as follows:

- MJPEG as the video format.
- 12 frames per second.
- Resolution of 320x240 pixels.

19 Application Connectivity

Application connectivity is supported by the system, e.g., with CSTA, TAPI, XMPP and Application Launcher.

19.1 CSTA

The CSTA interface enables high-performance CTI, Contact Center and Unified Communications applications, etc., to be connected to OpenScape Business.

CSTA uses the Transmission Control Protocol (TCP). A permanent connection is set up. Data packet loss is detected and automatically corrected.

Standards

The implemented CSTA protocol is based on:

- ECMA 269 Services for Computer Supported Telecommunications Applications (CSTA) Phase III
- ECMA-285ASN.1 for Computer Supported Telecommunications Applications (CSTA) Phase III
- Specific extensions

Prerequisites

The use of CSTA requires either UC Booster (Card or Server) or OpenScape Business S for the system connected with CSTA applications. The login credentials for CSTA applications must be configured in the system to enable the CSTA interface automatically. External CSTA applications must use these credentials for their access.

Features

CSTA provides the following features:

- Access via Ethernet LAN (TCP/IP)
- CSTA Phase III, ASN.1 encoding
- Support for the CSTA XML protocol for certified applications
- Wide range of supported system telephones
- Network-wide monitoring and control of all resources
- Multiplexing for monitor points

Supported Devices

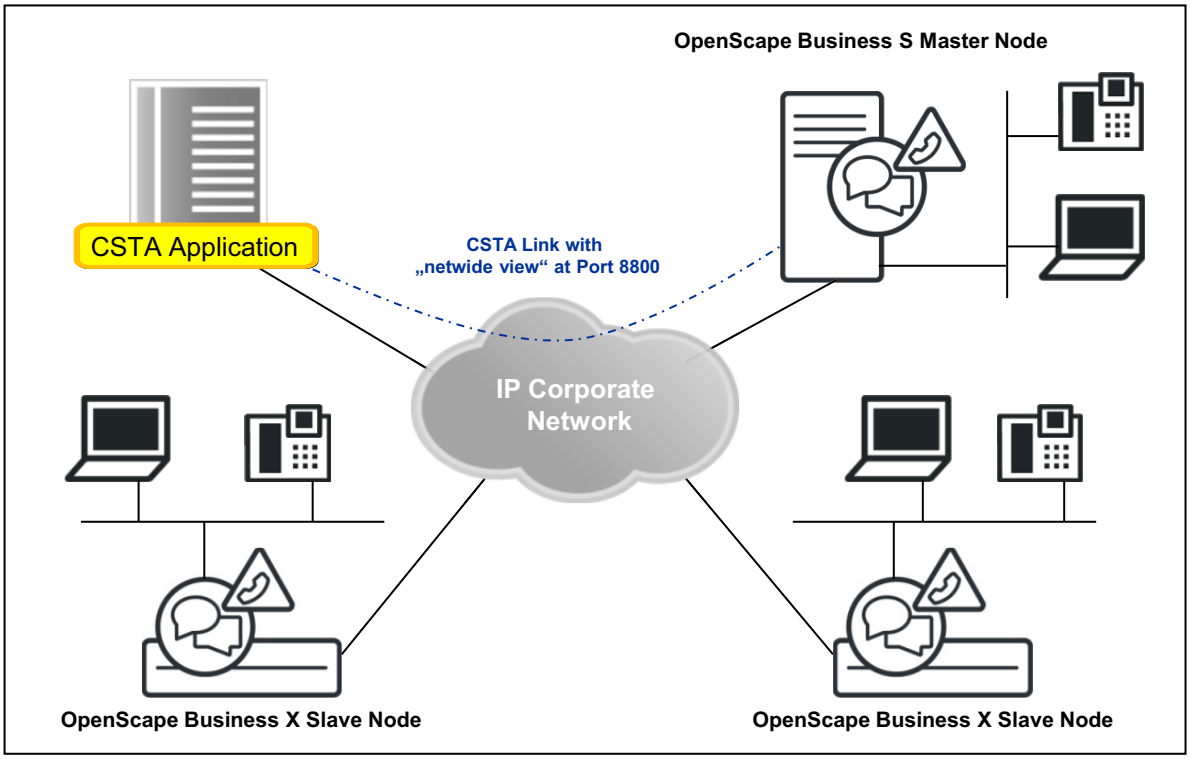
In addition to the phones supported by the system, CSTA supports the following devices:

- ITSP
  This makes it possible for Call Center applications to be used with SIP trunks
- ISDN

- Analog CO trunks
- Virtual stations
- UCD groups
- MULAPs

> ***INFO:*** For details on features and supported devices, please refer to the CSTA Interface Manual.

Connection for network-wide view



Ports

The following port numbers are available by default:

Port	Port number	Usage
CSP	8800	any CSTA application
CMD	8900	reserved for TAPI 120 clients; regardless of the number of clients, exactly one logical CSTA link is used

External CSTA applications and TAPI 120 Service Providers must use the IP address of the UC Server or of the system with the appropriate port number in order to set up the connection. The relevant IP address is displayed in the WBM under Application Selection.

CSTA Links

By default, a CSTA link of the CSP port is available for external CSTA applications. Three other CSTA links are assigned by default to the following integrated CSTA applications or services:

- CMD (CSTA Message Dispatcher) for TAPI 120 clients at the CMD port
- DSS (Direct Station Server)
- UC Suite

If these CSTA applications or services are not needed, the corresponding CSTA links can be assigned to external CSTA applications if required.

Plus Products

The following flags are always enabled in the system:

- Always transmit area code with phone number
- Enhanced CSTA-CAUSE handling
- CSTA CSP signaling
- MULAP monitoring

Related Topics

- Supported Phones

19.2 OpenScape Business TAPI 120/170

OpenScape Business TAPI 120 and OpenScape Business TAPI 170, in addition to CallBridge Collection, are two TAPI Service Providers (TSPs) that are optimized for the system architecture and network topology of OpenScape Business. These TSPs provide the Microsoft TAPI interface to TAPI-based applications for the connection to the OpenScape Business communication system.

The connection to OpenScape Business takes place exclusively via the LAN. Additional hardware and software components such as the CSTA Message Dispatcher (CMD) or CSTA Service Provider (CSP) are no longer required for operation with OpenScape Business. The licensing is station based and does not distinguish between OpenScape Business TAPI 120 or TAPI 170 stations. The licensing requirement begins with the first TAPI station.

The choice of the appropriate TAPI Service Provider essentially depends on the number of client PCs to be connected with TAPI applications as well as the existing IT infrastructure and the telephones used.

- **CallBridge Collection**
  is used as a traditional first-party TAPI Service Provider on system telephones that have a LAN or USB interface. It is suitable for installations with just a few PCs. A LAN is not necessary for the operation of the CallBridge Collection. The CallBridge Collection is installed on each PC that is running a TAPI application. Analog, Cordless and system telephones without USB/IP interfaces are not supported.
  TAPI connections via the CallBridge Collection are not licensed.

- **OpenScape Business TAPI 120**
  is used as the preferred first-party TAPI Service Provider in Microsoft networks with or without a domain controller when analog, Cordless and system telephones without USB/IP interface are also to be operated in conjunction with the TAPI application. The TAPI 120 Service Provider is installed on each PC client that is running a TAPI application.
  TAPI connections via OpenScape Business TAPI 120 are subject to licensing within OpenScape Business. To connect to OpenScape Business, depending on the operating mode or connection type, one CSTA link or a link to the Web Services Interface is required, regardless of how many TAPI 120 clients are being operated. The scope of functionality on the TAPI side depends on the operating mode and type of connection.
- **OpenScape Business TAPI 170**
  is a classic "third-party" TAPI Service Provider. It is installed on a server on the LAN and connected centrally to the OpenScape Business System. TAPI 170 can be used as an alternative to TAPI 120 if there is a domain controller in the Microsoft network. When using the so-called remote TAPI function, it is not necessary to install the TAPI Service Provider on the client PCs. This offers significant time savings in installations with many client PCs. Please note, however, that the use of OpenScape Business TAPI 170 is mandatory in the following constellations:
  – Connection of TAPI stations to networked OpenScape Business systems when the TAPI stations are located in different nodes.
  – Connection to TAPI applications running on a terminal server.
  – Connection to server-based TAPI applications.

  TAPI connections via OpenScape Business TAPI 170 are subject to licensing within OpenScape Business. To connect to OpenScape Business, one CSTA link is required, regardless of how many TAPI 170 stations are being operated.

19.2.1 OpenScape Business TAPI 120

OpenScape Business TAPI 120 is a first party telephony service provider that supports the Microsoft TAPI V2.1 functionality. OpenScape Business TAPI 120 enables Windows-based CTI applications to monitor and control a system telephone connected to OpenScape Business.

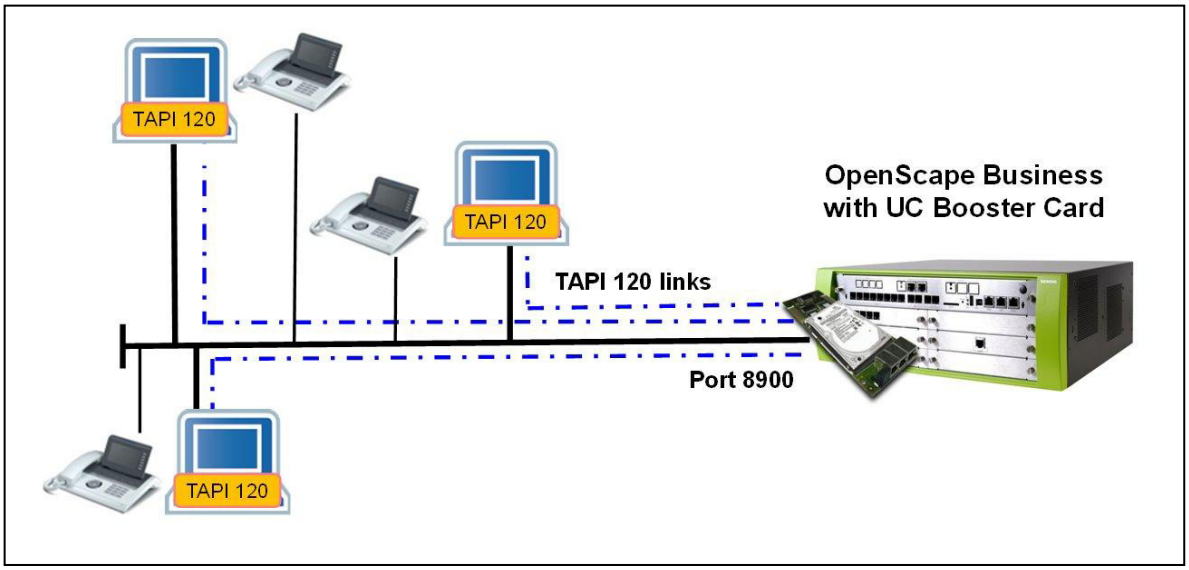
OpenScape Business TAPI 120 can be alternatively connected to OpenScape Business via the CSTA interface (CSTA mode) or the Web Services Interface (UC Smart mode). A mixed operation using both interfaces to the system is not possible. If a UC Booster Card is plugged into the OpenScape Business system or if a UC Booster Server has been enabled, TAPI 120 can only be operated in the CSTA mode. The system requirements, the maximum number of TAPI stations and the scope of functionality on the TAPI side depend on the operating modes.

OpenScape Business TAPI 120 Connections

The OpenScape Business TAPI 120 software is installed on a Microsoft Windows client PC. The connection to the OpenScape Business System occurs via a LAN. A physical connection between the Windows PC and the phone is not required.

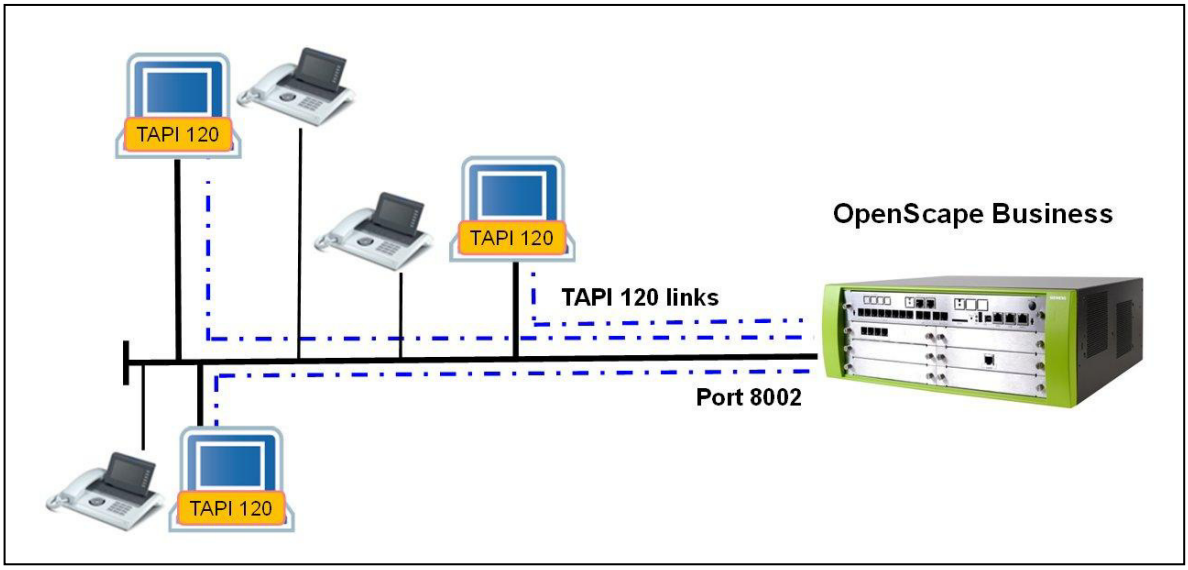
- **TAPI 120 CSTA mode**
  All TAPI 120 client PCs are connected to the same CSTA link of OpenScape Business. OpenScape Business internally multiplexes all TAPI 120 connections.
  TAPI 120 in CSTA mode supports OpenScape Business X3/X5/X8 and OpenScape Business S.

  Figure: TAPI 120 in CSTA Mode with OpenScape Business X5R and UC Booster Card



- **TAPI 120 UC Smart mode**
  All TAPI 120 client PCs are connected to the mainboard of OpenScape Business via the LAN and Web Server interface. OpenScape Business internally multiplexes all TAPI 120 connections.
  TAPI 120 in CSTA mode supports OpenScape Business X1/X3/X5/X8.

Figure: TAPI 120 in UC Smart Mode with OpenScape Business X5R



Features

The following features are supported:

Feature	TAPI 120 CSTA	TAPI 120 UC Smart
Central first-party TAPI Service Provider connected via a LAN	X	X
Compatible with the Microsoft TAPI 2.1 Standard	X	X
Connection to standalone OpenScape Business system	X	X
Support for the OpenScape Business CTI firewall	X	-
Features supported via TAPI		
Call signaling of incoming and outgoing calls with identification of call numbers and origin of call	X	X
Additional information in the call signaling for redirected calls	X	X
Answering internal and external calls	X	X
Controlled connection setup to internal and external called parties	X	X
Manual dialing / DTMF suffix dialing	X	X
Release existing calls	X	X
Set up consultation call to internal and external parties	X	X
Alternate (toggle/connect)	X	X
Screened call transfer	X	X
Screened call transfer with subsequent dialing of the consultation destination (one-step transfer)	X	X
Unscreened call transfer (blind transfer)	X	-

Feature	TAPI 120 CSTA	TAPI 120 UC Smart
Set and delete call forwarding	X	X
Set and clear DND	X	X
Initiate conference	X	-
Expand conference	X	-
Forward incoming call	X	-
Directed pickup (call pickup)	X	-
Group signaling and group pickup	X	-
Park existing calls	X	-
Resume parked calls	X	-
Place existing calls on hold manually	X	-
Resume calls placed on hold manually	X	-
Set callback	X	-
Support for code-driven functions	X	-
Call-related data exchange between TAPI applications	X	-
Control of keys on system telephones (HFA)	X	-
Control of microphone gain on system telephones (HFA)	X	-
Control/select use of handset/loudspeaker/headset for system telephones (HFA)	X	-
Control volume of handset/loudspeaker/headset/keyboard on system telephones (HFA)	X	-
Access to optiPoint/OpenStage displays and LEDs (with limitation to 50 active displays per system)	X	-

Maximum Values

The maximum number of TAPI 120 client PCs that can be connected to OpenScape Business depends on the model (see *Expansion Levels Available through Sales*).

Released Operating Systems

The currently released operating systems for the Microsoft Windows Server, the Terminal Server and the remote client PC are listed in the latest Sales Information.

Only Microsoft Windows operating systems can be used in conjunction with TAPI 120.

For installations on terminal servers, OpenScape Business TAPI 170 must be used instead of OpenScape Business TAPI 120.

Licensing

The use of OpenScape Business TAPI 120 is licensed on a subscriber basis. The TAPI licenses are managed within the OpenScape Business system and can be

used for both modes of TAPI 120. When using the MULAP feature, a TAPI license is required for each station within the MULAP.

> ***INFO:*** No UC Smart licenses are required for TAPI 120 in UC Smart mode.

Software Provisioning

The OpenScape Business TAPI 120 software is supplied on a separate data medium. It is not part of the OpenScape Business system software.

Hardware Requirements

The PC must comply with at least the system requirements specified by Microsoft for the operating system used as well as the requirements of the TAPI application. In addition, an Ethernet LAN interface is required.

- For TAPI 120 CSTA
  One CSTA link of OpenScape Business is required, regardless of how many TAPI 120 clients are connected. An OpenScape UC Business Booster (Card or Server) is mandatory for this purpose.
- For TAPI 120 UC Smart
  The Web Services interface is required. There must be no OpenScape UC Business Booster (Card or Server) present in/at the system.

Supported Devices

The supported devices as well as the supported features on these devices depend on the CSTA or the WSI functionality of the OpenScape Business system being used. This information is contained in the OpenScape Business Sales Information.

Default IP Port / IP Address Occupied by TAPI 120

In the TAPI 120 CSTA operating mode, the CSTA link to OpenScape Business occupies IP port 8900.

In the TAPI 120 UC Smart operating mode, the WSI link to OpenScape Business occupies IP port 8802 for an encrypted connection (HTTPS) or 8801 for an unencrypted connection (HTTP).

In the TAPI 120 configuration, the IP address of the OpenScape Business system must be entered in accordance with the operating mode. This IP address is displayed in the WBM under **Application Selection**.

19.2.2 OpenScape Business TAPI 170

OpenScape Business TAPI 170 is a third party telephony service provider that supports the Microsoft TAPI V2.1 functionality. TAPI 170 enables Microsoft Windows-based CTI applications to concurrently monitor and control telephones connected to OpenScape Business.

Features

OpenScape Business TAPI 170 provides the following features:

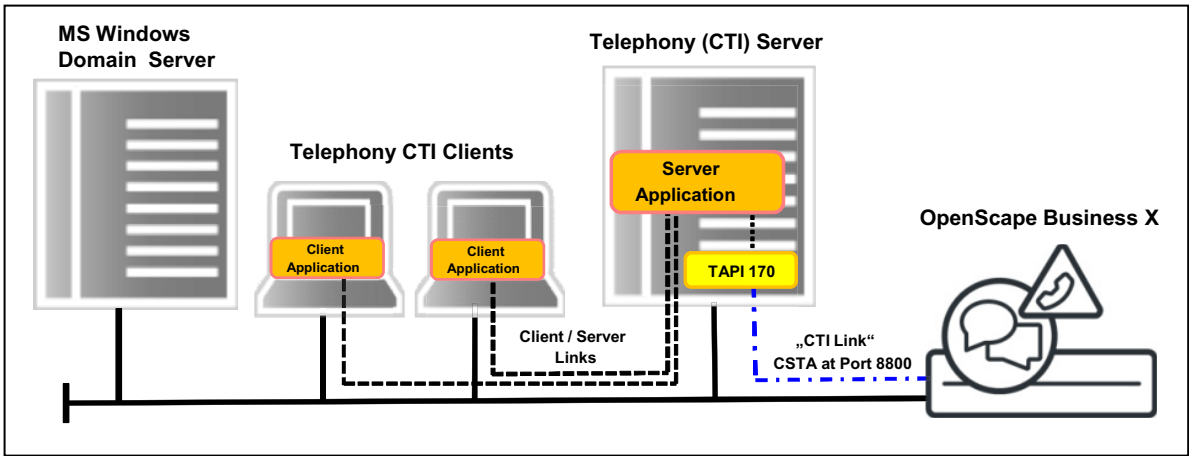
- Centrally connected third-party TAPI Service Provider
- Compatible with the Microsoft TAPI 2.1 Standard
- Telephony functions are available on each connected PC client via the TAPI 2.1 client/server architecture
- No additional TSP client software is required
- Supported telephony features:
  - Selection or dialing of incoming/outgoing calls from the PC
  - Transmission of incoming call number, if signaled
  - Consultation and transfer
  - Toggle/Connect
  - Conferencing
  - Call forwarding
  - Forwarding callers
  - Answering a call through the application
  - Initiating a call through the application
  - Blind/Supervised transfer (also called "transfer before answer / consultation transfer")
  - Transmission of feature codes
  - Monitoring of the phone (call states, failure, etc.)
  - Provision of an ACD interface
  - Monitoring/access to keypad for system telephones (HFA)
  - Control of display/LED for system telephones (HFA)
  - Connection to standalone and networked OpenScape Business systems
  - Support for MULAP members/station numbers

OpenScape Business TAPI 170 Connections

The OpenScape Business TAPI 170 software is installed on a Microsoft Windows server on the network. The connection to OpenScape Business occurs via a CSTA link. A physical connection between the Windows PC and the phone is not required. OpenScape Business TAPI 170 can be set up in different operating modes on standalone systems or in the OpenScape Business network. The TAPI server and clients must be managed by the same network domain controller.

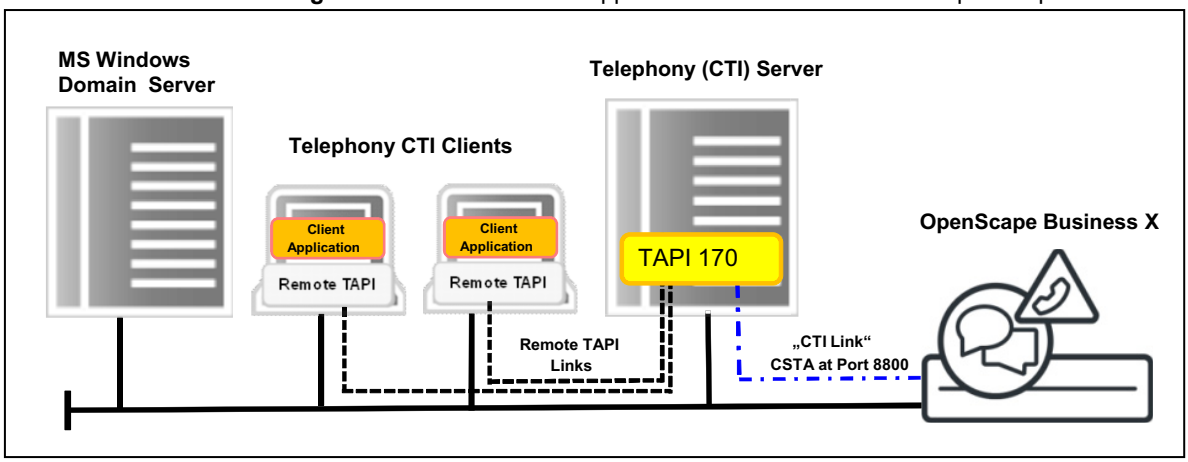
- **Connecting Server-based TAPI Applications to OpenScape Business using TAPI 170**
  The server applications and the TAPI 170 software are installed on the so-called "Telephony Server" in the network. The server applications provide their associated clients in the network with telephony features for the stations that are configured within OpenScape Business TAPI 170. The TAPI 170 software is connected to the CSTA interface of OpenScape Business over the LAN. For this connection, one CSTA link of OpenScape Business as well as one TAPI license for each configured TAPI station are required.

Figure: Server-Based TAPI Application via TAPI 170 to OpenScape Business



- **Connecting Client-based TAPI Applications to OpenScape Business using TAPI 170 with the "Remote TAPI" Function**
  In this scenario, the OpenScape Business TAPI 170 software is installed on a server on the network. On the client PCs with the TAPI applications, the so-called "Remote TAPI" function is enabled, via which the TAPI application on the client communicates with the TAPI 170 software on the server. No TAPI 170 software needs to be installed on the client for this purpose. The TAPI 170 software is connected to the CSTA interface of OpenScape Business over the LAN. For this connection, one CSTA link of OpenScape Business as well as one TAPI license for each configured TAPI station are required.

  Figure: Client-Based TAPI Application via "Remote TAPI" to OpenScape Business

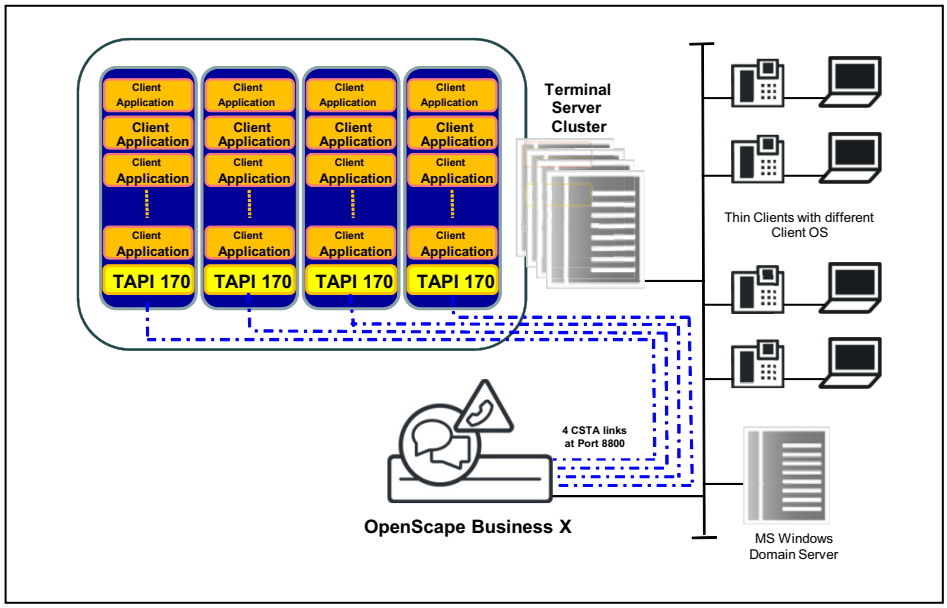


- **Connecting Terminal Server-based TAPI Applications to OpenScape Business using TAPI 170**
  In this scenario, the client-based TAPI applications are installed on one or more terminal servers. In this case, the TAPI 170 software is also installed on the terminal server. In the case of a cluster consisting of multiple terminal servers, the TAPI 170 software must be installed on each terminal server in the cluster. Each instance of the installed TAPI 170 software is connected to OpenScape Business over the LAN. For each instance of the TAPI 170 software installed on a terminal server, one CSTA link of OpenScape

Business is required. In addition, a TAPI license is also required for each configured TAPI station.
The maximum possible number of OpenScape Business TAPI 170 servers in conjunction with OpenScape Business must not be exceeded.

INFO: The number of terminal servers that can be operated in the cluster is limited to the number of free CSTA links available within OpenScape Business for connecting the TAPI 170 software. The maximum number of possible connections is reduced if the CSTA links of OpenScape Business are used by other CSTA applications.

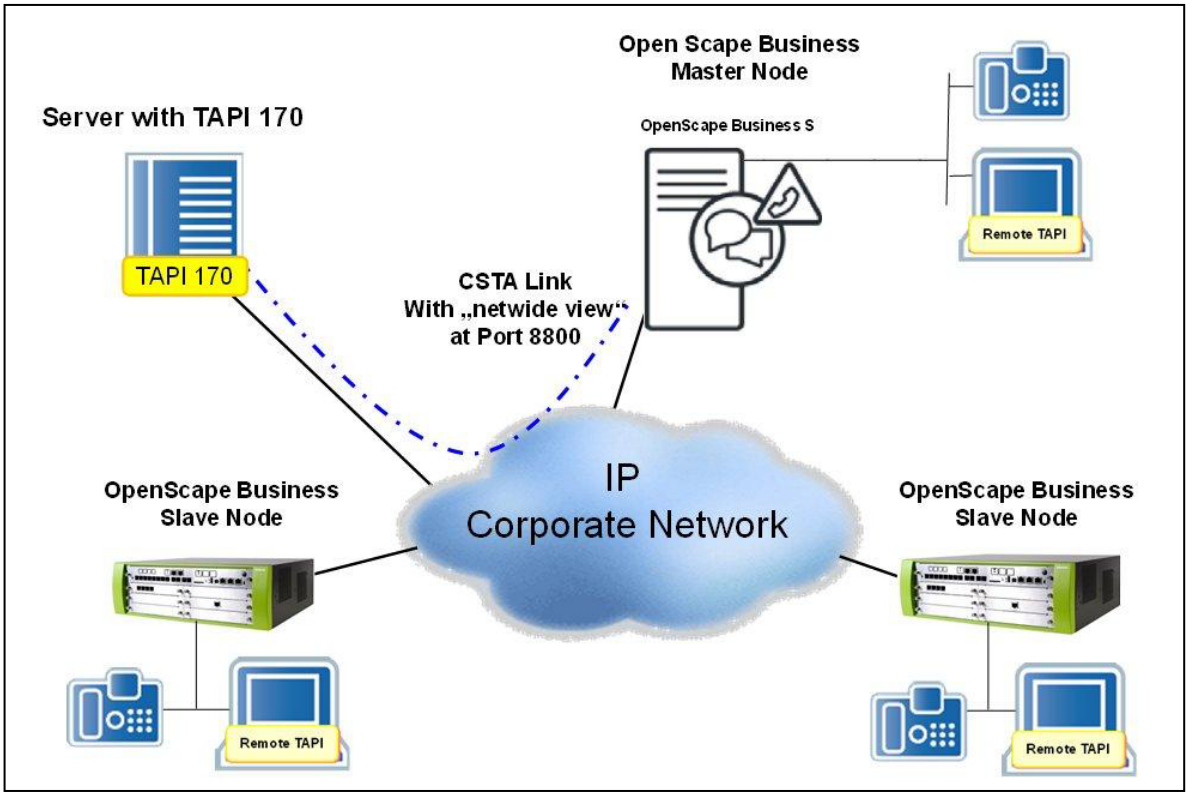
Figure: Client-Based TAPI Applications on Terminal Server to OpenScape Business



- **Connecting TAPI 170 to Networked OpenScape Business Systems**
  For networked OpenScape Business systems, the TAPI 170 software is installed on one server, which is connected via the LAN to the CSTA interface of the master node. This connection is independent of the previously mentioned operating modes of the TAPI 170 Service Provider (remote TAPI or server-based connection). To implement this connection, one CSTA link of the OpenScape Business master node as well as one TAPI license for each configured TAPI station are required.

  INFO: Via the master node, the TAPI 170 receives network-wide access to all stations in the network. If the TAPI 170 is connected to a slave node instead of the master node, TAPI 170 can access only the stations of the slave node. When using multiple TAPI 170 in a terminal server cluster, one CSTA link to the master node is required for each TAPI 170.

Figure: Connecting TAPI 170 to Networked OpenScape Business Systems



Capacity Limits

The maximum number of TAPI 170 client PCs that can be connected to OpenScape Business depends on the model. More information on this can be found in section 1.3.9.4

Released Operating Systems

The currently released operating systems for the Microsoft Windows Server, the Terminal Server and the remote client PC are listed in the latest Sales Information.

Only Microsoft Windows operating systems can be used in conjunction with TAPI 170.

In addition to the license for the server operating system, the Microsoft licensing model requires Microsoft device or User CALs corresponding to the number required for the planned expansion. These CALs are not included in the delivery of OpenScape Business TAPI 170 and must be purchased separately. Under certain conditions specified by Microsoft, a "Windows Server for embedded systems" with the so-called "embedded Telco license" can be used for OpenScape Business TAPI 170.

Licensing

The use of OpenScape Business TAPI 170 is licensed on a subscriber basis. The licenses are managed within the OpenScape Business system. When using the MULAP feature, a TAPI license is required for each station within the MULAP.

Software Provisioning

The OpenScape Business TAPI 170 software is supplied on a separate data medium. It is not part of the OpenScape Business system software.

Hardware Requirements

In order to connect to OpenScape Business TAPI 170, one CSTA link of OpenScape Office is required, regardless of how many TAPI 170 clients are connected. This also applies to networked OpenScape Business systems.

The PC must comply with at least the system requirements specified by Microsoft for the operating system used, provided that no further software applications other than TAPI 170 are being operated. In addition, an Ethernet LAN interface is required.

Supported Devices

The supported devices as well as the supported features on these devices depend on the CSTA or the WSI functionality of the OpenScape Business system being used. This information is contained in the OpenScape Business Sales Information.

19.3 Web Services Interface

The integrated web services interface enables the monitoring and control of telephony resources in a system with UC users.

Features

The web services interface provides the following features:

- Access via Ethernet LAN (TCP/IP)
- Support for HTTP and HTTPS
- Support for individual systems
- User-oriented, clearly structured functions for:
  - Call control
  - Device control
  - Monitoring devices
  - Directories
  - Journals of users
  - Presence status of users

> ***INFO:*** Depending on the WSI (Web Services Interface) client type, station flag Associated Services must be activated in order to enable execution of some of the WSI commands.

Web Server WebSessions

The number of available web server sessions is common to all relevant applications (e.g., myPortal to go, Application Launcher, optiClient Attendant (Server) and optiClient BLF.

Internal Monitor Points

The internal monitor points are independent of the monitor points of the CSTA interface. If several applications monitor the same UC user via the web services interface, only a single internal monitor point is used by the web server for this purpose.

Ports

The following port numbers are available:

Port	Protocol
8801	HTTP (unencrypted)
8802	HTTPS (encrypted)

19.4 Open Directory Service

Open Directory Service is an open, integrated metadirectory service that can be accessed by several different types of clients, applications and communication devices in a company. The Open Directory Service performs two functions: it enables additional contact data from external data sources to be integrated in the directories of the system, while also making the directories available to clients, communication devices and applications.

Open Directory Service runs as a separate service based on OpenLDAP. Firewalls must be open for port 389. Open Directory Service is disabled by default.

Internal Data Sources

The following internal data sources are available by default in the Open Directory Service:

- External directory
- Internal directory
- Central speed-dial numbers

For these internal data sources, the field names are permanently mapped to the data schema of the Open Directory Service.

These internal data sources cannot be deleted or modified.

External Data Sources

As an administrator, you can integrate contact information from the following types of databases as data sources for read-only access via ODBC.

- Relational data sources (Microsoft SQL Server, PostgreSQL, Sybase, SQL Server)
- Non-relational data sources require an installed and configured ODBC Bridge Server on the ODS client (downloadable via the WBM under **Service Center > Software**).

Maximum number of different types of databases: 3

Maximum number of external data sources: 4

Make sure that the Open Directory Service is authorized to access the external data source. Contact the responsible database administrator in advance to ensure that this is the case. A separate user may need to be added in the external data source for access by the system.

External data sources can be used in the context of both directory searches and the resolution of call numbers into names.

You can configure direct access to a database table from an external data source or a custom SQL query for the data source.

Any column which serves as an ID must contain unique and not null/not empty values. Use the UNIQUE or PRIMARY KEY property to ensure that this is the case.

In cases where external databases are integrated, the following restrictions apply:

- The special characters ´[]'" are not supported by the ODS in table names and column names.
- The column types "nchar" and "nvarchar" are not supported by the ODS.

In case of ODBC bridge data source for Access, Firebird and Excel data sources please add the word "access", "firebird", "excel" respectively to the description field.

Custom SQL Queries for External Data Sources

Custom SQL queries also support related tables, e.g.:

```
SELECT * FROM users LEFT OUTER JOIN phonenumbers ON users.id
= phonenumbers.uid;
```

The data structure must be of the type 1:1 or n:1, i.e., each record can have only a single row.

Access via custom SQL queries can sometimes run much slower than direct access to a database table.

Custom SQL queries with potential security risks are not executed, for example:

- Modifying data
- Stopping the SQL server
- Running programs via the SQL server
- Changing user rights

Custom SQL queries with the following SQL commands are therefore not executed:

- `CHECKPOINT`

- CLOSE
- CLUSTER
- COMMIT
- COPY
- CREATE
- DEALLOCTAE
- DECLARE
- DELETE
- DISCARD
- DO
- DROP
- END
- EXECUTE
- EXPLAIN
- FETCH
- GRANT
- INSERT
- LOAD
- LOCK
- MOVE
- PREPARE
- REASSIGN OWNED
- REINDEX
- RELEASE SAVEPOINT
- RESET
- REVOKE
- SAVEPOINT
- SECURITY LABEL
- SELECT INTO
- SET
- SHOW
- START TRANSACTION
- TRUNCATE
- UNLISTEN
- UPDATE
- VACUUM
- VALUES

Field Mapping for Data Sources

For these data sources, you can customize the mapping of field names to the data schema of the Open Directory Service. You can assign each field in the data schema of the Open Directory Service to no more than one field of the external

data source. However, you can assign a field of the external data source to multiple fields in the data schema of the Open Directory Service.

LDAP Data Output Mappings

An LDAP data output mapping determines which of the fields in the data schema of the Open Directory Service are to be output via LDAP, e.g., for specific LDAP clients or for different groups of subscribers who do not want to see all the details, but only a defined subset.

The LDAP data output mapping **web** is available by default and cannot be deleted or changed. All fields of the data schema in the Open Directory Service are permanently assigned to the LDAP output in it. You can also configure other LDAP data output mappings.

LDAP clients can access a specific LDAP data output mapping via the dc parameter in the LDAP login, for example: `dc=web`.

Normalization of Phone Numbers in the Canonical Format

For each data source, you can configure the normalization of phone numbers in the canonical format. During this process, blanks, parentheses, hyphens and commas are removed. This is required to correctly identify the caller's name and for desktop dialing. You should not skip the normalization, unless the phone numbers used in the data source are already present in canonical format. You can have the normalization-related values such as the area code, etc., entered automatically from the system. If the external data source is located at a different site than the system, you may need to adjust these values.

Status of Data Sources

The status display under **OpenDirectory > Data Sources** has the following significance:

Color	Status
green	active
red	ODBC and LDAP is not OK, wrong configuration or data source unavailable
yellow	LDAP not ok: restart the Open Directory Service
gray	Configuration incomplete

Provision of directories

The following types of clients, communication devices and applications can use the directories provided by the Open Directory Service:

- UC Clients
- Application Launcher
- System Directory
- OpenStage with local LDAP support
- DECT IP phones (via LDAP)

- SIP phones (via LDAP)
- Applications, e.g., CRM Suites such as Microsoft Dynamics CRM (via LDAP, ODBC or OpenLDAP CSV export)

Open Directory Service can identify in the search results the data source from which a hit is obtained.

19.5 XMPP

XMPP (Extensible Messaging and Presence Protocol) is an Internet standard for XML routing and is used mainly for instant messaging. XMPP enables the integration of external communication partners for instant messaging and the mapping between the presence status and the XMPP status.

XMPP is supported for the following clients:

- myPortal for Desktop
- myPortal for Outlook
- myAttendant

An external XMPP communication partner may be a Google Talk or Microsoft Lync Office Communicator user, for example.

The integrated Openfire XMPP server is externally addressed via port 5269 by default. The connections to other XMPP servers can be secured with TLS, provided they support TLS. Port 5222 is used to communicate internally with clients. The ports must be opened in the appropriate firewall. XMPP is disabled in the system by default and can be configured by the administrator. The required configuration of XMPP in each client can be performed by the subscriber. External XMPP gateway servers are not supported. XMPP IDs of external communication partners must conform to the pattern `xmpp:john.public@osbiz.example-for-a-domain.com` and may be present at the following locations:

- external directory
- External offline directory (LDAP)
- Personal directory (myPortal for Desktop)
- Outlook contacts (myPortal for Outlook)
  IM address field
- Favorites

Related Topics

- Instant Messaging

19.6 Application Launcher

Application Launcher is a Java-based Windows application for the call-related control of applications running on the client PCs of UC Suite users. Application Launcher could typically be used to automatically open the contact form in a CRM system for each respective caller, for example.

Application Launcher provides the following features:

- Obtaining call-related information on a phone number (e.g., phone number, name of the caller, customer ID) from either the Open Directory Service or from system directories
- Launching Windows applications or web applications for incoming and outgoing calls
- Transfer of call-related information to Windows applications or web applications
- Automatic operation in the background for incoming calls
- Optional, configurable screen pops for incoming calls with call-related information and buttons for user actions
- Caller list with call function
- Preview functions for testing during configuration
- System configuration profile for simple transfer of the configuration settings of the first configured client to all other clients

19.6.1 Prerequisites for Application Launcher

In order to use Application Launcher, the client PC of the individual user must be equipped with the appropriate hardware and software.

Local administrator rights on the client PC are required for the installation, but not for automatic updates.

Operating System

Application Launcher can be used in combination with the following operating systems:

- Microsoft Windows 10 / 8.1 / 8 / 7 (both 32-bit or 64-bit are possible)
- Microsoft Windows Vista (32 bit)

> ***INFO:*** The used operating system always requires the latest version of all available updates (Service Packs and patches).

Windows Update

The PCs always need the current status of all available updates, including Service Packs.

Additional Software

Latest Oracle Java version (see **Service Center > Software**)

Web Services for Mobile Phones

Web services for mobile phones has been enabled in the system for the system connection. The ports configured in the system must be open in the firewalls on the LAN and the client PCs.

Open Directory Service (optional)

If Application Launcher is to use the data from the Open Directory Service, the Open Directory Service must be configured in the system. The port configured for this in the system must be open in the firewalls on the LAN and the client PCs.

Related Topics

- Configuring myPortal to go and Mobility Entry

19.6.2 Profile with Configuration Data for Application Launcher

A profile with configuration data for Application Launcher enables the easy and fast configuration of Application Launcher on all client PCs.

The profile contains all the configuration data, except for the system connection and the user data. As soon as Application Launcher has been fully configured for an initial user, as an administrator, you can make that profile with the Application Launcher configuration data available in the communication system. All other users can then perform the configuration of Application Launcher by importing this profile.

19.7 Circuit

It is possible for OpenScape Business mobility groups and users to use the Circuit functionality. To do that, you must configure the Circuit connectivity with OpenScape Business and add the Circuit users.

20 Accounting

Accounting includes the collection of call data and account codes, the transmission and display of connection data, cost control and accounting tools.

20.1 Connection Data

Connection data includes the collection of call data and account codes.

20.1.1 Connection Data Recording

The system can log the connection data of used lines.

For every completed connection and/or every incoming connection, a connection data record is created. A separate connection data record is stored for each new connection segment (for example, as a result of transferring or forwarding to another subscriber). Internal connections are not logged.

The administrator can enable the following options for recording connection data:

- Recording on or off
- Connection duration
- Currency amounts or call charge units:
  Call charge units are converted into currency amounts based on the configurable call charge factor (currency amount per call charge unit).
- Decimal format
  Divides the currency amount by100 to display 6 cents as 0.06, for example
- Suppress last four digits of destination numbers
- Log incoming connections
- Outgoing calls without connection:
  For example, this gives the calling party proof that the destination station did not accept the attempted call (marked with the connection duration 00:00:00). This option applies to ISDN connections and to all subscribers.
- Connection protocol
  Start logging on beginning the call
- Log MSN
- Output LCR number outgoing or dialed number incoming
  - outgoing:
    the actual call number which is sent by LCR to the PSTN
  - incoming:
    the originally dialed internal number

If call charges accrue before the call is set up (as occurs in Austria, for instance), these are recorded, irrespective of whether or not logging of outgoing calls without connection is enabled.

The system takes connections via QSIG trunks into account only if a trunk code has been configured for them.

No logging occurs for:

- premature termination of the call attempt
- unauthorized connections (LCR, Denied lists).

Related Topics

- Account codes

20.1.2 Account codes

Account codes (ACCT) can be used to assign connection data and charges to specific projects. For this purpose, the system logs the account codes entered by users on their phones in the relevant connection data records.

ACCT is used in combination with connection data recording and is available to all subscribers.

The subscriber can enter an ACCT at the phone before or after dialing. It is not possible to dial from a client with ACCT enabled.

An ACCT entered during a conference with external stations is assigned to all participating connections and trunks.

The administrator can set whether an ACCT should be saved for redialing.

The personal directory (also called a phonebook) can save the code for the ACCT feature + an ACCT + a phone number together in one entry:

ACCT Input Procedure

The administrator defines the ACCT input procedure in the LCR dial plan:

- Mandatory
  The ACCT must be entered before setting up the connection (before or after seizing a route).
- Optional
  The ACCT may optionally be entered before setting up the connection. IP phone clients support input during a call, including incoming calls.

ACCT Checking Procedure

The system can check the validity of an ACCT entered for the following types:

- List verification
  Only predefined ACCTs are valid. After a valid ACCT has been entered, the subscriber can immediately continue dialing. The system rejects an invalid

ACCT. "Incorrect entry" appears on the display and a negative confirmation tone is output.

- Check number of characters
  All ACCTs that are theoretically possible with the configured number of digits are valid. After a valid ACCT has been entered by the subscriber, he or she can immediately continue dialing.
- No Check
  The validity of the ACCT is not checked. ACCTs with less than 11 digits must be separated from the other digits dialed by the subscriber with “#”. For ISDN phones, this variant always requires a 11-digit account code; otherwise, no dialing occurs.

If the subscriber determines during a connection that the assigned ACCT is not correct, he or she can enter some other ACCT. The system will overwrite the currently set account code. Connection data recording creates a connection data record after each segment. Therefore, previously completed connection segments will be identified with the old account code number.

Related Topics

- Connection Data Recording

20.2 Displaying and Transmitting Connection Data

The display and transmission of connection data includes different ways of displaying connection data on system phones and file transfer methods.

20.2.1 Call-Charge Display with Currency (not for U.S.)

The system can display the currency amount transmitted for the current external connection by the network provider on the display of the telephone.

The network provider must support the transfer of currency amounts with the Advice Of Charge (AOC-D or AOC-S) feature. The system aggregates the amounts of the relevant call charge units.

The currency amount can basically be transferred at the following times:

- on starting the call and possibly during the call (AOC-S)
- during the call (AOC-D)

The administrator can avoid inaccuracies in recording connection data via the "Computing accuracy" parameter. The computing accuracy determines:

- the number of decimal digits for evaluating the connection data (minimum currency amount)
- the maximum total of cumulative currency amounts.

The preset computing accuracy must equal to or higher than the computing accuracy used for ISDN. If the maximum of three decimal places is insufficient, the system automatically rounds up the number to the next unit. Possible values for computing accuracy:

Computing accuracy	Minimum currency amount	Maximum currency amount
No decimal digits	1	around. 4.3 billion
1 decimal digit	0.1	around 430 million
2 decimal digits (e.g., for Euro)	0.01	around 43 million
3 decimal digits (e.g., for British pounds sterling)	0.001	about 4.3 million

20.2.2 Displaying the Connection Charges on the Phone

The system can display information about the cost of an existing external connection on the phone display as a currency amount.

The system aggregates the amounts of the relevant call charge units. The currency amount is calculated from the call charge units and the configured call charge factor. The service provider must support the Advice Of Charge (AOC) feature.

The connection charges information can be transmitted at the following times:

- On starting the call and possibly during the call (AOC-S)
- During the call (AOC-D)
- At the end of the call (AOC-E)

At the end of the call, the display shows the final charges for the completed call for about 5 seconds, provided the subscriber has not started some other action.

Connection charges for the current connection are always displayed when toggling.

For an unsuccessful blind transfer, the overall amount is displayed and charged.

A subscriber to whom a call is transferred will only see and be charged for the relevant amount from that point in time during the call.

20.2.3 Displaying the Connection Duration on the Phone

The system can show the duration of outgoing and incoming external connections on the phone's display.

The format is HH:MM:SS.

If the connection duration display is disabled, the connection charges information of the PSTN is shown on the phone's display instead. If there is no connection charges information available, the display shows the caller's number (if known).

20.2.4 Transmission of Connection Data

The system can transmit connection data in a file using HTTPS.

The transmitted file can then be evaluated with a suitable program.

A continuous output of the connection data is only possible via CSTA.

The administrator can choose between the following formats for the connection data (ASCII 8-bit):

- Compressed format
- Uncompressed format

Compressed format, Standard

A connection data record in compressed format contains the following fields, delimited by |, and each connection data record is terminated with CRLF:

Field position	Length	Description
1	8	Date (at end of call)
2	8	Time (at end of call)
3	3	Number of seized trunk
4	16	Internal station number
5	8	Alert time for incoming connection
6	8	Duration of the connection
7	Max. 25	Dialed or received external station number
8	11	Call charge unit/Amount
9	2	Additional information (such as incoming call, outgoing call, transferred connection, conference, DISA, connection setup charges)
10	Max. 11	Acc. code
11	Max. 11	Only for a point-to-multipoint connection: used MSN
12	6	LCR access code, CO access code
13	2	LCR route used, dial rule
14	25	Dialed or received call number (optional)

Examples of connection data records:

- Outgoing connection:
  `13.02.13|14:18:02|201|33388|00:02|00:00:07|0123456789||1||||||`

- Incoming connection:
  `13.02.13|14:28:02|202|33388|00:05|00:00:12|0123456789||1|||||`

Compressed format, USA-specific

A connection data record in compressed format contains the following fields, delimited by |, and each connection data record is terminated with CRLF:

Field position	Length	Description
1	8	Date (at end of call)
2	8	Time (at end of call)
3	3	Number of seized trunk
4	16	Internal station number
5	8	Alert time for incoming connection
6	8	Duration of the connection
7	Max. 25	Dialed or received external station number
8	11	Call charge unit/Amount
9	2	Additional information (such as incoming call, outgoing call, transferred connection, conference, DISA, connection setup charges)
10	Max. 11	Acc. code
11	Max. 11	Only for a point-to-multipoint connection: used MSN
12	6	LCR access code, CO access code
13	2	LCR route used, dial rule
14	2	PRI Nodal Service
15	1	PRI WATS band
16	3	PRI CIC
17	25	Dialed or received call number (optional)

NOTICE: In *HKEY_LOCAL_MACHINE\SOFTWARE* registry keys for *Accounting Tool*, the value of the **DateFormat DWORD** should be set to 1 for North America date format (MM.DD.YY). The default value is 0 and corresponds to European/Latin America date format (DD.MM.YY).

INFO: Data record of Accounting manager in compressed format are seperatrd by the delimiter |. This can be configured only through Manager E.

Uncompressed format

The uncompressed format is suitable for printing. In addition, a header and form feed are output. A connection data record in compressed format contains the following fields, delimited by |:

Field position	Character position, Length	Description
1	1-8 (8)	Date at end of connection: DD.MM.YY (DD = day: value range 01 ... 31, MM = month: value range 01 ... 12, YY = year: value range 00 ... 99)
2	9-16 (8)	Time at the end of a connection segment or an unanswered incoming call: hh:mm:ss a (hh = hours: value range 00 ... 23, mm = minutes: value range 00 ... 59, ss = seconds: value range 00 ... 59)
3	17-19 (3)	Trunk: trunk number Value range 1 ... 250
4	20-35 (16)	Station: Internal station number For unanswered calls, this is the last station called (e.g., a hunt group, call forwarding, call forwarding—no answer). For group calls, this is the last station entered. For answered calls, the station that accepted the call is shown. A programmed SNO prefix (with networking only) is not output. If the internal numbering was converted to a maximum 7-digit numbering plan, the converted station number is output. The internal station number may be preceded by a max. 7-digit node number If the total resulting from the node number and the station number is greater than seven, only the last seven digits of the number are output.
5	36-40 (5)	Call duration of an incoming connection: mm:ss (mm = minutes: value range 00 - 59, ss= seconds: value range 00 - 59) The display occurs for all incoming calls, provided the output of the ring duration has been configured in the system. If a counter overflow occurs (duration > 59:59), “59:59” is output. A change in date or time during system operation can result in this situation. In the case of an incoming call to a busy station, the ring duration is "00:00".
6	41-48 (8)	Duration of the connection or connection segment: hh:mm:ss (hh = hours: value range 00 ... 23, mm = minutes: value range 00 ... 59, ss = seconds: value range 00 ... 59) If a connection has not been established for an incoming call, 8 blanks are output here. If a counter overflow occurs (duration > 23:59:59), “23:59:59” is output.
7	49-73 (25)	Dialed or received external station number (if available): nnnnnnnnnnnnnnnnnnnnnnnnn (n = dialed or received character: value range 0 ... 9, *, #, ?) The output occurs for incoming and outgoing calls, to the extent available. For outgoing calls, the dialed call number or, if available, the call number transmitted via COLP, is displayed. If the data protection function is enabled, the last four digits dialed are replaced by "????" If no station number information is available, 25 blanks are output.

Field position	Character position, Length	Description
8	74-84 (11)	Call charge units for a connection segment: ddddddddddd (d = digit: value range 0 ... 9) You can select either call charge units or currency amounts. Call charge units are converted into currency amounts using the call charge factor that is defined by the administrator as the currency amount (including any applicable surcharges) per call charge unit. The following applies when setting the call charge factor: • With calculation detail: call charge factor = 100% + any applicable surcharge • Without calculation detail: call charge factor = amount/unit + any applicable surcharge The system records the connection charges with or without a surcharge depending on the calculation detail: The output always occurs whenever connection charges accrue for the connection segment (e.g., even for transferred connections).
9	85-86 (2)	Information element: additional information Value range: 0 - 9 Meaning: • 1 = Incoming connection (Voice / 3.1 kHz Audio Call) • 2 = Outgoing connection (Voice / 3.1 kHz Audio Call) • 3 = Incoming connection (Other Services) • 4 = Outgoing connection (Other Services) • 5 = Incoming connection, routed • 6 = Outgoing connection, routed • 7 = int/ext/ext conference with incoming connection / transit through external transfer • 8 = Conference with outgoing connection / Transit through external transfer • 9 = Outgoing connection via call forwarding to external destination • 0 = Connection information (caller list) is output immediately on receiving an incoming call (the output can be suppressed). This can be used, for instance, for a database search from a PC. In cases where multiple stations are called, a separate line is output for each individual station (without ring duration, connection duration, call charge information). • +20 = Offset as a code for connection setup charges (connection setup without connection duration) • +30 = Offset as a code for a follow-up data record in the case of – Call duration > 24 h. – contiguous connection segments with the same line/station number (e.g., after transferring a connection or clearing a conference). • +40 = Offset for a data record with transit code (by an extension in the subsystem). Can occur in combination with offset +30. • +50 = Offset as a code for DISA connections • +70 = combination of offsets +30 and +40

Field position	Character position, Length	Description
10	87-97 (11)	Account code (ACCT) entered by the user for this connection: aaaaaaaaaaa (a = ACCT digit: value range 0 ... 9) Missing digits are replaced by spaces.
11	98-108 (11)	Used MSN: mmmmmmmmmmm (m = digit of the MSN: value range 0 ... 9) The output occurs if the user has programmed an MSN key. For outgoing connections of a MULAP subscriber, the call number of the seized MULAP is displayed. Missing digits are replaced by spaces.
12	109-113 (5)	Seizure code used, access code: sssss (s = digit of the seizure code: value range 0 ... 9)
13	114-115 (2)	Used LCR route: rr (r = digit of the selected route: value range 0 ... 9)

Communication Sequence

The transfer of connection data can be requested (download request), whereupon the system responds accordingly (download response).

Subsequently, the deletion of connection data can be requested (delete request), whereupon the system responds accordingly (download response).

Download Request - Definition

Element	Contents
HTTP header	Request method = GET
URL	https://<IP address of the system>/management/portlet
Parameters	portlet=hipath-accountingdownload::HiPathAccountingDownloadPortlet
	entity=accounting
	action=get
	username = <username>
	password=<password>

INFO: When accessing charge data with the referenced interface, HTTP GET request restrictions are applied. The following special characters are not allowed to be used as pass word, when someone attempts to get data via URL request:
:/?#[]@ !$&'()*+,;=

Example:

```
https://192.148.108.151/management/portlet/?portlet=hipath-
accountingdownload::HiPathAccountingDownloadPortlet&entity=
accounting&action=get&username=xbert@system&password=not4u;
-)
```

Download Response - Definition

Element	Contents
HTTP header	ContentType = "text / plain"
Parameters	attachment filename = "<charging file>"
	data = <content of the charging file>

Response Code	Meaning
SC_OK(200)	Success
SC_BAD_REQUEST(400)	Missing parameter in request
SC_UNAUTHORIZED(401)	Login failure or wrong user name or password
SC_INTERNAL_SERVER_ERROR(500)	Internal error

Delete Request - Definition

Element	Contents
HTTP header	Request method = POST
URL	https://<IP address of the system>/management/portlet
Parameters	portlet=hipath-accountingdownload::HiPathAccountingDownloadPortlet
	entity=accounting
	action=delete
	username = <username>
	password=<password>

Example:

```
https://192.148.108.151/management/portlet/?portlet=hipath-
accountingdownload::HiPathAccountingDownloadPortlet&entity=
accounting&action=delete&username=xbert@system&password=not
4u;-)
```

Delete Response - Definition

Response Code	Meaning
SC_OK(200)	Success
SC_BAD_REQUEST(400)	Missing parameter in request
SC_UNAUTHORIZED(401)	Login failure or wrong user name or password
SC_INTERNAL_SERVER_ERROR(500)	Internal error

Related Topics

- Accounting Tools

20.3 Cost control

Cost control includes the features Expensive Connection Route Advisory and Toll Fraud Monitoring.

20.3.1 Expensive Connection Route Advisory

If the telephone is currently unable to reach a call destination via the least-cost routing path, it can notify the subscriber of the use of an expensive connection path via an advisory signal.

The subscriber can thus decide whether or not to conduct the call at that time despite the expensive connection path. The advisory signal may occur as follows:

- Text in the display
- Tone
- Text in the display and tone

The system issues an advisory message for the expensive connection path if a corresponding warning has been configured in the routing table and if the system is not using the route of index 1 of the routing table.

The advisory message is only displayed on the screen if no name is configured for the associated dial rule. If a name is configured, it is displayed.

20.3.2 Toll Fraud Monitoring

The system can monitor connections to detect possible occurrences of toll fraud. Monitoring is performed for connections that arrive via a trunk and then leave via a trunk.

The first station signals when the configured connection duration is exceeded and thus enables you to disconnect the call if required. As an administrator, you can configure whether or after what connection duration such a connection is to be signaled.

20.4 Accounting Tools

Accounting tools are provided by Accounting Manager and Teledata Office.

Related Topics

- Service Center – Documents
- Transmission of Connection Data

20.4.1 Accounting Manager

Accounting Manager is a Windows application for retrieving connection data via HTTPS and evaluating this data using tables and graphics.

Accounting Manager ships with its own documentation. Accounting Manager retrieves connection data from the individual network nodes. You can also use Accounting Manager to test the Connection Data interface. You can download Accounting Manager in the **Service Center** of the WBM. Accounting Manager requires local administration rights and the activation of TLS 1.2 in Microsoft Internet Explorer.

20.4.2 Teledata Office

Teledata Office is a Windows application for analyzing connection data.

21 Maintenance

The system offers several maintenance options. This includes changing the telephony settings, backing up and restoring the configuration data, updating the software with updates and upgrades and restarting/reloading functions. In addition, appropriate functions for status identification, monitoring and maintenance are available. Remote access to the system is possible via different Remote Services.

Maintaining the UC Booster Server

If a UC Booster Server is being operated in addition to the communication system, several maintenance options are offered by UC Booster Server as well. The maintain the UC Booster Server, the administrator does not specify the IP address of the communication system when calling the WBM, but the IP address of the Linux server.

21.1 Telephony Configuration

The communication system offers various configuration options for telephony, e.g., date and time, SNTP, customized display, and Music on Hold.

21.1.1 Date and Time

The communication system features a system clock with date and time. This system time is shown in myPortal for Desktop and on every terminal's display.

You can define the basic system time or synchronize it as follows:

- via a time server using SNTP
- via an ISDN trunk through an outgoing call
- by a manual setting

System-specific settings are not possible for the system time after activating an SNTP server.

If ever an SNTP server cannot be reached and HFA system phones use a different time source than the system, the time displayed on the phones may differ from the system time.

A system time manually set after system startup is always overwritten by ISDN time information the first time an outgoing ISDN call is made, provided the network provider transmits this information. If the difference between the system time manually set and the ISDN time information in a live system is between 2 and 70 minutes, the ISDN time information is applied. Otherwise, the system time manually set is maintained.

The administrator can select one of the following formats to display the date on the terminal. The format is additionally dependent on the type of phone:

Date format	OpenStage	OptiPoint 410, OptiPoint 420
Europe	Tue 20.11.07	20. NOV 07
USA	Tue 11/20/07	Tue NOV 20.07
International1	Tue 20.11.07	Tue 20 NOV 07
International2	Tue 20.11.07	TUE 20.11.07

If you inadvertently set a date before 2007 as an administrator, you will subsequently no longer be able to access the WBM. This will only be possible after a restart, which resets the date to 01.01.2007.

21.1.2 SNTP

Over SNTP, you can synchronize the date and time of your systems with NTP time servers on a network-wide basis.

SNTP (Simple Network Time Protocol) is a simplified version of NTP (Network Time Protocol), a standard for synchronizing date and time via packet-based communication networks. Your system needs a connection to an NTP server to synchronize date and time. This connection can occur in your local network or on the Internet. A number of different NTP servers are available on the Internet; you can select one that is located in your time zone. Note the conditions of use for the relevant server and, if necessary, request permission.

21.1.3 Telephone Logos

System telephones with a display may show the logo as a background of the Telephony User Interface (TUI).

As an administrator, you can import, assign or delete phone logos for system telephones with a display. Different types of system telephones may use different phone logos.

21.1.4 Customized Display

A customized display enables the company name, for example, to be displayed on system phones in the idle state.

Only the right portion (max. 18 characters) of the second display line, which displays "OpenScape" by default, can be changed. The text lines up with the left part of the date if the length of the text allows it:

```
16:30       FR 29.FEB 08         123456  Post Office Hotel>
```

21.1.5 Multilingual Text Output

The language for display messages can be selected system-wide or for a specific station only.

Available languages: Bulgarian, Catalan, Chinese, Czech, Danish, Dutch, English (UK), English (US), Estonian, Finnish, French, German, Greek, Hungarian, Italian, Latvian, Lithuanian, Macedonian, Norwegian, Polish, Portuguese, Romanian, Russian, Serbian, Serbo-Croatian, Slovak, Slovenian, Spanish, Swedish, German (Telekom), Turkish.

You set the language when you enter the country initialization code during system booting.

Related Topics

- Configuring Stations

21.1.6 Flexible Menus

Flexible menus allow you to customize the menu items shown on the display of system telephones.

As an administrator, you can select the menu items to be shown or hidden individually.

21.1.7 Music on Hold

The communication system can play back Music on Hold (MOH) to waiting subscribers during switching operations. Callers hear MOH while in the hold state, parked state or transfer state. This also applies to callers in the call distribution queue.

The system can import Music On Hold from the following sources:

- Music On Hold
- Xpressions Compact (IVM)
  See the documentation of Xpressions Compact. For configuration, see IVM in the documentation of Manager E.
- EXMR
  See Installing OpenScape Business X1, Service Documentation or Installing OpenScape Business X3/X5/X8, Service Documentation.
- MUSIC plugin module
  See Installing OpenScape Business X1, Service Documentation or Installing OpenScape Business X3/X5/X8, Service Documentation.
- MPPI USB EXM module (only for OpenScape Business X3/X5)
  See Installing OpenScape Business X3/X5/X8, Service Documentation.

Audio Files

The administrator can transfer audio files for the internal Music on Hold from the PC to the communication system for use as an alternative internal Music on Hold.

INFO: Before using announcements or music from other sources, make sure that you do not infringe on any copyrights.

IMPORTANT: If the station on hold is an IP workpoint client or an IP trunk, the internal MOH is used. External MOH is not intended for IP.

The audio files must be available as `Wave` files with the following properties:

- 16 bit PCM
- Mono or stereo
- Possible sample rates: 8 / 22.05 / 24 / 32 / 40 / 44.1 or 48 kHz.
- Maximum length for the audio file name: 30 characters

Recommended: **16 bit PCM - Mono - 8 kHz, length approx 2 min**

Music On Hold

Different Music on Hold can be configured for the day and night service.

The administrator can configure the following functions:

- Music on hold with ringing tone (ringback):
  The subscriber on hold first hears the MOH melody during the consultation. After the party on hold is transferred to the destination, the ring tone is heard instead of the music on hold.
- Music on hold without ringing tone (ringback):
  The held party will hear MOH until the called party answers the call.
- No music on hold:
  The held party hears nothing (silence). The caller hears the ringback tone in the event of an unscreened transfer for an external call.

21.1.8 Announcements

The communication system allows on-hold announcements to be played for callers before answering a call and also when using call distribution and DTMF direct inward dialing. You can also replace the MOH melody in certain situations by an announcement, for example, if a party is placed on hold or if a subscriber is busy or being routed.

The system can import announcements from the following sources:

- Internal announcements

- Announcement Player (only with UC Booster functionality)
  The announcement player is an internal software program that is available together with the UC Booster functionality (UC Booster Card or UC Booster Server). On calling a subscriber, the announcement player first plays the desired announcement and then sets up the connection to the subscriber. Manager E is required for the configuration.
- Analog Announcement Device
  See the section on Auxiliary Equipment - Analog Announcement Device in the OpenScape Business Administrator Documentation.
- MPPI USB EXM module (only for OpenScape Business X3/X5)
  See Installing OpenScape Business X3/X5/X8, Service Documentation.

The administrator can configure announcements for single or continuous playback.

An external announcement device must behave like a station, i.e., announce itself, play the announcement and switch the call (enter consultation hold, dial and hang up).

Audio Files

The administrator can transfer audio files with announcements from the PC to the communication system.

> ***INFO:*** Before using announcements or music from other sources, make sure that you do not infringe on any copyrights.

The audio files must be available as `Wave` files with the following properties:

- 16 bit PCM
- Mono or stereo
- Possible sample rates: 8 / 22.05 / 24 / 32 / 40 / 44.1 or 48 kHz.
- Maximum length for the audio file name: 30 characters

Recommended: **16 bit PCM - Mono - 8 kHz, length approx 2 min**

21.1.9 User to User Signaling

The communication system enables the transparent transmission of messages between stations (user to user signaling, UUS). UUS1 is supported for information exchange in control messages for connection setup and cleardown.

In the case of a point-to-multipoint connection, it is important to ensure that only one device transmits a message to an incoming call.

21.1.10 Voice Channel Signaling Security

The communication system offers a security mechanism that can be set up by the administrator to prevent undesirable tone injections into the voice channel. No

override is possible for a connection protected by this method. Every station configured as a Fax device automatically has this signaling security mechanism.

Recalls are deferred until the extension is free again.

Stations on-hold always have signaling security.

21.1.11 Time Parameters

The communication system offers the administrator options for setting various time parameters such as the "length of callback" or the "timer for automatic redial".

The time parameters are preset in the communication system and should normally not be changed.

21.1.12 Controlling Centrex Features

To control Centrex features, the dial tones for * and # must be transmitted to the ISDN and ITSP.

As an administrator, you can activate or deactivate this feature.

The input of a code must occur in the dialing state (e.g., after entering the trunk code). The input always begins with * or #, followed by a digit or digit combination, and ends with #.

21.2 Backup and Restore

The communication system's configuration data can be backed up and restored.

The configuration data is saved in a backup set. Every backup creates a separate backup set. Backups can be created manually immediately or scheduled for automatic execution at specific times.

INFO: It is strongly recommended to regularly back up the configuration data as backup sets.

When updating to a new minor release, it is necessary to create a new backup set.

Different backup media can be used to store the backup sets (such as USB media, network drives or the hard disk of the UC Booster Card, for example).

Depending on the system configuration, the use of the communication system and the type of backup medium involved, a backup or restore may take a long time - in some cases for systems with the UC Suite, up to three hours. This process should not be terminated manually or by a system reboot.

Aborting a data recovery may lead to an inconsistent system configuration in which an error-free operation of the system is not guaranteed. An aborted recovery should always be repeated until it is completed successfully. Otherwise, a complete reconfiguration of the system may be necessary. If the recovery fails repeatedly, please contact the Service Support and make sure in the meantime that your backup is not overwritten by new backups. To do this, the automatic data backup must be temporarily disabled.

Backup Sets for Diagnostic Purposes

"Smaller" backup sets containing diagnostic data for Service Support can be created for diagnostic purposes. In contrast to normal backup sets, significantly smaller data amounts are produced for this purpose and can thus be easily sent with an e-mail, for example. Diagnostics backup sets include, among other things, the configuration data of the communication system and the installed UC solution. Voicemails, fax messages and announcements are not included.

"Hard Disk" Backup Directory (Only for UC Booster Card)

If a UC Booster Card is installed, the configuration data of the communication system can be saved in a separate partition on the hard disk of the UC Booster Card in the backup directory. This backup directory is already provided as the standard archive "Hard Disk".

Backing up the Configuration Data of the UC Booster Server

If a UC Booster Server is being operated in addition to the communication system, then the configuration data of the UC Booster Server must also be backed up when backing up the configuration data of the system. Backing up the data of the UC Booster Server is basically identical to backing up the data of the communication system; the only difference is that the administrator does not specify the IP address of the communication system when calling the WBM, but the IP address of the Linux server.

21.2.1 Backup Sets

The configuration data of the communication system is saved in a backup set.

In addition to backup set, a text file associated with the backup set must also be saved. It contains information about the date and time of the backup and under which software version the backup was performed. The text file is necessary for the recovery of the backup set.

If the number of backup sets saved exceeds the set value, the oldest backup sets are deleted.

Backup Set Data

The following data for a backup set is presented:

- **Archive name**: Name of the backup set
- **Size**: Size of the backup set in bytes
- **Date**: Date on which the backup set was created.

- **Comment**: Comment that was specified when creating the backup set (optional).

Backup sets that have been grayed out cannot be restored.

21.2.2 Backup Media

The backup sets are stored on the selected backup media.

The following backup media can be used for the backup:

- Inserted USB storage device
- Network drive
- Client PC using HTTP (only possible with immediate backup)
- Hard disk of the UC Booster Card
- FTP/FTPS servers

For every backup medium, the maximum number of backup sets to be stored in the directory can be specified.

USB Storage Device

To use a USB storage device (e.g., a USB hard disk or flash drive) for backup, the USB device must be plugged into the USB server port of the communication system. In addition, the USB device must be formatted with FAT-32. USB media formatted with NTFS are read-only. Note that if multiple partitions exist, only the first partition can be used for the backup!

A bootable USB device is not supported.

With OpenScape Business S and OpenScape UC Booster Server, the USB device is plugged into the USB port of the Linux server.

FTP/FTPS servers and network drives

FTP/FTPS servers and network drives can be added, edited or deleted as new media. FTP/FTPS servers and network drives may also be specified more than once if different directories on them are used. TLS 1.2 is supported as the encrypted file transfer protocol (FTPS).

In order to back up the configuration data, the user must have write permission for the root directory of an FTP/FTPS server. To back up to a network drive, users only need write permission for the desired directory.

If the transmission speed to the FTPS server is too low, there may be a malfunction in the backup. If this occurs, the backup must be restarted.

For FTPS, certificates up to 2048 bits are supported. These certificates are required for authentication at the FTPS server.

21.2.3 Immediate Backup

The configuration data can be immediately backed up manually.

A variety of backup media can be used for data backup; By default, the backup medium is set up as **HTTPS**. You can thus store the backup set in all storage locations that can be accessed on the client PC with which you logged into the WBM. The chosen storage location must also be accessible when restoring the backup set. If a USB device is connected to the communication system, **USB Device** is displayed as an additional backup medium. If the UC Booster Card (incl. hard disk) is connected, a further backup medium called **Local hard disk** is displayed.

The name of the backup set is assigned automatically during the backup. It includes, among other things, the date on which the backup was performed. In addition, this data is also included in a text file that must also be stored. If desired, a comment can be optionally added to identify a backup set more easily prior to a subsequent restore.

21.2.4 Scheduled Backup

You can use a schedule to automatically back up configuration data. The time, frequency and location of the automatic backup is configurable.

The scheduled data backup can be scheduled for a fixed time daily or weekly and then started automatically. This "backup job" can be created for an internal or external backup medium. It is not possible to configure multiple backup jobs.

21.2.5 Restore

The restoration of configuration data must be performed manually using the backup sets.

All the supported backup media can be used to restore data;

21.3 Updates

Updates provide the latest software available for the system components within a version.

To install updates, you will need the 3-year software support.

The version of the installed software and the expiration date of the software support are displayed on the home page of the WBM. If more recent software updates are available, this is indicated there.

> ***INFO:*** When updating to a new minor release, it is necessary to create a new backup set.

The software update is performed using the WBM. On a hardware model, the software can also be optionally updated directly from a USB device without WBM

access. In a communication system with the UC Booster Server, the hardware model and the UC Booster Server are updated separately.

Using the WBM, the software can be updated via the Internet web server, a local web server or directly via image files.

The following system components are updated:

- Software of the communication system
- Software of the UC clients
- Software for system telephones (updates can also be performed individually)
- Documentation

The software for the UC clients is updated together with the software of the communication system. If a more recent software version is available, users of the UC clients are notified via an Auto-Update message that an update is available and can be installed.

The software update of the IP system telephones occurs automatically with the update of the communication system, but can also be done manually. For UP0 system telephones, the update is performed manually using Manager E.

The software update can be optionally started immediately or by defining the times for the software transfer and software activation independently. The update should be performed outside the business hours of the customer, since the communication system and/or the system telephones are restarted, existing calls are dropped, and the use of the UC clients is interrupted temporarily.

After the software has been transferred to the communication system, it is activated at the selected time. The latest phone image is then automatically loaded onto the IP system telephones. After a restart of the communication system and the IP system telephones, the newly loaded software will be active.

Image Files

To update system components, compressed image files containing the software of the system components are required. These image files can be downloaded from the software server (Internet web server) and stored independently on a local web server or in the internal network or on a USB stick, for example. There is a separate image file for the communication system without a UC Booster Card and a separate image file for a system with a UC Booster Card. Both image files also include the software for the system telephones. In addition, there is also a separate image file for each type of system telephone type in case the system telephones need to be updated separately.

The following types of image files are available:

- **tgz**: for the software of the communication system. The tgz file contains a tar file. The tar file must be unpacked from the tgz file with a decompressor such as WinZip or 7-zip, for example. The tgz file is offered for download because a check can be performed to determine whether or not the file is corrupted when downloading the software from the server.
- **tar**: for the software of the communication system. It contains the packed files for each system component.
- **app**: for the software of the system telephone.

Local Web Server

When performing a software update via a web server, the software server (Internet web server) is accessed by default.

However, it is also possible to use a local web server for updates. To do this, the image file must be stored on the local web server, and the path to the local web server must be configured in the WBM.

Speed Upgrade

A speed upgrade as with the HiPath 3000 is not possible.

IMPORTANT: Pulling out the SDHC card during operation will result in the loss of data!

21.3.1 Using a Local Web Server

The software can be updated via a local web server.

The current image files must be stored on the local web server. In addition, the access data for the local web server must be entered in the WBM. This change can only be performed by an administrator with the **Expert** profile. After the access data of the local web server has been entered, this will be set as the default for all future updates of the communication system. In other words, the local web server will now be used instead of the Internet web server.

21.3.2 Updating the Communication System

Updating the communication system includes updates to not only the software of the communication system itself, but also the software images of the system phones, which are stored on the communication system. A full update of all system components can thus be quickly and easily performed.

Before each software update, the configuration data of the communication system must be backed up (*Backup and Restore*).

Updating via a Web Server

When performing a software update via a web server, the software server (Internet web server) is accessed by default.

If a local web server is being used, the image file must be stored on the local web server.

For a communication system without a UC Booster Card, it does not matter if an image file for a system with or without a UC Booster Card is used. Only the necessary components are installed.

The system checks for the presence of new software updates after automatically setting up a connection to the web server. For systems without UC Booster,

individual software update packages can be unselected to reduce the download time. Only those packages that have changed with respect to the installed software version are transferred. The starting time for the software transfer and for the software activation can be selected. If the time of the software activation is reached before the software update has been completely transferred to the system, the activation is not executed automatically. A new time of activation must then be defined manually.

Updating via USB Storage Device

The image file is stored on a USB device. The USB storage device must be inserted in the USB server port of the communication system. This type of update can only be performed by an administrator with the **Expert** profile and is not possible for OpenScape Business S and OpenScape Business UC Booster Server.

Updating via a File Upload

The image file is in a directory in the internal network or on the admin PC.

Update via a USB Device without WBM Access

The communication system can be updated directly without WBM access via a USB device. This requires the USB device to be plugged into the USB server port of the system and the image file to be located at the top level of the USB device. If a reset of the communication system is performed with the USB device inserted, the software update is started automatically. This type of update is not possible with OpenScape Business S. In a system with the OpenScape Business UC Booster Server, the server must be updated additionally.

Updating the UC Booster Server

If a UC Booster Server is being operated in addition to the communication system, then the communication software of the UC Booster Server must also be updated when updating the system software. In other words, the software of the communication system and the UC Booster Server should always be at the same level. The software update of the UC Booster Server is basically identical to the software update for the communication system; the only difference is that the administrator does not specify the IP address of the communication system when calling the WBM, but the IP address of the Linux server.

21.3.3 Updating System Telephones

The software of the system telephones is updated via an image file. For each type of system telephone, there is a separate image file that contains the phone software of this type. These image files are included in the software of the communication system and are automatically loaded into the communication system during updates.

The IP system telephones are thus automatically supplied with the current software. Whenever an IP system telephone is reconfigured in the WBM (from a **System Client** to a **SIP Client**, or vice versa), the appropriate software stored in

the communication system is automatically loaded via the DLI into the IP system telephone. For IP system telephones that were already in operation at the system or at some other system, the factory settings must be first restored (factory reset) before the automatic software update can be performed.

Non-standard phone software can be transferred manually by the administrator to all IP system telephones of a specific type by using the WBM. The update of the software for UP0 system telephones is performed with Manager E.

If some specific phone software (image file) is flagged as the default in the WBM, the corresponding image will be automatically transferred to every IP system telephone associated with this type whenever that phone logs into the system for the first time.

When updating the software manually, it is important to ensure that the software of the system telephones is compatible with the software version of the communication system (see the Release Notes).

21.3.4 Software Status

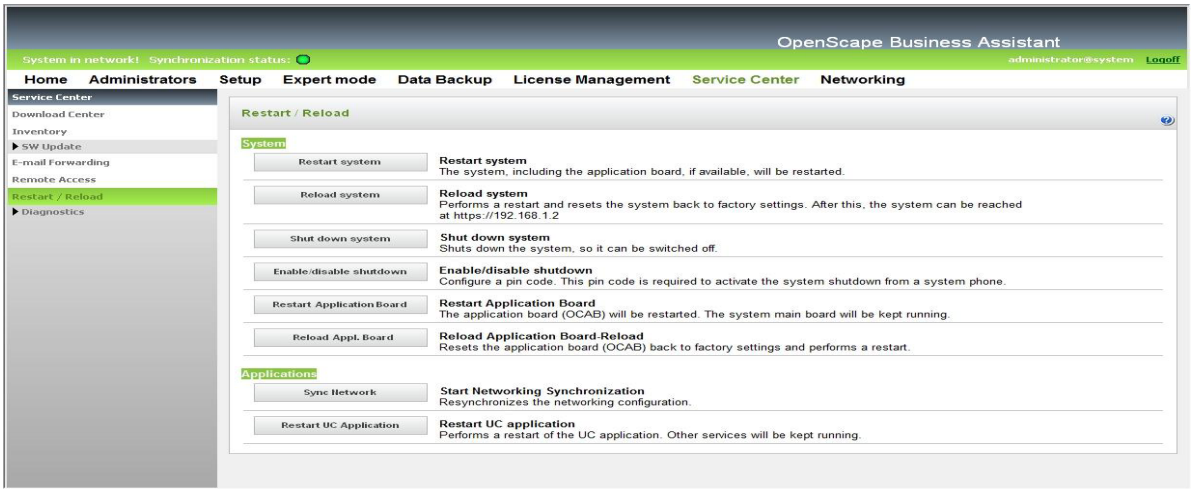
The software status provides information about the software version and the software update.

The following statuses can be displayed:

- Current version of the software
- Newer version available for an update
- Time at which the software update is to be performed
- New software being loaded into the system
- Successful or failure of the loading process

21.4 Restart, Reload, Shutdown

You can use the associated features to initiate a restart or reload of the OpenScape Business communication systems or the UC Booster Card and for a controlled shutdown of OpenScape Business X. In addition, a restart (reboot) of the UC application (UC Smart or UC Suite) is triggered. To enable the controlled shutdown of OpenScape Business X via a system telephone, a PIN can be defined.



Restarting and Reloading the UC Booster Server

If a UC Booster Server is being operated in addition to the communication system, the communication software of the UC Booster Server can also be restarted or reloaded. The restart/reload of the UC Booster Server is basically identical to the restart/reload of the communication system; the only difference is that the administrator does not specify the IP address of the communication system when calling the WBM, but the IP address of the Linux server.

21.4.1 Restarting OpenScape Business

The **Restart system** function can be used to initiate a controlled restart of OpenScape Business.

The following differences must be observed:

- OpenScape Business S and OpenScape Business X
  A controlled restart of the communication system occurs. The communication system will be operational again after the startup.
  The startup time depends on system configuration and the OpenScape Business networking scenario.
  If OpenScape Business X3/X5/X8 is equipped with a UC Booster Card (Application Board OCAB), a controlled restart (reboot) of the UC Application (UC Smart or UC Suite) also occurs.
- OpenScape Business UC Booster Server (Application Server)
  A controlled restart of the OpenScape Business portion and the UC Application (UC Suite) occurs. The UC Application will be operational again after the startup.

During a restart, all active applications such as myPortal for Desktop and myPortal for Outlook, for example, are disconnected. After the startup, all connections are automatically set up again.

21.4.2 Reloading OpenScape Business

The **Reload system** function can be used to initiate a reload of OpenScape Business.

The following differences must be observed:

- OpenScape Business S and OpenScape Business X
  The communication system is reloaded. After the subsequent startup, the communication system will be in its default state.
  - All country and customer-specific settings were deleted (system country code = Germany).
  - The communication system has the default IP address 192.168.1.2 and the internal IP range 192.168.3.xxx.
  - The licensing is retained.

  The startup time depends on system configuration.
- OpenScape Business UC Booster Server
  The OpenScape Business portion is reloaded. After the subsequent startup, the OpenScape Business portion will be in its default state.
  - All custom (i.e., customer-specific) settings of the OpenScape Business portion (e.g., the User Directory) were deleted.
  - The licensing is retained.

  The operating system will not be reset.

21.4.3 Shutting Down OpenScape Business X

The **Shut down system** function can be used to shut down the OpenScape Business X communication systems gracefully, i.e., to perform a controlled shutdown.

21.4.4 PIN for the controlled shutdown of OpenScape Business X

The activation of the shutdown via a system telephone is PIN-protected.

The PIN configured in the communication system must be entered for the activation via a system telephone. The configuration of this PIN is performed by an administrator with the **Advanced** profile.

21.4.5 Restarting (Rebooting) the UC Booster Card (Application Board OCAB)

As an administrator, you can use the **Restart Application Board** function to initiate a controlled restart of the Application Board OCAB, including the UC application (UC Smart or UC Suite).

During a restart, all active applications such as myPortal for Desktop and myPortal for Outlook, for example, are disconnected. After the startup, all connections are automatically set up again.

In addition, the integrated XMPP server, the CSTA interface, the Presence Manager, Announcement Player, Media Extension Bridge, Open Directory Service and the Gate View server are likewise restarted.

21.4.6 Reloading the UC Booster Card (Application Board OCAB)

The **Reload UC Booster Card** function can be used to initiate a reload of the Application Board OCAB, including the UC application (UC Smart or UC Suite).

The Reload UC Booster Card function is used to reset the card to the factory settings and then remove it from the system. This may be necessary if the card is no longer to be used in this system due to a switch to the UC Booster Server or if it is to be installed in another OpenScape Business system.

All customer-specific data and all diagnostic data are deleted from the UC Booster Card, and the system shuts down. Then, the system must be unplugged from the power supply, and the UC Booster Card must be removed.

After the UC Booster Card has been removed and the system is rebooted, a new backup set must be created, since the configuration data has changed and the old backup set is no longer compatible. If the hard disk of the UC Booster Card was previously used as a backup medium, then another backup medium such as a network drive, a USB device or an FTP/FTPS server must be now selected (see also the *Backup and Restore*).

21.4.7 Restarting the UC Application

The **Restart UC Application** function can be used by an administrator to initiate a controlled restart of the UC Application (UC Smart or UC Suite).

During a restart of the UC Application, all active applications such as myPortal for Desktop, myPortal Smart and myAttendant, for example, are disconnected. After the startup, all connections are automatically set up again.

21.5 Inventory Management

The term Inventory Management refers to the process for determining the current status of the OpenScape Business X and OpenScape Business S communication systems and the hardware configuration of the OpenScape Business X communication system.

21.5.1 System Status

The current status of the OpenScape Business X and OpenScape Business S communication systems can be determined by an administrator via the WBM. The following information can be retrieved: status of the stations, connection setup, ITSPs, VPNs and the list of configured IP addresses.

Station status

The station status enables the following information on the configured stations to be retrieved:

- Station number
- Name
- Device type
- IP address (for system telephones, an additional link through which the WBM of the phone can be opened is displayed.)
- MAC Address
- Current SW version
- HW version
- Status (On/Off)

Dial-up Network Status

The dial-up network status enables information on existing connections to PSTN partners (i.e., Public Switched Telephone Network partners such as public or home telecommunications networks, for example) of the OpenScape Business X communication system to be retrieved.

ITSP Status

The ITSP status enables information on the current status of preconfigured and any possibly added Internet Telephony Service Providers (ITSPs) to be retrieved. In addition, it shows which stations were set up for which ITSP.

The status of each active ITSP is indicated by the color of the associated rectangle (green = OK, orange = at least one of the stations was not properly configured).

VPN Status

The VPN status enables information on the configured VPN tunnels of the OpenScape Business X communication system to be retrieved:

Overview of IP Addresses

The IP addresses configured in the OpenScape Business X communication system are displayed.

In addition, the overview also shows with which wizards and with which menus in Expert mode the IP addresses can be configured.

Also, a status overview of the Booster Card and the Mainboard Ethernet Interfases is displayed.

21.5.2 Inventory

The Inventory enables an administrator to retrieve information on the hardware and software of OpenScape Business X and the software of OpenScape Business S.

OpenScape Business X

The following details can be retrieved:

- Communication system
  Among other things, the following information is displayed:
  - Graphical representation of the communication system and the boards
  - Part number of the mainboard, MAC address, IP address, host name and software version
  - Details on memory amounts, including the available and used space on the SDHC card.
  - Status of all applications
- Boards
  The displayed information includes the following: slot, type, part number and status of all installed boards.
- UC Booster Card (Application Board OCAB), if available
  Among other things, the following information is displayed:
  - MAC address, IP address, host name and software version
  - Details on memory amounts, including the available and used hard disk space.
  - Status of all applications
  - Overview of all Booster Card interfaces

  The link **UC Booster Card accessible** in the home page of WBM directs the user to the **Service Center > Inventory >Booster Card** for a detailed view. The link will exist, even if there is a problem with the Booster Card and the text shows **UC Booster Card not accessible**.
  The following error messages are displayed in the home page of WBM, depending on the error:

a) Inter-Integrated Circuit link with Booster Card not possible
b) Internet Protocol v6 connectivity to Booster Card not possible
c) Internet Protocol v4 connectivity to Booster Card not possible
d) Secure Socket Shell connectivity to Booster Card not possible
e) Network File System connectivity to Booster Card not possible
f) One or more Ethernet Interfaces are in Half Duplex mode, Full Duplex is highly recommended

OpenScape Business S

The following details can be retrieved:

- Software
  Among other things, the following information is displayed: MAC address, IP address, host name and software version.
- Hard Disk Information
  Details on memory amounts, including the available and used memory.
- Applications
  All applications and their respective statuses are displayed.

21.6 Automatic Actions

This function can be used to define actions to be executed once or at regular intervals. These actions are then executed automatically by the communication system at the set time.

21.6.1 Garbage Collection Automatic Action

The automatic action Garbage Collection enables an automatic garbage collection to be performed on the communication system. After each garbage collection has been completed, the communication system performs a restart (reboot).

The color of the list item displayed in the menu tree indicates the status of the action (green = action activated, red = action not activated).

Start/Stop Action can be used to enable or start an inactive action (red list item) and to disable or stop an active action (green bullet point).

The automatic action Garbage Collection is disabled by default.

21.6.2 DLS Notification Automatic Action

The automatic action DLS Notification can be used to initiate an automatic login at an external DLS server on starting up the communication system.

The color of the list item displayed in the menu tree indicates the status of the action (green = action activated, red = action not activated).

Start/Stop Action can be used to enable or start an inactive action (red list item) and to disable or stop an active action (green bullet point).

The automatic action DLS Notification is disabled by default.

21.6.3 Warning Mechanism for SDHC card lifetime

The automatic action Warning Mechanism for SDHC lifetime is a way to get information about the SDHC cards health state with a filesystem check during startup. A WBM wizard starts and leads the technician through the process of setting a time when the system should make a restart and execute the check. All information is logged in the Customer Trace.

WBM Home Screen recognizes two states:

- If the information from system is available a text will be presented in Home Screen informing about the general status of the card, **Card Health Status** (green, yellow or red).
  Green health status means that the manufacturing date is less than 3 years ago and the filesystem was created less than 2 years ago.
  Yellow health status means that the manufacturing date is between 3 and 6 years ago and the filesystem was created less than 3 years ago.
  Red health status means that the manufacturing date is more than 3 years ago and the filesystem was created maore than 3 years ago or that any filesystem error exist.
- If the information is not available then user will be prompted, **Card Health Status** unknown.

The text "**Card Health Status** " will also provide a link that will leads to the "Actions Page"

The automatic action Warning Mechanism for SDHC is disabled by default.

21.7 Power Management

Power management automatically switches the communication system to low power mode, depending on the system load. This reduces the energy consumption of the system and thus also contributes to environmental protection. The time period in which the system switches to low power mode can be set (e.g., at night).

Power management can be enabled only if is the LAN interfaces of the system are in the Ethernet Link Mode **Auto**. In the low power mode, the LAN interfaces of the system automatically switch to the 100 Mbit/s full-duplex mode. The LAN interfaces of the connected infrastructure should also be in the autosense mode.

Operating Modes

- Active Mode
  In active mode, the functions of the communication system are frequently used, and significant data transfers occur between the system and the connected infrastructure.
- Idle Mode
  In idle mode, the functions of the communication system are rarely used, and no significant data transfers occur between the system and the connected infrastructure. When a function is initiated, the system switches from idle mode to active mode.
- Low Power Mode
  Low-power mode has reduced energy requirements compared to the idle mode. The system operates in the 100 Mbit/s full-duplex mode.

It is also possible to operate the system permanently in the Ethernet Link Mode 100 Mbit/s full duplex or 100Mbit/s half duplex.

21.8 Monitoring and Maintenance of OpenScape Business

OpenScape Business offers different functions for monitoring the current status of the system and for finding and resolving errors.

21.8.1 Checking the Network Connection of OpenScape Business X

The network connection between an OpenScape Business X communication system and the target address can be checked by using an ICMP (Internet Control Message Protocol) request.

Echo request packets can be sent via both the **Ping** and **Traceroute** functions. The corresponding echo reply messages are displayed together with the round-trip times.

The **Traceroute** function sends echo request packets with various incremental TTL (Time-To-Live) values.

21.8.2 SNMP (Simple Network Management Protocol)

The Simple Network Management Protocol (SNMP) is a network protocol which can be used to monitor and operate networking components (such as routers, servers, switches, printers, PCs) from a central station (management console). The protocol controls communication between the monitored components and the monitoring station.

SNMP describes the structure of data packets that can be sent and the communication procedure. SNMP was designed so that all network-capable devices can be included in monitoring. SNMP-based network management tasks include

- monitoring networking components,
- performing remote control and remote configuration of networking components,
- error detection and notification.

Devices known as "agents" are used for monitoring. These are utilities that run directly on monitored components. These utilities are able to record the status of components, make settings, and trigger actions. SNMP allows the central management console to communicate with the agents over a network.

INFO: OpenScape Business supports SNMPv2c, but also responds to SNMPv1 snmpget requests.

Management Information Databases (MIB)

The volume of data that can be administered via SNMP is defined in MIBs (Management Information Base). MIBs are data models that describe the networking components to be administered in an established manner. The MIB of the OpenScape Business X communication systems can be downloaded via the WBM (Service Center).

The communication systems have a separate SNMP agent that allows access to various system data that is stored in its MIB or Management Information Base. The MIB provides basic system information, status information, event-related data, and information on installed hardware (slots) and configured connections (ports).

SNMP supports the central monitoring and administration of networking components, including the communication systems themselves. It is possible to

- address the communication system over the TCP/IP protocol.
- access data over external management applications.
- perform remote maintenance activities.
- visualize the operating status of the communication system.
- transmit service-specific errors (Traps).

Communities

Access to the SNMP data (MIBs) is governed by communities. A distinction is made here between read, write, and Trap communities. Each community has a specific IP address.

To enable read access to SNMP data (MIBs) on a PC, for example, the IP address of this PC must be entered in the list of read communities. To enable read and write access, the IP address must be entered in the list of write communities.

Trap Communities are used to manage the recipients of error messages (traps).

Traps

When problems occur in a communication system, traps are generated to indicate errors and failures. The following types of traps are available:

- System traps = System errors that require immediate action for recovery.

- Performance Traps = Information on performance problems that do not require corrective action.

Traps are classified by their effects and can be retrieved by an administrator with the **Expert** profile using the WBM. A list of all traps received is displayed with the following information:

Table column	Meaning
VarBind1 (Severity)	Trap effect classes The following entries are possible: Critical: Error Message. This error causes problems. Major: error message. This error could cause problems. Minor: error message. The error has no problematic consequences. Warning: report of a possibly problematic procedure or status, but not an error message. Deleted Information: plain status messages, no error messages. Intermediate status Other traps
VarBind2 (Name)	Trap name
Generic Name	General Description such as Enterprise Specific, for example
Specific Name	Trap type (1 = software, 2 = hardware)
Enterprise	–
Time	Time of error
Index	List number

Trap display is updated every 30 seconds. Traps are sorted in the sequence of occurrence.

Trap details can be displayed by clicking a trap name.

SNMP Code	Event Log Entry	Meaning	Required Measures	Note
Error Class 01 - General Messages				
	System Restart	Hard restart (reset) of entire system with current CDB.	None	
FP_EVT_ADM_000	out of service of signed port on slot	out of service of signed port on slot		

SNMP Code	Event Log Entry	Meaning	Required Measures	Note
FP_EVT_ADM_001	in service of signed port on slot	in service of signed port on slot		
FP_EVT_ADM_002	reload of signed slot	reload of signed slot		
FP_EVT_ADM_003	system restart	system restart		
FP_EVT_ADM_007	SNMP out of service signed port on slot	SNMP out of service signed port on slot		
FP_EVT_ADM_008	SNMP in service signed port on slot	SNMP in service signed port on slot		
FP_EVT_ADM_009	SNMP reload signed slot	SNMP reload signed slot		
FP_EVT_ADM_010	SNMP System Restart	Hard restart of entire system via SNMP.	None	
FP_EVT_ADM_014	SNMP local DB changes	?On site? changes to the database.	None	
FP_EVT_ADM_015	SNMP remote DB changes	?Remote? changes to the database.	None	
FP_EVT_ADM_016	SNMP APSXF result	APS transfer acknowledgement message via SNMP.	None	
FP_EVT_ADM_017	SNMP authentication fail	Unauthorized access attempt.	Check firewall settings in OpenScape Business/ Manager E (Network ? Firewall).	
FP_EVT_ADM_018	SNMP 80 % high watermark of log-file	Changes logged internally in the system: 80 % of write capacity used.	Read out data using OpenScape Business/ Manager E (Transfer ? Security ? Protocol).	

SNMP Code	Event Log Entry	Meaning	Required Measures	Note
FP_EVT_ADM_019	Sensor Alarm	Temperature in OpenScape Business housing is too high.	Check the fan and air supply in the 19? housing. Note the ambient temperature.	
FP_EVT_ADM_020	CDR buffer limit reached	Overflow in the CDR buffer (CDR information).	Check that the interfaces (V.24, LAN), ports and the connection are functioning or read out call data.	
FP_EVT_ADM_021	Authentication Failure	Unauthorized access attempt.	Check firewall settings in OpenScape Business/ Manager E (Network ? Firewall).	
FP_EVT_ADM_022	Flash deleted	Flash area deleted.	None	APS transfer possible again.
FP_EVT_ADM_023	Process stopped	Process stopped.	Perform hard restart (reset).	
FP_EVT_ADM_024	unauthorized application	Attempted access via an unauthorized application.	Check firewall settings in OpenScape Business/ Manager E (Network ? Firewall).	
FP_EVT_ADM_025	manual switch-back from HiPath Manager			
Error Class 02 - License Management Messages				
FP_EVT_LIC_002	START Grace Period	HiPath License Management: Start of grace period.	None	The remaining license validity period is shown on the display.

SNMP Code	Event Log Entry	Meaning	Required Measures	Note
FP_EVT_LIC_003	START Reg. Linc File	HiPath License Management: Start of regular licensing.	None	
Error Class 09 - Hardware Module Messages				
FP_EVT_HW_000	microprocessor fault on, common	Microprocessor error.	Check power at the power supply unit. If this error persists, replace the central control board.	
FP_EVT_HW_001	microprocessor fault off, common	The microprocessor error has been corrected.	None	
FP_EVT_HW_002	loadware memory fault on, common	Error in loadware memory.	Replace the board if necessary.	
FP_EVT_HW_003	loadware memory fault off, common	Error in loadware memory has been corrected.	None	
FP_EVT_HW_004	red alarm on-loss of multiframe alignm.	red alarm on-loss of multiframe alignm.		
FP_EVT_HW_011	SNTP-Client at PCS can't be activated	SNTP-Client at PCS can't be activated		
FP_EVT_HW_029	line interruption (error on)	Line interruption	Check the line and terminal.	
FP_EVT_HW_030	short circuit (error on)	Short circuit on the board specified.	Check the line, terminal, and port.	
FP_EVT_HW_031	under voltage (error on)	Under voltage.	Check the power and line at the terminal?s power supply unit.	
FP_EVT_HW_032	thermal overload (error on)	The specified board is overheated.	Check the fan and air supply in the 19'' housing. Note the ambient temperature.	
FP_EVT_HW_034	loss of frame on (STMD)	loss of frame on (STMD)		

SNMP Code	Event Log Entry	Meaning	Required Measures	Note
FP_EVT_HW_035	loss of frame off (STMD)	loss of frame off (STMD)		
FP_EVT_HW_036	slip detected on (STMD)	A bit slip has occurred on an ISDN line.	Check the S0 line. If necessary, reload the board or perform a hard restart. If the error persists, set up an ISDN trace.	The problem may be caused by asynchronous internal and external clock rates. Data loss possible/ connection may be terminated.
FP_EVT_HW_037	slip detected off (STMD)	The bit slip on the ISDN line has been corrected.	None	
FP_EVT_HW_038	alarm indication signal error on (TMS2M)	Alarm display: An S2M error has occurred. Physical line/ board problem (too many CRC/ SLIP errors).	Check the S2M line and board. Replace the board if necessary. If the error persists, set up an ISDN trace.	
FP_EVT_HW_039	alarm indication signal error off(TMS2M)	Alarm display: The S2M error has been corrected.	None	
FP_EVT_HW_040	degraded minute error on (TMS2M)	degraded minute error on (TMS2M)		
FP_EVT_HW_041	degraded minute error off (TMS2M)	degraded minute error off (TMS2M)		

SNMP Code	Event Log Entry	Meaning	Required Measures	Note
FP_EVT_HW_042	no signal error on (TMS2M/ STMD)	Alarm display: An S2M error has occurred. No physical connection available.	Check the S2M line and board. If necessary, reload the board or perform a hard restart. If the error persists, set up an ISDN trace.	
FP_EVT_HW_043	no signal error off (TMS2M/ STMD)	Alarm display: The S2M error has been corrected.	None	
FP_EVT_HW_044	receive remote alarm error on (TMS2M)	Alarm display: An S2M error has occurred. Physical problem with the communication partner (too many CRC/SLIP errors).	Check the board and partner system or arrange for a technician to do so.	
FP_EVT_HW_045	receive remote alarm error off (TMS2M)	Alarm display: The S2M error has been corrected.	None	
FP_EVT_HW_046	severely errored seconds error on(TMS2M)	severely errored seconds error on(TMS2M)		
FP_EVT_HW_047	severely errored seconds error of(TMS2M)	severely errored seconds error of(TMS2M)		

SNMP Code	Event Log Entry	Meaning	Required Measures	Note
FP_EVT_HW_048	bitslip error on (TMS2M)	A bit slip has occurred on an ISDN line.	Check the S2M line. If necessary, reload the board or perform a hard restart. If the error persists, set up an ISDN trace.	The problem may be caused by asynchronous internal and external clock rates. Data loss possible/ connection may be terminated.
FP_EVT_HW_049	bitslip error off (TMS2M)	The bit slip on the ISDN line has been corrected.	None	
FP_EVT_HW_050	loss of synchronization error on (TMS2M)	A synchronization error has occurred.	Check the S2M line. If necessary, reload the board or perform a hard restart. If the error persists, set up an ISDN trace.	The problem may be caused by asynchronous internal and external clock rates. Data loss possible/ connection may be terminated.
FP_EVT_HW_051	loss of synchronization error off (TMS2M)	The synchronization error has been corrected.	None	
FP_EVT_HW_052	clock can be used as ref. (TMS2M/STMD)	clock can be used as ref. (TMS2M/STMD)		
FP_EVT_HW_053	clock can not be used as reference	clock can not be used as reference		

SNMP Code	Event Log Entry	Meaning	Required Measures	Note
FP_EVT_HFP_EVT_HW_051W_058	Self test error on (SLMO)	Error while self-testing the specified SLMO board.	If necessary, replace the board or change the slot.	
FP_EVT_HW_059	Self test error off (SLMO)	Error while self-testing the specified SLMO board has been corrected.	None	
FP_EVT_HW_060	Access power feed error on (SLMO)	Access power feed error on (SLMO)		
FP_EVT_HW_061	Overcurrent on power controller on (SLMO)	Overcurrent on the specified SLMO board.	Check the power and line on the terminal and power supply unit. Replace hardware if necessary.	
FP_EVT_HW_062	Overcurrent on power controller off (SLMO	Overcurrent on the specified SLMO board has been corrected.	None	
FP_EVT_HW_063	ELIC error on (SLMO/SLMC)	ELIC error on (SLMO/SLMC)		
FP_EVT_HW_064	ELIC error off (SLMO/SLMC)	ELIC error off (SLMO/SLMC)		
FP_EVT_HW_065	Out of buffers for card error on	Insufficient pool capacity on the cified SLMO board.	Check lines and terminals. Set up a default trace. High traffic load: -> Distribute load to several boards. Board is faulty: -> Replace board.	
FP_EVT_HW_066	Out of buffers for card error off	Insufficient pool capacity on the specified SLMO board has been corrected.	None	
FP_EVT_HW_067	OCTAT error on (SLMC)	OCTAT error on (SLMC)		

SNMP Code	Event Log Entry	Meaning	Required Measures	Note
FP_EVT_HW_068	OCTAT error off SLMC)	OCTAT error off SLMC)		
FP_EVT_HW_096	unknown error from LW	unknown error from LW		
Error Class 11 - General Messages				
FP_EVT_DEV_041	L1 asynchron on	L1 asynchron on		
FP_EVT_DEV_042	L1 asynchron off	L1 asynchron off		
FP_EVT_DEV_043	Overload error on	Overload error on		
FP_EVT_DEV_044	Overload error off	Overload error off		
FP_EVT_DEV_045	Alive check error on	Alive check error on		
FP_EVT_DEV_046	optiPoint info	optiPoint info		
FP_EVT_DEV_048	Layer 2 error detected	Layer 2 error detected		
FP_EVT_DEV_049	Layer 3 error detected	Layer 3 error detected		
FP_EVT_DEV_052	Other errors	Other errors		
FP_EVT_DEV_057	NO TEI available	NO TEI available		
FP_EVT_DEV_058	Too many L1 errors	Too many layer 1 errors.	Check the lines, terminal, and port. A short circuit may have occurred.	
FP_EVT_DEV_059	Access not configured	Access not configured		
Error Class 16 - Operating System Messages				
FP_EVT_GEN_001	Error in get pool element	Error in get pool element	Set up a trace using information from BLS (Back Level Support). Create a stack dump. Save a snapshot.	

SNMP Code	Event Log Entry	Meaning	Required Measures	Note
FP_EVT_GEN_002	Error in release pool	Error in release pool	Set up a trace using information from BLS (Back Level Support). Create a stack dump. Save a snapshot.	
FP_EVT_GEN_004	Error in OSF-Send	Error in OSF-Send	Set up a trace using information from BLS (Back Level Support). Create a stack dump. Save a snapshot.	
FP_EVT_GEN_005	Error in OSF-Timer	Error in OSF-Timer	Set up a trace using information from BLS (Back Level Support). Create a stack dump. Save a snapshot.	
FP_EVT_GEN_006	Error in OSF-Receive	Error in OSF-Receive	Set up a trace using information from BLS (Back Level Support). Create a stack dump. Save a snapshot.	
FP_EVT_GEN_007	General OSF error	General OSF error	Set up a trace using information from BLS (Back Level Support). Create a stack dump. Save a snapshot.	

SNMP Code	Event Log Entry	Meaning	Required Measures	Note
FP_EVT_GEN_009	Watch dog	Watch dog	Set up a trace using information from BLS (Back Level Support). Create a stack dump. Save a snapshot.	
FP_EVT_GEN_010	RESTARTED: manual Reset	RESTARTED: manual Reset	Set up a trace using information from BLS (Back Level Support). Create a stack dump. Save a snapshot.	
FP_EVT_GEN_011	RESTARTED: manual Reload	RESTARTED due to manual Reload	Set up a trace using information from BLS (Back Level Support). Create a stack dump. Save a snapshot.	
FP_EVT_GEN_012	RESTARTED: Power down	RESTARTED due to Power down	Set up a trace using information from BLS (Back Level Support). Create a stack dump. Save a snapshot.	
FP_EVT_GEN_013	KDS backup not performed	KDS backup not performed	Set up a trace using information from BLS (Back Level Support). Create a stack dump. Save a snapshot.	

SNMP Code	Event Log Entry	Meaning	Required Measures	Note
FP_EVT_GEN_014	RESTARTED: unknown rest. HW ind. missmatch	RESTARTED due to unknown rest. HW ind. missmatch	Set up a trace using information from BLS (Back Level Support). Create a stack dump. Save a snapshot.	
FP_EVT_GEN_015	general error logging	general error logging	Set up a trace using information from BLS (Back Level Support). Create a stack dump. Save a snapshot.	
FP_EVT_GEN_017	CTXT take over failed	CTXT take over failed	Set up a trace using information from BLS (Back Level Support). Create a stack dump. Save a snapshot.	
FP_EVT_GEN_020	CSTA: length out of range	CSTA: length out of range	Set up a trace using information from BLS (Back Level Support). Create a stack dump. Save a snapshot.	
FP_EVT_GEN_021	CSTA: Alloc() error	CSTA: Alloc() error	Set up a trace using information from BLS (Back Level Support). Create a stack dump. Save a snapshot.	

SNMP Code	Event Log Entry	Meaning	Required Measures	Note
FP_EVT_GEN_023	new APS not ok switch back	new APS not ok switch back	Set up a trace using information from BLS (Back Level Support). Create a stack dump. Save a snapshot.	
FP_EVT_GEN_024	idle arrived after restart	idle arrived after restart	Set up a trace using information from BLS (Back Level Support). Create a stack dump. Save a snapshot.	
FP_EVT_GEN_030	exceed. of CSTA mon. pts	exceed. of CSTA mon. pts	Set up a trace using information from BLS (Back Level Support). Create a stack dump. Save a snapshot.	
Error Class 19 - Network Services Messages				
FP_EVT_NWS_002	SNTP-Server not responding	No connection to the SNTP server.	Check the application and the connection.	
FP_EVT_NWS_011	SNTP-Client at PCS can't be activated	SNTP-Client at PCS can't be activated		
Error Class 20 - Call Processing Messages				
FP_EVT_CP_002	RS232: DSR not Ready	The RS232/V.24 interface is out of order.	Check the interface, the line, and the application.	
FP_EVT_CP_011	RS232: DSR ready	The RS232/V.24 interface is now operational.	None	

SNMP Code	Event Log Entry	Meaning	Required Measures	Note
FP_EVT_CP_013	not connected ways	The maximum number of connection paths permitted has been exceeded.	Use the project planning tool to test the system configuration. Set up a trace using information from BLS. Create a stack dump. Save a snapshot.	
FP_EVT_CP_017	int. charg buf ovflw	Internal call data memory overflow.	Read out call data. If the error persists, check the call data application interface.	
FP_EVT_CP_029	Forced trunk disconnection	Manual line release (for U.S. only).	None	
FP_EVT_CP_032	CDR Mem. alloc. failed	Advanced call data memory cannot be created.	System with MMC module: MMC module is faulty. Replace the MMC. OpenScape Business: File system in flash is full or faulty.	
FP_EVT_CP_033	CDR Cache alloc. failed	Read cache for reading out CDR data cannot be created.	Perform a hard restart (normally occurs automatically).	This is caused by insufficient system memory capacity.
FP_EVT_CP_034	CDR Data write failed	Error while writing CDR data to the advanced call data memory.	MMC module: If necessary, read out call data via TFTP. The internal administration structure is also corrected, if this is required.	

SNMP Code	Event Log Entry	Meaning	Required Measures	Note
FP_EVT_CP_035	CDR Adm. write failed	Error while writing the administration structure to the advanced call data memory.	MMC module: If necessary, read out call data via TFTP. After this, replace the MMC module.	
FP_EVT_CP_036	CDR Data read failed	Error while reading CDR data from the advanced call data memory.	Set up a trace using information from BLS. Create a stack dump. Save a snapshot.	
FP_EVT_CP_037	CDR Adm. read failed	Error while reading administration structure from the advanced call data memory.	Set up a trace using information from BLS. Create a stack dump. Save a snapshot.	
FP_EVT_CP_038	CDR Data detected	An advanced call data memory was found during system startup.	None	
FP_EVT_CP_039	CDR Data overflow	The advanced call data memory is full.	Read out call data.	
FP_EVT_CP_040	CDR Mem. allocated	The advanced call data memory was successfully created.	None	

SNMP Code	Event Log Entry	Meaning	Required Measures	Note
FP_EVT_CP_041	CDR Mem. released	The advanced call data memory was temporarily released.	None	This message is issued after the call data memory has been completely read out. It must be followed by the ?CDR Mem. allocated? message.
FP_EVT_CP_042	MMC-size	Output of MMC module size	None	During system startup, the size of the MMC module is read out and hexadecimally output in bytes 1 and 2 of the info bytes. Value ?00 10? describes the 16-MB MMC, value ?00 40? describes the 64-MB MMC. This does not apply to OpenScape Business.

SNMP Code	Event Log Entry	Meaning	Required Measures	Note
FP_EVT_CP_043	CDR-MMC MMC full	Memory on the MMC module or in the OpenScape Business file system is insufficient for creating the advanced call data memory.		
Error Class 21 - Device Handler Messages				
FP_EVT_DH_000	no dial tone detected	No dial tone detected.	Use headset to check dial tone. Replace port or terminal if necessary.	
FP_EVT_DH_001	dial tone detected	Dial tone detected.	None	
FP_EVT_DH_004	Port out of service	Port out of service		
FP_EVT_DH_005	Port in service	Port in service		
FP_EVT_DH_007	Reference takt ON	Reference takt ON	None	
FP_EVT_DH_008	Reference takt OFF	Reference takt OFF	Check that the clock is available on the S0/ S2M line. If necessary, use OpenScape Business/ Manager E to correct the clock?s allowed/denied numbers list (Trunk ? Clock parameters). If necessary, perform a reset.	
FP_EVT_DH_011	Fan Alarm ON	Fan error.	Check the fan and air supply in the 19? housing. Note the ambient temperature.	

SNMP Code	Event Log Entry	Meaning	Required Measures	Note
FP_EVT_DH_012	Fan Alarm OFF	The fan error has been corrected.	None	
FP_EVT_DH_013	No ack from temp. sensor	No response from temperature sensor.		
FP_EVT_DH_014	Overload at code receiver	Not enough DTMF receivers.	Use a larger system.	
FP_EVT_DH_015	Overload at code transmit.	Not enough DTMF transmitters.	Use a larger system.	
FP_EVT_DH_016	Name in S0/ S2M msg discard	Name in S0/ S2M msg discard		
FP_EVT_DH_017	msg to long L3S int->ext	msg to long L3S int->ext		
FP_EVT_DH_018	msg to long L3S ext->int	msg to long L3S ext->int		
FP_EVT_DH_019	Shorten Msg not successful	Internal error: An overlong ISDN message could not be shortened by deleting Facility IEs.	Set up a trace using information from BLS. Create a stack dump. Save a snapshot.	
FP_EVT_DH_020	Msg longer than pool elem.	Msg longer than pool elem.		
FP_EVT_DH_021	Msg too long for segm-disc		Msg too long for segm-disc	
FP_EVT_DH_022	Auto PRI detec DMS250 prot	Auto PRI detec DMS250 prot		
FP_EVT_DH_023	Auto PRI detect NI2 prot		Auto PRI detect NI2 prot	I
FP_EVT_DH_024	Auto PRI detect 4ESS prot		Auto PRI detect 4ESS prot	
FP_EVT_DH_025	Name S0/S2M msg ext->int	Name S0/S2M msg ext->int		
FP_EVT_DH_026	key module overflow	key module overflow		
FP_EVT_DH_027	B-chan limit reached	B-chan limit reached		

SNMP Code	Event Log Entry	Meaning	Required Measures	Note
FP_EVT_DH_028	Power Alarm on	Emergency battery operation due to power outage.	Check line voltage. Note battery capacity.	
FP_EVT_DH_029	Power Alarm off	Power supply restored.	None	
FP_EVT_DH_093	si_cr_slot no logPort connected	si_cr_slot no logPort connected		
Error Class 23 - Device Handler Messages				
FP_EVT_NW_060	system hold, no buffer available	System hold, no more free buffer available.	Set up a trace using information from BLS. Create a stack dump. Save a snapshot.	
FP_EVT_NW_061	Check config rules for TMDID	For U.S. only: TMDID boards incorrectly configured.	Check TMDID board configuration using information from Pages 4-48 and correct if necessary.	
Error Class 26 - Board Administration Messages				
FP_EVT_PR_000	unknown card type	Unknown board.	System does not support the board type. Replace the board with a valid board type or remove it from the system.	The board may be too old or too new for the system.
FP_EVT_PR_001	card out of service	The specified board is out of order.	None	
FP_EVT_PR_002	card limit reached	The maximum number permitted for a certain board type is exceeded.	Reduce the number of boards of this board type. Note the maximum configuration.	

SNMP Code	Event Log Entry	Meaning	Required Measures	Note
FP_EVT_PR_003	other card type than old card type	Incompatible board type. The slot is already pre-assigned with a different board type.	Replace the board or use Assistant T to delete the pre-assigned board type so that the new board is recognized.	
FP_EVT_PR_004	card in service	The specified board is operational.	None	
FP_EVT_PR_005	error during database read	error during database read		
FP_EVT_PR_006	reason of reset card	reason of reset card		
FP_EVT_PR_007	Reload after load-LW-Code error	The specified board has been reloaded due to a startup error.	If this error persists, replace the board.	The board is reloaded due to a load error (length, checksum error) or a missing or delayed acknowledgement during startup.
Error Class 28 - Recovery Messages				
FP_EVT_RC_000	RESERVE	RESERVE	Set up a trace using information from BLS. Create a stack dump. Save a snapshot.	
FP_EVT_RC_004	SLC-Trace finished	SLC LW trace transferred to trace memory.	Trace memory can now be read out.	
FP_EVT_RC_005	X-trace output overflow	X-trace output overflow		

SNMP Code	Event Log Entry	Meaning	Required Measures	Note
FP_EVT_RC_006	Missing Timestamp in EventLog B	Missing Timestamp in EventLog B	None	A time stamp (current time and date) is entered when the event log B memory is copied. This facilitates analysis.
FP_EVT_RC_008	Missing APS in EventLog B	Missing APS in EventLog B	None	The current APS version is entered when the event log B memory is copied. This facilitates analysis.
Error Class 30 - Board Software Messages				
FP_EVT_LW_006	XCSEPBC: PBC error	PBC or ELIC error on the specified board.	Replace board.	
FP_EVT_LW_010	T1 reference clock problems		T1 reference clock problems	
FP_EVT_LW_016	HEATER ON - HXG3	Temperature in HiPath 3550/ HiPath 3350 wall housing is too high.	Check the fan kit and the air supply in the wall housing. Note the ambient temperature.	
FP_EVT_LW_017	HEATER OFF - HXG3	Temperature in HiPath 3550/ HiPath 3350 wall housing is normal.	None	
FP_EVT_LW_033	FAUC is reset	FAUC is reset		
FP_EVT_LW_061	short circuit on Upoe Port SLMC on	Short circuit in base station line.	Check lines. Replace base stations.	

SNMP Code	Event Log Entry	Meaning	Required Measures	Note
FP_EVT_LW_062	short circuit on Upoe Port SLMC off	Short circuit in base station line has been corrected.	None	
FP_EVT_LW_068	CMI base station breakdown off	CMI base station breakdown off		
FP_EVT_LW_069	CMI base station breakdown on	CMI base station breakdown on		
FP_EVT_LW_086	CMI base station overload	CMI base station overload		
FP_EVT_LW_090	E&M blockinginformation	E&M blockinginformation		
FP_EVT_LW_091	no message buffer on card avail. (1TR6)	no message buffer on card avail. (1TR6)		
FP_EVT_LW_092	message buffer on card available (1TR6)	message buffer on card available (1TR6)		
FP_EVT_LW_093	port not configurated (1TR6)	port not configurated (1TR6)		
FP_EVT_LW_094	unexpected message (1TR6)	unexpected message (1TR6)		
FP_EVT_LW_095	no USBS connection to system	no USBS connection to system		
FP_EVT_LW_0120	Layer 2 released	Layer 2 released		
FP_EVT_LW_0121	Layer 2 reestablished	Layer 2 reestablished		
FP_EVT_LW_0122	Layer 2 problem	Layer 2 problem		
FP_EVT_LW_0123	Layer 1 problem	Layer 1 problem		
FP_EVT_LW_0124	LW board error	LW board error		
FP_EVT_LW_0125	LW port error	LW port error		
Error Class 32 - Messages Concerning IVM (HiPath Xpressions Compact) and EVM (Entry Voice Mail)				
FP_EVT_SV_000	Configuration link up			
FP_EVT_SV_001	Configuration link down			
FP_EVT_SV_008	TIMEOUT during server-msg			

SNMP Code	Event Log Entry	Meaning	Required Measures	Note
FP_EVT_SV_010	IVM: Exception (unexpected error)	IVM: An unexpected error has occurred.	Set up an IVM trace.	
FP_EVT_SV_011	IVM: SW-error	IVM: A software error has occurred.	Set up an IVM trace. Upgrade IVM if necessary.	
FP_EVT_SV_012	IVM: SW-warning	IVM: SW-warning		
FP_EVT_SV_013	IVM: HD assignment of memory space 80%	IVM: 80% of hard disk used.	Search IVM statistics for mailboxes with too many undeleted messages.	
FP_EVT_SV_014	IVM: HD full	IVM: Hard disk is full.	Search IVM statistics for mailboxes with too many undeleted messages.	
FP_EVT_SV_015	IVM: Mailbox not available	IVM: Mailbox is not available.	Check whether the subscriber in question is available in the event log. Set up IVM system mailbox if necessary.	
FP_EVT_SV_016	IVM: SW_Upgrade not possible	IVM: Software upgrade is not possible.	Reload the board if necessary. Upgrade software again.	
FP_EVT_SV_017	IVM: Reload occurred	IVM: Reload performed.	None	
FP_EVT_SV_018	IVM: Restore faulty	IVM: Faulty restore.	Perform restore again.	
FP_EVT_SV_019	IVM: HD assignmentof memoryspace <70 %	IVM: Hard disk load less than 70%.	None	

SNMP Code	Event Log Entry	Meaning	Required Measures	Note
FP_EVT_SV_020	IVM: Unauthorized call attempt	IVM: Unauthorized call attempt.	If the attempt is unintentional, deactivate the station number length. If the attempt is intentional, create an IVM trace to determine the subscriber who made the attempt.	
FP_EVT_SV_030	VMM Cmd-resp timeout	EVM: Command response timeout.	Reload the board. If the error persists, replace the board.	
FP_EVT_SV_031	memory level of 60%	memory level of 60%		
FP_EVT_SV_032	memory level of 80%	EVM: 80 % of memory used.	Check EVM mailboxes for too many undeleted messages.	
FP_EVT_SV_033	Presence evt from EVM	EVM: Presence Event from EVM.		
FP_EVT_SV_035	VMM unexp. EVM error	VMM unexp. EVM error		
FP_EVT_SV_036	EVM out of service	EVM out of service		
FP_EVT_SV_037	VMM config. Fault	VMM config. Fault		
FP_EVT_SV_038	VMM inconsistent msg	VMM inconsistent msg		
FP_EVT_SV_040	VMM no/unexp reaction	VMM no/unexp reaction		
FP_EVT_SV_041	VMM msg limit reached	EVM: Message limit reached.	Check EVM mailboxes for too many undeleted messages.	

SNMP Code	Event Log Entry	Meaning	Required Measures	Note
FP_EVT_SV_042	no language available	EVM: No language file available.	Check available languages on the EVM. Load a language if necessary.	
FP_EVT_SV_043	VMM multiple greeting	VMM multiple greeting		
FP_EVT_SV_044	VMM buffer overflow	EVM: VMM buffer overflow.		
FP_EVT_SV_045	VMM no pool memory	VMM no pool memory		
FP_EVT_SV_046	EVM error during DM	EVM: EVM error during Data Mode.		
FP_EVT_SV_047	EVM error during FM	EVM error during FM		
FP_EVT_SV_048		DH_EVM error		
FP_EVT_SV_049	DH_EVM->reset EVM	EVM: System - DH_EVM -> reset EVM.		
FP_EVT_SV_052	AM com during DM	EVM: AM Command during Data Mode.		
FP_EVT_SV_053	Memory Full	EVM: Memory Full.		
FP_EVT_SV_055	No Pill File selected	EVM: No Pill File Selected.	Check available languages on the EVM. Load a language if necessary.	
FP_EVT_SV_057	HW failure detected	HW failure detected		
FP_EVT_SV_058	Philips API ERROR	EVM: Philips API ERROR.		
FP_EVT_SV_059	I2C failure detected	EVM: I2C failure detected.		
FP_EVT_SV_070	EVM dir not available	EVM dir not available		
FP_EVT_SV_071	Daily Backup FS check failed	Daily Backup FS check failed		
FP_EVT_SV_072	wrong tar file	wrong tar file		

SNMP Code	Event Log Entry	Meaning	Required Measures	Note
FP_EVT_SV_073	invalid bin file	invalid bin file		
FP_EVT_SV_074	EVM memory full	EVM memory full		
FP_EVT_SV_075	inv. para from WBM	inv. para from WBM		
FP_EVT_SV_076	EVM checksum failure	EVM checksum failure		
Messages Concerning Resource Manager				
FFP_EVT_RM_000	Resource Manager error admin	Resource Manager error admin		
FP_EVT_RM_001	Resource Manager error configuration	Resource Manager error configuration		
Messages Concerning UPM				
FP_EVT_UPM_010	UPM: restarted	UPM: restarted		

SNMP Code	Event Log Entry	Meaning	Required Measures	Note
MSG_DLSC_BOOTSTRAP_OK	DLS client successfully bootstraped.	DLS client successfully bootstraped.		
MSG_STRC_STOP	Secure trace stopped.	Secure trace stopped.		
MSG_STRC_START	Secure trace started for protocols.	Secure traces have been activated by user for the mentioned protocols.		
MSG_SPE_CERT_MISSING	SPE certificate missing.	No SPE certificate installed.	Import SPE certificate plus private key (PKCS#12 file).	
MSG_SPE_CERT_AVAIL	SPE certificate available.	SPE certificate is now available.		
MSG_SPE_CERT_UPDATED	SPE certificate has been updated successfully.	SPE certificate has been updated successfully.		
MSG_SPE_CERT_EXPIRED	SPE certificate expired.	Validity period of installed SPE certificate is passed.	Install a new valid certificate.	

SNMP Code	Event Log Entry	Meaning	Required Measures	Note
MSG_SPE_CRL_EXPIRED	SPE CRL for a specific CA has been expired.	CDP inaccessible or retrieved CRL is expired.	Import a SPE CA certificate with valid CRLs configured in CDP.	
MSG_SPE_CRL_UPDATED	SPE CRL for CA has been updated successfully.	SPE CRL for CA has been updated successfully.		
MSG_SPE_ALL_CRLS_UPTODATE	All SPE CRLs are up to date again.	All SPE CRLs are up to date again.		
MSG_MIKEY_REBOOT	Mikey Stack: assertion failed.	Mikey Stack: assertion failed.		
MSG_IPSEC_REBOOT	Fatal error in IPSec stack.	Fatal error in IPSec stack.		
MSG_CAT_H323_REBOOT		Reboot with H.323		
MSG_CAT_HSA_REBOOT		Reboot with HAS		
MSG_GW_SUCCESSFULLY_STARTED				
MSG_IP_LINK_FAILURE				
MSG_IP_LINK2_FAILURE		IP-Link 1 up/ down		
MSG_IP_LINK3_FAILURE				
MSG_WEBSERVER_MAJOR_ERROR				
MSG_NEW_SW_AVAILABLE				
MSG_ADMIN_REBOOT		Reboot with WBM/CLI-Admin, software upgrade or data restore		
MSG_SYSTEM_REBOOT		Automatic reboot, for example with Garbage Collection		
MSG_EXCEPTION_REBOOT		Reboot with SW exception		

SNMP Code	Event Log Entry	Meaning	Required Measures	Note
MSG_GW_OBJ_MEMORY_EXHAUSTED		Out of memory		
MSG_TLS_POOL_SIZE_EXCEEDED		No more internal pools		
MSG_OAM_RAM_THRESHOLD_REACHED		RAM limit reached		
MSG_OAM_DMA_RAM_THRESHOLD_REACHED		DRAM limit reached		
MSG_OAM_THRESHOLD_REACHED		Limit reached, for example, for flash memory or IP pools		
MSG_OAM_HIGH_TEMPERATURE_EXCEPTION		Temperature limit reached (too hot)		
MSG_FIREWALL_ALARM				
MSG_HACKER_ON_SNMP_PORT_TRAP		Unauthorized access to SNMP port		
MSG_DVMGR_LAYER2_SERVICE_TRAP		B channel up/down		
MSG_DVMGR_SECURED_LICENSE_FAILURE				
MSG_SSM_NUM_OF_CALL_LEGS_2BIG	More than 2 call Legs: not supported! CSID: %x/%x	No more than two call Legs per session are permitted. This has caused the software to become unstable. The necessary reboot is executed.		
MSG_SSM_SESSION_CREATION_FAILED	Session creation failed	Signalling is no longer possible because a session could not be created. The necessary reboot is executed. An SNMP trap is generated.		

SNMP Code	Event Log Entry	Meaning	Required Measures	Note
MSG_IPNCV_STARTUP_ERROR	IPNCV Startup: Creating IPNCV Manager failed	IPNCV could not be started. An SNMP trap is generated.	Create a TR/MR	
MSG_IPNCV_STARTUP_SHUTDOWN	IPNCV start/stop: IPNCV Manager created successfully or IPNCV start/stop: Shutdown of IPNCV Manager successfully	IPNCV was started or stopped successfully.An SNMP trap is generated		
MSG_IPNCV_INTERNAL_ERROR	Internal IPNCV error: %s	Software error: invalid internal data found.An SNMP trap will be generated with the profile IPNCV-Detailed.		
MSG_IPNCV_MEMORY_ERROR	IPNCV Memory: %s	Memory overflow: an SNMP trap is generated.	Restart the gateway. Create a TR/MR.	
MSG_IPNCV_SIGNALING_ERROR	IPNCV Signaling Error: %s	Software error: invalid internal data found.		
MSG_CAR_ALIVE_IP_CONNECTION_LOST	CAR : Alive : ip connection %d.%d.%d.%d lost	CAR: Alive: IP connection lost.		
MSG_LIC_DATA_ACCEPTED		License data accepted		
MSG_LIC_DATA_CORRUPTED		License data incomplete		
MSG_LIC_DATA_NOT_ACCEPTED		License data accepted		
MSG_VCAPI_ADD_OBJECT_FAILED				
MSG_VCAPI_COULD_NOT_DELETE_OBJECT				

SNMP Code	Event Log Entry	Meaning	Required Measures	Note
MSG_VCAPI_COULD_NOT_STORE_REQ				
MSG_KERNEL_REBOOT_EVENT				
MSG_SPE_CERT_MISSING	No SPE certificate installed!	SPE certificate missing.	Install SPE certificate.	

21.8.3 Manual Actions

Many different logs (diagnostics data and diagnosis logs) can be loaded via manual actions.

Administrators with the **Advanced** profile can load diagnostic data (diagnosis logs) by using the **Trace** wizard.

Administrators with the **Expert** profile can load diagnostic data (diagnosis logs) in **Expert mode**.

The following logs can be loaded:

Protocol	Explanation	Application case
Trace log	Standard trace file, if trace profiles have been activated. A selection can be made between the following options: • **Complete Trace Log**: The full set of existing system trace log files is downloaded. • **Log from Today**: The system trace log files of the current day (as of 00:00 hours) are downloaded. • **Own Selection**: **From:** XXX **To:** YYY: The system trace log files of the selected time period are downloaded.	No special application
Event Log	Actions/events of the communication system (Reset, On/Off, etc.)	No special application
Admin log (also called admin protocol)	Messages about administration processes at the communication system (login attempts, etc.)	No special application
License Protocols	Messages about the communication system components that require licenses	Problems with licensing (the license file cannot be activated, and so on)
Customer Trace	Messages for the customer trace are provided in a more detailed format than in the trace log, for example (remote login, ITSP login, etc.).	Problems with the ITSP (Internet Telephony Service Provider) connection or the remote login
Framework Protocol	WBM messages	Problems with licensing, backup, restore or with the WBM
Diagnosis Log	Diagnosis logs of the communication system (FP/LDH)	System crash or uncontrolled shutdown of the communication system

Protocol	Explanation	Application case
UC Suite Logs	Messages of the UC Suite of the communication system (UC Suite, CSP and MEB logs) A selection can be made between the following options: • **Complete Trace Log**: All existing UC Suite, CSP and MEB log files are downloaded. • **Log from Today**: The UC Suite, CSP and MEB log files of the current day (as of 00:00 hours) are downloaded. • **Own Selection**: **From:** XXX **To:** YYY: The UC Suite, CSP and MEB log files of the selected time period are downloaded. All log files are archived together in a compressed file. The following file naming conventions apply to the OpenScape Business logs: UC Suite log files = `vs_yyyy_mm_dd.log`, CSP log files = `csptrace_yyyy_mm_dd.log`, MEB log files = `mebtrace_yyyy_mm_dd.log`. ***INFO***: diagnostic data can be downloaded only when operating with the UC Booster Card OCAB. When using the OpenScape UC Business Booster Server, diagnostic data must be downloaded from the server itself.	Problems with the UC Suite and/or the client (myPortal for Desktop, myAttendant, etc.)
Application Protocols	Messages of the application side of the communication system (for example, CSP protocols) An administrator with the **Expert** profile can select between the following options in **Expert Mode**: • **Complete Trace Log**: All existing log files are downloaded • **Log from Today**: The log files of the current day (as of 00:00 hours) are downloaded. • **Own Selection**: **From:** XXX **To:** YYY: The log files of the selected time period are downloaded. All log files are archived together in a compressed file.	Problems with the application side of the communication system
System Diagnosis Logs	Diagnosis logs of the communication system	No special application
PPP Logs	Messages for the Point-to-Point Protocol	Problems with Dial-In or Dial-Out connections
CoreLog Protocol	CoreLogs are created for resets, etc. (e.g., memory dumps at a PC).	System crash or uncontrolled shutdown of OpenScape Business

After the desired logs have been selected, a compressed file is created and stored in a specified directory.

21.8.4 Traces

Traces can be used to record the execution of individual program steps and their results during the execution of a program. In combination with further diagnostics data, an incorrectly executing program can be traced back to the source of the

error. The individual traces to be recorded and their respective levels of detail are configured via the trace profiles and trace components.

> ***INFO:*** Activating traces can have a negative impact on system performance and must hence only be performed by experienced administrators and only after consulting with the responsible Service Support.
>
> The console trace, in particular, requires substantial system resources and thus has an adverse effect on the performance of the communication system.

Networking

In order to diagnose networked communication systems, the trace data of each individual node must be collected separately. It is not possible to acquire the trace data of networked communication systems centrally.

Trace Format Configuration

The Trace Format Configuration function can be used by an administrator with the **Expert** profile to define which header data is to be included in the trace output and how the trace data is to be formatted.

Header data for the trace output (all options are activated in the default setting):

- Global Trace Header Format Settings
  If this option is enabled, the options for the following header data can be activated or deactivated.
- Subsystem ID
- Task Name
- Task ID
- Time
- Module Name
- Line Number

Formatting the Trace Data

- Full formatting with parameter expansion (default) = large data volume, normal trace performance. Default setting
- Limited formatting (message types binary, special X-Tracer format) = medium data volume, fast trace performance.
- Limited formatting (expansion of basic data types only) = low data volume, very trace performance.
- Performance optimized trace without parameter expansion = very low data volume, extremely fast trace performance.

> ***INFO:*** Note that adding more trace header data and extensive trace data formatting will decrease the overall trace performance.

Trace output interfaces

This function enables an administrator with the **Expert** profile to define the interfaces for the trace output. It is possible to either enable the file trace or trace via LAN or to disable both interfaces.

Trace output interface	Explanation	Default setting
File Trace	**Switch File Trace On** Trace messages are entered into a log file in the communication system. The following settings apply when the option is enabled: **Max. Trace Quota (kByte)**: Indicates the maximum size of the trace memory **Policy to handle reach of max. quota**. You can choose between **Wrap Around (delete oldest file)** and **Stop temporarily the file trace**. **Time between creation of new trace files (sec):** 900 **Time period for which trace files are available:** The actual time period is specified.	Enabled
Trace via LAN	**Switch Trace via LAN On** Trace messages are transmitted via the LAN interface. The following setting applies when the option is enabled: **Timer value** = 25 sec. (delay period until data is transmitted.)	Not activated

Trace log

If the trace output interface Switch File Trace On is enabled, the resulting log files can be transferred by an administrator with the **Expert** profile to a PC or deleted.

Digital Loopback

Digital loopbacks are used to test the B channels of S_0, S_{2M} and T1 interfaces of any existing boards. Digital loopbacks should only be activated if requested by the service provider.

They can only be configured using E Manager.

Event Viewer / Customer Trace Log

The **Event Viewer** wizard can be used by an administrator with the **Advanced** profile to start the event display (customer trace) In addition, the customer trace log file can be copied to a PC or deleted.

The following functions, which can be started using the wizard, are described here:

- *Displaying or Editing Event and Customer Trace Logs*
- *Downloading or Opening the Event Log / Customer Trace Log*
- *Clearing the Event Log / Customer Trace Log*

Administrators with the **Expert** profile can start displaying the customer trace log file in **Expert mode**. In addition, the customer trace log file can be copied to a PC or deleted.

M5T Trace Components

This function is used to monitor the SIP stack by an administrator with the **Expert** profile. For each M5T trace component, the level of detail for the trace can be defined via trace levels (0 = lowest level of detail to 4 = maximum level of detail).

Secure Trace

This function is used by an administrator with the **Expert** profile to record encrypted VoIP payload and signaling data streams.

If the Signaling and Payload Encryption (SPE) feature has been enabled, the VoIP payload and signaling data streams from and to the communication system and between IP phones will be encrypted.

To ensure that errors are properly analyzed, additional trace information (**Secure Trace**) can be transmitted in the LAN for a limited period of time. In this case, asymmetrically encrypted secure trace files are generated, which can only be decrypted and analyzed by Development.

The following security features have been implemented to restrict the use of the secure trace function:

- A service technician must import a so-called public key (certificate) into the relevant communication system. The certificate is part of an X.509 file and is required to generate a secure trace. The X.509 file is provided by Development. The included certificate is valid for a maximum of one month.
- A special password (passphrase) must be entered to start and stop the secure trace. This password is known only to the customer.

Thus, the certificate is the key of the service technician and the password (passphrase) is the key of the customer. Both keys are required to activate the secure trace function.

Process for generating a secure trace:

1. A service technician finds a problem in the customer's LAN. Together with Development, the service technician recognizes the need to generate a secure trace.
2. The customer is notified accordingly and must confirm that he has been notified. The customer then issues an order for the creation of a secure trace, specifying the date and time when monitoring should start and end.
3. A developer creates a key pair consisting of the public key and the private key. This key pair can only be used to create a single secure trace. The certificates are used in the following manner

- The certificate with the private key is strictly confidential and can only be used by authorized developers.
  The private key is required to decrypt the secure trace files.
- The certificate with the public key is passed to the service technician in the form an X.509 file in PEM or binary format.
  This certificate must be imported into the relevant communication system to be able to generate a secure trace.

4. The service technician notifies the customer that the generation of the secure trace is to start soon. The customer, in turn, must notify all affected parties.

   NOTICE: The live recording of calls and connection data is a criminal offence, unless the affected parties have been notified in advance.

5. The service technician imports the certificate with the public key into the relevant communication system.
6. The customer starts the secure trace by entering the password (passphrase). The secure trace files are generated.
   Start and stop of the secure trace are logged by the communication system.
7. Upon completion of secure trace generation, the customer is notified that all secure trace activities have been stopped. The service technician removes the certificate from the communication system.
8. The secure trace files are made available to Development.
9. A developer decrypts the secure trace files using the private key and then analyzes the decrypted data.

   NOTICE: Once the analysis has been completed, all relevant data must be destroyed in a secure manner. This includes the destruction of the private key so that any potential unauthorized copy of the secure trace files can no longer be decrypted.

H.323 Stack Trace

This function can be used by an administrator with the **Expert** profile to set the H.323 Stack Trace Configuration. The level of detail for the trace can be defined via trace levels (0 = lowest level of detail to 4 = maximum level of detail). The following settings can be selected for the H.323 stack trace output:

Trace output interface	Explanation	Default setting
Console Trace	**Switch Console Trace On** H.323 Stack Trace messages are output on the console.	Not activated
File Trace	**Switch File Trace On** H.323 Stack Trace messages are written to a log file. The following settings apply when the option is enabled: Max. size of the trace buffer = 50000 bytes (amount of data stored in the buffer.) Max. size of the trace file = 1000000 bytes (maximum size of the log file.) Trace Timer = 60 sec. (delay period until data is written to the log file.)	Not activated

By activating and/or deactivating H.323 modules, you can define for which components of the H.323 stack trace the process and status information is to be recorded. The status of each H.323 module is indicated by the color of the associated bullet point (green = H.323 module active, red = H.323 module inactive).

The H.323 Stack Trace log can be transmitted to a PC or deleted.

License Component Trace

This function is used by an administrator with the Expert profile to monitor the system-internal license agent (Customer License Agent, CLA). The level of detail for the trace can be defined via trace levels (low = lowest level of detail (default), standard = medium level of detail, all = maximum level of detail).

By default, the license component trace is enabled (trace level = low).

Changing the trace level can have a negative impact on system performance and must hence only be performed by experienced administrators and only after consulting with the responsible Service Support.

Trace Profiles

Trace profiles define what data is to be recorded and at what level of detail. Trace components are assigned to a trace profile. This allows you to specify for which system components the process and status information should be logged by the trace profile.

Predefined trace profiles are provided for all standard scenarios. In addition, an administrator with the **Expert** profile can also create his or her own profiles. When you start a trace profile, logging is activated via this profile. When you stop the profile, logging is deactivated.

- Administrators with the **Advanced** profile can start and/or stop trace profiles by using the **Trace** wizard. The status of every trace profile is indicated by the

color of the associated list item (green = trace profile active, red = trace profile not active). **Start/Stop** can be used to enable or start an inactive trace component (red bullet point) and to disable or stop an active trace component (green bullet point).
Load Trace is used to transfer the generated log files to a PC or open them.
Delete Trace is used to delete the generated log files.
The following functions, which can be started using the wizard, are described here:

- *Downloading Traces / Trace Logs*
- *Clearing Traces / Trace Logs*
- *How to Display all Trace Profiles*
- *Start Trace Profile*
- *Downloading Diagnostics Data / Diagnosis Logs*

- Administrators with the **Expert** profile can collectively stop all trace profiles and selectively start and/or stop individual trace profiles in **Expert mode**.
  In the menu tree display, the color of the list item indicates the status of the trace profile (green = trace profile is activated, red = trace profile is not activated). **Start/Stop Trace Profile** can be used to enable or start an inactive trace component (red bullet point) and to disable or stop an active trace component (green bullet point).
  By selecting **Display Trace Profile** you can view the details of the desired trace profile: This includes the profile name, details about write protection and the status of the profile, as well as information on when, i.e., for which problems, this trace profile should be used. In addition, you can see which trace components belong to the trace profile.

Trace Profile	Application case
Actors / Sensors / Door Opener	No information is currently available!
Basic	No information is currently available!
Calls_with_Analog_Subscriber_Trunks	No information is currently available!
Calls_with_ISDN_Subscriber_Trunks	No information is currently available!
Calls_with_System_Device_HFA	No information is currently available!
Calls_with_System_Device_Upn	No information is currently available!
CDR_Charging_data	No information is currently available!
CMI	No information is currently available!
CSTA_application	No information is currently available!
Display_problems	No information is currently available!
Gateway_Stream_detailed	No information is currently available!
Gateway_Stream_overview	No information is currently available!
IP_Interfaces	No information is currently available!
License_problem	No information is currently available!
Network_Call_Routing_LCR	No information is currently available!
Peripheral_cards	No information is currently available!

Trace Profile	Application case
RAS_or_Internal_access	No information is currently available!
Resources_MOH_Conferencing	No information is currently available!
SIP_Interconnection_Subscriber_ITSP	No information is currently available!
SIP_Registration	No information is currently available!
Smart_VM	No information is currently available!
UC_Smart	No information is currently available!
Voice_fax_connection	No information is currently available!
VPN	No information is currently available!
Web_based_Assistant_Expert_Mode	No information is currently available!
Xpressions Compact	No information is currently available!

Trace Components

Trace components can be used to record the process and status information of individual components of the communication system.

All trace components can be stopped together and started or stopped individually by an administrator with the **Expert** profile. Starting and stopping a trace component activates and deactivates the recording. The level of detail for the trace can be defined via trace levels (0 = lowest level of detail to 9 = maximum level of detail).

The color of the list item displayed in the menu tree indicates the status of the trace component (green = trace component activated, red = trace component not activated). **Start/Stop Trace Component** can be used to enable or start an inactive trace component (red bullet point) and to disable or stop an active trace component (green bullet point).

A Trace Component display shows the subsystem name, the trace component index, the set trace level, the status information and whether or not the trace component is currently active. If a trace component needs to be edited, apart from changing the trace level, the trace component can also be started or stopped.

21.8.5 TCP Dump

A TCP dump is used for monitoring and evaluating data traffic in an IP network.

> ***INFO:*** Activating a TCP dump can have a negative impact on system performance and must hence only be performed by experienced administrators and only after consulting with the responsible Service Support.

TCP dump files are stored in the communication system. An appropriate application is required for the diagnosis of the files.

TCP dumps are often used to

- generate a LAN trace for a short period of time (e.g., for a reproducible error image).
- allow authorized service technicians to remotely access a LAN trace, for example via SSDP.

Advantages over RPCAP daemon: remote access is possible, so trace files do not have to be sent by e-mail

Disadvantages compared to RPCAP daemon: long-term traces are not meaningful; limited storage space, no capture filter can be set, more complex handling for several individual traces

21.8.6 RPCAP daemon

An RPCAP (Remote Packet Capture) daemon is used for monitoring and evaluating data traffic in an IP network.

INFO: Activating an RPCAP daemon can have a negative impact on system performance and must hence only be performed by experienced administrators and only after consulting with the responsible Service Support.

The RPCAP daemon enables external applications to remotely access the TCP/IP packets on the LAN interfaces of the communication system.

An RPCAP a daemon is often used for long-term traces, since the trace files are stored on a PC and not in the communication system.

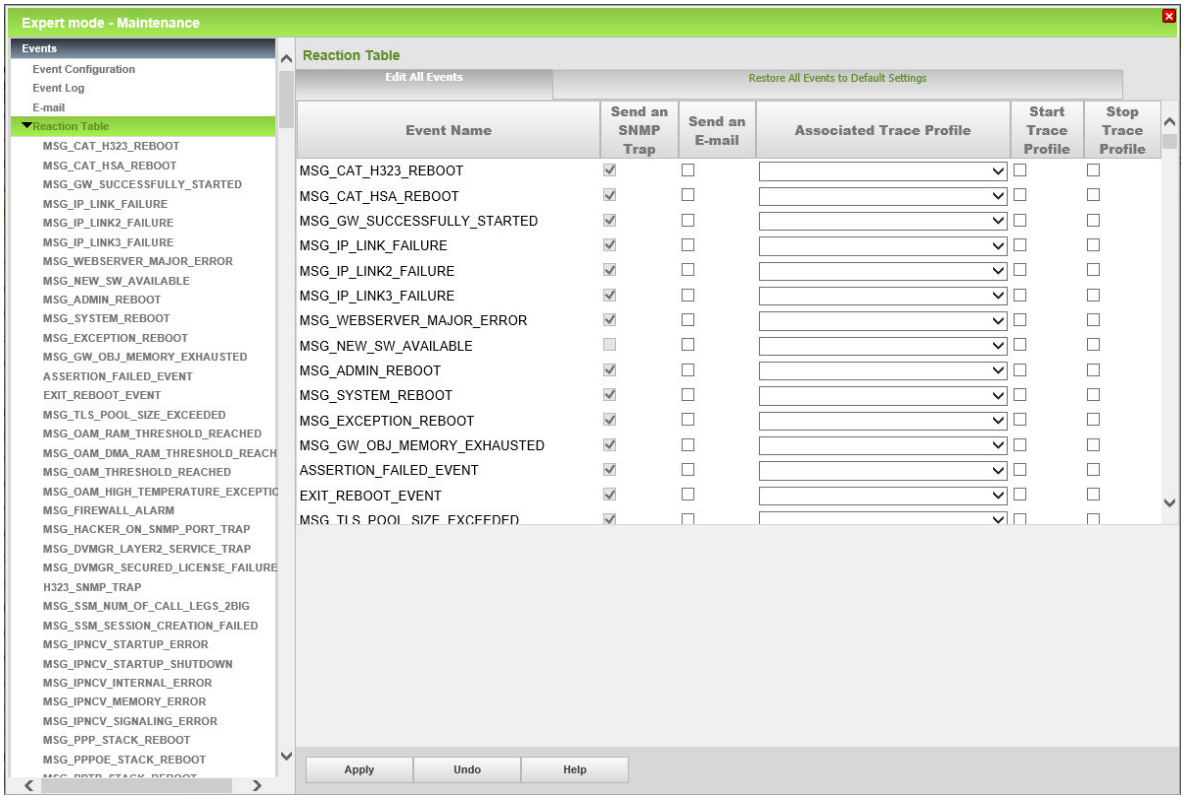
Advantages over TCP dump: faster and easier to use, long-term traces possible, number and/or size of the trace files can be freely selected, trace of internal LAN possible

Disadvantages compared to TCP dump: double network traffic and therefore increased load on the LAN interfaces of the communication system, special opening of ports needed (firewall)

21.8.7 Events

Events provide information about communication system deficiencies. All events are written to a log file that is restricted in size. A new file is created if the maximum file size is exceeded. Up to seven files can be created.

Depending on the setting in the reaction table and the problem class, events may generate an SNMP trap, trigger an e-mail and/or start or stop trace monitoring. The event log (Event Viewer) can be evaluated, configured, and saved via the WBM.



To interpret the event log file, you must download and extract the file with the WBM. The file can then be opened, edited and printed using any text editor. Once the event log file has been transferred, the file can be deleted from the communication system's memory.

Events that can trigger actions are defined by the following properties:

- Event code:
  Identifies an event such as `MSG_ADMIN_LOGGED_OUT` = Logout information of an administrator.
- Event type:
  The following different types exist:
  - Information: plain status messages, no error messages.
  - Warning: report of a possibly problematic procedure or status, but not an error message.
  - Minor: error message. The error has no problematic consequences.
  - Major: error message. This error could cause problems.
  - Critical: Error Message. This error causes problems.
  - Cleared: error message. The error was already corrected by the communication system.
  - Indeterminate: error message. The cause of the error cannot be accurately determined.
- Event text
  Some event texts contain variable data. These are identified in the following manner:

- %s: character string
- %u: positive or negative decimal number
- %f: floating point number
- %p: indicator (memory address)
- %x: hexadecimal number (with lower-case letters)
- %X: hexadecimal number (with upper-case letters)
- %C: single character
- %d and %I: positive decimal number

Reaction Table

For each possible event, the Reaction Table can be used by an administrator with the **Expert** profile to independently define what action is to be taken when that event occurs.

You can set whether an SNMP trap should be sent, whether the communication system should be restarted, whether the e-mail should be sent, and whether a trace profile should be started or stopped. If the event is assigned a trace profile, the name of this profile is shown.

E-mail Settings

These settings can be made by an administrator with the **Expert** profile to define how e-mails are sent when an event occurs.

Diagnosis Logs

The communication system logs certain process-specific actions in diagnosis logs. These log files can be evaluated for diagnostic purposes by an administrator with the **Expert** profile.

Alarm Signaling on Exceeding Critical Temperatures

Two critical temperature values are stored in the communication system. If the temperature of the system exceeds the first value, a warning is sent via an SNMP trap or e-mail to indicate that the system temperature is too high. In addition, this message can also be indicated on the displays of up to three system telephones (UP0 & HFA). If the second value is exceeded, the boards responsible for the overheating are shut down in a controlled manner (e.g., OpenScape Business Booster Card) or switched off (e.g., SLAV/SLAD). To clear the alarm and put the boards back into service, the system must be switched off and then switched on again.

The 3 destinations (system telephones) to be notified at on exceeding a temperature can be set.

21.8.8 Configuration Data for Diagnostics

"Smaller" backup sets containing diagnostic data for Service Support can be created for diagnostic purposes. In contrast to normal backup sets, significantly smaller data amounts are produced for this purpose and can thus be easily sent with an e-mail, for example.

Diagnostics backup sets include, among other things, the configuration data of the communication system and the UC Application (UC Smart or UC Suite). Voicemails, fax messages and announcements are not included.

The following media can be used to save backup sets for diagnostics:

- **USB Device**
  The data can be backed up to a connected USB drive or a connected USB stick, for example.

  NOTICE: If a USB hard disk, a partition thereof, or a USB stick is to be used for the backup, it must be formatted with FAT 32. USB media formatted with NTFS are read-only. Note that if multiple partitions exist, only the first partition can be used for the backup.

  If a bootable USB device is used for the backup, this USB device must be safely removed after the backup.

- **HTTPS**
  The data can be saved via HTTPS on the hard disk of the client PC.
- **Hard Disk** (only for OpenScape UC X3/X5/X8 UC Booster Card (OCAB Application Board))
  The data can be saved on the hard disk of the OCAB Application Board.

  INFO: It is not possible to create a backup on the hard disk of the communication system.

21.8.9 Card Manager

The Card Manager is a tool with which the software of the communication system can be written to an SDHC card. To do this, the software of the communication system must be available as an image file.

The software on the SDHC card is standard system software without customer data. SDHC cards cannot be used for software updates or for backing up customer data.

The Card Manager can be launched either as a Java application on a Linux PC (also possible in a virtual environment) or by using a Linux boot DVD.

Use Cases

- Before the delivery of the system, the software should be replaced with the latest software version.
- The used SDHC card is defective and must be replaced by a new SDHC card on which no software has yet been stored.
- The used software is corrupted and needs to be reloaded. All customer data is deleted in the process.
  If a backup set exists for the recovery of the customer data, the newly installed software should match the software version with which the backup set was

created so that the settings contained in the backup set can also be supported and processed by the installed software.

Hardware and Software Prerequisites

The following hardware and software are required:

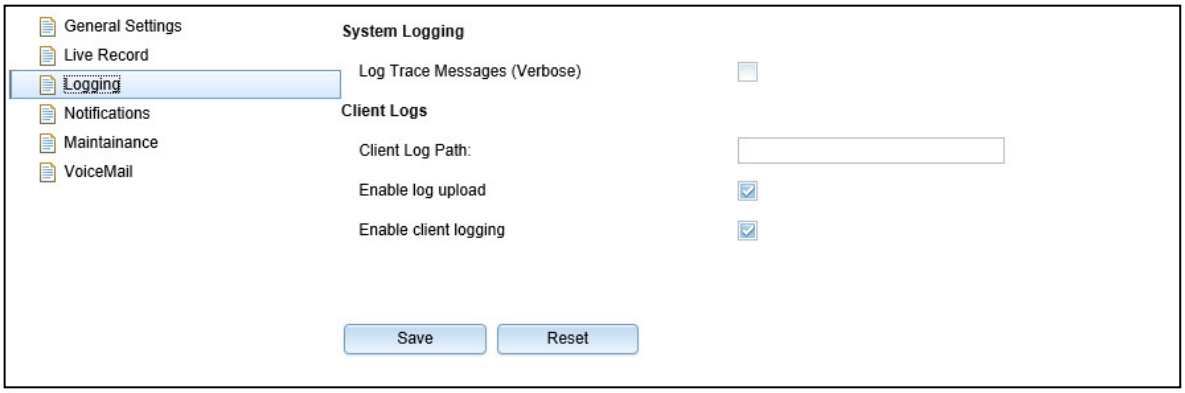
- External USB SDHC card reader. PC-internal SDHC card readers are not supported.
- For an SDHC card replacement: shared SDHC card.
- Image tar file with the latest communication software
- Card Manager File:
  - Alternative 1 - Card Manager jar file: this Java application can be launched directly from a Linux PC or from a Linux PC in a virtual environment.
  - Alternative 2 - Card Manager iso file: this file can be used to burn a Linux boot DVD that starts the Card Manager automatically after booting the Linux system.

21.9 Monitoring and Maintaining the UC Suite

The WBM **Expert** profile offers administrators numerous functions for monitoring and maintaining the UC Suite.

21.9.1 Logging

The execution of the UC Suite is monitored internally by the system. **System Logging** can be used to set whether logs should be created. In addition, a log of the activities of the UC Suite (e.g., the start of a UC Suite client) is maintained in **Client Logs**.



System Logging

The following system logs can be enabled or disabled:

System log	Default setting
Log Trace Messages (Verbose)	Not activated

The results of the enabled system log are written daily to a log file with the designation `vs-yyyy-mm-dd.log` (e.g., `vs-2013-01-222.log`) and stored in the communication system under `/var/system/trace_log/vsl/log`.

INFO: The analysis of these log files can only be performed by Development.

Client Logs

Client Logs are the log files of the UC Suite. For each UC Suite client (myPortal for Desktop, myAttendant, etc.) and station (user), a separate directory is created, and the relevant log files are stored in it. The logs record the activities of a subscriber such as starting the client, outgoing and incoming calls, etc.

INFO: The storage of client logs is supported only for the UC Suite clients used with Microsoft Windows operating systems.

The path in which the `CC-Logs` directory with the subdirectories for the individual UC Suite clients is to be stored can be defined. You can also select whether the directory is to be stored on every client PC or on a central PC or server on the network.

By default, the `CC-Logs` directory is stored in the following path:
`<Drive>:\Documents and Settings/<PC User Name>/CC-Logs`

The retention period for **Client Logs** is 5 days. No changes are possible.

The logging of the UC Suite activities in **Client Logs** is enabled by default. Administrators with the **Advanced** profile can disable logging on a station-specific basis by using the **User Directory** wizard. An administrator with the **Expert** profile can disable logging on a station-specific basis in **Expert Mode**.

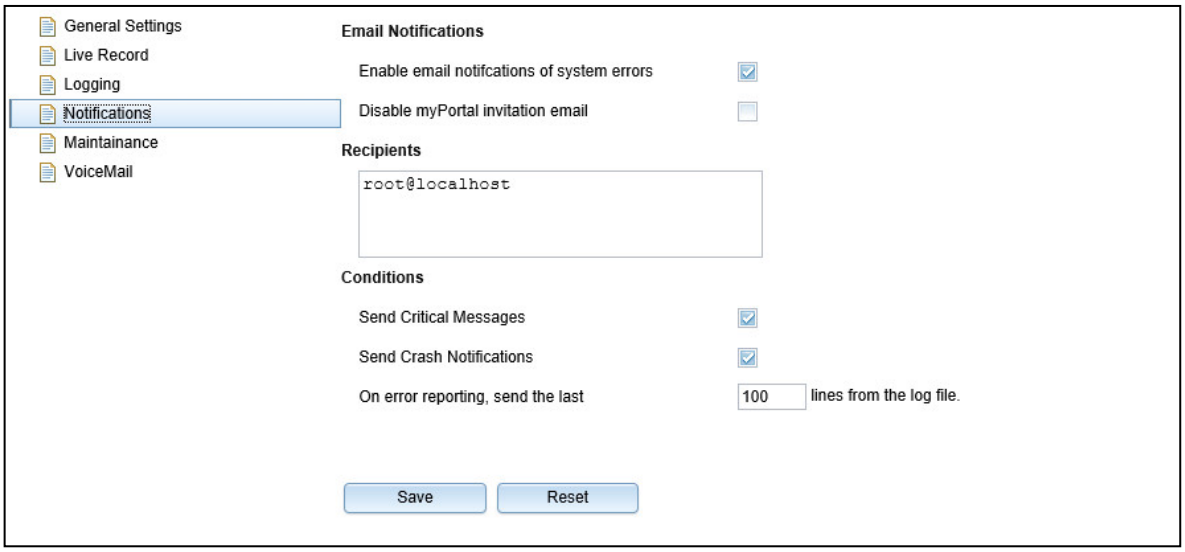
Depending on the scenario, the client logs are also stored by default on the hard disk of the UC Booster Card (OCAB), the UC Booster Server or the OpenScape Business S communication system. An administrator with the **Expert** profile can disable the saving of client logs on the system hard disk in **Expert Mode**.

An administrator with the **Advanced** profile can use the **Trace** wizard to download the client logs (log files) of the UC Suite clients (myPortal for Desktop, myAttendant, etc.) used by the internal subscribers.

An administrator with the **Expert** profile can use the **Expert mode** wizard to download the client logs (log files) of the UC Suite clients (myPortal for Desktop, myAttendant, etc.) used by the internal subscribers.

21.9.2 Notification

E-mail notifications can be sent to the entered **Recipients** to provide advance warnings about critical disk usage levels for the hard disk, for example, or about errors.



The sending of e-mails can be linked to the following **conditions**:

Conditions	Default setting
Send Critical Messages	Enabled
Send Crash Notifications	Activated

The Send Critical Messages and Send Crash Notifications settings should be enabled and thus sent. These messages warn the entered recipients about a potential problem that needs to be reported to the responsible Service Support.

In addition, you can define how many of the last lines of a log file should be included with the sent e-mail. The following system errors can be reported (in English only):

System error
NULL monitor
Could not notify Call Handler
Terminate call failed
Unable to load VM Structure from file
Alsa stuck
Alsa cancel failed
MEN CallID 0
NULL alsa handle

System error
Database connection failed
Rules engine logic failure
Config schema format failure
90% Disk usage mark
Main: Could not connect to the database !
Main: Could not load the configuration from the database!
Main: Could not open configuration file !
Main: Could not read the settings from the configuration file !
A segmentation fault was detected.
Database logic error
Database schema error
Connection Server failed to start
MultisiteSync failed to start
Multisite failed to start
TransferManager failed to start
IPC failed to start
ConferenceManager failed to start
CallManager failed to start
MediaProcessing failed to start
Queues failed to start
Import failed to start
Data client failed to start
DirectoryClient failed to start
DirectoryServer failed to start
FV failed to start
IM failed to start
Switch failed to start
No Switches
Exchange Integration failed to start
Outbound Fax failed to start
SQL connection pool failed to start
Task scheduler failed to start
Trunks failed to start
Unknown switch type
Users failed to start

System error
MEB has been disconnected
MEB ACK timeout
Switch Heartbeat timeout

21.9.3 Maintenance

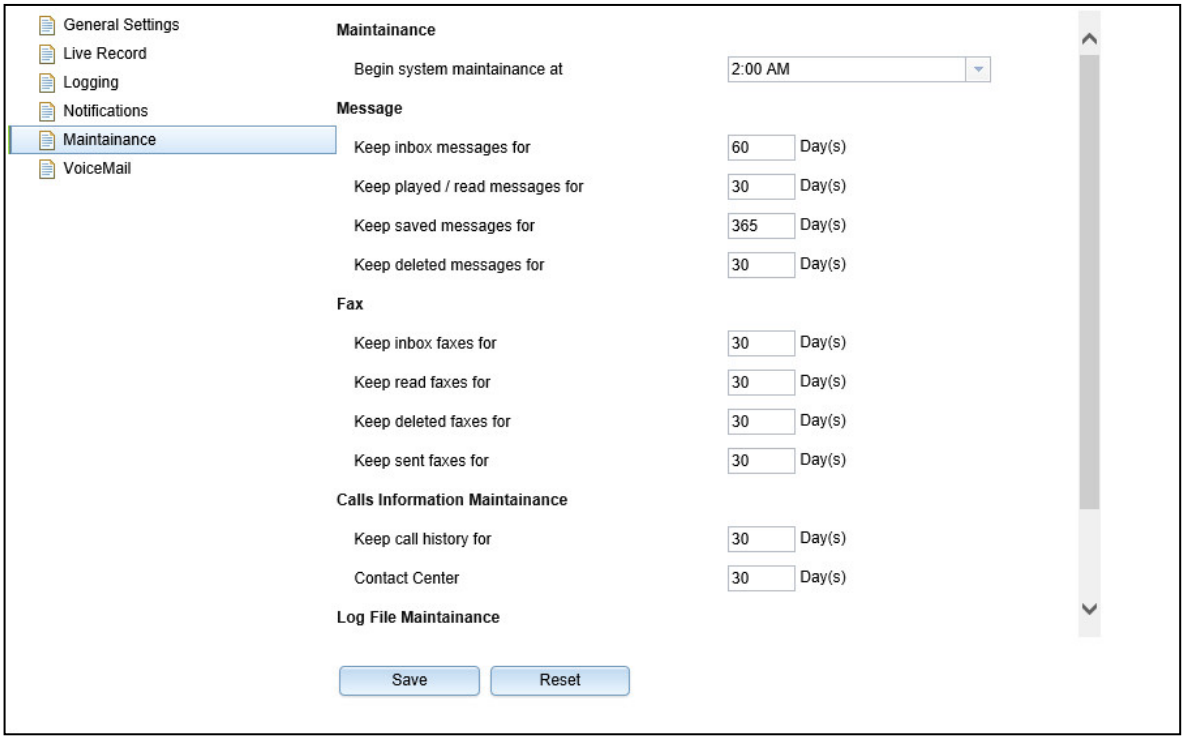
Retention periods can be defined via the Maintenance for messages, for call information in the Call Journal, for calls recorded with myAgent, for faxes and e-mails received and sent for the Contact Center and for log files.

You can also set at what time the following data for which the set retention periods have expired is deleted on a daily basis:

- Messages
- Call information in the call journal (call history)
- Calls recorded with myAgent (contact center)
- Faxes and e-mails received and sent for the Contact Center
- Log files

The default setting is 2:00 a.m.

In addition, it is also possible to start the system maintenance immediately and to thus initiate the immediate deletion of the above data for which the respectively set retention periods have expired. This may be necessary, for example, if the hard disk capacity of the communication system has reached a critical level.



For more information on Message Maintenance, see *Voicemail Box*.

For more information on **Maintaining Fax Messages**, see *Administrator Documentation, UC Suite*.

For more information on Calls Information Maintenance: Call History, see *Journal*.

With **Calls Information Maintenance**: **Contact Center**, the calls recorded with myAgent and the received and sent faxes and e-mails for the Contact Center that have exceeded the set retention period are deleted. The default setting for the retention period for contact center data is 60 days.

> ***INFO:*** The retention periods for the maintenance of the call information are independent of one another.
>
> Contact Center reports are based on the call history. If a shorter retention period was set for the call history than for the contact center data, some reports may no longer be available.

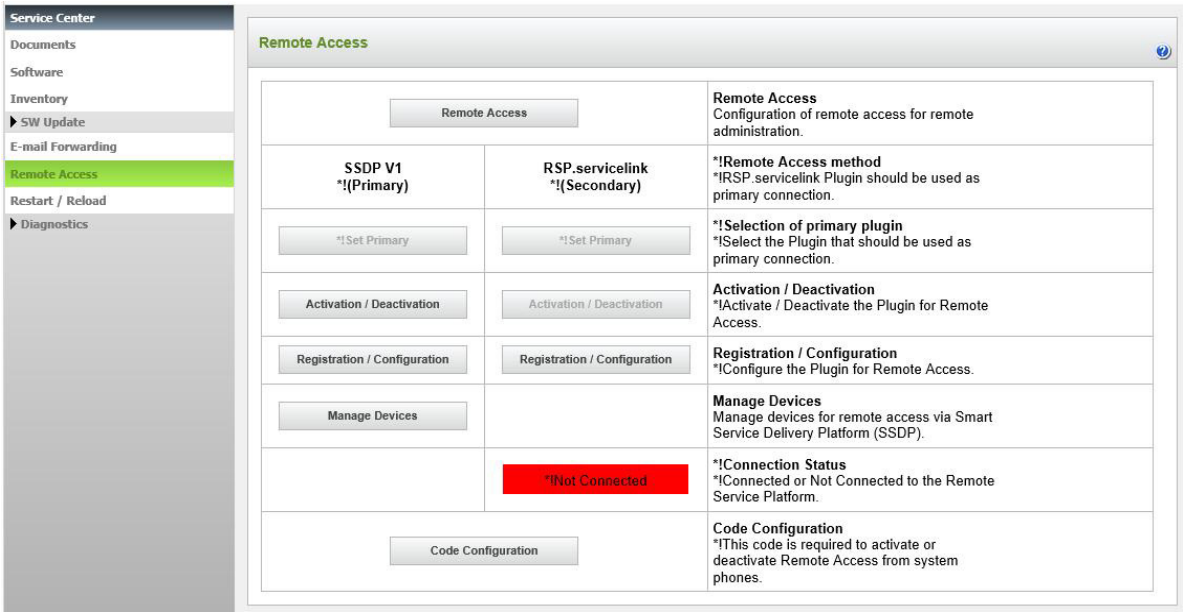
During **Log File Maintenance**, the log files for which the set retention periods have expired are deleted. The default setting for the retention period for log files is 10 days.

21.10 Monitoring the UC Smart

Administrators can query the current status of the UC Smart using the WBM in **Expert** mode.

21.11 Remote Services

Different Remote Services provide remote access to the communication system and the connected components to authorized service technicians. This reduces the cost of maintenance activities, while still providing users with on-site support in solving their problems.



Due to the high bandwidth and the highest level of security, the Remote Service should be given precedence over RSP.servicelink. For more information see RSP.servicelink.

21.11.1 RSP.servicelink

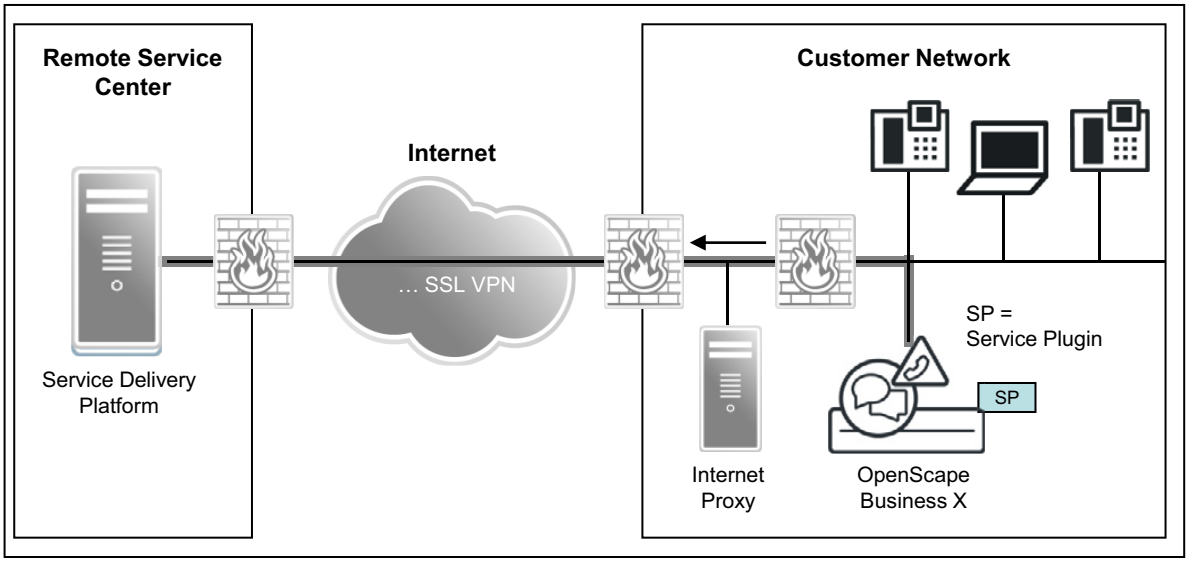
Remote access with RSP.servicelink connectivity (**R**emote **S**ervice **P**latform) offers authorized service technicians of a Remote Service Partner the option to remotely administer the communication system as well as the UC Booster applications comfortably and securely from a distance. To configure RSP.servicelink, only an Internet connection, a web browser, the partner ID and the parner password of the remote service partner are required. RSP.servicelink ensures a broadband connection with high security.

RSP.servicelink is based on OpenVPN technology. It uses the SSL/TSL protocol and encryption and provides the highest level of security with an additional client certificate.The term RSP.servicelink is abbreviated to RSP in the documentation.

RSP offers the following major advantages in combination with OpenScape Business:

- High security through outbound Internet connection
  The entire remote connection setup is always initiated by the communication system. This means that the firewall of the customer network must only allow one HTTP connection to a single address in the Remote Service Center (port 443). Under normal circumstances, no change is required in the security policies of customers or their firewalls, since this port is usually already open for outbound internet call in the firewall of the customer. High security for the customer network is thus guaranteed.
  With RSP, the administrator of the communication system retains control over the remote connection by simply enabling and disabling access. In the case of RSP.servicelink, a client certificate is automatically installed as well.
- High bandwidth
  Due to the broadband Internet connection, diagnostics data can be transmitted much faster, thus increasing the quality of service.
- Simple and cost-effective setup
  The software of the communication system already includes a so-called RSP.servicelink. When activating the service plugin, the partner ID of the Remote Service Partner and also the partner password must be entered.
  Every remote service partner who uses the RSP.servicelink has a separate partner ID.
- Future-proof
  RSP is the basis for future (value-added) services such as automated backups, reporting and monitoring, for example.

Figure: RSP/SSDP - Overview for OpenScape Business X



RSP supports all the usual Web Services Standards, including the Hypertext Transfer Protocol Secure (HTTPS), Simple Object Access Protocol (SOAP) and Extensible Markup Language (XML).

Communication between the client side and the Remote Service Center is always secured with an AES-256-CBC encryption for RSP.servicelink.

Service Plugins

The RSP.servicelink plugin can be enabled or disabled individually.

The RSP.servicelink plugin must be reset after the mainboard has been replaced, for example. Resetting the service plugin deletes the entire RSP configuration and disables the plugin.

INFO: In case the system is not in DTAG mode and the RSP.servicelink plugin is active, it is not possible to change the proxy settings configuration. The **Registration / Configuration button is disabled.**

In DTAG mode, if RSP.servicelink plugin is active, pressing Registration / Configuration button shows directly Proxy Settings page with Abort/Finish buttons. This is also possible from the remote server.

Device Management (Managed Device)

In communication systems without a UC Booster, remote access to further devices (e.g., Xpressions Compact) in the customer LAN can be enabled by configuration on the SIRA side. IP phones can be configured on the SIRA side by using the "Managed Devices" function.

INFO: Remote access to other OpenScape Business communication systems in the customer LAN is not possible. Each OpenScape Business must be configured for remote access.

Activating/Deactivating

The following options are available for activating or deactivating the service plugins:

- Using the **Activation / Deactivation** wizard
  There is a separate activation/deactivation wizard for the RSP service plugins.
- By entering a code at the system telephone (default: activation via *996, deactivation via #996)
  For security reasons, a 4-digit PIN must be entered in addition to the code for the activation and deactivation via a system telephone. The configuration of this PIN is performed in the WBM of the communication system with the **Advanced** profile.

Prerequisites

- Internet access for the communication system or the HTTP proxy in the customer LAN.
- Any existing firewall in the customer LAN must be opened for Registrar:
  - https://188.64.18.51
  - https://188.64.17.51

- Any existing firewall in the customer LAN must be opened for VPN:
  - https://188.64.18.50
  - https://188.64.17.50
- A default router must be specified in the Internet configuration.

> ***INFO:*** In case the system is in DTAG mode during system startup and has internet access without the RSP.serviceplugin being installed and configured, then a script will automatically install, configure and activate RSP.serviceplugin using the PartnerID and password for DTAG (device name will be the MAC address of the system). The script will also be called periodically every 10 minutes (e.g for the case where is no internet access after initial system installation). The script will not activate automatically RSP.serviceplugin in case the user has manually deactivated it.

21.11.2 Remote Access

Remote access can be used by authorized service technicians to access the OpenScape Business X communication systems remotely via an ISDN PSTN or Internet connection. This ensures that support is available when solving administration tasks or performing troubleshooting.

You must enable remote access to activate remote access to the communication system. The following access methods are possible:

- Remote Access via ISDN PSTN connection

  > ***INFO:*** Note that for remote access via an ISDN PSTN connection, longer waiting times may be experienced due to the limited transmission speed.

  To dial in via ISDN, the service technician needs a valid direct inward dialing phone number (**MSN/DID Number**) for the communication system.

  > ***INFO:*** Password for PPP authentication (CHAP password or PAP password) should be changed the first time after installation or migration, otherwise connection will not be established.

  The UC Booster applications (e.g., UC Suite, Open Directory Service, Gate View) can be administered via this remote access if the IP address of the mainboard for the UC Booster is configured as a router (e.g., the default router).
- Remote Access via Internet Connection

INFO: Remote access via an Internet connection presents a higher security risk.

To dial in via the Internet, the service technician needs a special port (**Port Number**) to access the communication system. Port number 10099 is specified by default. When using an external router, port forwarding must be set up in the external router for this port number.
The port number must not be blocked by a possible firewall on the PC of the service technician. Port number selection should therefore be coordinated with the service technician.
The UC Booster Applications (e.g., UC Suite, Open Directory Service, Gate View) cannot be administered via this remote access.

You must disable remote access to block remote access to the communication system.

NOTICE: To prevent unauthorized access to the communication system, remote access must be turned off on completing the remote administration.

Remote maintenance of the communication system is also possible via ISDN X.75 using the Manager E service tool. The access number required for this purpose is configured in Manager E under **Digital Modem (x75)**.

21.11.3 Online User

The Online User enables the remote control, verification and monitoring of OpenStage telephones via a Windows PC. The behavior of an OpenStage telephone is recreated via the Online User on the PC.

In order to communicate with an OpenStage phone, the phone software must have a so-called dongle key.

The following entries must be made via the Online User in order to access an OpenStage telephone:

- OpenStage phone type
- IP address of the OpenStage telephone
- Administrator password of the OpenStage telephone

Details on using the Online User can be obtained from the following documentation: *OpenStage HUSIM Phone Tester User Guide*. Access to this document is available via the intranet portal for technical product documentation at `http://apps.g-dms.com:8081/techdoc/search_en.htm`.

The Manager E service tool provides online users for the remote control, testing and monitoring of OpenStage phones.

22 Configuration Limits and Capacities

The configuration limits and capacities are based on system-specific maximum values and the maximum values for a network.

The maximum values refer to

- the system-specific capacity limits
- the software capacities

22.1 System-Specific Capacity Limits

The configuration limits described here are based on system-specific maximum values for stations and trunks.

NOTICE: For each system configuration, it must be checked whether the rated power output of the native power supply is sufficient or whether an external auxiliary power supply is required (see *OpenScape Business Service Documentation - Power Requirements of a Communication System*).

Maximum values for stations

Stations	Maximum values				
	OpenScape Business				
	X1	X3R X3W	X5R X5W	X8	S
Sum total of all IP, TDM and Mobility stations	30 IP / TDM plus 30 Mobility stations	500	500	500	2000
IP stations					
Total of system phones, SIP stations, adapters, WLANs per communication system	20	500	500	500	2000 (max. 500 SIP stations)
TDM stations					
ISDN stations (S_0 stations) per communication system	4 (2 S_0 on OCCS)	20 (2 S_0 on OCCMR + 2 x STLSX4R) 20 (2 S_0 on OCCM + 2 x STLSX4)	52 (2 S_0 on OCCMR + 6 x STLSX4R) 52 (2 S_0 on OCCM + 6 x STLSX4)	128	–

Stations	Maximum values				
	OpenScape Business				
	X1	X3R X3W	X5R X5W	X8	S
Analog stations per communication system	4 (4 a/b on OCCS)	20 (4 a/b on OCCMR + 2 x SLAV8R) 20 (4 a/b on OCCM + 1 x SLAV16)	52 (4 a/b on OCCMR + 6 x SLAV8R) 68 (4 a/b on OCCM + 4 x SLAV16)	384	–
$U_{P0/E}$ stations (master) per communication system	8 (8 $U_{P0/E}$ on OCCS)	24[1](8 $U_{P0/E}$ on OCCMR + 2 x SLU8R) 24[1] (8 $U_{P0/E}$ on OCCM 2 x SLU8)	56[1] (8 $U_{P0/E}$ on OCCMR + 6 x SLU8R) 56[1] (8 $U_{P0/E}$ on OCCM 6 x SLU8)	384[1]	–
Additional stations via OpenStage Phone Adapter ($U_{P0/E}$ slave phones, analog phones)	8	24 24	56 56	116	–
Cordless phones (DECT phones for the integrated Cordless solution) per communication system	16 (DECT Light)	64 (DECT Light[2]) 	64 (DECT Light[2]) 64 (DECT Light[2]) / 64 (1 x SLC16N)	250	–
Base stations (for the integrated Cordless solution) per communication system	7 (connection to $U_{P0/E}$ on OCCS (DECT Light[2]))	7 (connection to $U_{P0/E}$ on OCCMR + 8 (connection to Up0/E on SLU8NR) (DECT Light[2])) 7 (connection to $U_{P0/E}$ on OCCM + 8 (connection to Up0/E on SLU8NR) (DECT Light[2]))	7 (connection to $U_{P0/E}$ on OCCMR + 8 (connection to Up0/E on SLU8NR) (DECT Light[2])) 7 (connection to $U_{P0/E}$ on OCCM + 8 (connection to Up0/E on SLU8NR) (DECT Light[2])) or 16 (connection to SLC16N)	64 (connection to 4 x SLCN)	–
Mobility User					

Stations	Maximum values				
	OpenScape Business				
	X1	X3R X3W	X5R X5W	X8	S
Mobility Entry: stations per communication system	30	150	150	150	250
myPortal to go (UC Smart): stations per communication system	30	250/50[2]	250/50[3]	250/50[3]	250
myPortal to go (UC Suite): stations per communication system	–	250/100[3]	250/100[4]	250/100[4]	250
Virtual stations (freely configurable)	30	250	250	250	250

1 Depending on the types of phones and the total power requirements of the communication system.
2 1st. value: maximum expansion with UC Booster Server or UC Booster Card/ 2nd. value: maximum expansion with mainboard
3 1st. value: maximum expansion with UC Booster Server / 2nd. value: maximum expansion with UC Booster Card

Maximum values for trunks

Trunks	System Values				
	OpenScape Business				
	X1	X3R X3W	X5R X5W	X8	S
Total of all trunks per communication system	250 (IP and ISDN trunks)	250 (IP, ISDN and analog trunks)	250 (IP, ISDN and analog trunks)	250 (IP, ISDN and analog trunks)	250 (IP trunks) ISDN and analog trunks via gateway
ISDN trunks					
S_0 trunks	4 (2 S_0 on OCCS)	10 (2 S_0 on OCCMR + 2 x STLSX4R) 10 (2 S_0 on OCCM + 2 x STLSX4)	26 (2 S_0 on OCCMR + 6 x STLSX4R) 26 (2 S_0 on OCCM + 6 x STLSX4)	128 (limited by system software)	ISDN trunks via gateway
S_{2M} trunks	–	–	30 (1 x TS2RN) 30 (1 x TS2N)	180 (3 x DIUT2)	ISDN trunks via gateway
CAS trunks	–	–	30 (1 x TCASR-2) 30 (1 x TCAS-2)	180 (3 x TMCAS2)	CAS trunks via gateway

Trunks	System Values				
	OpenScape Business				
	X1	X3R X3W	X5R X5W	X8	S
Analog Trunks					
Analog Trunks	–	8 (2 x TLANI4R) 16 (2 x TLANI8)	24 (6 x TLANI4R) 48 (6 x TLANI8)	120 (15 x TMANI)	Analog trunks via gateway
Info for OpenScape Business X3/X5/X8: A total of up to 250 IP, ISDN and analog trunks can be used. Examples for the maximum configuration: • OpenScape Business X3R: 2 x TLANI4R (= 8 x a/b) = 8 analog trunks + 242 IP trunks • OpenScape Business X3W: 2 x STLSX4 (= 8 x S_0) + 2 x S_0 on OCCM = 20 ISDN trunks + 230 IP trunks • OpenScape Business X5W: 1 x TS2 (= 1 x S_{2M}) + 5 x STLSX4 (= 20 x S_0) + 2 x S_0 on OCCM = 74 B channels + 176 IP trunks • OpenScape Business X8: 3 x DIUT2 (= 6 x S_{2M}) = 180 B channels + 70 IP trunks					

Maximum values for resources

Resource	System Values				
	OpenScape Business				
	X1	X3R X3W	X5R X5W	X8	S
DSP channels (Gateway channels) ***Info***: Connections between IP and TDM phones/trunks are "gateway connections"; each gateway connection requires one DSP channel (gateway channel).					
DSP channels with the G.711 codec enabled	8 (on OCCS)	8 (on OCCMR/ OCCM)	8 (on OCCMR/ OCCM)	8 (on OCCL)	–
	8 (on OCCS)	48 (8 on OCCMR/OCCM + 40 on OCCB1)	48 (8 on OCCMR/OCCM + 40 on OCCB1)	128 (8 on OCCL + 120 on OCCB3)	–
DSP channels with the G.711 and G.729 codecs enabled	8 (on OCCS)	8 (on OCCMR/ OCCM)	8 (on OCCMR/ OCCM)	8 (on OCCL)	–
	8 (on OCCS)	40 (8 on OCCMR/OCCM + 32 on OCCB1)	40 (8 on OCCMR/OCCM + 32 on OCCB1)	104 (8 on OCCL + 96 on OCCB3)	–

Resource	System Values				
	OpenScape Business				
	X1	X3R X3W	X5R X5W	X8	S
DSP channels with the G.711 codec enabled and the SPE feature enabled	6 (on OCCS)	6 (on OCCMR/ OCCM)	6 (on OCCMR/ OCCM)	6 (on OCCL)	–
	6 (6 on OCCS)	38 (6 on OCCMR/OCCM + 32 on OCCB1)	38 (6 on OCCMR/OCCM + 32 on OCCB1)	102 (6 on OCCL + 96 on OCCB3)	–
DSP channels with the G.711 and G.729 codecs enabled and the SPE feature enabled	6 (on OCCS)	6 (on OCCMR/ OCCM)	6 (to OCCMR/ OCCM)	6 (on OCCL)	–
	6 (6 on OCCS)	31 (6 on OCCMR/OCCM + 25 on OCCB1)	31 (6 on OCCMR/OCCM + 25 on OCCB1)	81 (6 on OCCL + 75 on OCCB3)	–
T.38 channels (number of T.38 faxes to be simultaneously transmitted and received)	3 on OCCS	3 on OCCMR/ OCCM 6 on OCCMR/ OCCM + OCCB1 12 on OCCMR/ OCCM + OCCB3	3 on OCCMR/ OCCM 6 on OCCMR/ OCCM + OCCB1 12 on OCCMR/ OCCM + OCCB3	3 on OCCMR/ OCCM 6 on OCCMR/ OCCM + OCCB1 12 on OCCMR/ OCCM + OCCB3	T.38 fax channels via Gateway
MEB (Media Extension Bridge) channels	30	30	30	30	60
Music on Hold (MOH)					
MOH channels (G.711, G.729)	0 to 4 (depending on configuration)	0 to 4 (depending on configuration)	0 to 4 (depending on configuration)	0 to 4 (depending on configuration)	32
PPP Channels	8	8	8	8	–
DTMF					
DTMF receiver	16	16	16	16	Per call via ITSP

22.2 Software Capacities

The maximum values described here are based on the software capacities of OpenScape Business.

Table: Topic: Connection to Service Provider

Topic: Connection to Service Provider	Maximum values						
	OpenScape Business					UC Booster	
	X1	X3R X3W	X5R X5W	X8	S	UC Booster Server	UC Booster Card
ITSP (Internet Telephony Service Provider) connection:							
ITSP trunks per communication system	30	60[1]	60[1]	60[1]	180	–	–
Simultaneously activated ITSPs per communication system	8	8	8	8	8	–	–
Routes:							
Routes per communication system	16	16	16	16	16	–	–
Overflow routes per route	1	1	1	1	1	–	–

1 If> 60 trunks are required, OpenScape Business S must be used as networked ITSP gateway

Table: Topic: Stations

Topic: Station	Maximum values						
	OpenScape Business					UC Booster	
	X1	X3R X3W	X5R X5W	X8	S	UC Booster Server	UC Booster Card
Classes of Service:							
Classes of Service per communication system	15	15	15	15	15	–	–
Station number/DID number:							
Digits per station number/DID number	16 (default setting = 3)	16 (default setting = 3)	16 (default setting = 3)	16 (default setting = 3)	16 (default setting = 3)	–	–

Table: Topic: UC Smart

Topic UC Smart	Maximum values						
	OpenScape Business					UC Booster	
	X1	X3R X3W	X5R X5W	X8	S	UC Booster Server	UC Booster Card
Maximum number of licensed UC Smart users (Sum of myPortal Smart, myPortal to go, myPortal for OpenStage, Application Launcher, OpenScape Business Attendant, OpenScape Business BLF and 3rd Party WSI Clients)	30	50	50	50	250	250	150
myPortal Smart	30	50	50	50	250	250	150
Simultaneous WSI sessions	60	100	100	100	500	500	300
Call journal:							
Call journal entries per user	100	100	100	100	100	100	100
Voicemail box:							
Voicemail boxes per communication system	30	320	320	320	1500	500	320
Max. recording length per call	2 minutes	2 minutes	2 minutes	2 minutes	2 minutes	2 minutes	2 minutes
Total recording duration per communication system	32 hours	32 hours	32 hours	32 hours	32 hours	32 hours	32 hours
Messages per voicemail box	100	100	100	100	100	100	100
Simultaneous calls (incoming and outgoing)	10	10	10	10	10	10	10
Presence status:							
Status per Smart subscriber UC	9	9	9	9	9	9	9
Voicemail announcements per presence status	1	1	1	1	1	1	1
Favorites:							
Favorite entries per UC Smart user	100	100	100	100	100	100	100
Favorite groups per UC Smart user	10	10	10	10	10	10	10

Table: Topic: UC Suite

Topic: UC Suite	Maximum values						
	OpenScape Business					UC Booster	
	X1	X3R X3W	X5R X5W	X8	S	UC Booster Server	UC Booster Card
Maximum number of simultaneously active UC Suite clients (Sum of myPortal for Desktop, myPortal for Outlook, myPortal for OpenStage, Application Launcher, myAttendant, myAgent)	–	–	–	–	1500	500	150
myPortal for Desktop	–	–	–	–	1500	500	150
myPortal for Outlook	–	–	–	–	1500	500	150
myAttendant	–	–	–	–	20	20	20
Call journal (myPortal for Desktop and myPortal for Outlook):							
Archiving duration in the UC clients	–	–	–	–	30 days (default setting = 30 days)		
Archiving duration in the communication system	–	–	–	–	365 days (default setting = 30 days)		
Call journal entries	–	–	–	–	Unrestricted		
Recording calls/conferences:[1]							
Recording length per call/conference	–	–	–	–	Limited by the length of the call/ conference		
Application-controlled conferences:							
Simultaneous UC conferences per communication system	–	–	–	–	10	5	5
Participants per conference	–	–	–	–	18	16	16
External participants per conference	–	–	–	–	15	15	15
Conference channels	–	–	–	–	40 for Meet-Me and Ad Hoc	20 for Meet-Me and Ad Hoc	20 for Meet-Me and Ad Hoc
External database connectivity (LDAP, SQL, etc.):							
External database connections per communication system	–	–	–	–	10	10	10
LDAP connection of the system telephones	See the operating instructions of the system telephones					–	–
LDAP usage via UC clients (myAttendant, myPortal for Desktop, etc.)	–	–	–	–	Every client can use the central LDAP connection of the communication system		
SQL usage via UC clients (myAttendant, myPortal for Desktop, etc.)	–	–	–	–	Every client can use the central SQL connection of the communication system		

Topic: UC Suite	Maximum values						
	OpenScape Business					UC Booster	
	X1	X3R X3W	X5R X5W	X8	S	UC Booster Server	UC Booster Card
Voicemail box:[1]							
Voicemail boxes per communication system	–	–	–	–	1500	500	150
Recording length	–	–	–	–	15 minutes per call (1 minute of voice corresponds to approx. 1 MB of storage space)		
Recording length up to which voicemail messages can be forwarded by email	–	–	–	–	Approx. 10 minutes		
Simultaneous calls (incoming and outgoing)	–	–	–	–	30	30	30
Fax box:[1]							
Fax boxes per communication system	–	–	–	–	1500	500	150
Fax length in pages	–	–	–	–	500 (1 standard fax (2 DIN A4 pages) corresponds to approx. 48 KB of storage space)		
Faxes to be simultaneously sent and received	–	–	–	–	8	8	8
Merge fax recipients	–	–	–	–	Unrestricted		
Fax box groups per communication system	–	–	–	–	60	60	60
Stations per fax box group	–	–	–	–	10	10	10
Announcements:[1]							
Announcements per UC Suite subscriber	–	–	–	–	1 greeting announcement, 1 name announcement, 1 presence status based announcement and 1 announcement for the personal AutoAttendant		
Presence status:							
Status per UC Suite subscriber	–	–	–	–	9	9	9
Voicemail announcements per presence status	–	–	–	–	1	1	1
Multi-user chat:							
Internal communication partner	–	–	–	–	Unrestricted		
External XMPP communication partner	–	–	–	–	1	1	1

Topic: UC Suite	Maximum values						
	OpenScape Business					UC Booster	
	X1	X3R X3W	X5R X5W	X8	S	UC Booster Server	UC Booster Card
AutoAttendant:							
Personal AutoAttendant	–	–	–	–	20	20	20
Company AutoAttendant	–	–	–	–	1	1	1

1 The total recording duration for voice announcements, voicemails, recorded voice calls and faxes depends on the hard disk capacity in the communication system. There are no individual limits per subscriber.
Example for a 160 GB hard drive: the storage volume of the partition for recording voice announcements, voicemails, voice calls and faxes is 20 GB. This corresponds to a total recording time of about 20000 minutes.

Table: Topic: Functions at the Telephone

Topic: Functions at the Telephone	Maximum values						
	OpenScape Business					UC Booster	
	X1	X3R X3W	X5R X5W	X8	S	UC Booster Server	UC Booster Card
Caller list:							
Caller lists per communication system	650	650	650	650	1300	–	–
Entries per caller list	10	10	10	10	10	–	–
Saved digits per entry	25-digit phone number and seizure code					–	–
Direct station select keys (DSS keys):							
Key modules per communication system	30	250	250	250	250	–	–
Key modules per telephone	2	2	2	2	2	–	–
Keys per key module	12 for OpenStage Key Module 18 for OpenStage Key Module 15					–	–
Busy Lamp Fields (BLF) per communication system	12	12	12	12	12	–	–
Keys per Busy Lamp Field	90	90	90	90	90	–	–
Individual Speed Dialing (ISD):							
Entries in the KWI pool per communication system	2000	2000	2000	2000	2000	–	–
Entries per station	10	10	10	10	10	–	–
Digits per entry	25-digit phone number and seizure code					–	–
System Speed Dialing (SSD):							
Entries per communication system	8000	8000	8000	8000	8000	–	–
Character length of name	16	16	16	16	16	–	–
Digits per entry	25-digit phone number and seizure code					–	–
Redialing:							

Topic: Functions at the Telephone	Maximum values						
	OpenScape Business					UC Booster	
	X1	X3R X3W	X5R X5W	X8	S	UC Booster Server	UC Booster Card
Entries per telephone with display	3 for optiPoint 410/420 and OpenStage 20E/20/20G/ 40/40G 10 for OpenStage 15 In the OpenStage 60/60G/80/80G, a max. of 30 entries each can be used for the "Answered", "Missed" and "Dialed" call lists					–	–
Entries per telephone without display	1	1	1	1	1	–	–
Saved digits per entry	25-digit phone number and seizure code					–	–
Call waiting/call waiting tone							
Waiting callers per telephone	16	16	16	16	16	–	–
Parking:							
Park positions per communication system	10	10	10	10	10	–	–
Callback calls:							
Callback entries per telephone	5	5	5	5	5	–	
Advisory messages/Message texts:							
Advisory messages per communication system	250	250	250	250	250	–	–
Message texts per communication system	150	150	150	150	150	–	–
Configurable advisory messages + message texts per communication system	10 + 10	10 + 10	10 + 10	10 + 10	10 + 10	–	–
Character length of a configurable advisory message/message text	24	24	24	24	24	–	–
Received advisory messages/message texts per telephone with display	5	5	5	5	5	–	–
Received advisory messages/message texts per telephone without display	1	1	1	1	1	–	–
Ringing group on:							
Stations included	5	5	5	5	5	–	–
Call Forwarding (CF):							
FWD destinations per telephone	4	4	4	4	4	–	–
Digits per external CFW destination	25-digit phone number and seizure code					–	–
Chained FWD destinations					5	–	
System-controlled conferences:							

Topic: Functions at the Telephone	Maximum values						
	OpenScape Business					UC Booster	
	X1	X3R X3W	X5R X5W	X8	S	UC Booster Server	UC Booster Card
Simultaneous system conferences per communication system	10	10	10	10	8	–	–
Participants per conference	8	8	8	8	9	–	–
External participants per conference	7	7	7	7	7	–	–
Conference channels	32	32	32	32	40	–	–
Entrance Telephone/Door Opener:							
Connections via a/b interfaces per communication system	4	4	4	4	–	–	–
Digits per code entry	5	5	5	5	–	–	–
Trunk queuing:							
Simultaneous entries per communication system	32	32	32	32	–	–	–

Table: Topic: Working in a Team (Groups)

Topic: Working in a Team (Groups)	Maximum values						
	OpenScape Business					UC Booster	
	X1	X3R X3W	X5R X5W	X8	S	UC Booster Server	UC Booster Card
Call pickup groups:							
Call pickup groups per communication system	32	32	32	32	120	–	–
Stations per call pickup group	32	32	32	32	32	–	–
Group calls, hunt groups, Basic MULAPs, Executive MULAPs, Team groups, Top groups and voicemail groups:							
Total of group calls, hunt groups, Basic MULAPs, Executive MULAPs and voicemail groups per communication system	800	800	800	800	800	–	–
Total number of Team groups and Top groups per communication system	500	500	500	500	500	–	–
Subscribers per group call, hunt group, Basic MULAP	20	20	20	20	20	–	–
Subscribers per Executive MULAP, Team group, Top group	10	10	10	10	10	–	–
Stations per voicemail group	20	20	20	20	20	–	–
MULAP keys per telephone	10	10	10	10	10	–	–
Fax box groups:							

Topic: Working in a Team (Groups)	Maximum values						
	OpenScape Business					UC Booster	
	X1	X3R X3W	X5R X5W	X8	S	UC Booster Server	UC Booster Card
Fax box groups per communication system: see Table: Topic: UC Suite							
Internal paging:							
Simultaneous announcements per communication system	1	1	1	1	6	–	–
Recipients of the announcement	20	20	20	20	20	–	–
UCD groups:							
UCD groups per communication system	60	60	60	60	60	–	–
Announcements per UCD group	7	7	7	7	7	–	–
Priority levels per UCD group	10	10	10	10	10	–	–
Queued calls per UCD group	30	30	30	30	30	–	–
UCD agents:							
UCD agent IDs per communication system	330	330	330	330	330	–	–
Simultaneously active UCD agents per communication system	64	64	64	64	64	–	–
Announcements for UCD:							
Number of callers, per communication system, for whom an announcement can be simultaneously played	8	8	8	8	8	–	–

Table: Topic: Call Routing

Topic: Call Routing	Maximum values						
	OpenScape Business					UC Booster	
	X1	X3R X3W	X5R X5W	X8	S	UC Booster Server	UC Booster Card
Toll restriction:							
Allowed lists	6	6	6	6	6	–	–
Denied lists	6	6	6	6	6	–	–
Allowed list, short (10 entries)	5	5	5	5	5	–	–
Allowed list, long (100 entries)	1	1	1	1	1	–	–
Short Denied list (10 entries)	5	5	5	5	5	–	–
Long Denied list (50 entries)	1	1	1	1	1	–	–
Number of characters in list entries	32	32	32	32	25	–	–
Least Cost Routing LCR):							

Topic: Call Routing	Maximum values						
	OpenScape Business					UC Booster	
	X1	X3R X3W	X5R X5W	X8	S	UC Booster Server	UC Booster Card
Dialed/Verified digits	24	24	24	24	24	–	–
Dial Plans	1000	1000	1000	1000	1000	–	–
Route tables	254	254	254	254	254	–	–
Routes per routing table	16	16	16	16	16	–	–
Dial rules per route	254	254	254	254	254	–	–
Digits per dial rule	40	40	40	40	40	–	–
Night service:							
Authorized stations per communication system	5	5	5	5	5	–	–
E911 Emergency Call Service (for the U.S. only):							
Digits per LIN (Location Identification Number)	16	16	16	16	16	–	–
Hotline after Timeout/Hotline:							
Hotline destinations per communication system	6	6	6	6	6	–	–
CON groups:							
CON groups per communication system	64	64	64	64	64	–	–

Table: Topic: Attendants

Topic: Attendants	Maximum values						
	OpenScape Business					UC Booster	
	X1	X3R X3W	X5R X5W	X8	S	UC Booster Server	UC Booster Card
myAttendant: see Table: Topic: UC Suite							
AutoAttendant (UC Smart): see Table: Topic: UC Smart							
AutoAttendant (UC Suite): see Table: Topic: UC Suite							
AutoAttendant (Xpressions Compact):							
Personal AutoAttendant	–	30 with IVMP4R / 100 with IVMS8NR 30 with IVMP4 / 100 with IVMS8N	100 with IVMNL	–		–	–

Topic: Attendants	Maximum values						
	OpenScape Business					UC Booster	
	X1	X3R X3W	X5R X5W	X8	S	UC Booster Server	UC Booster Card
OpenScape Business Attendant:							
OpenScape Business Attendants per communication system	8	8	8	8	8	8	–
OpenScape Business BLF per communication system	30	50	50	50	250	250	150

Table: Topic: Multimedia Contact Center

Topic: Multimedia Contact Center	Maximum values						
	OpenScape Business					UC Booster	
	X1	X3R X3W	X5R X5W	X8	S	UC Booster Server	UC Booster Card
myAgent:							
Licensable agents	–	–	–	–	192	192	192
Simultaneously active agents	–	–	–	–	64	64	64
myReports	–	–	–	–	1	1	1
Queues:							
Queues per communication system	–	–	–	–	50	50	50
Wrap up:							
Wrap up codes per queue	–	–	–	–	Unrestricted	Unrestricted	Unrestricted

Table: Topic: Mobility

Topic: Mobility	Maximum values						
	OpenScape Business					UC Booster	
	X1	X3R X3W	X5R X5W	X8	S	UC Booster Server	UC Booster Card
Teleworker workplaces:							
Teleworker workplaces via VPN per communication system	10	10	10	10	Possible via external router	–	–
Mobility Stations:							

Topic: Mobility	Maximum values						
	OpenScape Business					UC Booster	
	X1	X3R X3W	X5R X5W	X8	S	UC Booster Server	UC Booster Card
Mobility Entry: stations per communication system	30	150	150	150	250	250	150
myPortal to go (UC Smart): stations per communication system	30	50	50	50	250	250	150
myPortal to go (UC Suite): stations per communication system	–	–	–	–	250	250	100

Table: Topic: Security

Topic: Security	Maximum values						
	OpenScape Business					UC Booster	
	X1	X3R X3W	X5R X5W	X8	S	UC Booster Server	UC Booster Card
VPN:							
VPN tunnel	256	256	256	256	Possible via external VPN router	–	–
VPN rules	634	634	634	634		–	–
Individual lock code:							
Digits per phone lock code	5	5	5	5	5	–	–
Permitted characters	0 through 9	0 through 9	0 through 9	0 through 9	0 through 9	–	–

Table: Topic: Networking OpenScape Business

Topic: Networking OpenScape Business[1]	Maximum values
Networking OpenScape Business X3R/X3W, OpenScape Business X5R/X5W, OpenScape Business X8, OpenScape Business S and OpenScape Business UC Booster Server:	
Networked communication systems (nodes)	8 (with UC Suite) / 32 (without UC Suite)
Stations in the network	1000

1 Project-specific releases can be requested for networking requirements beyond the configuration limits listed here. Please also refer to the current Sales Release.

Table: Topic: Auxiliary Equipment

Topic: Auxiliary Equipment	Maximum values						
	OpenScape Business					UC Booster	
	X1	X3R X3W	X5R X5W	X8	S	UC Booster Server	UC Booster Card
OpenStage Gate View:							
Cameras per communication system	–	–	–	–	8 (license-dependent)	8 (license-dependent)	2 (license-dependent)
Telephones (OpenStage HFA 60, 60 G, 80, 80 G, 80 E) displaying the camera image of the communication system	–	10 (with OCAB) 20 (with Application Server)			20	–	–
iPhone apps or web clients to display the camera image per communication system	–	10 (with OCAB) 20 (with Application Server)			20	–	–

Table: Topic: Application Connectivity

Topic: Application Connectivity	Maximum values						
	OpenScape Business					UC Booster	
	X1	X3R X3W	X5R X5W	X8	S	UC Booster Server	UC Booster Card
CSTA:							
CSTA links via CSP per communication system	–	–	–	–	4	4	4
TAPI 170 middleware server	–	–	–	–	1	1	1

Table: Topic: Accounting

Topic: Accounting	Maximum values						
	OpenScape Business					UC Booster	
	X1	X3R X3W	X5R X5W	X8	S	UC Booster Server	UC Booster Card
Call Detail Recording Central:							
Entries in the call data buffer per communication system	20000	20000	20000	20000	20000	–	–
Account Code (ACCT):							
Account code entries per communication system	1000	1000	1000	1000	1000	–	–
Verifiable digits per Acc. code	11	11	11	11	11	–	–
Permitted characters	0 through 9	0 through 9	0 through 9	0 through 9	0 through 9	–	–

23 Appendix

This appendix contains reference information such as the supported languages, standards, configuration limits and capacities, Euro-ISDN features, codes for enabling and disabling features, feature codes using DTMF and the IP protocols and port numbers used.

23.1 Supported Standards

This section contains information on the supported standards.

Ethernet

- RFC 894 Ethernet II Encapsulation
- IEEE 802.1Q Virtual LANs
- IEEE 802.2 Logical Link Control
- IEEE 802.3u 100BASE-T
- IEEE 802.3ab Gigabit Ethernet
- IEEE 802.3X Full Duplex Operation

IP Routing

- RFC 768 UDP
- RFC 791 IP
- RFC 792 ICMP
- RFC 793 TCP
- RFC 2822 Internet Message Format
- RFC 826 ARP
- RFC 2131 DHCP
- RFC 1918 IP Addressing
- RFC 1332 The PPP Internet Protocol Control Protocol (IPCP)
- RFC 1334 PPP Authentication Protocols
- RFC 1618 PPP over ISDN
- RFC 1661 The Point-to-Point Protocol (PPP)
- RFC 1877 PPP Internet Protocol Control Protocol
- RFC 1990 The PPP Multilink Protocol (MP)
- RFC 1994 PPP Challenge Handshake Authentication Protocol (CHAP)
- RFC 2516 A Method for Transmitting PPP Over Ethernet (PPPoE)
- RFC 3544 IP Header Compression over PPP

NAT

- RFC 2663 NAT

IPSec

- RFC 2401 Security Architecture for IP
- RFC 2402 AH - IP Authentication Header
- RFC 2403 IPsec Authentication - MD5
- RFC 2404 IPsec Authentication - SHA-1
- RFC 2405 IPsec Encryption - DES
- RFC 2406 ESP - IPsec encryption
- RFC 2407 IPsec DOI
- RFC 2408 ISAKMP
- RFC 2409 IKE
- RFC 2410 IPsec encryption - NULL
- RFC 2411 IP Security Document Roadmap
- RFC 2412 OAKLEY

SNMP

- RFC 1213 MIB-II

QoS

- IEEE 802.1p Priority Tagging
- RFC 1349 Type of Service in the IP Suite
- RFC 2475 An Architecture for Differentiated Services
- RFC 2597 Assured Forwarding PHB Group
- RFC 3246 An Expedited Forwarding PHB (Per-Hop Behavior)

Services

- RFC 2597 Assured Forwarding PHB Group
- RFC 3246 An Expedited Forwarding PHB (Per-Hop Behavior)

Codecs

- G.711
- G.729

VoIP over SIP

- RFC 2198 RTP Payload for Redundant Audio Data
- RFC 2327 SDP Session Description Protocol
- RFC 2617 HTTP Authentication: Basic and Digest Access Authentication
- RFC 2782 DNS RR for specifying the location of services (DNS SRV)
- RFC 2833 RTP Payload for DTMF Digits, Telephony Tones and Telephony Signals
- RFC 3261 SIP Session Initiation Protocol
- RFC 3262 Provisional Response Acknowledgement (PRACK) Early Media
- RFC 3263 SIP Locating Servers

- RFC 3264 An Offer/Answer Model with the Session Description Protocol
- RFC 3310 HTTP Digest Authentication
- RFC 3311 Session Initiation Protocol (SIP) UPDATE Method
- RFC 3323 A Privacy Mechanism for the Session Initiation Protocol (SIP)
- RFC 3325 Private Extensions to the Session Initiation Protocol (SIP) for Asserted Identity within Trusted Networks
- RFC 3326 The Reason Header Field for the Session Initiation Protocol (SIP)
- RFC 3489 STUN - Simple Traversal of User Datagram Protocol (UDP) Through Network Address Translators (NATs)
- RFC 3515 The Session Initiation Protocol (SIP) Refer Method
- RFC 3550 RTP: Transport Protocol for Real-Time Applications
- RFC 3551 RTP Profile for Audio and Video Conferences with Minimal Control
- RFC 3581 An Extension to the Session Initiation Protocol (SIP) for Symmetric Response Routing
- RFC 3891 The Session Initiation Protocol (SIP) Replaces Header

XMPP

- RFC 3920 Extensible Messaging and Presence Protocol (XMPP): Core
- RFC 3921 Extensible Messaging and Presence Protocol (XMPP): Instant Messaging and Presence

Other

- RFC 959 FTP
- RFC 1305 NTPv3
- RFC 1951 DEFLATE

23.2 Euro-ISDN Features

The Euro-ISDN features can be used at every Euro-ISDN port if the available hardware (phone or ISDN card, for instance) is appropriately configured. The features are either available permanently in the Central Office or activated/ deactivated with codes.

The availability of features depends on the network provider. Some of the named features are subject to charges.

Topic	Explanation
Multiple Subscriber Number (MSN)	Every point-to-multipoint connection can be assigned several phone numbers. The user can assign these phone numbers to the individual terminals directly at the terminals.
Calling Line Identification Presentation (CLIP)	The actual phone number is transmitted to the called station and appears, for example, on the phone's display or in the caller list if the call is not answered. Incorrect phone numbers cannot be transmitted. Direct inward dialing from TC systems cannot be checked, however. Phone number transmission can be suppressed on a case-by-case basis or for all calls.
Calling Line Identification Restriction (CLIR)	Phone number transmission can also be deactivated either permanently or on a case-by-case basis. If deactivated, phone numbers are only displayed at specially defined B stations (emergency help lines, police, fire department).
Malicious Call Identification (MCID)	The called party can have an anonymous caller traced by the attendant console, even if phone number transmission is deactivated. A charge is applied for this feature.
Terminal Portability (TP)	This feature lets you move the ISDN phone you are using and plug it into a different ISDN jack without interrupting an ongoing call. You must park the ongoing call before you move the ISDN phone.
Subaddressing (SUB)	This function is subject to an additional charge and can be used in addition to the normal phone number. Subaddressing lets you operate a dialable phone (for example, a program on the PC) depending on the caller.
User to User Signaling (UUS)	Information can be exchanged over the D channel during connection setup and clear-down. Transmission is possible in both directions.
Closed User Group (CUG)	If you activate this feature, no calls are possible outside the user group (apart from the emergency numbers 110 and 112). External callers can also be blocked.
Call Forwarding Busy (CFB)	This call forwarding variant routes calls on busy to an arbitrary available phone. Call forwarding is performed in the attendant console. This leaves both B channels free.
Call Forwarding Unconditional (CFU)	This call forwarding variant routes calls immediately to an arbitrary available phone. Call forwarding is performed in the attendant console. This leaves both B channels free.
Call Forwarding No Reply (CFNR)	This call forwarding variant routes calls after 20 seconds (if the destination cannot be reached) to an arbitrary available telephone. Call forwarding is performed in the attendant console. This leaves both B channels free.
Call waiting (CW)	A second caller is signaled during an ongoing connection. The caller meanwhile hears the ringback tone. The camp-on connection can be accepted, declined or simply ignored.

Topic	Explanation
Toggle (Hold = Call Hold)	The Consultation feature lets you set up a second connection while another connection is already ongoing. Switching back and forth between two connections is known as toggling. The party on hold cannot overhear the other active call.
Three Party Service (3-PTY)	Two existing connections can be joined together. A three-party conference can be conducted by three subscribers.
Completion of Calls to Busy Subscriber (CCBS; automatic callback on busy)	You can activate this feature if a station called is busy. You hear a signal as soon as this station's port is free. The connection is cleared down by replacing the handset.
Advice of Charge (End) (AOCE)	You can program the application to display call charges at the end of a call. This does not take account of any discounts or tariffs.
Advice of Charge (During) (AOCD)	You can program the application to display call charges during a call. This does not take account of any discounts or tariffs.

23.3 Used Ports

The OpenScape Business system components use different ports, which may need to be opened in the firewall as required. For the ports of the web-based clients (e.g., myPortal to go), port forwarding must be configured in the router.

INFO: The ports identified with "O" in the list below are optional, i.e., are not permanently open in the firewall (e.g., the TFTP port is open only when Gate View is activated).

Description	TCP	UDP	Port number	OpenScape Business X	UC Booster Card	OpenScape Business S	UC Booster Server
System components							
Admin Portal (https)	X		443	X	X	X	X
CAR Update Registration	X		12061	X		X	
CAR Update Server	X		12063	X		X	
CLA	X		61740	O		O	O
CLA Auto Discovery		X	23232	X		X	X
Csta Message Dispatcher (CMD)	X		8900		X	X	X
CSTA Protocol Handler (CPH)	X		7004	X		X	
Csta Service Provider (CSP)	X		8800		X	X	X

Description	TCP	UDP	Port number	OpenScape Business X	UC Booster Card	OpenScape Business S	UC Booster Server
DHCP		X	67	X			
DLI	X		18443	X		X	X
DLSC	X		8084	X		X	X
DNS	X	X	53	X			
FTP	X		21	O		O	
FTP Passive	X		40000:40040	O		O	
Gate View	X		8000:8010		O	O	O
HFA	X		4060	X		X	
HFA Secure	X		4061	X		X	
JSFT	X		8771		X	X	X
JSFT	X		8772		X	X	X
LAS Cloud Service	X		8602	X			
LDAP server	X		389		X	X	X
Manager E	X		7000	X			
MEB SIP	X		15060		X		X
NAT traversal (NAT-T)		X	4500	X			
NTP		X	123	X			
Openfire Admin (https)	X		9091		X	X	X
OSBiz Multisite	X		8778		X	X	X
OSBiz myReports (http)	X		8101		X	X	X
OsBiz status server	X		8808	X		X	X
OSBiz user portal	X	X	8779		X	X	X
Postgres	X		5432	X	X	X	X
RTP (embedded)		X	29100:30530	X	X	X	X
RTP (server)		X	29100:30888	X	X	X	X
SIP (server)	X	X	5060	X		X	
SIP TLS SIPQ (server)	X		5061	X		X	
SIP TLS Subscriber (server)	X		5062	X		X	
SNMP (Get/Set)		X	161	X		X	
SNMP (traps)		X	162	X		X	
SSDP	X		3011	X		X	X
TFTP		X	69		O	O	O
VSL	X		8770		X	X	X
Webadmin for Clients	X		8803	X	X	X	X

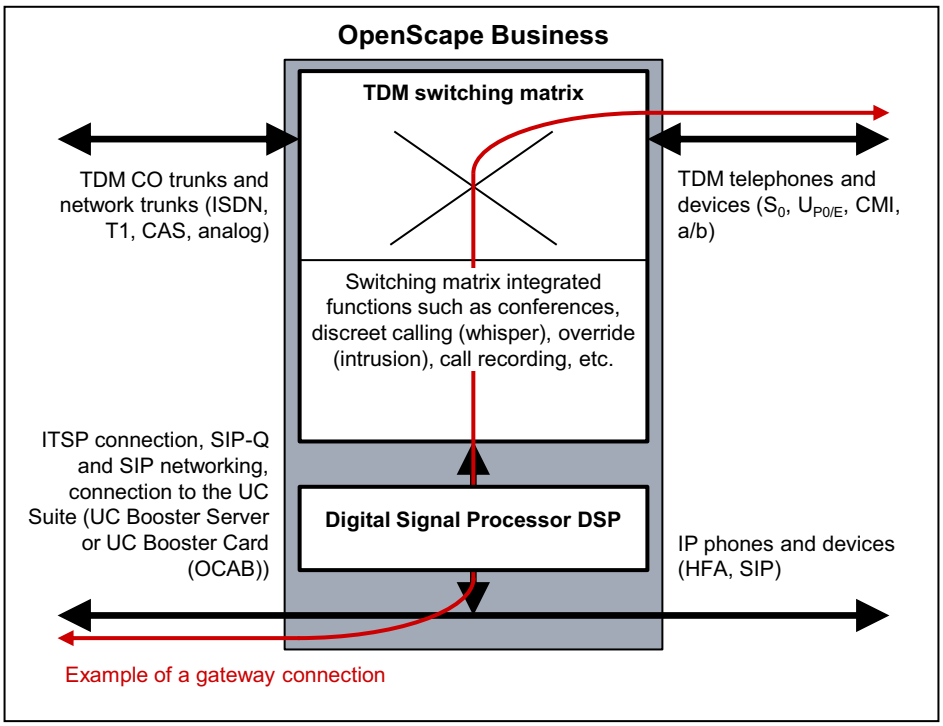
Description	TCP	UDP	Port number	OpenScape Business X	UC Booster Card	OpenScape Business S	UC Booster Server
XMPP Connection Manager	X		5262		X	X	X
XMPP server	X		5269		X	X	X
Web-based clients							
Web-based clients (http)	X		8801	X	X	X	X
Web-based clients (https)	X		8802	X	X	X	X

INFO: For security reasons, we recommend that only https be used for the web-based clients and that port forwarding be set up from external TCP/443 to internal TCP/8802.

23.4 Project Planning of DSP Channels for the OpenScape Business X3/X5/X8 Communication Systems

Connections between IP and TDM phones/trunks are "gateway connections"; each gateway connection requires one DSP (Digital Signal Processor) channel. In addition, DSP channels are required on activating the Signaling And Payload Encryption (SPE) feature.

No DSP channels are required for pure TDM connections and IP-only connections.



The mainboards of the OpenScape Business X3/X5/X8 communication systems provide a maximum eight DSP channels.

If the DSP channels of a mainboard are not sufficient, additional channels can be provided by plugging in a Voice Channel Booster Card (OCCB1 or OCCB3 subboard):

- OCCB1 provides up to 40 additional DSP channels.
- OCCB3 provides a maximum of 120 additional DSP channels.

The number of DSP channels available for gateway connections is reduced by the use of the G.729 codec and when using Signaling and Payload Encryption (SPE).

Ultimately, the number of simultaneous gateway connections (simultaneous voice connections with IP-TDM transition) determines whether and which OCCB subboard should be used.

In the case of UC-Suite conferencing and IP Phones, an OpenScape Business X3/X5/X8 communications system can include up to eight DSP channels; one DSP channel is reserved for the Music on Hold channel, while seven DSP channels can be allocated for the IP phones (one DSP channel per IP phone). In addition, one DSP channel is reserved for the configuration of the Signaling and Payload Encryption (SPE). When the available DSP channels are exhausted, the number of DSP channels can be increased with the use of the corresponding OCCB cards (OCCB1 or OCCB3 as stated previously).

> ***INFO:*** For more details on the maximum DSP channels available on the mainboard and the OCCB subboards, see System-Specific Capacity Limits.

The undersizing of DSP channels can result in DSP bottlenecks that typically manifest themselves through busy states when setting up connections (busy tone during call setup, display showing `Not currently possible`).

When a DSP bottleneck occurs, an entry is made in the event log file of the communication system.

The following measures should be taken if DSP bottlenecks frequently occur:

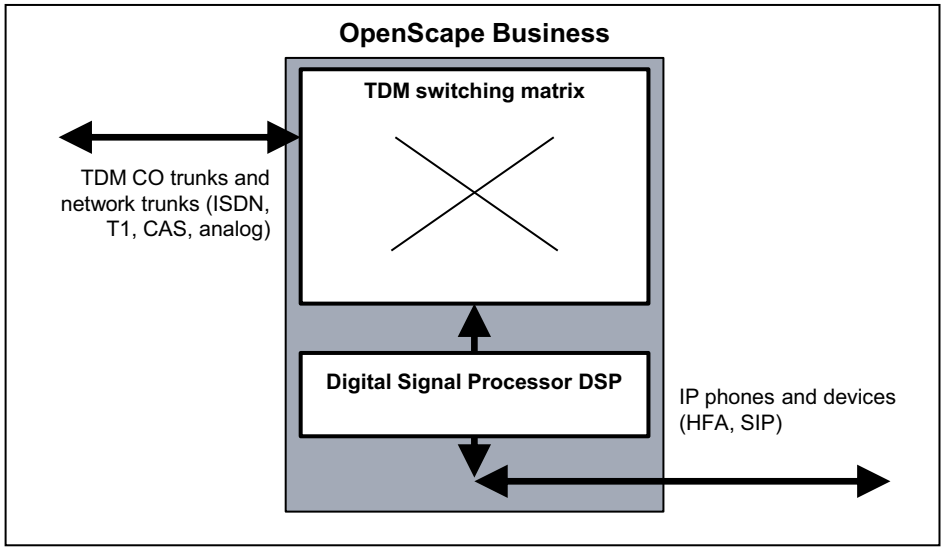
If	Then
The DSP channels on the mainboard are being used.	Insert the OCCB1 or OCCB3 subboard into the mainboard.
The DSP channels on the mainboard and the OCCB1 subboard are being used.	Insert the OCCB3 subboard into the mainboard.
The DSP channels on the mainboard and the OCCB3 subboard are being used.	Check whether the communication system can be operated only with the G.711 codec. This increases the number of DSP channels to the maximum. ***INFO:*** The **Use G.711 only** option can be activated by an administrator with the **Expert** profile in **Expert Mode** (**Telephony > Voice Gateway > Codec Parameters**).

The The following table provides orientation values for which OCCB subboard, if any, should be used.

Sum of the TDM channels: CO trunks and network trunks (ISDN, T1, CAS, analog)	Sum of IP channels: ITSP connection, SIP-Q and SIP networking, connection to the UC Suite (UC Booster Server or UC Booster Card (OCAB))	Sum of TDM telephones and TDM devices (S_0, $U_{P0/E}$, CMI, a/b)	Sum of IP phones and devices (HFA, SIP)	Which OCCB subboard?	Notes
Any number	Announcements (up to 16) 0	Any number	0	No OCCB subboard	Smart VM and system conferences are processed through the switching matrix.
			up to 8	No OCCB subboard	Independent of the TDM channels Smart VM and system conferences in combination with IP phones and IP devices require DSP resources.
			9 to 100	OCCB1	Ditto, up to 40 simultaneously
			> 100	OCCB3	Ditto, up to 120 simultaneously
	> 0	up to 8		No OCCB subboard	
	> 0	9 to 100		OCCB1	Up to 40 simultaneously
	> 0	> 100		OCCB3	Up to 120 simultaneously
> 0	up to 8			No OCCB subboard	The combination is essentially relevant for SIP-Q and UC Suite.
> 0	up to 9			OCCB1	Ditto
> 0	> 40			OCCB3	Ditto

The following examples provide orientation values for which OCCB subboard, if any, should be used.

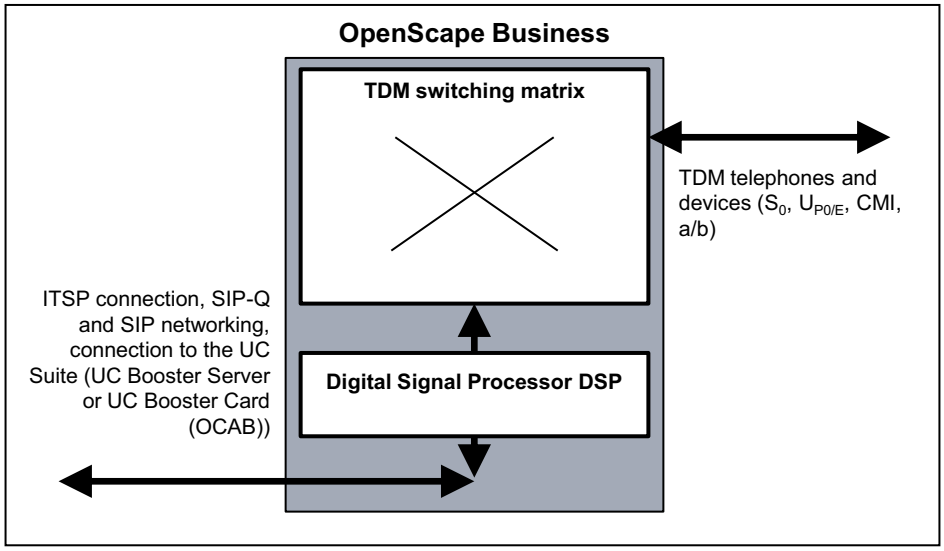
Example 1: OpenScape Business with TDM Trunks and IP Phones and Devices



If	Then
OpenScape Business with: • 1 x TDM-CO (ISDN) • 20 x IP telephones (HFA, SIP)	The DSP channels on the mainboard are sufficient. No OCCB subboard is required.
OpenScape Business with: • 1 x TDM-CO (ISDN) • 100 x IP telephones (HFA, SIP)	Subboard OCCB1 is required. Alternatively, the OCCB3 subboard can be used.
OpenScape Business with: • 2 x TDM-CO (ISDN) • 100 x IP telephones (HFA, SIP)	Subboard OCCB3 is required.
OpenScape Business with: • 4 x TDM-CO (ISDN) • 500 x IP telephones (HFA, SIP)	Subboard OCCB3 is required. ***NOTE:*** In order to achieve the maximum number of DSP channels, only the G.711 codec may be used in this system configuration.

If the communication system is to be equipped with TDM phones and devices as well (S_0, $U_{P0/E}$, CMI, a/b), additional DSP channels for this must be taken into account.

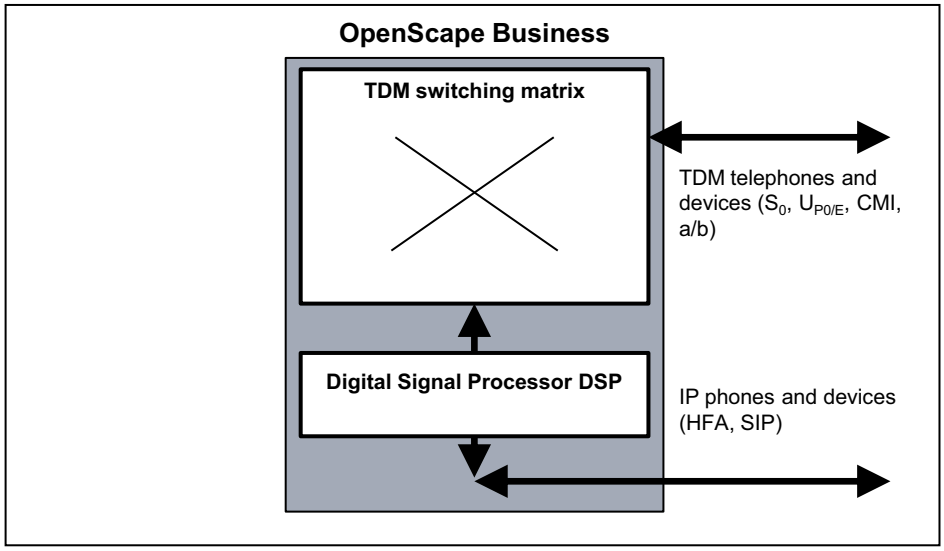
Example 2: OpenScape Business with ITSP Connections and TDM Phones and Devices



If	Then
OpenScape Business with: • 6 x ITSP connections (6 B channels) • 20 x TDM telephones (S_0, $U_{P0/E}$, CMI, a/b)	The DSP channels on the mainboard are sufficient. No OCCB subboard is required.
OpenScape Business with: • 30 x ITSP connections (30 B channels) • 100 x TDM telephones (S_0, $U_{P0/E}$, CMI, a/b)	Subboard OCCB1 is required. Alternatively, the OCCB3 subboard can be used.

If the communication system is to be equipped with IP phones and devices as well (HFA, SIP), additional DSP channels for this must be taken into account.

Example 3: OpenScape Business with TDM Phones and Devices and IP Phones and Devices



If	Then
OpenScape Business with: • 6 x TDM telephones (S_0, $U_{P0/E}$, CMI, a/b) • 6 x IP telephones (HFA, SIP)	The DSP channels on the mainboard are sufficient. No OCCB subboard is required.
OpenScape Business with: • 100 x TDM telephones (S_0, $U_{P0/E}$, CMI, a/b) • 100 x IP telephones (HFA, SIP)	Subboard OCCB3 is required.

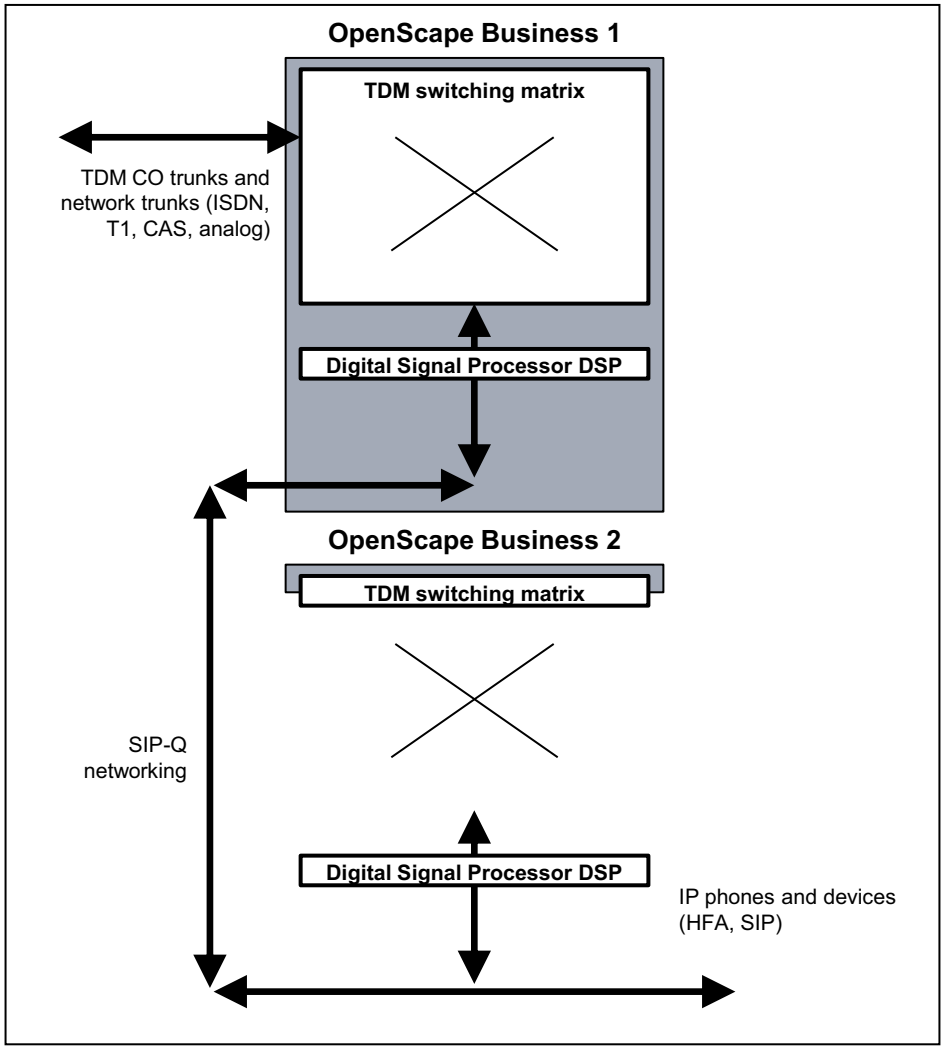
If the communication system is to be equipped with TDM trunks or IP trunks as well, additional DSP channels for this must be taken into account.

Example 4: SIP-Q Networking with OpenScape Business

The OpenScape Business 1 communication system acts as a gateway for TDM Central Office.

IP phones (HFA, SIP) are connected only to the OpenScape Business 2 communication system.

Depending on the number of IP phones at the OpenScape Business 2 communication system, the DSP channels for the OpenScape Business 1 communication system must be planned. DSP channels are required exclusively in the TDM gateway.


OpenScape Business 1
TDM switching matrix
TDM CO trunks and network trunks (ISDN, T1, CAS, analog)
Digital Signal Processor DSP
OpenScape Business 2
TDM switching matrix
SIP-Q networking
Digital Signal Processor DSP
IP phones and devices (HFA, SIP)

If	Then
OpenScape Business 1 with: • 1 x TDM-CO (ISDN) OpenScape Business 2 with: • 100 x IP telephones (HFA, SIP)	Subboard OCCB1 is required in OpenScape Business 1. Alternatively, the OCCB3 subboard can be used. No OCCB subboard is required in OpenScape Business 2.
OpenScape Business 1 with: • 2 x TDM-CO (ISDN) OpenScape Business 2 with: • 100 x IP telephones (HFA, SIP)	Subboard OCCB3 is required in OpenScape Business 1. No OCCB subboard is required in OpenScape Business 2.
OpenScape Business 1 with: • 4 x TDM-CO (ISDN) OpenScape Business 2 with: • 500 x IP telephones (HFA, SIP)	Subboard OCCB3 is required in OpenScape Business 1. ***NOTE:*** In order to achieve the maximum number of DSP channels, only the G.711 codec may be used in this system configuration. No OCCB subboard is required in OpenScape Business 2.

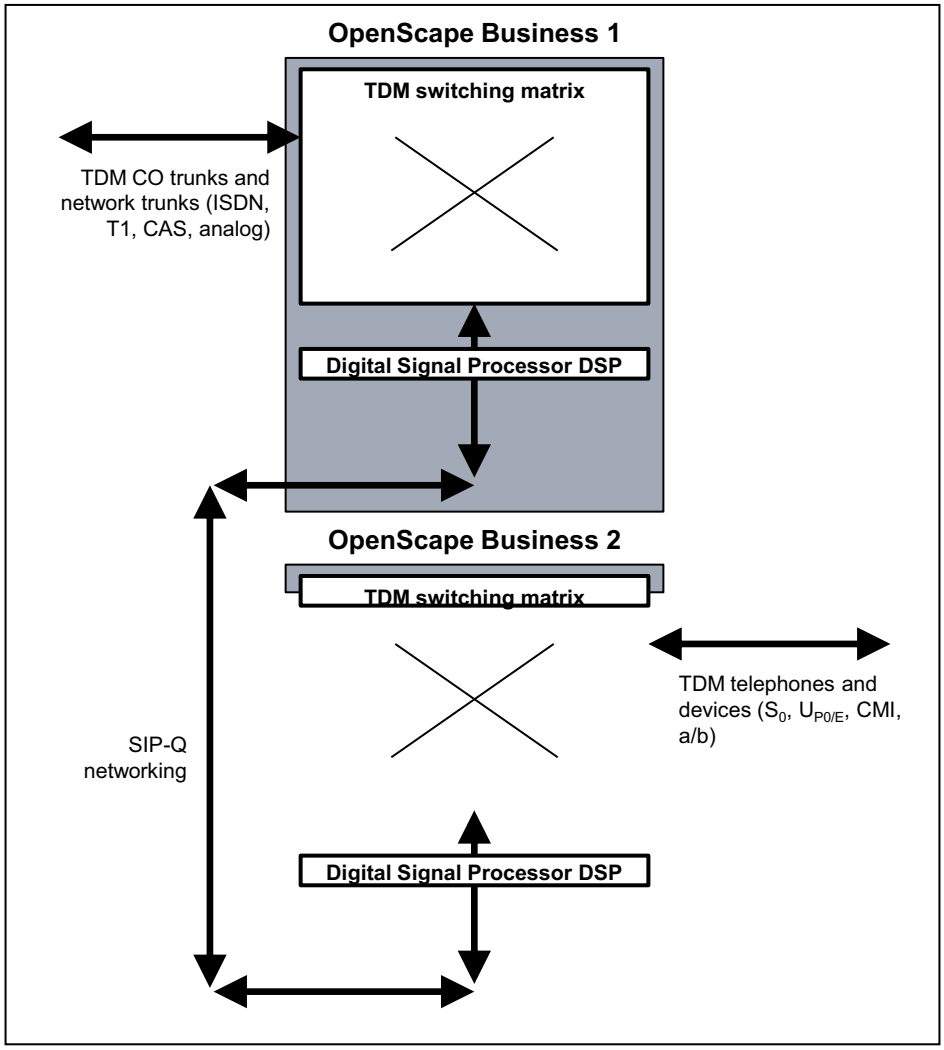
If the OpenScape Business 2 communication system is to be equipped with TDM trunks or TDM phones and devices (S_0, $U_{P0/E}$, CMI, a/b) as well, additional DSP channels must be taken into account for this.

Example 5: SIP-Q Networking with OpenScape Business

The OpenScape Business 1 communication system acts as a gateway for TDM Central Office.

TDM phones (S_0, $U_{P0/E}$, CMI, a / b) are connected only at the OpenScape Business 2 communication system.

Since gateway connections are required in both communication systems (OpenScape Business 1: TDM CO <-> SIP-Q Networking, OpenScape Business 2: SIP-Q Networking <-> TDM phone), DSP channels are needed in both systems.



If	Then
OpenScape Business 1 with: • 1 x TDM-CO (ISDN) OpenScape Business 2 with: • 100 x TDM telephones (S_0, $U_{P0/E}$, CMI, a/b)	Subboard OCCB1 is required in OpenScape Business 1 and OpenScape Business 2. Alternatively, the OCCB3 subboard can be used in both cases.
OpenScape Business 1 with: • 2 x TDM-CO (ISDN) OpenScape Business 2 with: • 100 x TDM telephones (S_0, $U_{P0/E}$, CMI, a/b)	Subboard OCCB3 is required in OpenScape Business 1 and OpenScape Business 2.

If the OpenScape Business 1 communication system is to be equipped with TDM phones and devices (S_0, $U_{P0/E}$, CMI, a/b) as well, additional DSP channels must be taken into account for this.

Example 6 OpenScape Business with IP Phones and Devices

If	Then
OpenScape Business X3/X5/X8 with: • 7 x IP telephones (HFA, SIP)	The DSP channels on the mainboar subboard is required.
OpenScape Business: • 30 x IP telephones (HFA, SIP)	Subboard OCCB1 is required.Alterr subboard can be used.
OpenScape Business with: • 100 x IP telephones (HFA, SIP)	Subboard OCCB3 is required.

24 Glossary

The glossary provides short explanations of the terms used (for instance, protocols and standards).

24.1 Glossary

10BaseT, 100BaseT, 1000BaseT

This refers to a specification (IEEE. 802.3i)) for networks with 10 Mbps base band transmission over a symmetrical 100-Ohm four-wire cable. 100BaseT, on the other hand, is used for bandwidths of up to 100 Mbps and 1000BaseT for bandwidths of up to 1000 Mbps.

AES (Advanced Encryption Standard)

AES is a symmetric encryption system that was ratified by the National Institute of Standards and Technology as the successor to the earlier DES and 3DES Standards. It is used for VPN, for example.

ADSL with dynamic IP address

ADSL stands for Asymmetric Digital Subscriber Line and means that the bandwidths from the Internet (download, downstream) and to the Internet (upload, upstream) are different. The classic Internet telephony connection is ADSL. A dynamic IP address is sufficient if the web and mail services are provided by the Internet Service Provider.

ADSL with fixed IP address

ADSL stands for Asymmetric Digital Subscriber Line and means that the bandwidths from the Internet (download, downstream) and to the Internet (upload, upstream) are different. The classic Internet telephony connection is ADSL. ADSL with a fixed IP address is required if you want to run your own web and mail server on your site.

AF-EF (Expedited Forwarding - Assured Forwarding)

The codepoints AF and EF define the various priorities of IP packets for QOS (Quality of Service).

AF: guarantees minimum bandwidth for the data

EF: guarantees constant bandwidth for this data.

ARP (Address Resolution Protocol)

The Address Resolution Protocol (ARP) is a network protocol that facilitates the assignment of network addresses to hardware addresses. Although it is not limited to Ethernet and IP protocols, it is almost exclusively used in conjunction with IP addressing in Ethernet networks.

Authentication

Authentication is the verification of a person's or PC's identity. The check can be performed with a simple user name, for example, as well as with a fingerprint.

Authorization

Authorization is a mechanism for granting rights, e.g., access rights in a data network.

B channel

A B channel is the transmission path for the payload (voice, data) of an ISDN connection.

Busy Lamp Field (BLF)

myPortal provides a so-called Busy Lamp Field (BLF) to display the call status of the specified subscribers.

Broadcast

A broadcast is a message sent to everyone in a PC network. The message (i.e., a data packet) is transmitted from one point to all subscribers in the network. A broadcast is mainly used in a data network if the address of the message recipient is unknown.

CA (Certification Authority)

The CA is an organization that issues certificates with digital signatures. Digital signatures are required for a VPN (Virtual Private Network), for example.

CAPI Interface (Common Application Programming Interface)

CAPI is an ISDN-compliant standardized software interface. CAPI enables the development of ISDN software without requiring any knowledge about the manufacturer-specific ISDN hardware being used.

Centrex

Centrex (Central Office Exchange) provides the functions of a telephone system via a PSTN or ITSP. This is also known as virtual telephone system, hosted PBX (Private Branch Exchange) or NetPBX.

CHAP (Challenge Handshake Authentication Protocol)

CHAP is an authentication protocol used within the framework of the Point-to-Point protocol.

COS (Classes Of Service)

QoS is a procedure that ensures the transmission quality for data in IP networks.

CLIP (Calling Line Identification Presentation)

With station number transmission, the caller's phone number is displayed on the called party's station. The called party can therefore identify the caller before picking up the call.

CLIR (Calling Line Identification Restriction)

The caller suppresses the display of his or her call number on the called station. As a result, the called party cannot identify the caller before picking up the call.

COLP (Connected Line Identification Presentation)

With Connected Line Identification Presentation, the called party's number is displayed for the caller if the connection is successful.

COLR (Connected Line Identification Restriction)

With Connected Line Identification Restriction, the called party's number is not displayed for the caller, even if the caller activated COLP.

Comfort User

Comfort User is the standard user of the communication system.

Comfort Plus User

The Comfort Plus User is the Advanced User of the communication system. In contrast to the Comfort User, the Comfort Plus User can use more features (such as Fax, Mobility and Conferencing).

CorNet

CorNet is a proprietary protocol for networking the HiPath and OpenScape communications systems. In contrast to the generally supported QSIG, all manufacturer-specific features of the HiPath and OpenScape communication systems are integrated in CorNet.

CorNet-IP

CorNet-IP is a protocol variant of CorNet that enables the cross-networking of systems or the connection of system telephones (such as optiPoint) over IP.

CorNet-NQ

A proprietary QSIG-based signaling protocol for interconnecting communication systems to one or more QSIG PBX systems.

CSTA (Computer Supported Telecommunications Applications)

CSTA is a protocol interface for applications that support the European Computer Manufacturers' Association (ECMA) standard. Telecommunication tasks are controlled and monitored using SIP via CSTA.

CSV (Character Separated Values)

A CSV file is a text file for saving or exchanging simply structured data. CSV stands for Character Separated Values, Comma Separated Values or Colon Separated Values, since the individual values are delimited by a special separator character such as a comma or semicolon. CSV files must be available in ANSI/ ASCII format.

CRL (Certificate Revocation List)

A CRL or Certificate Revocation List is a list or all revoked certificates. CRLs always have to be generated by the certification authority where the certificates originate.

Delay

A delay has two meanings in telecommunications:

- The delay by which an event is postponed.
- The time between the occurrence of an event and the appearance of a expected follow-on event.

Dedicated (Permanently Assigned) Gateway

If a dedicated gateway is entered in the LCR for a route, then routing via this gateway is enforced. All contradictory rules are then invalid for the routing.

DHCP (Dynamic Host Configuration Protocol)

DHCP is a procedure by which a PC is assigned a certain IP configuration (IP address, subnet mask, etc.) at startup.

DS (DiffServ, Differentiated Services)

DS is a procedure for managing packets in data networks. The routing method for a specific data packet is specified as is a particular service level in regard to bandwidth, queuing theory, and packet discard decisions.

Diffie-Hellman algorithm

The Diffie-Hellman algorithm is used for the exchange of keys in a VPN. The data produced by this algorithm is configured with a specific set of mathematical parameters. The key exchange only works properly if both subscribers use identical values for these parameters.

DLI (Deployment License Service Integrated)

DLI enables the unattended installation and upgrading of IP system telephones.

DMZ (Demilitarized Zone)

A demilitarized zone (DMZ) refers to a PC network that offers a number of security features for accessing connected network nodes (PCs, routers, etc.).

DNS (Domain Name Service)

Name resolution on the Internet and in the LAN. DNS translates the names of PCs or web pages into the relevant IP addresses.

DSL (Digital Subscriber Line)

DSL is a technological solution for providing high-bandwidth Internet access. Internet telephone bridges the gap between the provider's attendant and the customer's telephone jack.

DSS (Direct Station Selection)

The function keys on a telephone or add-on device can be programmed as Direct Station Select (DSS) keys. These are programmed with the phone number of an internal subscriber or a group for this. Pressing a DSS key initiates an immediate call to the programmed destination.

DTMF (Dual Tone Multifrequency)

See DTMF.

EIM (Enterprise Instant Messaging)

EIM is an Instant Messaging Service that runs on private servers in a company on platforms such as the Live Communications Server or Office Communications Server 2007 from Microsoft.

Enterasys Switches

Enterasys switches are produced by Enterasys Networks as secure network solutions. The stackable switches support QoS features and can classify and prioritize voice, video and data applications.

ESP (Encapsulating Security Payload)

ESP is an IPsec protocol that guarantees packet encryption, packet integrity as well as packet authenticity. The integrity and authentication check does not extend to the IP header. It is only performed for the actual data (payload).

FoIP (Fax over IP)

FoIP is a method for transmitting fax messages over an IP network.

FTP

The File Transfer Protocol (FTP) is a network protocol specified in RFC 959 for the transmission of data via TCP/IP networks.

Functional Numbers

Functional numbers (also called function codes) are MSN/DID numbers or pilot numbers, e.g., for parking, conferencing and the AutoAttendant. The functional numbers correspond to virtual stations. The functional numbers in an internetwork must be unique.

G.711

G.711 is a standard for digitizing analog audio signals. It is used in classic fixed-network telephony (PCM technology). G.711 can also be used for voice encoding in VoIP.

G.729AB

G.729 is a codec for voice compression in digital signals and is used in IP telephony. G.729 is very CPU-intensive. Though only marginally inferior in terms of quality, G.729AB is a somewhat simplified version and therefore less CPU-intensive.

Gateway / Gateway Modules

A gateway is the entrance and exit to a communications network, usually connecting two disparate traffic flows.

GSM (Global System for Mobile Communications)

GSM is a standard for digital mobile networks that is primarily used for telephony, but also for line- and packet-switched data transmissions as well as short messages (SMS).

Handover

The term handover designates the process in a mobile cellular communication network in which the mobile phone switches from one cell to another during a call or a data connection. The term is also used when switching between GSM and UMTS with a dual-mode mobile phone.

Hash value

Hash or dispersion range values are usually scalable values from a subset of natural numbers. A hash value is also referred to as a "fingerprint" because it is a virtually unique identification of a quantity in much the same way as a fingerprint is a virtually unique identification of a person.

H.323

H.323 designates a group of standards that define a variety of media types for packet networks. The standards cover voice, data, fax and video, and define how signals are to be converted from analog to digital and what signaling is to be used.

OpenScape Business Assistant

OpenScape Business Assistant is used to administer the communication system. It provides all wizards for the quick support of administration tasks.

Hosted Services

Hosted Services are traditional IT services such as e-mail, instant messaging (IM) and unified communications (UC), which are provided to a company by an Internet Provider from a remote site, thus eliminating the company's need to run and manage these services on their own servers on-site.

ICMP (Internet Control Message Protocol)

ICMP is used in data networks for the exchange of information and error messages using the Internet Protocol IP.

IDS (Intrusion Detection System)

IDS is a security system that monitors all incoming and outgoing network activities to identify possible security violations. These include both intrusion (attacks from outside the organization) and abuse (attacks from within the organization).

IEEE Standards

IEEE Standards are a set of specifications defined by the Institute of Electrical and Electronic Engineers (IEEE) (such as Token Ring, Ethernet) to establish common networking standards among vendors.

IEEE. 802.1p

IEEE. 802.1p is an IEEE standard for regulating the transport of data packets with different priorities in computer networks. The data packets are classified into priority classes from 1 to 7. The Standard only stipulates ascending priorities from 1 through 7, but does not deal with how the individual data packets should be handled.

IKE Protocol

The IKE protocol has two different tasks. Start by creating an SA (Security Association) exclusively used by the IKE protocol (IKE-SA). The existing IKE-SA is then used for secure negotiation of all further SAs (payload SA) for the transmission of payload data.

IM (Instant Messaging)

IM is a procedure for the real-time exchange of text messages over the Internet using computers, Pocket PCs and mobile phones. Modern IM services enable VoIP and video conferencing, file transfers and desktop application sharing.

IP PBX

IP PBX is a communication system that supports both VoIP and normal voice connections over traditional phone lines.

IPSec

IPSec is a framework of open standards for ensuring private, secure communications over Internet Protocol (IP) networks through the use of various security services and protocols.

ISP (Internet Service Provider)

An ISP is a business that supplies Internet connectivity services to individuals, businesses, and other organizations. Some ISPs are large national or multinational corporations that offer access in many locations, while others are limited to a single city or region.

ITSP (Internet Telephony Service Provider)

An ITSP is a business that supplies Internet connectivity services to individuals, businesses, and other organizations.

DP (Dial Pulsing)

DP is the oldest signaling method used for automatic telephone switching. Today, DP has generally been superseded by DTMF.

Jitter

Jitter refers to packet delay variations in voice transmissions. An excessive delay between the sending of packets and their arrival at the receiving end results in irregular voice communications infectivity are difficult to understand.

ISD (Individual Speed Dialing)

Individual Speed Dialing (ISD) enables 10 external individual speed-dial numbers to be saved at every authorized phone in addition to the system speed dialing (SSD).

SSD - System Speed Dialing

Frequently required external phone numbers can be stored in the system memory of the communication system. Every number is represented by a speed-dial number, which can be used instead of the full phone number by all stations.

Latency

Latency is the time required to transport a data packet from one application to another, including the time for transmission over the network and for preparing and processing the data at the transmitting and receiving devices.

LCR (Least Cost Routing)

You can use the Least Cost Routing (LCR) function to specify the provider you want to use, e.g., for trunk calls, mobile phone calls or international calls. You use the communication system to define the least-cost provider and conduct all calls via this specific path.

LIN (Location Identification Number)

LIN is an unique, max. 16-digit number that corresponds to the 10-digit NANP (North American Numbering Plan).

LWCA (Lightweight CA)

LWCA is a restricted certification function.

Media Stream Channel

A media gateway can terminate circuit-switched ISDN B channels and use the voice data carried to generate media stream channels for an IP-based packet-switched network. Media stream channels feature a combination of audio, video, and T.120 media.

DTMF (Dual Tone Multifrequency)

Dual Tone Multifrequency (DTMF) is the dialing method in analog telephony that is predominantly used in switching technology today for transmitting the phone number to the telephone network.

MIM (Mobile Instant Messaging)

MIM is a Presence and Instant Messaging Service for mobile phones.

Mobility

The term mobility designates the use of Pocket PCs and mobile phones and their integration in the communication system of a company.

MOH (Music on Hold)

Music on Hold (MOH) can be played to callers who cannot be switched through immediately.

MSN (Multiple Subscriber Number)

When connecting ISDN phones via an S0 bus (point-to-multipoint connections), every single ISDN phone (ISDN station) is assigned a unique Multiple Subscriber Number (MSN). The ISDN stations can be reached via their MSNs.

MULAP (Multiple Line Appearance)

MULAPs are special groups in which multiple telephones are combined. A group member may be assigned multiple phones under a single call number (Basic MULAP) here. In addition, such a group can be used to implement special features required for communication between an Executive and Secretary, for example, or within teams (Executive MULAP, Team MULAP).

Multi-Gateway

In the case of a multi-gateway network, calls are routed via several different gateways.

myAttendant

myAttendant is the attendant console of the communication system.

myPortal

myPortal is the Java-based user portal that enables subscribers to access the Unified Communications functions. Apart from information on the presence status, convenient dialing aid via favorites and directories, subscribers can also access voicemail messages and faxes.

myPortal for Outlook

myPortal for Outlook is the user portal integrated in Microsoft Outlook that enables subscribers to access unified communications functions. It is analogous to myPortal. myPortal for Outlook also provides a convenient Desktop Dialer.

NAC (Network Admission Control)

NAC is a technology that supports defenses against viruses and worms from within the network. With NAC, terminal devices are checked for conformity with guidelines during the authentication. If the virus scanner is not up-to-date, for example, or if the client operating system does not have the latest security patch installed, the device involved is quarantined and provided with the current updates until it meets the applicable security guidelines.

NAT (Network Address Translation)

NAT is a procedure for replacing one IP address in a data packet with another. It is used to map private IP addresses to public IP addresses. Masking or PAT (Port Address Translation) is when the port numbers are also rewritten.

NTBA (Network Termination for ISDN Basic Access)

An NTBA (Network Termination for ISDN Basic Access), also known as NT (Network Termination), is the network termination device for the ISDN basic rate interface. It is the link between the network operator's digital network and the ISDN configurations on the subscriber side.

NTPM (Network Termination for Primary Rate Multiplex Access)

An NTPM (Network Termination for Primary Rate Multiplex Access) is the network termination device for the ISDN primary rate interface. It is the link between the network operator's digital network and the ISDN configurations on the subscriber side.

OLSR - Optimized Link State Routing Protocol

OLSR is special ad-hoc protocol that enables the missing routing capability on the OSI Layer 2 to be optimized on the OSI Layer 3.

ONS (One Number Service)

Call number directly assigned to a user One or more resources (telephones) may be assigned to a user. When a user is called via his or her ONS number, the call is forwarded to the phone that is currently being used by that user (e.g., a mobile phone).

PAP (Password Authentication Protocol)

PAP is an authentication procedure based on the point-to-point protocol. It is used for dialing into an ISP. PAP transmits the password for authentication as clear text together with a user ID.

PBX (Public Branch Exchange)

A PBX is a switching system that interconnects multiple terminals such as phones, fax and answering machines between themselves and also to the public phone network.

Peer

A peer is the terminal device for communication in a peer-to-peer network. During communication, every peer makes its services available and uses the services of the other peer.

Peer-to-peer

In a peer-to-peer network, all PCs have equal rights and may use and also provide services on the network.

Peer-entity authentication

The corroboration that the peer entity in an association is the one claimed.

PKI (Public Key Infrastructure)

In cryptology, a PKI (public key infrastructure) is a system for generating, distributing, and verifying digital certificates. The certificates issued within a PKI are used to protect computer-driven communication.

PPP (Point-to-Point Protocol)

PPP is an IETF standard for transmitting IP packets over serial lines. PPP is mainly used for dialing into the Internet.

PPPoE (Point-to-Point Protocol over Ethernet)

The PPPoE Protocol (PPP over Ethernet) enables the use of the Point-to-Point network protocol over an Ethernet connection.

Pre-shared Key

The pre-shared key is a key that is defined for the tunnel configuration (for VPNs). In order for VPN peers communicating via the tunnel to authenticate themselves, the same password must be used for both of the tunnel endpoints.

PPTP (Point-to-Point Tunneling Protocol)

PPTP is a technology used for configuring a virtual private network (VPN). Because the Internet is essentially an open network, PPTP is used to ensure that messages transmitted from one VPN node to another are secure. PPTP lets users dial into their corporate network via the Internet.

Presence

The term Presence refers to the capability of a Unified Communications system to determine the location and status of a user at any time. This makes it easier to respond to the specific communication needs of a user by phone, e-mail, Instant Messaging or fax.

Proxy Server

The proxy server is the connecting link between a client application and a Web server. It performs the task of filtering client application requests and thus relieves the load on the Web server.

PSTN (Public Switched Telephone Network)

As the name implies, PSTN refers to a public switched telephone network. Public networks may be owned by private or public entities.

QoS (Quality of Service)

You must guarantee a minimum bandwidth for Voice over IP for the entire transmission duration. If multiple applications with equal rights are operating via IP, then the available bandwidth for a transmission path is split. In this case, a voice connection may experience packet losses which can reduce voice quality. There are different ways to guarantee the highest possible quality for transmission; these methods are collectively referred to as Quality of Service (QoS).

RAS (Remote Access Service)

A RAS (Remote Access Service) user is an IP subscriber (e.g., a teleworker) who logs into the system remotely and behaves like an internal IP station. This subscriber can therefore use the complete functional scope of the communication system.

RJ45 (Registered Jack 45)

RJ45 is an eight-pin connector that is used for connecting a 10BaseT cable in network technology, for example.

Roaming

Roaming is the capability of a mobile network subscriber to automatically make calls or access other mobile network services in a foreign network, i.e., one that differs from the home network of the subscriber.

RTCP (Real-Time Control Protocol)

The real time control protocol (RTCP) is used for the negotiation and compliance of Quality of Service (QoS) parameters through the periodic exchange of control messages between senders and receivers.

RTP (Real-Time Transport Protocol)

RTP is an IETF Standard for streaming real-time multimedia data using the Internet Protocol. Typically, RTP runs on top of the UDP protocol, and uses dynamic UDP ports negotiated between the sender and receiver of specific media streams.

RTT (Round Trip Time)

RTT is the time interval required by a data packet to move from the source to the target and back.

SA (Security Association)

SA is a security association between two communicating units in computer networks. It describes how the two parties will use security services to communicate securely with each other.

SDSL (Symmetric Digital Subscriber Line)

SDSL is particularly suited to Internet telephony, intranet applications in companies with local networks, for video conferencing and is, for example, designed for teleworkers who can use it to send and receive data with the same bandwidth. In contrast to ADSL, SDSL uses identical bandwidths from and to the Internet.

Secure CLI

Secure CLI is a security feature that provides secure command line and data transfer interfaces with the help of the Secure File Transfer Protocol (SFTP).

SFTP (Secure File Transfer Protocol)

SFTP is a security protocol for transporting connection data records.

ShrewSoft VPN Client

The ShrewSoft VPN client is an open source and free VPN client with a graphical user interface. It includes, among other things, ISAKMP, Xauth and RSA support, and AES, Blowfish and 3DES encryption protocols.

Single Gateway

In the case of a single-gateway network, calls are routed via a single gateway.

SIP (Session Initiation Protocol)

SIP is a standard Internet protocol defined in RFC 3261 for setting up and managing voice connections and video conferences over an IP network.

SNMP (Simple Network Management Protocol)

SNMP is a procedure for obtaining information on the status of network components and PCs.

SPE (Signaling and Payload Encryption)

Signaling & Payload Encryption (SPE) serves to enhance security when transmitting voice data. The VoIP payload and signaling data streams from and to the gateway and between IP phones are encrypted.

SRTP (Secure Real-Time Transport Protocol)

SRTP is an encrypted RTP protocol. It is particularly suitable for transmitting communication data over the Internet and is used in IP telephony.

SSH (Secure Shell)

SSH is a protocol that provides support for secure remote login, secure file transfer, and secure TCP/IP forwarding. It can automatically encrypt, authenticate, and compress transmitted data.

SSL (Secure Socket Layer)

SSL is a protocol for transporting documents over the Internet. With SSL, data is provided with a private key before it is transmitted. By convention, URLs that require an SSL connection start with https: instead of http:.

Status

The status, together with the "Presence" concept, indicates whether a subscriber is available, busy, offline, etc., so that other subscribers in the communication system know if this subscriber can be reached.

STUN (Simple Traversal of UDP through NAT)

STUN is a network protocol for detecting, identifying, and bypassing firewalls and NAT routers.

Survivability

Survivability is the capability of an internetwork to maintain service continuity in the presence of faults within the network.

TAE (Telekommunikations-Anschluss-Einheit) - German standard for telephone plugs and sockets

A TAE is a type of connector for analog phone connections with the a/b interface and for ISDN connections to plug the NTBA into the main line. It is used to connect analog telephones, fax machines and ISDN phone systems.

TCP (Transmission Control Protocol)

TCP is a protocol that governs how data should be exchanged by PCs. All operating systems in modern PCs support TCP and use it for data exchange with other PCs.

TFTP (Trivial File Transfer Protocol)

TFTP is a trivial file transfer protocol that supports only the reading and writing of files. Many of the functions supported by the superordinate protocol are unavailable, for example, functions allocating rights, displaying existing files or user authentication.

Telnet

A protocol that links two PCs in order to provide a terminal connection to the remote PC. Instead of dialing into the PC, the user connects over the Internet via Telnet. The user initiates a Telnet session, connects to the Telnet host and logs in. The connection enables the user to work with the remote PC as though it were a terminal connected to it.

TOS (Type of Service)

TOS is a field in the header of IP data packets. It is used for the prioritization of these packets and evaluated for Quality of Service, for example.

UCD (Uniform Call Distribution)

UCD enables incoming calls in the communication system to be uniformly distributed to a group of stations (UCD-group).

UDP (User Datagram Protocol)

UDP is a network protocol that belongs to the Transport layer of the Internet protocol family. UDP is responsible for routing data transmitted over the Internet to the correct application.

UMTS (Universal Mobile Telecommunications System)

UMTS is a third-generation mobile network standard with which significantly higher data transmission rates (384 kbps to 7.2 Mbit/sec.) can be achieved as compared to the mobile network standards of the second generation or the GSM standard.

Unified Communications

Unified Communications is the integration of various communication systems, media, devices and applications within an environment (e.g., IP telephony, site-based and mobile telephony, e-mail, instant messaging, desktop applications, voicemail, fax, conferencing and unified messaging).

Unified Messaging

Unified Messaging is the integration of different communication data such as e-mail, SMS, fax, telephony, etc., in a uniform message store. This message store can be accessed by several different devices.

VAD (Voice Activity Detection)

VAD (Voice Activity Detection) is an algorithm in speech processing to detect the presence or absence of speech in the digital transmission of audio data.

VCAPI Interface

VCAPI is a virtual CAPI interface that emulates the presence of a local ISDN card. If an ISDN card has been installed on a PC in the internal network, then this ISDN card can be made available to all stations on the network via the VCAPI interface.

VDSL (Very High Speed Digital Subscriber Line)

VDSL is used to transfer symmetrical or asymmetrical data streams at high speed over short distances. VDSL is an alternative to ADSL and SDSL that additionally offers higher transmission speeds.

VoIP (Voice over IP)

VoIP is the transmission of voice data over IP-based networks.

VPN (Virtual Private Network)

A VPN uses the public infrastructure of the Internet to connect sites and provide teleworkers with access to internal networks. External partners are provided with

secure access to the internal data network by using encryption and authentication mechanisms.

WAN (Wide Area Network)

WAN is the designation for wide area data networks such as the Internet, for example.

WBM (Web-Based Management)

WBM is a web-based user interface that is displayed in an Internet browser using HTML or JAVA pages (web pages) and a web protocol (HTTP or HTTPS).

X.509 standard (VPN certificate)

X.509 is an ITU-T standard for a public key infrastructure and currently the most important standard for digital certificates.

XMPP (Extensible Messaging and Presence Protocol)

Internet standard that is primarily used for Instant Messaging. XMPP supports the interaction with users of other networks such as AIM, ICQ or Windows Live Messenger (WLM), for example. Among other things, XMPP and its extensions support conferencing with multiple users (e.g., multi-user chats) and the display of the online status.

Second Degree

Second degree means that a station is calling and already has a second call waiting for that station.

Index

D

E

F

G

H

I

J

K

L

M

N

O

P