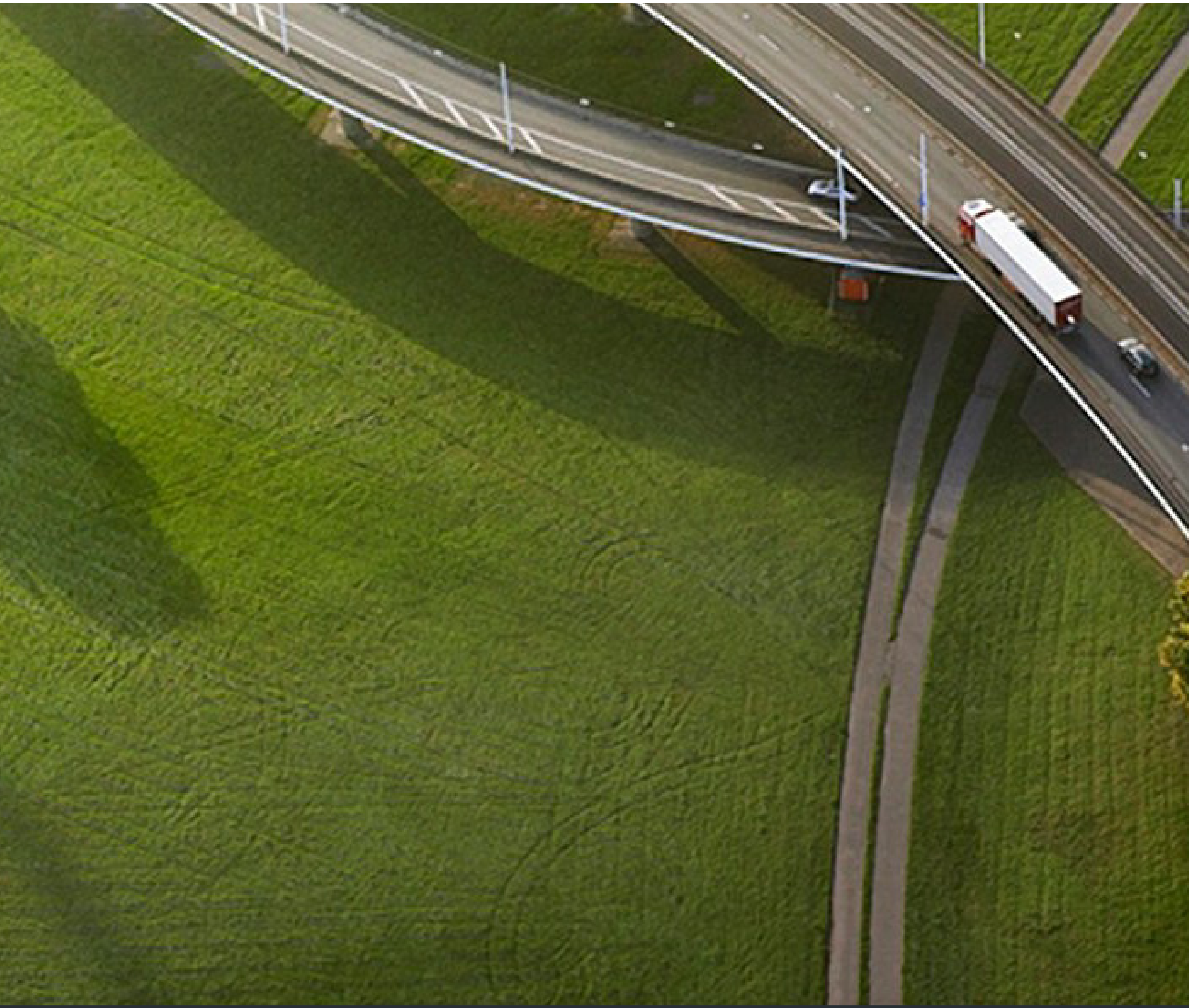
Harmonize
your enterprise



OpenScape Business V2
Last Changes

Description

A31003-P3020-T101-8-7618

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.

Mies-van-der-Rohe-Str. 6, 80807 Munich/Germany

Reference No.: A31003-P3020-T101-8-7618

The information provided in this document contains merely general descriptions or characteristics of performance which in case of actual use do not always apply as described or which may change as a result of further development of the products.
An obligation to provide the respective characteristics shall only exist if expressly agreed in the terms of contract.

Availability and technical specifications are subject to change without notice.

Harmonize
your enterprise

unify.com

Contents

1 About this Document

This document provides you with information on the latest changes and additions to the administrator and user documentation for OpenScape Business V2.

Examples:

- Changes due to MRs and ICTS (International Case Tracking System) tickets
- Additions due to new features

This information, which was received after the cut-off date, was not available at press time and could therefore not be considered in the current issues of the administrator and user documentation. It will automatically be taken into account in subsequent editions.

Display Conventions

This document uses the following display conventions to indicate changes and additions.

Purpose	Presentation	Example
Changes	red	Only IP phones (system clients) are supported for this.
Deletions	red and crossed out	~~Only IP phones (system clients) are supported for this.~~
Additions	green	Only internal extensions for which the first and last names of the subscriber are entered in the internal directory are supported here.

2 V2R0.3: Door View Possible for Multiple Devices

Affected Documentation	Administrator Documentation
Issue	9
Reference No.	A31003-P3020-M100-09-76A9

2.1 Chapter 21.2.3.1 How to Configure the Entrance Telephone

The **Door Opener** wizard can be used to specify which subscribers are allowed to operate the door opener. You can configure up to ten entrance phones.

Prerequisites

- You are logged in at the WBM.

Step by Step

1. In the navigation bar, click on **Setup**.
2. In the navigation tree, click on **Wizards > Central Telephony**.
3. Click on **Edit** to start the **Door Opener** wizard. The **Edit Door Opener** window appears.
4. Select one or more **Stations**.
5. Enter the **Destination**.
6. Select the relevant functions such as **Door Opener**, **DTMF** and **FWD** in the check box.
7. Click on **OK & Next** followed by **Finish**.
8. Follow steps 1 to7 to configure each entrance phone.

2.2 Chapter 21.5.7.1 How to Set up the Entrance Telephone

Prerequisites

- The entrance telephone function and the corresponding button on the telephones have been set up in the communication platform.
- The call number and the password for the entrance telephones are known.
- You are logged in at the OpenStage Gate View Assistant

Step by Step

1. Navigate in the menu to **Administration** > **Entrance Telephone** > **Add Entrance Telephone**.
2. Select the **Enabled** check box.
3. For **Name**, enter any name for the entrance telephone.
4. For **Web Services Server IP**, enter the IP address of the UC Suite or of the UC Smart Assistant.
5. For **Web Services Server Port**, enter the port of the UC Smart Assistant.

6. If desired, select the **SSL** check box for a secure connection.
7. For **Door Opener Station Number**, enter the call number of the entrance telephone.
8. Enter the configured password for the entrance telephone function under **Door Opener UC Password**.
9. Under **Gate View IP Client**, hold down the <Ctrl> key and select the names of the telephones that were configured for use with the entrance telephone function in Stage Gate View.
10. Under **Camera**, select the name of the camera that was configured for use with the entrance telephone function in OpenStage Gate View.
11. Click on**Save**.
12. Navigate in the menu to **Administration >** Phones **>** Installed Phones.
13. Click on **Configure Phone Buttons** in the list for the last processed phone.
14. Click on **Transfer to Phone** and confirm with **OK**.
15. Click on **Save**.

The entrance telephone function has been set up. When the doorbell rings, the video image from the camera is automatically displayed on the phones. Pressing the door opener button on one of the configured phones opens the door.

3 V2R0.3: HFA-Proxy Dual Mode for myPortal to go

Affected Documentation	Administrator Documentation
Issue	9
Reference No.	A31003-P3020-M100-09-76A9

3.1 Chapter 18.2.6 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.

3.2 Chapter 18.2.7.2 How to Integrate Dual-Mode Telephones (GSM/WLAN) with HFA or SIP Client

The **Mobile Phone Integration** wizard can be used to configure a mobile phone as a dual-mode phone with system client (HFA client) or SIP client (WLAN mode).

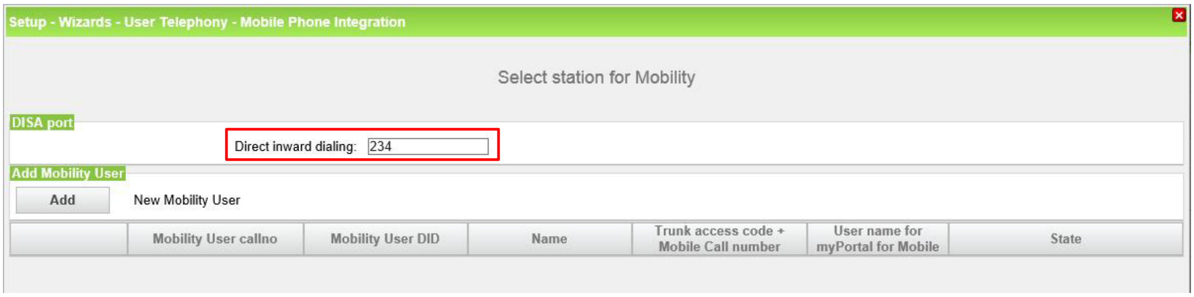
Prerequisites

- You are logged on to the WBM with the **Advanced** profile.
- The HFA device or SIP station must be configured via the WBM.
- Mobility user license has been assigned to the subscriber.

Step by Step

1. In the navigation bar, click on **Setup**.
2. In the navigation tree, click **Wizards > User Telephony**.

3. Click **Edit** to start the **Mobile Phone Integration** wizard. The **Select Station for Mobility** window appears.
4. Under **DISA access**, select (or enter) the **DID** number with which mobile stations can dial into the communication system.



Setup - Wizards - User Telephony - Mobile Phone Integration

Select station for Mobility

DISA port

Direct inward dialing: 234

Add Mobility User

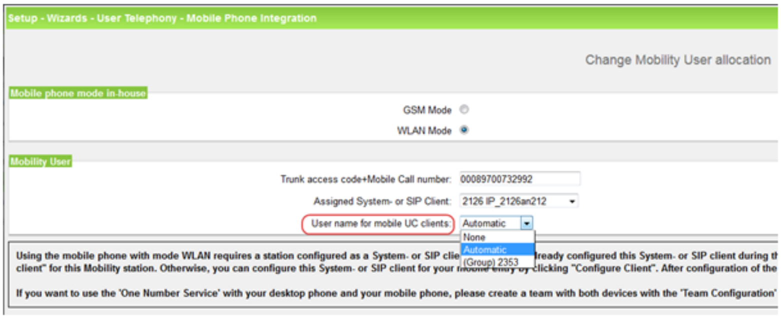
Add New Mobility User

	Mobility User callno	Mobility User DID	Name	Trunk access code + Mobile Call number	User name for myPortal for Mobile	State

> ***INFO:*** DISA is required for Mobility Entry (to control the system using DTMF) and for myPortal for Mobile (only when using Call Through).

5. Click on **Add** or **Edit** for the appropriate subscriber whose GSM mobile phone is to be integrated into the communication system. The **Assign Mobility Stations** window appears.
6. Select **WLAN Mode** as the mode for your mobile phone operation.
7. Under **Trunk access code+Mobile phone number**, enter the phone number of the mobile phone (e.g., 0016012345678).
8. Select **Assigned System- or SIP Client** from the drop-down list.

   If the assigned system (HFA client) or SIP client is not yet configured, click on **Configure Client** and set up a system or SIP client. After the system or the SIP station configuration, you will be automatically returned to this page.
9. In the **Username for myPortal to go (Web Edition)** drop-down list, select the corresponding SIP or HFA device. If you select **Automatic**, the internal number of the user will be used as the user name.



Setup - Wizards - User Telephony - Mobile Phone Integration

Change Mobility User allocation

Mobile phone mode in-house

GSM Mode ○

WLAN Mode ●

Mobility User

Trunk access code+Mobile Call number: 00089700732992

Assigned System- or SIP Client: 2126 IP_2126an212

User name for mobile UC clients: Automatic

Using the mobile phone with mode WLAN requires a station configured as a System- or SIP clie lready configured this System- or SIP client during t client" for this Mobility station. Otherwise, you can configure this System- or SIP client for your clicking "Configure Client". After configuration of the

If you want to use the 'One Number Service' with your desktop phone and your mobile phone, please create a team with both devices with the 'Team Configuration'

10. Click **OK & Next**.
11. Click **OK & Next** followed by **Finish**.

3.3 Chapter 27.3.7.14 Station > Stations > Mobility User

It is recommended to set up mobile users via the "User Telephony > Mobile Phone Integration" wizard.

Parameter Description of Tabs:

- **Change Station**

Parameters	Description
Call no	Input of the internal extension number of the Mobility user (e.g., 777). This internal call number must not have already been assigned.
DuWa	Input of the internal DID number of the Mobility user. This internal DID number must not have already been assigned.
Name	Input of any internal name for the Mobility user.
Type	Displays the type of Mobility user.
Device Type	Displays the system telephone type associated with the image file.
Clip/Lin	Sequence of digits to be displayed at the called party instead of the actual number for outgoing external calls (e.g., for E911 emergency services in the USA) Value range: max. 16 digits
Access	Displays the physical interface at which the device is connected.
Mobile Callno	Input of the mobile phone number. The entry must include the leading dialout prefix (i.e., the CO code), e.g., 0016012345678.
Web Feature ID	The Web Feature ID defines how the subscriber should log in at the mobile web client (user name). Choice between "no" (Mobility Entry user without myPortal to go) and "automatic" (internal call number of the subscriber or Mulap) or selection of the station number of the client or phone from the drop-down list.
Search	You can also have selected subscribers displayed by entering a search term in the **Search** fields and pressing the Return key. The subscribers who match the search term are displayed. If you leave all the **Search** fields empty and press the Enter key, all subscribers will be listed again.
Items per page	Selection to determine whether 10, 25, 50 or 100 items are to be displayed per page.
Buttons	
Blue arrow in the **Call no** column	Brings up the page with the **Edit station parameters**, **Edit station flags**, **Edit workpoint client data** and **Edit Group/CFW** tabs.
>	Moves one page forward.
<	Moves one page back.
>|	Moves to the end of the list.
|<	Moves to the beginning of the list.

Parameter Description of Tabs:

- **Secondary Gateway**
  Only for networked systems (multi-location)

Parameters	Description
Call number	Internal call number of the Mobility User.
Name	Name of the Mobility User.
Node ID	Input of the node ID via which the mobile subscriber is externally accessible.

4 V2R0.3: SIP Provider Profiles

Affected Documentation	Administrator Documentation
Issue	9
Reference No.	A31003-P3020-M100-09-76A9

4.1 Chapter 27.2.12.4, Application Diagnostics> Developer Settings> SIP Provider Profiles

Parameter Description of Tabs:

- **Add SIP Provider Profiles**
- **Edit SIP Provider Profiles**

Parameters	Description
Base Template	Selection of an empty template (default) or a predefined sample configuration for a particular service provider. This can be adapted to meet individual requirements and saved as a new ITSP.
Provider Name	Desired name of the ITSP. The configured ITSP will appear in the list of ITSPs under this name.
Serial Number	The provider's serial number
Domain Name	The Domain Name of the ITSP
Provider Registrar	
Use Provider Registrar	Must be selected if the ITSP works with registration.
IP Address / Host name	Domain name or IP address of the Registrar server (e.g., sip-voice.de)
Port	Port number of the Registrar server, e.g., 5060. Enter port 00 if the ITSP uses multiple servers and DNSSRV.
Reregistration Interval at Provider (sec)	Interval (in seconds) at which ITSP registration is repeated. The value of the interval must not be 0 and must not be set too high because on repeating the registration at the ITSP, a dropped connection can also be detected, and an alternate route (via ISDN or an alternate Provider) may be selected if required. Default value: 120 seconds
Provider Proxy	
IP Address / Host name	Domain name or IP address of the proxy server. The entry is mandatory and is usually identical to the provider registrar entry.
Port	Port number of the proxy server (e.g., 5060). As a rule, this is identical with the Provider port number. Enter port 0 if the ITSP uses multiple servers and DNSSRV.
Provider Outbound Proxy	
Use Provider Outbound Proxy	Only set if the SIP Provider uses an outbound proxy that is different from the provider proxy.
IP Address / Host name	Domain name or IP address of the outbound proxy.

Parameters	Description
Port	Port number of the outbound proxy. Enter port 0 if the ITSP uses multiple servers and DNSSRV.
Provider STUN	
Use STUN	Only set if the SIP Provider uses a STUN server. The system-wide setting under the STUN configuration applies as the STUN mode for all ITSPs.
IP Address / Host name	STUN IP address if the SIP Provider is using a STUN server.
Port	STUN port number if the SIP Provider is using a STUN server.
Buttons	
Delete Data	Deletes the SIP Provider Profile.

Related Topics

4.2 Chapter How to Configure SIP Provider Profiles

The SIP Provider Profiles wizard can be used to add, edit, delete, import and export SIP Provider profiles.

Prerequisites

- The Internet connection is operational.
- You are logged on to the WBM with the **Expert** profile.
- The following SIP Provider specific Internet access data is available:

Parameters	Description
Base Template	Selection of an empty template (default) or a predefined sample configuration for a particular service provider. This can be adapted to meet individual requirements and saved as a new ITSP.
Provider Name	Desired name of the ITSP. The configured ITSP will appear in the list of ITSPs under this name.
Serial Number	The provider’s serial number
Domain Name	The Domain Name of the ITSP
Provider Registrar	
Use Provider Registrar	Must be selected if the ITSP works with registration.
IP Address / Host name	Domain name or IP address of the Registrar server (e.g., sip-voice.de)
Port	Port number of the Registrar server, e.g., 5060. Enter port 00 if the ITSP uses multiple servers and DNSSRV.
Reregistration Interval at Provider (sec)	Interval (in seconds) at which ITSP registration is repeated. The value of the interval must not be 0 and must not be set too high because on repeating the registration at the ITSP, a dropped connection can also be detected, and an alternate route (via ISDN or an alternate Provider) may be selected if required. Default value: 120 seconds
Provider Proxy	
IP Address / Host name	Domain name or IP address of the proxy server. The entry is mandatory and is usually identical to the provider registrar entry.

Parameters	Description
Port	Port number of the proxy server (e.g., 5060). As a rule, this is identical with the Provider port number. Enter port 0 if the ITSP uses multiple servers and DNSSRV.
Provider Outbound Proxy	
Use Provider Outbound Proxy	Only set if the SIP Provider uses an outbound proxy that is different from the provider proxy.
IP Address / Host name	Domain name or IP address of the outbound proxy.
Port	Port number of the outbound proxy. Enter port 0 if the ITSP uses multiple servers and DNSSRV.
Provider STUN	
Use STUN	Only set if the SIP Provider uses a STUN server. The system-wide setting under the STUN configuration applies as the STUN mode for all ITSPs.
IP Address / Host name	STUN IP address if the SIP Provider is using a STUN server.
Port	STUN port number if the SIP Provider is using a STUN server.
Buttons	
Delete Data	Deletes the SIP Provider Profile.

Step by Step

1. In the navigation bar, click on **Expert Mode**.
2. In the navigation tree, click **Application Diagnostics> Developer Settings** .
3. In the menu tree, click on **SIP Povider Profiles**.
4. Click **Add** to set up a new SIP Provider profile. A configuration window for the new SIP Provider appears.
5. Assign a name of your choice for the SIP Provider profile in the **Provider Name** field.
6. Enter the values provided by your ITSP in the remaining areas (see table immediately after prerequisites).

   INFO: The values under the "Extended SIP Provider Data" may only be changed by authorized service personnel, in collaboration with Development!

7. Click **OK**.

   You have added a new SIP Provider profile. You are redirected to the initial SIP Provider Profile page.

8. Click **Edit** to reconfigure the parameters of the SIP Provider profile if needed. A configuration window for the SIP Provider appears.
9. Edit the required parameters.

   INFO: The values under the "Extended SIP Provider Data" may only be changed by authorized service personnel, in collaboration with Development!

10. Click **OK**.

    You have edited the SIP Provider profile. You are redirected to the initial SIP Provider Profile page.

11. Click **Export** to export the SIP Provider profiles if needed.

12. Click **OK** and then save the file in a directory of your choice.

    You have exported the SIP Provider profiles.

13. Click **Import** and select the SIP Provider profiles to be imported if needed.

14. Click **OK**.

    You have imported the SIP Provider profiles. You can check the new SIP Provider profiles under **Expert Mode> Telephony Server> Voice Gateway> Internet Telephony Service Provider**.

15. Click **Transfer to SIP** to transfer the SIP Provider profiles to SIP.

16. Click **Finish**.

    You have configured the SIP Provider profile parameters.

Related Topics

5 V2R0.3: Support Comtel3 and Highvoltage with SLMAV (OSBiz X8)

Affected Documentation	Administrator Documentation
Issue	9
Reference No.	A31003-P3020-M100-09-76A9

5.1 Chapter 27.3.7.10 Stations > Station > Station Parameters

Parameter Description of Tabs:

- **Edit station parameters**

Parameters	Description
Stations - ...	
Type	Type of the station.
Call number	Internal call number of the station.
Name	Freely selectable name for the station. Value range: max. 16 characters, no umlauts or special characters
Direct inward dialing	DID number of the station.
Device type	Displays the device associated with the subscriber.
Clip/Lin	Sequence of digits to be displayed at the called party instead of the actual number for outgoing external calls (e.g., for E911 emergency services in the USA) Value range: max. 16 digits
Access	Displays the physical interface at which the device is connected.
Fax	
Call number	If a fax box has been set up (e.g., with the UC clients myPortal for Desktop or myPortal for Outlook), the fax number at which fax messages from internal locations can be received by the subscriber should be entered here.
Direct inward dialing	If a fax box has been set up (e.g., with the UC clients myPortal for Desktop or myPortal for Outlook), the fax number at which fax messages from external locations can be received by the subscriber should be entered here.
Mobility	
Mobile phone number	Only for SIP clients and mobile users: For the One Number Service, this number is used for the authentication of DISA access via the mobile service. Enter the mobile phone number associated with the subscriber together with the dialout prefix (i.e., the CO code), e.g., 0017312345678).
Web Feature ID	The Web Feature ID defines how the subscriber should log in at the mobile web client (user name). Choice between "no" (Mobility Entry only) and "automatic" (internal call number of the subscriber) or selection of the station number of the client or phone from the drop-down list.

Parameters	Description
Parameters	
Station type	Type of the connected device (drop-down list)
Station type: **Standard**	System telephones or analog telephones
Station type: **Fax**	Fax machine, e.g., no override possible
Station type: **Loudspeaker**	For paging via the a/b port
Station type: **Answering Machine**	Only for analog: if an answering machine is connected to this interface, this setting enables a call to be taken over from the answering machine from any device even though the answering machine has already accepted the call. To do this, the terminal must be programmed with the internal call number of the analog station. Besides being selected for answering machines, this entry should also be selected for virtual ports where no physical equipment has been set up. This prevents the communication system from checking the operating status of the port. Only for virtual ports: If a station without access was configured as a type of answering machine in Manager E, the port must be additionally configured as a virtual port. Otherwise, it will not be visible as a station in the WBM.
Station type: **P.O.T. MW LED**	For standard analog telephones (P.O.T = Plain Old Telephone) with a message-waiting LED Not for U.S.
Station type: **Door station with pulsed loop**	When using a pulsed loop device with the door opener function
Station type: **Modem**	Call override is not possible with this setting. It is intended for modems.
	When a fax or modem station is deleted (i.e., the call number and DID are deleted), the extension type must also be reset to the default (standard).
Language	Language for the menu control of the device (system telephone).
Call signaling internal	Every station can be assigned one of a total of eight possible internal ringing tones here. This means that in addition to the external ringing tone, an internal ringing tone is assigned here and subsequently transmitted for internal calls. Default value: Ring type 1
Call signaling external	Three different ring types for signaling external calls can be selected here: – System Phones: Ring type 1 = External call (e.g., double ring), Ring type 2 = External call CO 2 (e.g., triple ring), Ring type 3 = External call CO 3 (e.g., short/long/short) – Analog telephones for Germany: Ring type 1 = External call, Ring type 2 = Automatic recall, Ring type 3 = Door bell ring – Analog telephones for other countries: Ring type 1 = External call, Ring type 2 = External call, Ring type 3 = External call Default value: Ring type 1
Class of Service (LCR)	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). Default value: 15
Hotline Mode	Selection of the hotline options
Hotline Mode: **off**	Disables the hotline feature.

Parameters	Description
Hotline Mode: **Off-hook alarm after timeout**	The call to the hotline takes place after a predefined delay (off-hook alarm time), see Telephony/Basic Settings/System/Intercept-Attendant-Hotline
Hotline, Mode: **Hotline**	Enables the hotline feature. On lifting the handset, the connection to the hotline destination is established immediately, see Telephony/Basic Settings/System/ Intercept-Attendant-Hotline
Hotline	For details on selecting hotline destinations, see Telephony/ Basic Settings/System/ Intercept-Attendant-Hotline
Hotline: **none**	No destination defined
Hotline: **Digits 1 to 6**	For details on hotline destinations, see Telephony/ Basic Settings/System/ Intercept-Attendant-Hotline
Payload Security	Only for IP system clients: enable or disable the encryption of phone conversations (SPE). To do this, all stations involved must have SPE enabled.
MWI protocol	Selection of MWI protocol for analog stations. Available only for SLMAVx (OSBiz X8), 4SLAV onboard and SLAVx OSBiz X3,X5.
MWI protocol: Comtel3	Comtel 3 protocol selected. Default value.
MWI protocol: High Voltage	The formatting of <TEXT> following a <p> is not supported. Wrap the <TEXT> that follows in a <p>. High Voltage protocol selected.
Buttons	
>	Moves to the next station. If the stations matching the search term entered in the **Search** fields were previously filtered, it is possible to move between only those specific stations.
<	Skips back one station.

Parameter Description of Tabs:

- **Edit station flags**

Parameters	Description
Stations - ...	
Type	Type of the station.
Call number	Internal call number of the station.
Name	Station name.
Station flags	
Override class of service on	When this flag is activated, the subscriber can break into (i.e., override) an internal subscriber's ongoing connection. The subscribers involved are notified of the busy override by a warning tone and a display message. Default value: Disabled

Parameters	Description
Override Do Not Disturb	When this flag is activated, the following applies: when the subscriber calls a station for which Do Not Disturb has been activated, he or she can override Do Not Disturb. After five seconds, the call is signaled at the called station. If the flag is disabled, the Do Not Disturb function cannot be overridden. Subscribers who call a station for which Do Not Disturb has been activated receive the busy tone. Default value: Disabled
FWD external permitted	When this flag is activated, the subscriber can activate call forwarding to an external destination. Charges incurred for the execution of an external call forwarding are allocated to the subscriber who activated the call forwarding. Default value: Enabled
Prevention of voice calling off	When this flag is activated, the station can be called directly. This enables an internal call to be set up without lifting the handset. The loudspeaker on the called station is activated automatically in the process. Default value: Enabled
DISA class of service	When this flag is activated, external subscribers can activate or deactivate functions of the communication system via DISA (Direct Inward System Access) and set up outbound external connections just like any other internal subscribers. This also includes activating and deactivating call forwarding, the Do Not Disturb feature and the lock code, for example. Default value: Disabled
Transit allowed via Hook-on	When this flag is activated, the subscriber can transfer an external call to another external subscriber by hanging up. Example: The subscriber is the conference controller and hangs up: if there are other internal subscribers still in the conference, the longest participating internal subscriber automatically becomes the conference controller. If there are only external participants remaining in the conference, the conference is terminated, and all connections are cleared. Default value: Disabled
System telephone lock reset	When this flag is activated, the subscriber can reset the individual lock code of other internal subscribers to the default code. Default value: Disabled
CLIP analog (only for analog devices)	When this flag is activated, the caller's phone number is shown on the phone display of the analog station. As a prerequisite, the analog phone of the subscriber must support CLIP (Calling Line Identification Presentation). Default value: Enabled
MCID access	When this flag is activated, the subscriber can have malicious external callers identified via the ISDN Central Office. As a prerequisite, the "Trace call" (Malicious Call Identification, MCID) feature must have been applied for and activated by the network provider. After the "Trace call" feature has been activated by the network provider, the following must be noted: for each incoming call from the ISDN CO, the release of the connection to the called station is delayed for a specific timeout period after the caller hangs up. This timeout enables the called station to activate the "Trace call" feature. The ISDN trunk availability is somewhat reduced as a result. Default value: Disabled

Parameters	Description
Entry in telephone directory	When this flag is activated, the name and number of the subscriber will be displayed in the system directory. Default value: Enabled
Editing the Telephone Number	When this flag is activated, the subscriber can edit the digits of the call number entered via the keypad before the digit transmission. This requires a system phone with a display. Default value: Disabled
No group ringing on busy	When this flag is enabled, the following applies: The status of the station with group ringing programmed (i.e., the primary station) determines whether or not group ringing occurs. If the primary station is free, all stations included in the group are called immediately. If call waiting is enabled at the primary station: all stations included in the group are called after a delay of 5 seconds. If the primary station cannot receive a call or if call waiting is inactive: group ringing does not take place. Default value: Disabled
Associated dialing/services	Associated dialing: when this flag is activated, the subscriber can dial a number on behalf of another internal subscriber as if that station itself were dialing. Associated services: When this flag is activated, the subscriber can control features on behalf of another internal subscriber as if that station itself were controlling these features. This includes activating and deactivating call forwarding, group ringing and the lock code, for example. Default value: Disabled
Call waiting rejection on	When this flag is activated, subscribers who are conducting a call are not informed about other incoming calls via a call waiting tone or a display message. Default value: Enabled
Discreet call	When this flag is activated, the subscriber can discreetly join an existing voice call of another internal subscriber. He or she can silently monitor the call and speak with the internal subscriber without the other party hearing this conversation. This is only possible in the case of a two-party call. Discreet calling is not possible with consultation calls or conferences. Default value: Disabled
Discreet Call Lock	When this flag is activated, the station cannot be called discreetly. Default value: Disabled
DTMF-based feature activation	Only relevant for Mobility Entry stations: This flag must be set in order to be able to activate features during a call (i.e., in the talk state). The code receiver remains active. (Attention: limited resources) Default value: Disabled
Headset	When this flag is activated, the station can be equipped with a headset that plugs into the handset connection. Setting the flag enables the user to accept a call by pressing a headset button on the system telephone without lifting the handset. When a headset is connected to the system telephone connection, it is recognized automatically by the communication system; an authorization enable is not necessary in this case. When this flag is set, calls cannot be released by pressing the speaker key; a disconnect key must be programmed so that calls can be released. Default value: Disabled

Parameters	Description
Last destination mailbox active	If this flag is activated and the called party is not available, the call is forwarded to the substitute mailbox, and the caller's number is displayed on the substitute telephone. Default value: Disabled
Call prio./immed. tone call wait.	When this flag is activated (Call priority/immediate tone call waiting), calls through this station are signaled with a higher priority to partners. The priority is set to be the same as the priority of external calls. In other words, the prioritized calls are thus queued before existing internal calls, but after existing external calls. Note that existing first calls (not waiting calls) are usually never displaced, regardless of their ring type. If the same priority is also to be set for an internal call in another node, then the station flag "Call prio./immed. tone call wait." (Area: Circuit flags, Call prio./immed. tone call wait.) must be likewise set for the corresponding trunk. If this flag is set, the caller receives a ring tone immediately instead of a busy tone. This has no impact on the acoustic signaling. The prioritized calls are still signaled like an internal call. This feature is important for phonemail connections. Default value: Disabled
Voice recording	If the flag is activated, the subscriber can activate voice recording during a call. In addition, the "Warning tone during voice recording" switch under Flags can be used to specify whether or not a warning tone should be output on starting the voice recording. Furthermore, a suitable Live Recording device must be configured under PhoneMail. If the IVM is to be used for voice recording, then the maximum length of the voice recording can be set via "IVM | Additional Settings/General", and the appropriate signaling method to be used before starting a voice recording (if any) can be defined. Default value: Disabled
Compress display data	When this flag is enabled, the display outputs are compressed for improved performance. If the display on a UP0/E terminal changes, the communication system only updates the data that differs from the previous display. If an application (e.g., Smartset/TAPI) is connected via an RS 232 adapter (data or control adapter), this feature must be deactivated. The flag must be deactivated for applications that obtain the call number information from the telephone's display, (i.e., uncompressed output with call number instead of compressed output with name). Names are generally displayed only when the flag "Calling ID only" under "Display name/call number" is deactivated. Default value: Enabled
Door release DTMF	If this flag is enabled, the station can open a door with the DTMF/MFV code signaling when a door relay is connected to the relevant port. Default value: Disabled
Autom. connection, CSTA (only for OpenStage SIP telephones)	When the flag is enabled, the following applies: speakerphone mode is activated on the associated SIP telephone when dialing or answering calls via myPortal or myAttendant. The information contained in the documentation of the SIP telephone must be observed, since additional settings on the SIP phone may be required for the proper use of the feature. When the flag disabled, the call setup occurs only after lifting the handset. Default value: Enabled
Call Monitoring (for specific countries only)	When this flag is activated, the subscriber can silently monitor (i.e., listen in on) the conversation of any internal subscriber. The microphone of the party listening in is automatically muted. The monitored subscriber is not notified via a signal tone or display message. When you start and end call monitoring, you may encounter a lapse of up to two seconds of the conversation. Default value: Disabled

Parameters	Description
Disable handsfree microphone	If this flag is activated, the handsfree microphone cannot be used. This flag is only supported by OpenStage phones. Default value: Disabled
Forced Number Presentation	If this flag is activated, the caller's phone number appears on the display of the called party instead of his or her name. Default value: Disabled
Usage (for specific countries only)	This drop-down list can be used to configure the output current of the interfaces of an analog board (in mA, e.g., 27 mA for China).
Operating Mode	In this drop-down list, an operating mode can be selected for the subscriber line.
Payload Security (only for TDM system telephones)	If this flag and the **SPE Support** system flag are activated, the Signaling & Payload Encryption (SPE) feature is supported for the selected subscriber(s). The signaling and payload data for this/these subscriber/s is encrypted. An option can be set to indicate in the display whether or not a part of a connection path to an IP station is encrypted (off = no information is displayed). The payload security setting does not work for any other telephones. Default value: Disabled
Missed Calls List	When this flag is activated, the missed calls list is activated for the subscriber at his or her telephone (only for phones with a display). Calls that were not answered by the subscriber are provided with a time stamp (time and date) and added to a chronologically sorted list. Only the calls which also contain a phone number or name are recorded. If a subscriber calls more than once, only the time stamp for the entry is updated, and a call counter for that caller is incremented.
Central busy signaling	This flag must be set (see also QSIG features) for subscribers who have busy signaling on a centralized communication system. Does not apply to the USA. The implementation of central busy signaling is contingent on a maximum number of 100 stations per node.
Display of Emergency text	If this flag is activated, a configurable Emergency text is shown on the phone's display in emergency mode.
Priority for outbound calls	
Call Supervision	
Buttons	
>	Moves to the next station. If the stations matching the search term entered in the **Search** fields were previously filtered, it is possible to move between only those specific stations.
<	Skips back one station.

Parameter Description of Tabs:

- **Edit workpoint client data**

Parameters	Description
Stations - ...	
Type	Type of the station.
Call number	Internal call number of the station.
Name	Station name.

Parameters	Description
Parameters	
Status message	For system clients only: this flag activates the "keep-alive" mechanism for system telephones. If a system phone fails, for example, it is flagged as inactive after four minutes. The flag must not be enabled when setting up a system telephone as a home client or when using the "Short-Hold" feature. Disabling this flag reduces the message traffic between the communication system and the system telephones.
Authentication active	If you want the IP client to be able to identify himself/herself at the communication system with a password, authentication must be activated and a password set. This is an advantage especially for clients that are not connected to the internal LAN, but that dial in from outside.
New password	Password for authentication.
Confirm password	Password to repeat the authentication.
SIP User ID / Username	Only for SIP clients: freely selectable user name for authentication of the SIP subscriber, e.g., "SIP-120". The value defined here must also be entered at the SIP telephone.
Realm	Only for SIP clients: freely selectable names for the associated zone, e.g., "OSBIZ-SIP". This value must be the same for all SIP clients. The value defined here must also be entered at the SIP telephone.
Fixed IP address	For SIP clients only: entering a fixed IP address ensures that only one SIP client can log on to the system with this IP address. If this flag is activated, the IP address and the call number are verified. If this flag is not activated, only the call number is verified.
IP Address	Only for SIP clients: IP address of the SIP client (e.g., the IP address of the SIP telephone)
Type	Only for system clients: A mobile IP client (Mobile option) is not permanently assigned to any IP phone. The call no. of a mobile IP client can be used by a subscriber to log on to any IP terminal (that permits this) via the logon procedure (*9419) (provided the option Mobile blocked is not activated).
Type: **Mobile**	Only for system clients: No IP device is permanently assigned to the subscriber. The feature is only supported from the third station port onwards.
Type: **Non-mobile**	Only for system clients: The call number is permanently assigned to the IP device of the subscriber. When using a WLx phone, the option Non mobile must be set before registering the WLx phone with the communication system.
Type: **Non-mobile and blocked**	Only for system clients: A subscriber cannot log into this IP device with a mobile system client.
Blocked for Deskshare User	Only for system clients: This system phone can be shared by multiple subscribers (Desksharing).
Secondary system ID	This parameter has two different functions: 1. For all stations: defines the multi-location gateway assigned to the station. 2. Only for system clients: If the "Emergency" flag has been set (under the "Stations/ IP Clients/Secondary Gateway") for networked systems, the node ID of the failover system for system clients can be entered here.
Internet registration with internal SBC	Enables the SIP@Home feature. This makes it possible for an external STUN-enabled SIP phone to register at OpenScape Business over the Internet and thus be used as an internal telephone.

Parameters	Description
Buttons	
>	Moves to the next station. If the stations matching the search term entered in the **Search** fields were previously filtered, it is possible to move between only those specific stations.
<	Skips back one station.

Parameter Description of Tabs:

- **Edit Group/CFW**

Parameters	Description
Stations - ...	
Type	Type of the station.
Call number	Internal call number of the station.
Name	Station name.
Call forwarding	
Day destination	Displays the call forwarding destinations for incoming external calls during the day (see the wizard User Telephony/Call Forwarding)
Night destination	Displays the call forwarding destinations for incoming external calls during the night (see the wizard User Telephony/Call Forwarding).
Internal destination	Displays the call forwarding destinations for incoming internal calls (see the wizard User Telephony/Call Forwarding).
Class of Service	
Day	Every subscriber can be assigned a class of service for day. There are 15 classes of service to choose from (see Telephony/Classes of Service).
Night	Every subscriber can be assigned one class of service for night. There are 15 classes of service to choose from (see Telephony/Classes of Service).
Call Pickup	
Group	Every station can be assigned to a call pickup group. You can choose between 32 call pickup groups (120 with OSBiz S; see also Incoming Calls / Call Pickup).
Buttons	
>	Moves to the next station. If the stations matching the search term entered in the **Search** fields were previously filtered, it is possible to move between only those specific stations.
<	Skips back one station.

6 V2R0.3: RSP.servicelink enhancements

Affected Documentation	Administrator Documentation
Issue	9
Reference No.	A31003-P3020-M100-09-76A9

6.1 Chapter 24.11.1 RSP.servicelink and SSDP V1

RSP.servicelink (**R**emote **S**ervice **P**latform) and SSDP-V1 (**S**mart **S**ervices **D**elivery **P**latform) offer 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. Only an Internet connection, a web browser and the partner ID of the remote service partner are required for this. With RSP.servicelink, a partner password is additionally required. RSP.servicelink and SSDP V1 ensure a high bandwidth and maximum security.

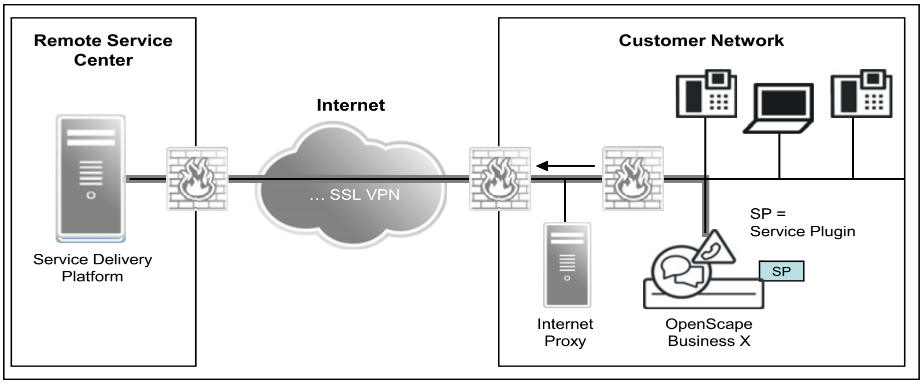
RSP.servicelink is the evolution of SSDP V1 and is based on OpenVPN technology. It uses the SSL/TSL protocol and encryption and provides the highest level of security with an additional client certificate. SSDP V1 will still be supported for some time, but RSP.servicelink should be the preferred remote service. The term RSP.servicelink/SSDP V1 is abbreviated to RSP/SSDP in the documentation.

RSP/SSPD offers the following major advantages in combination with OpenScape Business:

- Maximum 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 in the firewall of the customer. High security for the customer network is thus guaranteed.
  With RSP/SSDP, 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 so-called service plugins for RSP.servicelink and SSDP V1. When activating the service plugin, the partner ID of the Remote Service Partner (and also the partner password for RSP.servicelink) must be entered.
  Every remote service partner who uses the RSP.servicelink or SSDP V1 has a separate partner ID. The preset partner ID "Unify" can be used to activate remote access by authorized service personnel of the manufacturer.
- Future-proof
  RSP/SSDP 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/SSDP supports all the usual Web Services Standards, including the Hypertext Transfer Protocol (HTTP), 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 and with a 128-bit SSL encryption for SSDP.

Service Plugins

There are separate service plugins for the RSP.servicelink and SSDP V1 services, which can be enabled or disabled individually.

The service plugins must be reset after the mainboard has been replaced, for example. Resetting the service plugin deletes the entire RSP or SSDP configuration and disables the plugin.

Device Management (Managed Device / Device SPoA)

In the case of SSDP V1, in communication systems without a UC Booster, remote access to further devices (e.g., Xpressions Compact) in the customer LAN can be enabled using Device Management (Managed Device).

> ***INFO:*** Remote access to other OpenScape Business communication systems in the customer LAN is not possible.

With RSP, the Managed Device corresponds to the so-called SPoA (Single Point of Access) Device. The configuration of the SPoA Device occurs on the SIRA side.

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 each of the service plugins RSP.servicelink and SSDP V1.
- 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.
  Activation enables the service plugin for which the associated service was set to **Primary**. Deactivation causes both the SSDP V1 Service plugin and the RSP Service plugin to be disabled.

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

> ***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.

6.2 Chapter 24.11.1.8 How to Migrate the Remote Access of an OpenScape Business from SSDP to RSP.servicelink

In this chapter you will find all necessary steps to migrate the OpenScape Business remote connectivity from SSDP to RSP.servicelink. This can be performed remotely. In case of on-site migration, steps 1 to 2 can be performed on-site.

Prerequisites

- Upgrade to OpenScape Business V1 R3.4 or OpenScape Business V2.
- The OpenScape Business must be able to reach the IP addresses https://188.64.18.51; https://188.64.17.5, https://188.64.18.50; and https://188.64.17.50. The firewall must be opened for these addresses.

Step by Step

1. Search for the relevant device in SSDP and establish a SSDP connection to the OpenScape Business Assistant.
2. OS Business configuration for RSP.servicelink:
   a) In the OpenScape Business Assistant, navigate to Service Center / Remote Access.

   b) Select Registration / Configuration in the RSP.servicelink column.

   c) Enter the proxy data if necessary.

   d) Register the device with its partner ID and password, and define a device name (optional).

   e) After the installation of RSP.servicelink, select Activation of RSP.servicelink connection and assign it as primary remote access.

   Successful case: Device status is “connected” and Device appears in SIRA Equipment Explorer with MAC address and device name.

   Error case: Error message is displayed and device status is “not connected”. Device does not appear in the SIRA Equipment Explorer.

   If connection fails, check the customer firewall settings. If the required IP Addresses are blocked, contact the customer administrator and make sure the IP-Addresses of the Registration Server (https://188.64.18.51; https://188.64.17.51) and the central RSP Server (https://188.64.18.50; https://188.64.17.50) are not blocked.
3. Final device configuration in the Remote Center (Admin account necessary):
   a) Search for the device in the SIRA Equipment Explorer.finalize device configuration. Add customer data, Single Sign On or special notes for the customer and add Applications and Products, e.g. Booster card, Xpressions Compact and Applications behind the OS Business (e.g. Contact Center,…)

   b) Add customer data, Single Sign On or special notes for the customer.

   c) Add Applications and Products, e.g. Booster card, Xpressions Compact and Applications behind the OpenScape Business (e.g. Contact Center,…).

4. Test connection from Remote Center:
   a) Start a connection to the OpenScape Business to check the connectivity and Single Sign On (if configured).
   b) Check the connection to other configured Applications and Products.
5. SSDP V1 deactivation and deinstallation in the OpenScape Business:
   a) Use the new RSP.servicelink connection to connect to the same device.
   b) Navigate to Service Center / Remote Access.
   c) Select Deactivation in the SSDP V1 column.
   d) Select Registration / Configuration and choose the "Deinstallation" button.
6. Delete the OpenScape Business in the SSDP Enterprise.
   a) After the connection test, the deactivation and deinstallation of SSDP in the OpenScape Business, delete the device entry in the SSDP Enterprise Server.

V2R0.3: RSP.servicelink enhancements

Chapter 24.11.1.8 How to Migrate the Remote Access of an OpenScape Business from SSDP to RSP.servicelink

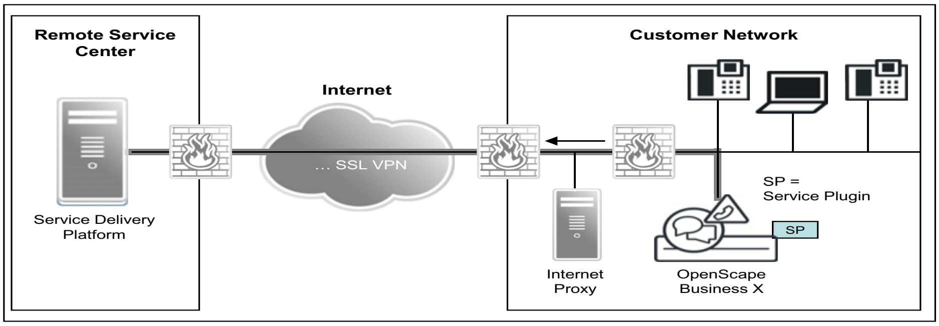
7 V2R0.3: VPN access from mobile Android Devices

Affected Documentation	Administrator Documentation
Issue	9
Reference No.	A31003-P3020-M100-09-76A9

7.1 Chapter 19.3.2 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.

7.2 Chapter 19.3.2.1 How to Connect Teleworkers via a VPN

The **VPN** wizard can be used to grant VPN teleworkers (VPN partners) access to the internal LAN and to connect communication systems via a VPN (virtual private network). If the communication system does not have any fixed external IP address (public IP address, global IP address), a DynDNS service will need to be configured (at www.dyndns.org, for example).

Prerequisites

- Internet access via the WAN interface has been configured.
- If the WAN interface has no fixed (public) IP address, DynDNS must be configured. A connection to the Internet is required for a successful DynDNS test.
- You are logged on to the WBM with the **Advanced** profile.

Step by Step

1. In the navigation bar, click on **Setup**.
2. In the navigation tree, click **Wizards > Network / Internet**.
3. Click **Edit** to start the **VPN Configuration** wizard. The default setting is **VPN is switched off**.
4. Click **Configuration of VPN**.
5. If you want to edit a configured VPN connection, click on **Edit** for the desired VPN connection.
6. If you want to create a new VPN connection, click on **Add**.
7. Enter a name for the VPN connection (e.g., `node2mch.dyndns.org`) in the **System name** field.
8. If desired, enter a **Comment** in the corresponding field.
9. Select the **enabled** check box (already preset by default).
10. Select the check box **Use Data of own System**.
11. If required, select the **Address Type**:
    - If the WAN interface has a fixed (public) IP address, select the entry **IP Address** from the **Address Type** drop-down list and enter the fixed (public) IP address under **Global Address / DNS Name (WAN)**.

- If the WAN interface does not have a fixed (public) IP address, select the entry **DNS Name** from the **Address Type** drop-down list. The DNS name of the communication system that is already configured for DynDNS will be displayed under **Global Address / DNS Name (WAN)**.

12. The **Local IP Address (LAN)** should only be changed if required.

13. The **Local Subnet Mask (LAN)** should only be changed if required.

14. If you want to edit one of the already configured teleworkers, click on **Edit** next to the desired teleworker in the **Teleworkers** area.

15. If you want to create a new teleworker, click on **Add** in the **Teleworkers** area.

16. Enter a teleworker configuration name in the **Name** field.

17. Configure the type of the VPN client being used:

- For pure IPSec VPN teleworkers (NCP and Shrew Soft VPN Clients):

  Clear the **L2TP/IPSec** check box and select the **IP Address** as **Address Type**. Enter a virtual IP address / DynDNS name for the teleworker in the field **Virtual IP address/DynDNS Name** if the VPN client being used supports virtual IP addresses (regardless of whether the teleworker has an Internet connection via a DSL router or DSL modem).

- For L2TP/IPSec VPN teleworkers (iOS, Android and MAC OS X VPN clients):

  Select the **L2TP/IPSec** check box and assign a **User name** and a **Password** to the teleworker.

18. Select the **enabled** check box (already preset by default).

19. Click **OK**. The window with the overview of teleworkers is displayed again. You can enter further teleworkers.

20. When you have set up all teleworkers, click **OK & Next**. The **System Selection** window is displayed.

21. Click **OK & Next**. The **Security setup for connections** window appears.

22. To ensure a secure VPN connection, assign a key for the newly configured VPN connection under **PreShared Secret** and repeat it under **Repetition of the PreShared Secret**. The key must be at least 20 characters in length.

23. Enter a **Comment** if required.

24. Click **OK**. The **VPN Status Information** window appears.

25. Click on **Switch VPN on**.

26. Only if the address type DNS Name has been selected: Check the already configured data of the DynDNS account and click on **Connection test**. The DNS access data is now transmitted to the service provider. This procedure takes approximately 10 seconds. If the test is not successful, check your access data. After the test succeeds, click **OK**.

27. Click **OK & Next**. The teleworkers can now access the WAN interface of the communication system.

28. Click **Finish**.

7.3 Chapter 19.3.6 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.

7.4 Chapter 19.3.6.4 How to Configure an iOS or Android VPN Client

An L2TP VPN connection must be configured on the teleworker device for a secure VPN connection to the communication system.

Prerequisites

- The administrator of your communication system has configured you as a teleworker in the WBM of OpenScape Business and has communicated the user name, the password and the PreShared secret key for the VPN connection to you.
- The teleworker device has an existing and active connection to the Internet.

Step by Step

1. Open the **Settings > General > VPN** menu on the iOS or Android teleworker device.
2. Click on **Add VPN** to add a new VPN connection.
3. Click on the **L2TP** tab.
4. Enter a name for the VPN connection in the **Description** field.
5. Enter the public IP address or the DNS name of the communication system in the **Server** field.
6. Enter the teleworker user name in the **Account** field.
7. Enter the teleworker password in the **Password** field.
8. Enter the PreShared secret key for the VPN tunnel in the **Shared Secret** field.
9. Enable the **For all data** option.
10. Select the **VPN** option in the **Settings** menu.

8 V2R0.3: Improved SSL certificate handling

Affected Documentation	Administrator Documentation
Issue	9
Reference No.	A31003-P3020-M100-09-76A9

8.1 Chapter 19.27.3.2.9 Security > VPN > Lightweight CA

Parameter Description of Tabs::

- **Generate CA Certificate**

<table>
<tr><th>Parameters</th><th>Description</th></tr>
<tr><td><b>Name of the Certificate</b></td><td>Freely definable flat name for the generated certificate</td></tr>
<tr><td><b>Serial Number of Certificate</b></td><td>Input of a serial number that you specify. This number must be a positive integer.</td></tr>
<tr><td><b>Type of Signature Algorithm</b></td><td>Selection of the signature algorithm to be used for this certificate
Value range: md5RSA, sha1RSA, sha25RSA, sha512RSA</td></tr>
<tr><td><b>Public key length</b></td><td>Selection of a key length used for this certificate
Value range: 1024, 1536, 2048</td></tr>
<tr><td colspan="2"><b>Start Time of Validity Period (GMT)</b>
Point of time as of which the certificate should be valid. The time specified is interpreted as Greenwich Mean Time (GMT).</td></tr>
<tr><td colspan="2"><b>End Time of Validity Period (GMT)</b>
Point of time until which the certificate should be valid. The time specified is interpreted as Greenwich Mean Time (GMT).</td></tr>
<tr><td colspan="2"><b>Subject Name</b>
Input of the subject name data of the certificate applicant according to the conventions of the X.509 standard (e.g., DE for Germany in the Country (C) field).</td></tr>
<tr><td colspan="2"><b>Alternative Subject Name</b>
This optional information distinguishes between the Distinguished Name Format (such as the data under Subject Name) and some other format (for example, the IP address entry). The input mask depends on the selected format. If other format is selected, more than one SAN entries is possible to be configured.</td></tr>
<tr><td><b>Distinguished Name Format</b></td><td></td></tr>
<tr><td><b>Other Format</b></td><td></td></tr>
<tr><td><b>Subject Alternative Name Extension</b></td><td>Value range: DNS Name, IP Address, E-mail Address, Uniform Resource Indicator, Other</td></tr>
<tr><td><b>Alternative Subject Name</b></td><td></td></tr>
</table>

Parameters	Description
CRL Distribution Point Type	Value range: DNS Name, IP Address, E-mail Address, Uniform Resource Indicator, Other
CRL Distribution Point	Specification of a URL from where the Certificate Revocation Lists (CRL) will be distributed.
Generate Certificate	

8.2 Chapter 27.3.2.13 Security > VPN > Peer Certificates

Parameter Description of Tabs::

- **Generate Certificate Signing Request (CSR)**
- **Import Peer Certificate (PKCS#12)**

Parameters	Description
Certificate Request Name	A CA-signed peer certificate based on a CA certificate can be generated. This requires at least one CA certificate to have already been generated. The certificate generated is saved in a PKCS#12 file. PKCS#12 files (Personal Information Exchange Syntax Standard) save certificates with the private key. A PKCS#12 file therefore contains the necessary data for personal encryption and decryption.
Type of Signature Algorithm	Select the signature algorithm to be used for this certificate. Value range: md5RSA, sha1RSA, sha25RSA, sha512RSA
Public key length	Value range: 1024, 1536, 2048
Subject Name	Subject name data of the certificate applicant according to the conventions of the X.509 standard (e.g., DE for Germany in the Country (C) field).
Country (C)	
Organization (O)	
Organization Unit (OU)	
Common Name (CN)	
Alternative Subject Name	This optional information distinguishes between the Distinguished Name Format (such as the data under Subject Name) and Other Format (for example, the IP address entry). The input mask depends on the selected format. If other format is selected, more than one SAN entries is possible to be configured.
Distinguished Name Format	
Country (C)	
Organization (O)	
Organization Unit (OU)	
Common Name (CN)	
Other Format	

Parameters	Description
Subject Alternative Name Extension	Value range: DNS Name, IP Address, E-mail Address, Uniform Resource Indicator, Other
Subject Alternative Name	This optional information distinguishes between the Distinguished Name Format (such as the data under Subject Name) and Other Format (for example, the IP address entry). The input mask depends on the selected format.
Import Peer Certificate [PKCS#12]	
Name of the Certificate	
Passphrase for decryption	Password to decrypt the peer certificate Value range: min. 7 and max. 32 characters
File with Certificate	Click on Browse. A search dialog is displayed.
View Fingerprint of Certificate	
Import Certificate from File	

8.3 Chapter 27.3.2.21 Security > SSL > Certificate Generation

Administrative access is encrypted over HTTPS using the SSL/TLS protocol. Certificates are used to authenticate the connection. By default, a self-signed certificate is used. A customer-specific certificate issued by a certificate authority (CA) can be used to enhance security. The communication system uses the certificates generated or imported by the WBM for authentication at the admin 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.

Parameter Description of Tabs::

- **Generate CA Certificate**
- **Generate Self-Signed Certificate**

Parameters	Description
Name of the Certificate	Name of the certificate to be generated.
Serial Number of Certificate	Serial number for the certificate. This number must be a positive integer
Type of Signature Algorithm	Signature algorithm to be used Value range: md5RSA, sha1RSA, sha256RSA, sha512RSA
Public Key Length	Value range, default value: 1024 - 1536, 2048
Start Time of Validity Period (GMT) Point of time as of which the certificate should be valid. The time specified is interpreted as Greenwich Mean Time (GMT).	
Day, Month, Year, Hrs, Mins, Sec.	Time specification units for the certificate validity period

Parameters	Description
End Time of Validity Period (GMT)	
Point of time until which the certificate should be valid. The time specified is interpreted as Greenwich Mean Time (GMT)	
Day, Month, Year, Hrs, Mins, Sec.	Time specification units for the certificate validity period
Subject Name	
Subject name data of the certificate applicant according to the conventions of the X.509 standard (e.g., DE for Germany in the Country (C) field). All four fields must be filled.	
Country (C)	
Organization (O)	
Organization Unit (OU)	
Common Name (CN)	
Alternative Subject Name	
This optional information distinguishes between the Distinguished Name Format (such as the data under Subject Name) and Other Format (for example, the IP address entry). The input mask depends on the selected format. If other format is selected, more than one SAN entries is possible to be configured.	
Distinguished Name Format	
Other Format	
Subject Alternative Name Extension	
Subject Alternative Name	
CRL Distribution Point Type	
CRL Distribution Point	The location from which certificate revocation lists (CRL) are to be distributed can be optionally specified here (with a URL)

8.4 Chapter 27.3.2.23 Security > SSL > Certificate Management > Server Certificates

Parameter Description of Tabs::

- **Generate Certificate Signing Request (CSR)**
- **Import Server Certificate (PKCS#12)**
- **View a Certificate**
- **Remove Certificate**
- **Export Certificate (X.509)**
- **Import Updated Certificate (X.509)**
- **Activate Certificate**

Parameters	Description
Certificate Request Name	Name of the certificate to be generated.
Type of Signature Algorithm	Signature algorithm to be used for this certificate Value range: md5RSA, sha1RSA, sha256RSA, sha512RSA
Public Key Length	Value range: 1024, 1536, 2048
Subject Name Subject name data of the certificate applicant according to the conventions of the X.509 standard (e.g., DE for Germany in the Country (C) field). All four fields must be filled.	
Country (C)	
Organization (O)	
Organization Unit (OU)	
Common Name (CN)	
Alternative Subject Name This optional information distinguishes between the Distinguished Name Format (such as the data under Subject Name) and Other Format (for example, the IP address entry). The input mask depends on the selected format. If other format is selected, more than one SAN entries is possible to be configured.	
Distinguished Name Format	
Other Format	
Subject Alternative Name Extension	(optional) Value range, default value: DNS Name, IP Address, E-mail Address, Uniform Resource Indicator, Other
Subject Alternative Name	(optional)
Name of the Certificate	Name of the certificate to be imported.
Passphrase for decryption	Password that was used when the file was created. Value range: 7 to 32 characters
File with Certificate	Enter the required certificate in the **File with Certificate** field or select it using Browse. The **Fingerprint** of the certificate must displayed first and can then be imported.

V2R0.3: Improved SSL certificate handling
Chapter 27.3.2.23 Security > SSL > Certificate Management > Server Certificates

9 V2R0.3: Windows 10 OS

Affected Documentation	Administrator Documentation
Issue	9
Reference No.	A31003-P3020-M100-09-76A9

9.1 Chapter 12.2.6 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
- 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: 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)

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

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)

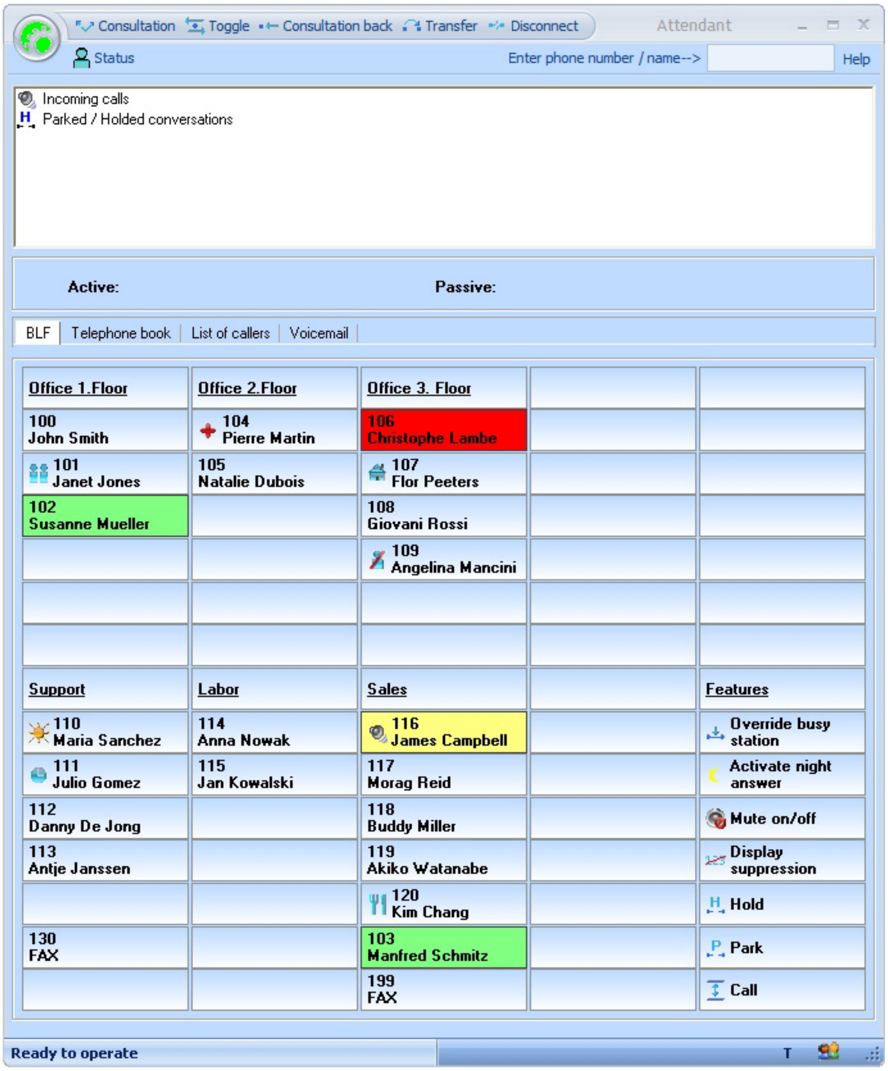
Hardware Prerequisites: The number of installable clients depends on the server performance and on the amount of available memory. If the server is also being used for other applications, their memory requirements must also be taken into account.

More information on the configuration of Citrix XenApp Server can be found under:

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

9.1.0.1 Chapter 16.3 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 with a BLF server, the OpenScape Business Attendant can be expanded to show network-wide BLF and presence information.



Incoming calls
Parked / Holded conversations

Active:

Passive:

Office 1.Floor	Office 2.Floor	Office 3. Floor		
100 John Smith	104 Pierre Martin	106 Christophe Lambe		
101 Janet Jones	105 Natalie Dubois	107 Flor Peeters		
102 Susanne Mueller		108 Giovani Rossi		
		109 Angelina Mancini		
Support	Labor	Sales		Features
110 Maria Sanchez	114 Anna Nowak	116 James Campbell		Override busy station
111 Julio Gomez	115 Jan Kowalski	117 Morag Reid		Activate night answer
112 Danny De Jong		118 Buddy Miller		Mute on/off
113 Antje Janssen		119 Akiko Watanabe		Display suppression
		120 Kim Chang		Hold
130 FAX		103 Manfred Schmitz		Park
		199 FAX		Call

Ready to operate

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 (network-wide exclusively with BLF server):

- 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)

Three 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 *Chapter 12.2.6 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

9.2 Chapter 16.3.1 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

9.3 Chapter 16.3.2 BLF server

The BLF server distributes busy indicators and presence states to OpenScape Business Attendant and OpenScape Business BLF and is used primarily for networking OpenScape Business systems.

The BLF server establishes connections to the communication system directly. No telephone is required for this purpose.

The BLF server requires one IP User license and one UC User license per node:

- System with UC Smart: IP User and UC Smart User License
- System with UC Suite: IP User and UC Suite User License

Before starting the BLF server, the IP User license and the UC User license must be set up, and an appropriate UC password must be assigned for it.

The BLF server can serve up to 10 nodes.

Technical Requirements

- Standard Windows PC or Windows Server
- 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)
- Microsoft Windows Server 2012 (32-bit / 64-bit)
- Microsoft Windows Server 2008 R2 (64 bit)
- We recommend using a Windows Server operating system, since the BLF server must be in continuous operation (can be virtualized using VMware vSphere).
- Fixed IP address for the PC (no DHCP)

9.4 Chapter 16.4 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

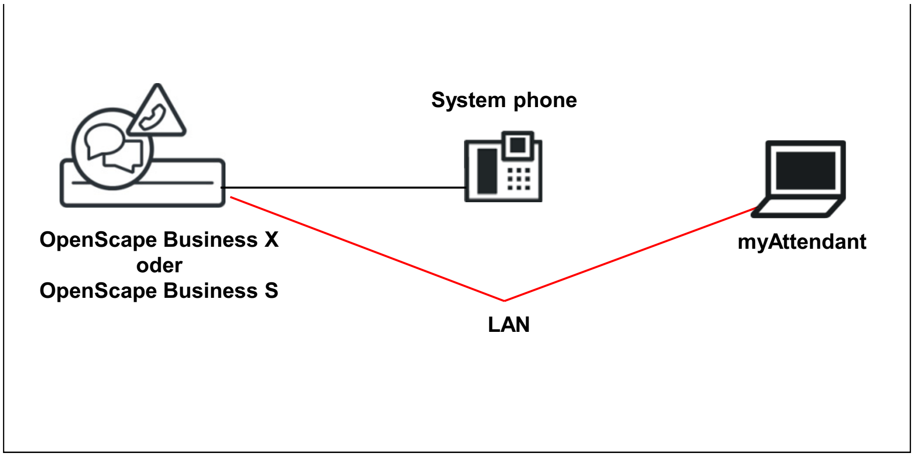
Additional Software

- 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
- SIP phones with RFC 3725 support, e.g., OpenScape Desk Phone IP 35G/55G 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).



9.4.1 Chapter 17.1.2 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
- 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.

9.5 Chapter 17.1.4 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.

9.6 Chapter 22.6.1 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

10 V2R0.3: Security Certificate Import for Encryption of UC Suite Client

Affected Documentation	Administrator Documentation
Issue	9
Reference No.	A31003-P3020-M100-09-76A9

10.1 Chapter 19.4.4 How to Import Server Certificates (PKCS#12)

Prerequisites

- You are logged into the WBM with the **Expert** profile.

Step by Step

1. In the navigation bar, click on **Expert Mode**.
2. In the navigation tree, click **Telephony > Security**.
3. Navigate in the menu tree down to **SSL > Certificate Management > Server Certificates**.
4. Click on the **Import Server Certificate (PKCS#12)** tab in the **Server Certificates** window.

> ***INFO:*** Certificates may be imported for OpenScape Business, UC Booster Server or UC Booster Card.

5. Enter the **Certificate Name**.
6. Enter the **Passphrase for decryption**.
7. Under **File with Certificate**, enter the desired certificate file by using the **Browse** button.
8. Click on **Apply** followed by **OK**.

11 V2R0.3: Fax Transport - G.711

Affected Documentation	Administrator Documentation
Issue	9
Reference No.	A31003-P3020-M100-09-76A9

11.1 Chapter 12.11.8 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. T.38 must be activated for the fax box. In order to send faxes

INFO: T.38 must be activated 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.

12 V2R0.3: Application Launcher - Normalization of CLI Number

Affected Documentation	Application Launcher User Guide
Issue	17
Reference No.	A31003-P3010-U109-17-7619

12.1 Chapter 5.10 How to Enable Phone Number Normalization

Prerequisites

- Application Launcher has been started.

Step by Step

1. Click in the context menu of the Application Launcher tray icon on **Settings**.
2. Click on **General Settings** in the navigation area.
3. Enable the check box **Enable Phone Number Normalization**.
4. Enable the check box **Override System Settings**, if needed.
5. Enter the value for the maximum internal call number length in the **Max Int. Call Number Length** field, i.e. **3**.
6. Enable the check box **Enable on Internal Call Numbers**, if needed.
7. Click **Save**.
8. Click **Close**.

13 V2R0.3: DHCP Server - Wiki

Affected Documentation	Administrator Documentation
Issue	9
Reference No.	A31003-P3020-M100-09-76A9

13.1 Chapter 8.2.2 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

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.

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.

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.

14 V2R1.0: myPortal to go for Mobile (tablets)

Affected Documentation	myPortal to go User Guide
Issue	4
Reference No.	A31003-P3010-U115-4-7619

14.1 Chapter 4.3.2 Favorites List

The Favorites List shows you all the contacts you have configured as favorites at a glance. These contacts can also be called very easily directly from the Favorites list.

The Favorites list manages contacts in groups.

With the UC solution UC Smart, you can edit your Favorites list, i.e. add or delete contacts and delete and rename groups. In addition, you can add contacts from the directories to your Favorites list. With the UC solution UC Suite, you cannot edit the Favorites list; thus, adding or deleting contacts, call deletion and goup renaming can be performed only via the UC Suite clients (e.g., myPortal for Desktop).

All internal subscribers that were copied over from the internal directory into the Favorites List can be seen with their respective presence status and connection status (in online mode).

The Favorites List also displays the hook status of status of internal users if available. Supported states:

- When VoIP is registered and/or
- When the application is configured to run in desk phone mode

Picked up calls can have one of the following states:

Bar	Symbol	Activity	Status	Type of call
🟨	🔔	Blinking	Ringing	Internal
🟨	🔔	On	Busy	Internal
🟧	🔔	Blinking	Ringing	External
🟧	🔔	On	Busy	External

14.2 Chapter 4.3.1.1 How to Search in Directories

Step by Step

1. Tap on the search symbol in the header row.
2. Enter the first letters of a name in the input field.

   A list of matching entries is displayed (instant search).
3. Tap on the desired entry to call the contact.
4. Alternatively, tap “All results (full search)” to perform a full search:

   a) Tap on an entry in the full search result list to see details of the contact and further options, e.g. e-mail.

   INFO: Full search is performed in the personal, internal, system and mobile directories.

14.3 Chapter 4.3.2.5 How to Pick up a Call for Another Subscriber

Prerequisites

- The Favorites List area is displayed.
- A favorite contact is ringing

Step by Step

1. Under the Favorites List, tap on the subscriber being called.
2. Tap on **Call Pickup**.

   You have picked up the call for this contact.

14.4 Chapter 4.6.3 How to Send an SMS from a Directory Search

Prerequisites

- A mobile number has been stored for the contact.
- An application for sending SMS is installed on the smartphone.

Step by Step

1. Tap on the **Journals** menu button.
2. Tap on the search symbol in the header row.

› Enter the first letters of a name in the input field.

A list of matching entries is displayed.

3. Tap on the desired contact.

4. Tap in the contact on the SMS symbol. The locally installed application for sending SMS opens.

   > ***INFO:*** If multiple applications for sending SMS are installed, you will receive a selection list.

5. Write and send the SMS with your application.

14.4.1 Chapter 4.6.4 How to Send an E-mail from a Directory Search

Prerequisites

- An e-mail address has been stored for the contact.
- An application for sending e-Mail is installed on the Smartphone, and an e-mail account has been set up.

Step by Step

1. Tap on the **Journals** menu button.
2. Tap on the search symbol in the header row.
3. Enter the first letters of a name in the input field.

   A list of matching entries is displayed.
4. Tap on the desired contact.
5. Tap in the contact on the E-mail symbol. The locally installed application for sending e-mail opens.

   > ***INFO:*** If multiple applications for sending e-mail are installed, you will receive a selection list.

6. Write and send the e-mail with your application.

14.5 Chapter 3.1 User Interface

myPortal to go user interface has been designed to dynamically adapt to mobile devices with different screen sizes and display resolutions, such as tablet devices, phablets and mobile phones. The user interface of myPortal to go consists of several areas, such as the header line, the main window, the menu bar and the favorites list area.

These areas are dynamically rearranged according to the screen size and resolution in the following layouts:

- One-column layout: All user interface areas are arranged in one column.
- Two-column layout: The user interface areas are arranged in two columns (menu bar and main window).
- Three-column layout: The user interface areas are arranged in three columns (menu bar, main window and favorites).

User Interface Areas

1 **Header Line**

The header consists of the following elements:

- Go to Previous Page symbol:
  Back to last page viewed
- Title:
  Title of the current menu
- Search symbol:
  Opens an input field for the search by phone numbers or names

(in the single column layout)

2 **Main window**

The content of the main window depends on the selected menu button.

3 **Menu bar**

The menu bar contains the following menu buttons:

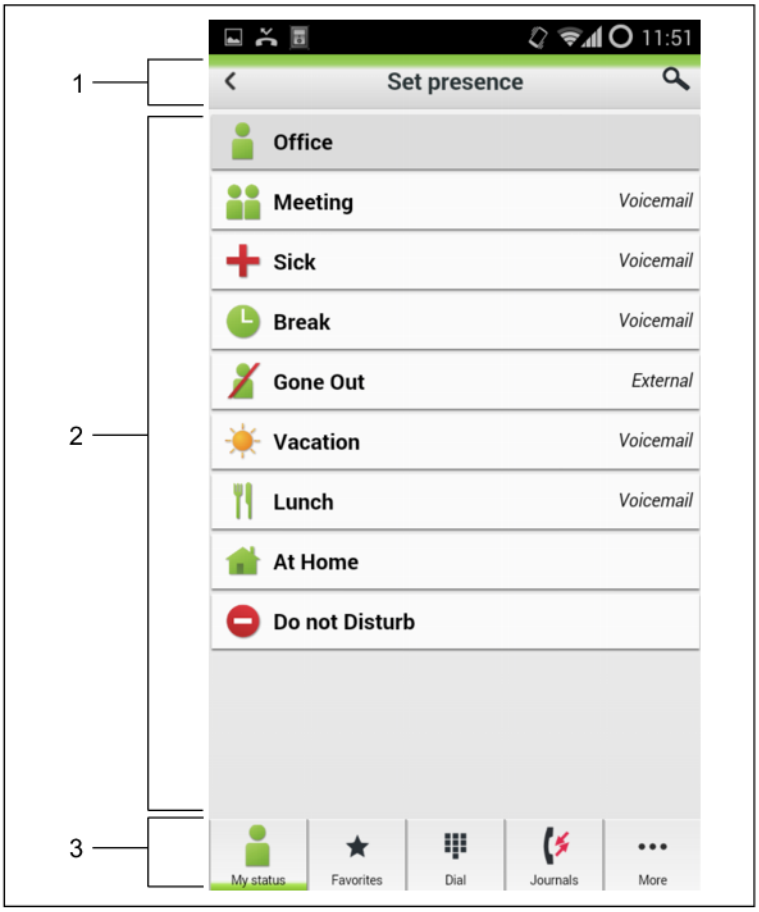
- **My status**:
  Display and change the presence status.
- **Favorites**:
  Display the Favorites set up by the user, sorted by Favorites groups in the single and two-column layouts. (In the three-column layout, the Favorites list area appears in the main window as a new column).
- **Dialing**:
  Initiate manual call or callback. Offers more CTI functions during the call (e.g., to initiate a conference or forward a call).
- **Journals**:
  Display journals and voice messages.
- **More**:
  Access to additional features and the configuration of myPortal to go.

4 **Favorites**:

Display the Favorites set up by the user, sorted by Favorites groups in the three-column layout. (In the single column and the two-column layouts, the Favorites List is displayed as part of the menu bar).

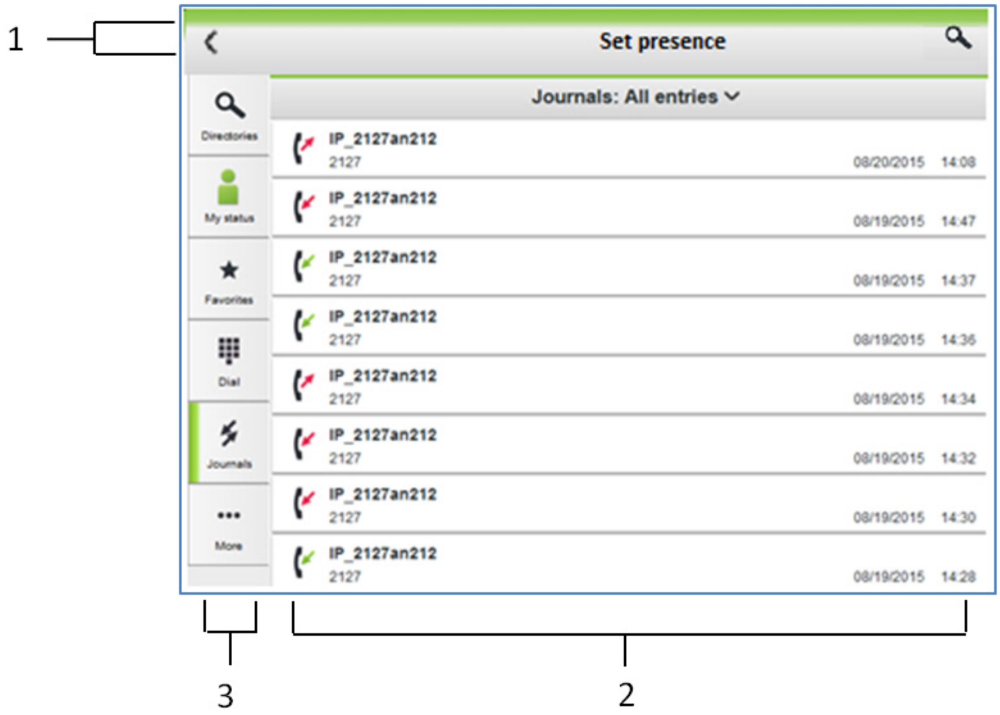
User Interface Layouts

One-column layout (used on mobile phones):



Two-column layout: (used on some phablets)

- Web view resolution: > 400 pixel (horizontal and vertical).
- The menu bar appears on the left and the main window is displayed on the right.



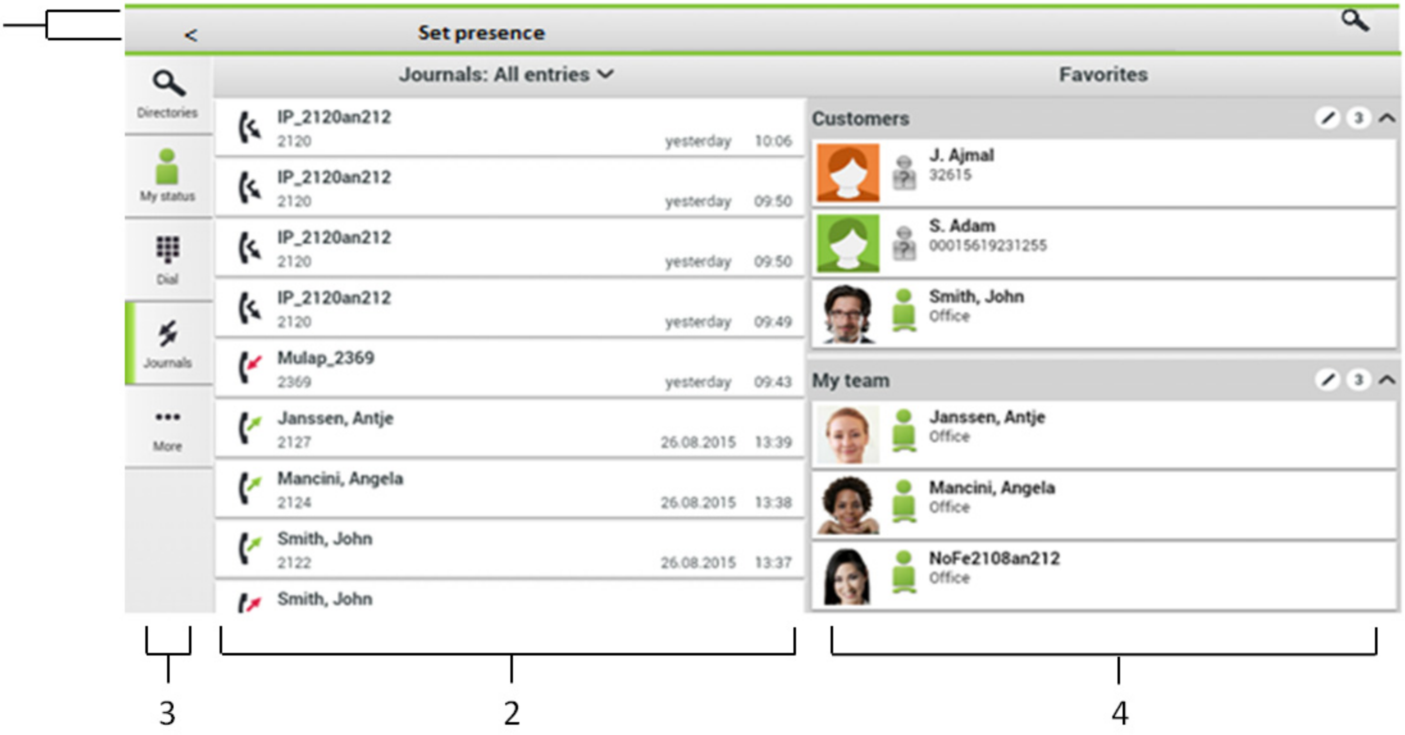
Set presence

Journals: All entries

IP_2127an212 2127 08/20/2015 14:08
IP_2127an212 2127 08/19/2015 14:47
IP_2127an212 2127 08/19/2015 14:37
IP_2127an212 2127 08/19/2015 14:36
IP_2127an212 2127 08/19/2015 14:34
IP_2127an212 2127 08/19/2015 14:32
IP_2127an212 2127 08/19/2015 14:30
IP_2127an212 2127 08/19/2015 14:28

Three-column layout (used on tablets):

- Web view resolution: > 750 pixel (horizontal) and > 400 (vertical)
- The menu bar appears on the left, the main window is displayed in the middle and the favorites appear on the right.



Set presence

Journals: All entries

IP_2120an212 2120 yesterday 10:06
IP_2120an212 2120 yesterday 09:50
IP_2120an212 2120 yesterday 09:50
IP_2120an212 2120 yesterday 09:49
Mulap_2369 2369 yesterday 09:43
Janssen, Antje 2127 26.08.2015 13:39
Mancini, Angela 2124 26.08.2015 13:38
Smith, John 2122 26.08.2015 13:37
Smith, John

Favorites

Customers 3

J. Ajmal 32615
S. Adam 00015619231255
Smith, John Office

My team 3

Janssen, Antje Office
Mancini, Angela Office
NoFe2108an212 Office

~~Tooltips~~

~~Tooltips are tiny windows in which myPortal to go displays more information on objects of the graphical user interface such as icons, input fields or buttons, for example. The appropriate tool tip appears when you let the mouse pointer hover over that element for a brief period of time.~~

14.5.0.1 Chapter 3.1.1 Support of specific Devices

Gigaset Maxwell 10

Device specific features are also supported for certain devices. Maxwell 10 is used as an example for 3rd party Android based touch phone devices whith a handset. In general, myPortal to go VoIP support for such devices idepends on the handset integration into the Android environment. In addition to the general tablet features of Maxwell 10, the following device specific features are also supported:

- Handset support with off hook / on hook detection for wired handset or wireless DECT handset
- Screen-saver deactivation on incoming calls
- Optimized UI scaling

> ***INFO:*** Minimum Maxwell 10 firmware requirement: Android 4.2 or higher required, minimum version: Firmware 1.2.16.

14.6 Chapter 5.2.7 VoIP in myPortal to go

Integrated VoIP can be enabled on myPortal to go for secure signalling via HTTPS. It can be used with both UC Smart and UC Suite solutions, supporting a variety of configurations, such as mobile HFA only or as part of a Mulap, in all operating modes (Mobility and Desk phone).

VoIP support is available:

- For most Android devices with Android firmware 4.2. or higher
- For myPortal to go iOS[1]

INFO: VoIP is not supported in myPortal to go - Web Edition.

Limitations

- VoIP is available only in Wi-Fi (WLAN) environments. VoIP access from a remote Wi-Fi environment requires OpenScape Business system software V2R1 or higher.
- Most Smartphones with Android 4.2 and higher are delivered with VoIP capabilities, but some vendors remove this support from their firmware distributions. In this case, VoIP cannot be used in myPortal to go.
- The voice quality of the VoIP feature depends on the Smartphone hardware, firmware and on the resources consumed by other software running in parallel with myPortal to go. This may affect the voice latency and other quality related parameters.

14.6.1 Chapter 5.2.7.1 How to Enable VoIP

Prerequisites

- OpenScape Business system software V2R0.3 or higher.
- Smartphone or tablet with built-in VoIP capabilities
- One configured HFA virtual number per VoIP enabled application including an IP user license
- myPortal to go V2 or higher is installed on your smartphone
- Mobility user license for One Number Service (if applicable)

Step by Step

1. Tap on the **More** menu button.
2. Tap on **VoIP settings**.
3. Tap on **VoIP enabled**.
4. In case you are in a MULAP, tap on **Controlled device** to select the required device.
5. Select the call number of the HFA device to be controlled in the **Controlled device** field.

[1] Release pending

If the status is “Registered”, you have successfully enabled VoIP on myPortal to go.

6. If your administrator has configured the system for remote VoIP access, you may set the enable **Use VoIP in remote WiFi networks** to use VoIP also in Wi-Fi networks outside the company.
7. Select the option **Bluetooth headset** if you use such a device.
8. Enable the flag **Force loudspeaker ringer** if you want the loudspeaker to ring at incoming calls, even if a headset is connected.

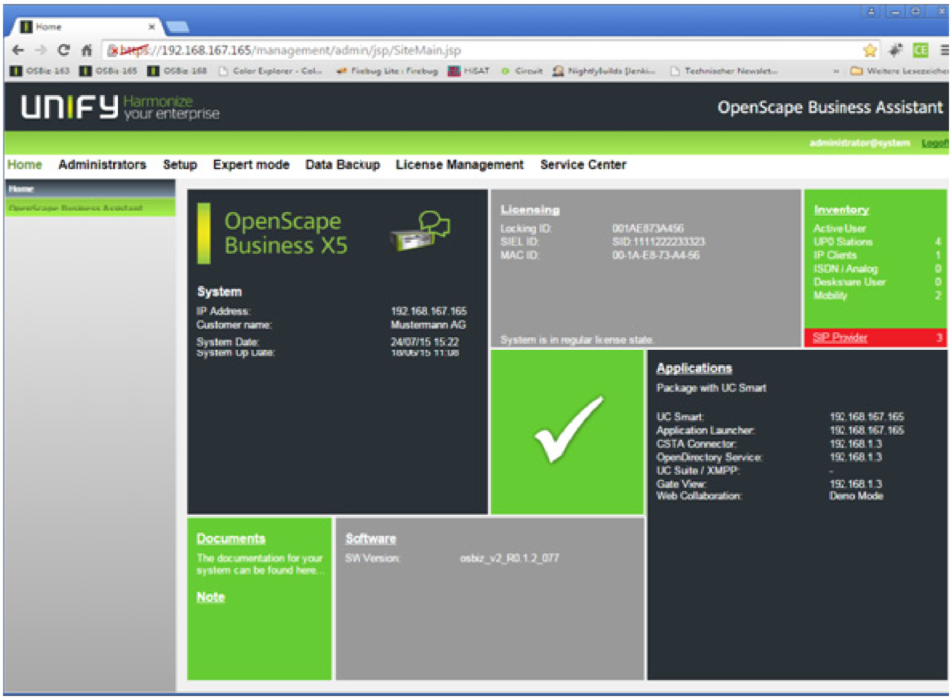
15 V2R0.3/ V2R1.0: Additional info in WBM landing page

Affected Documentation	Administrator Documentation
Issue	9
Reference No.	A31003-P3020-M100-09-76A9

15.1 Chapter 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.



System
IP Address: 192.168.167.165
Customer name: Mustermann AG
System Date: 24/07/15 15:22
System Up Date: 10/06/15 11:08

Licensing
Locking ID: 001AE873A456
SIEL ID: SID:1111222233323
MAC ID: 00-1A-E8-73-A4-56
System is in regular license state.

Inventory
Active User
UP0 Stations 4
IP Clients 1
ISDN / Analog 0
Deskshare User 0
Mobility 2
SIP Provider 3

Applications
Package with UC Smart
UC Smart: 192.168.167.165
Application Launcher: 192.168.167.165
CSTA Connector: 192.168.1.3
OpenDirectory Service: 192.168.1.3
UC Suite / XMPP: -
Gate View: 192.168.1.3
Web Collaboration: Demo Mode

Documents
The documentation for your system can be found here...

Software
SW Version: osbiz_v2_R0.1.2_077

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 software update
  - Notes when operating in an internetwork (system is master or slave, display of node ID)
  - Synchronization status
  - Notes on performing a backup and restore
- Area: **Documents**
  - Link to the documentation
- 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: **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

    INFO: 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
- Area: **Licensing**
  - Locking ID for licensing
  - SIEL ID for licensing
  - Note on the licensing status
- Area: **Inventory**
  - Type and number of active stations
  - Number of activated ITSPs and link to the ITSP status dialog in Service Center of active stations
- Area: **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.

16 V2R1.0: Support Suse SLES 11 SP4

Affected Documentation	Administrator Documentation
Issue	9
Reference No.	A31003-P3020-M100-09-76A9

16.1 Chapter 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.

16.2 Chapter 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.

16.3 Chapter 5 Initial Setup for OpenScape Business S

The initial setup of OpenScape Business S (also referred to as the Softswitch in short) is described here. This includes the integrating the softswitch and related components into the existing customer LAN as well as setting up Internet access for Internet telephony and configuring the connected stations.

For OpenScape Business S, the OpenScape Business communication software is installed on the Linux operating system SLES 11 SP4 64 Bit. The communication software can be operated directly on a Linux server or in a virtual environment with VMware vSphere. The installation of the Linux operating system is described in the installation guide *OpenScape Business, Installing the Linux Server*.

The initial setup of OpenScape Business S is carried out using the OpenScape Business Assistant administration program (web-based management, also called WBM in short).

This section describes the configuration of the most common components. Not all of these components may be used by you. During the initial setup, you may need to choose between multiple options in some places or even skip some configurations entirely, depending on which components you use.

The detailed administration of any features that are not covered by the initial setup is described in subsequent chapters.

The initial setup requires the creation of an IP address scheme and a dial plan.

Summary of the most important installation steps:

- System settings
- System Phone Numbers and Networking
- Internet Telephony
- Station configuration
- Licensing
- Data backup

16.4 Chapter 5.1 Prerequisites for the Initial Setup

Meeting the prerequisites for the initial setup ensures the proper operation of OpenScape Business S.

General

Depending on the used hardware (phones, ...) and the existing infrastructure, the following general conditions apply:

- The LAN infrastructure (Internet routers, switches, etc.) is present and usable.
- The IP phones are connected to the customer LAN.
- The Linux server required for OpenScape Business S was installed as per the instructions in the *OpenScape Business Linux Server Installation Guide*, was integrated into the customer LAN, and is ready for use.
- All licenses required for OpenScape Business S are present (e.g., UC clients, Gate View, Directory Services, etc.).
- An IP address scheme exists and is known.
- A dial plan (also called a numbering plan) is present and known.

Software

The following software is required for the installation of OpenScape Business S:

- DVD with the OpenScape Business communication software
  Contains the OpenScape Business communication software. This DVD is included in the delivery package.
- DVD with Linux operating system SLES 11 SP4 64 bit
  The Linux DVD may be needed during the installation of the OpenScape Business communication software, since some software packages (RPM) required for the communication software may need to installed later from this DVD.

Administration

For the initial setup of OpenScape Business S with the OpenScape Business Assistant (WBM), the Linux server or the Admin PC can be used. The WBM is browser-based and is thus independent of the operating system.

- Web browsers:
  The following HTML 5-enabled web browsers are supported:
  - Microsoft Internet Explorer Version 10 and later (Admin PC).
  - Mozilla Firefox Version 17 and later (Linux server / Admin PC)

  If an older version of the web browser is installed, you will need to install an up-to-date version before you can start the initial setup of the system.
- Oracle Java:
  The latest version of Oracle Java must be installed. If an older version is installed, you will need to update it to the latest version before you can start setting up the system for the first time.
- Screen resolution: 1024x768 or higher

Firewall

When connected to the Internet, a firewall is needed for the Linux server to prevent unauthorized access from outside. After installing Linux, the Linux firewall is enabled. The installer of the communication software adjusts the firewall settings so that the communication software can be operated properly. The ports for the communication software are opened, and all other ports are closed.

If an external firewall is used in the network, the Linux firewall must be disabled, and the addresses and ports required for the communication software must be opened (see *Used Ports*).

Internet Access

The Server PC must have broadband Internet access for:

- Security patches and general Linux software updates

OpenScape Business requires an Internet connection for:

- OpenScape Business software updates
- OpenScape Business features such as Internet telephony, for example
- OpenScape Business Mobility Clients such as myPortal to go, for example
- Remote Service (SSDP)

E-mail Server (Optional)

OpenScape Business requires access to an e-mail server in order to send e-mails. For this purpose, the access data to the E-mail server must be entered in OpenScape Business, and the relevant accounts (IP address, URL, login data of the E-mail server) must be set up in the E-mail server.

If the e-mail functionality is not used within OpenScape Business, this data need not be entered.

Internet Telephony, VoIP (Optional)

If Internet telephony is used within OpenScape Business, then OpenScape Business will require broadband access to the Internet and to an Internet Telephony Service Provider (ITSP, SIP Provider) for SIP telephony over the Internet. To do this, the appropriate accounts must be obtained from the ITSP, and the access data for the ITSP (IP address, URL, login data of the SIP Provider) must be set up in OpenScape Business.

Second LAN Port

If OpenScape Business S (or the Linux server) has a second LAN port, you can use this as a WAN interface for Internet access and Internet telephony via an ITSP. The first LAN port is used as usual as a LAN interface for the internal phones and PCs. The configuration of Internet access occurs in the external Internet router of the customer LAN. The setup of the second LAN port occurs directly during the initial setup of Linux or can be performed later using YaST. In the WBM, the second LAN port only needs to be activated as a WAN interface.

Fax as PDF

If faxes are to be saved in PDF format, the server PC requires at least 4 GB RAM. If OpenScape Business S is being operated in a virtual environment, the virtual machine must also be assigned 4GB RAM.

16.5 Chapter 5.5.1 How to Install the Communication Software

Prerequisites

- The SLES 11 SP4 64 bit operating system has been correctly installed and started on the Linux server.
- DVD with OpenScape Business communication software.
- DVD with the Linux operating system SLES 11 SP3 64 bit for any subsequent installation of software packages (RPM) that may be required.
- The root access data (user name and password) for logging into the Linux server is available.

IMPORTANT: The OpenScape Business communication software overwrites any existing configuration files (e.g., for DHCP, FTP, Postfix, etc.) during the installation.

Step by Step

1. Log into the Linux server with root privileges.
2. Insert the OpenScape Business DVD into the DVD drive.
3. Confirm the message with **Run**. The "Welcome" window appears.
4. Select the desired setup language (e.g., **English**) and click **Start**. The rest of the installation is described here for the English language.
5. Select the desired product from the list and click on **Select**. A check is performed to determine whether the hardware meets all the requirements for the installation. A warning is displayed for minor shortfalls in meeting the requirements. After confirmation, the installation can then be continued. For severe shortfalls, the installation is canceled automatically.
6. A check is performed to determine whether additional RPM packages need to be installed. If yes, confirm this with **Confirm**. If this occurs, you will need to switch back to the SLES 11 DVD later.
7. A window with the terms of the license (i.e., the End User License Agreement or EULA) appears. Read the terms of the license and accept the license agreement with **Yes**.
8. If a DHCP server is already present in the customer LAN (e.g., the DHCP server of the Internet router), stop the configuration of the Linux DHCP server here with **No** and proceed to step 12 to continue.

INFO: In order to ensure that the software of system telephones can be updated automatically even when using an external DHCP server, you have two options:

a) The IP address of the Linux server must be entered as the DLS address at each system telephone.

b) The network-specific data must be entered at the external DHCP server. The parameters for this can be found under `/var/log/OPTI.txt`.

9. If you want to use the Linux DHCP server, click on **Yes** to enable and configure the Linux DHCP server.

10. Enter the following values (preset with default values):

    - **Default Route**: IP address of the default gateway; as a rule, the IP address for the Internet router, e.g., `192.168.5.1`.
    - **Domain** (optional): the domain specified during the Linux installation, e.g., `<customer>.com`
    - **DNS-Server** (optional): IP address of the DNS server specified during the Linux installation. If no DNS server is available in the internal network, you can enter the IP address of the Internet router (e.g., `192.168.5.1`) here.
    - **SNTP Server**: IP address of the internal or external NTP server.
    - **DLS/DLI Server**: IP address of DLS server, i.e., the IP address of the Linux server (e.g.: `192.168.5.10`).
    - **Subnet**: appropriate subnet for the IP address range, e.g.: `192.168.5.0`.
    - **Netmask**: Subnet mask of the Linux server that was specified during the Linux installation, e.g.: `255.255.255.0`.
    - **IP range begin** and **IP range end**: IP address range from which the DHCP server may assign IP addresses, e.g.: `192.168.5.100` to `192.168.5.254`.

11. Click on **Continue**.

12. After the installation, the Linux operating system needs to be restarted. Select the check box **PC Reboot** and confirm with **Continue**.

13. If additional RPM packages need to be installed, you will be prompted to insert the SLES 11 DVD. Insert the DVD and confirm with **Continue**. Following the successful installation of the RPM packages, reinsert the OpenScape Business DVD and confirm this with **Continue**, followed by **Run**.

14. The OpenScape Business communication software is installed. The operating system then automatically performs a restart.

15. After the restart, log in with the user account that was set up earlier during the Linux installation.

16. Right-click on the DVD drive icon on the desktop and select the menu item **Eject**. Remove the OpenScape Business DVD from the DVD drive.

INFO: It takes a few minutes until all components of the OpenScape Business communication software are active. Using the OpenScape Observer, you can check when the OpenScape Business communication software is ready for use.

16.6 Chapter 6 Initial Setup of OpenScape Business UC Booster

This section describes the initial installation and configuration of the OpenScape Business UC Booster at the OpenScape Business X3/X5/X8 communication system. Note that a distinction is made here, depending on whether the OpenScape Business UC Booster Card or the OpenScape Business UC Booster Server is to be used for the UC Booster functionality.

The initial setup of the OpenScape Business UC Booster is carried out using the OpenScape Business Assistant administration program (web-based management, also called WBM in short).

The detailed administration of any features that are not covered by the initial setup is described in subsequent chapters.

Initial Setup of the OpenScape Business UC Booster Card

The OpenScape Business UC Booster Card is installed in the OpenScape Business X3/X5/X8 communication system and configured for operation. This is followed by the configuration of the OpenScape Business UC Booster functionality.

The specific installation steps required for the initial setup differ, depending on whether the UC Booster Card is being put into operation with the OpenScape Business X3/X5/X8 communication system for the first time or whether it is being integrated later in an existing and already configured OpenScape Business X3/X5/X8 communication system.

Overview of the installation steps for both options:

Integration in a New Communication System	Integration in an Existing Communication System
	Backing up the Configuration Data of the Communication System
Installing the UC Booster Card The UC Booster Card is installed in the OpenScape Business X3/X5/X8 communication system. For a description, see the OpenScape Business Service Documentation, Hardware Installation - Description of the Boards.	Installing the UC Booster Card The UC Booster Card is installed in the OpenScape Business X3/X5/X8 communication system. For a description, see the OpenScape Business Service Documentation, Hardware Installation - Description of the Boards.

Integration in a New Communication System	Integration in an Existing Communication System
Configuring the UC Booster Card The configuration of the UC Booster Card is performed together with the initial installation of the OpenScape Business X3/X5/X8 communication system. For a description, see the *Integration into the Customer LAN*.	Configuring the UC Booster Card The configuration of the UC Booster Card is performed later on an already configured OpenScape Business X3/X5/X8 communication system. For a description, see the *Integration into the Customer LAN*. For the specifics of the configuration, see *Configuring the UC Booster Card*
Basic Configuration The basic configuration is performed together with the initial installation of the OpenScape Business X3/X5/X8 communication system. For a description, see the *Basic Configuration*.	Basic Configuration The basic configuration is performed later on an already configured OpenScape Business X3/X5/X8 communication system. For a description, see the *Basic Configuration*. For the special features of the basic configuration, see *Basic Configuration*
Closing Activities The closing activities (including the licensing of the UC Clients) are performed together with the initial installation of the OpenScape Business X3/X5/X8 communication system. For a description, see the *Closing Activities*.	Closing Activities The closing activities (including the licensing of the UC Clients) are performed together with the initial installation of the OpenScape Business X3/X5/X8 communication system. For a description, see the *Closing Activities*. For the special features of the closing activities, see *Closing Activities*

Initial Installation of the OpenScape Business UC Booster Server

The OpenScape Business UC Booster Server is integrated together with the OpenScape Business X3/X5/X8 communication system in the customer LAN.

The OpenScape Business communication software for the OpenScape Business UC Booster Server, which provides the OpenScape Business UC Booster functionality, is installed on the Linux operating system SLES 11 SP4 64 bit. The communication software can be operated directly on a Linux server or in a virtual environment with VMware vSphere. The installation of the Linux operating system is described in the installation guide *OpenScape Business, Installing the Linux Server*.

The OpenScape Business UC Booster Server has its own WBM. This WBM is used for software updates, backing up the configuration data and diagnostics of the OpenScape Business UC Booster Server. The initial installation of the OpenScape Business UC Booster server is performed with the WBM of the communication system.

The specific installation steps required for the initial installation differ, depending on whether the UC Booster Server is being put into operation with the OpenScape Business X3/X5/X8 communication system for the first time or whether it is being connected later to an existing and already configured OpenScape Business X3/X5/X8 communication system.

Overview of the installation steps for both options:

Integration in a New Communication System	Integration in an Existing Communication System
	Backing up the Configuration Data of the Communication System
Installing the Linux Server The installation of the Linux server is described in the OpenScape Business Linux Server Installation Guide.	Installing the Linux Server The installation of the Linux server is described in the OpenScape Business Linux Server Installation Guide.
Installing the Communication Software	*Installing the Communication Software*
Function Check with the OpenScape Observer	*Function Check with the OpenScape Observer*
Configuring the UC Booster Server The configuration of the UC Booster Server is performed together with the initial installation of the OpenScape Business X3/X5/X8 communication system. For a description, see the *Integration into the Customer LAN*.	Configuring the UC Booster Server The configuration of the UC Booster Server is performed later on an already configured OpenScape Business X3/X5/X8 communication system. For a description, see the *Integration into the Customer LAN*. For the specifics of the configuration, see *Configuring the UC Booster Server*
Basic Configuration The basic configuration is performed together with the initial installation of the OpenScape Business X3/X5/X8 communication system. For a description, see the *Basic Configuration*.	Basic Configuration The basic configuration is performed later on an already configured OpenScape Business X3/X5/X8 communication system. For a description, see the *Basic Configuration*. For the special features of the basic configuration, see *Basic Configuration*
Closing Activities The closing activities (including the licensing of the UC Clients) are performed together with the initial installation of the OpenScape Business X3/X5/X8 communication system. For a description, see the *Closing Activities*.	Closing Activities The closing activities (including the licensing of the UC Clients) are performed together with the initial installation of the OpenScape Business X3/X5/X8 communication system. For a description, see the *Closing Activities*. For the special features of the closing activities, see *Closing Activities*

16.7 Chapter 6.1 Prerequisites for the Initial Setup

Meeting the requirements for the initial setup ensures the proper operation of the OpenScape Business UC Booster.

General

Depending on the used hardware (phones, ...) and the existing infrastructure, the following general conditions apply:

- The OpenScape Business X3/X5/X8 communication system is configured and ready for use.
- The LAN infrastructure (Internet routers, switches, etc.) is present and usable.

- The IP phones are connected to the customer LAN.
- A broadband Internet connection is recommended for software updates and remote access.
- All licenses required for the OpenScape Business UC Booster are present (e.g., UC clients, Gate View, Directory Services, etc.). When integrating in an already licensed communication system, there is no activation period.
- An IP address scheme exists and is known.
- A dial plan (also called a numbering plan) is present and known.

For UC Booster Card

The following requirements must be observed for the operation of the UC Booster Card.

- OpenScape Business Hardware:
  The UC Booster Card is installed.
- Switch:
  The switch through which the UC Booster Card is connected with the communication system should be IPv6-enabled for the UC Booster Card to receive an IP address during the initial setup.
  If the switch is not IPv6-enabled, the red LED of the communication system flashes. In this case, the Admin port of the system must be connected to the second LAN port of the UC Booster Card using an additional Ethernet cable. This causes the UC Booster Card to automatically receive an IPv4 IP address via the IPv6 protocol. As soon as the UC Booster Card is reachable over IP, the red LED of the communication system goes out. The desired IP address for the UC Booster Card can then be entered during the initial setup. Communication between the system and UC Booster Card now takes place through the IPv4 connection of the switch.

  INFO: The additional Ethernet cable should be left connected in case a restart or a reload is required.

- Fan kit:
  The UC Booster Card requires an additional fan. The fan kit depends on the communication system.
- Housing cover:
  For the OpenScape Business X3W, a new housing cover is required for the UC Booster Card fan kit.
  When migrating from HiPath 3000 systems, new housing covers to accommodate the UC Booster Card fan kit are required for OpenScape Business X3W/X5W and X3R/X5R.
- Communication software:
  The software of the communication system must be upgraded to the latest released software version. Note that the image including the UC Booster Card software must be used for this purpose.

- Web browsers:
  The Admin PC is used for the initial setup of the UC Booster Card with the OpenScape Business Assistant (WBM). The WBM is browser-based and is thus independent of the operating system. A screen resolution of 1024 x 768 or higher is required.
  The following HTML 5-enabled web browsers are supported:
  – Microsoft Internet Explorer Version 10 and later.
  – Mozilla Firefox Version 17 and later
  If an older version of the web browser is installed, you will need to install an up-to-date version before you can start the initial setup of the system.

For UC server Booster

The following requirements must be observed for the operation of the UC Booster Server.

- Linux server:
  The Linux server required for OpenScape Business S was installed as per the instructions in the *OpenScape Business Linux Server Installation Guide*, was integrated into the customer LAN, and is ready for use.
- OpenScape Business communication software:
  The installation DVD with the OpenScape Business communication software is available. After the software installation, the software of the communication system and communication software of the UC Booster Server must be updated separately to the same, latest released software version.
- DVD with Linux operating system SLES 11 SP4 64 bit
  The Linux DVD may be needed during the installation of the OpenScape Business communication software, since some software packages (RPM) required for the communication software may need to installed later from this DVD.
- Web browsers:
  For the initial setup of the UC Booster Server with the OpenScape Business Assistant (WBM), either the Linux server or the Admin PC can be used. The WBM is browser-based and is thus independent of the operating system. A screen resolution of 1024 x 768 or higher is required.
  The following HTML 5-enabled web browsers are supported:
  – Microsoft Internet Explorer Version 10 and later (Admin PC).
  – Mozilla Firefox Version 17 and later (Linux server / Admin PC)
  If an older version of the web browser is installed, you will need to install an up-to-date version before you can start the initial setup of the system.
- Firewall:
  When connected to the Internet, a firewall is needed for the Linux server to prevent unauthorized access from outside. After installing Linux, the Linux firewall is enabled. The installer of the communication software adjusts the firewall settings so that the communication software can be operated properly. The ports for the communication software are opened, and all other ports are closed.
  If an external firewall is used in the network, the Linux firewall must be disabled, and the addresses and ports required for the communication software must be opened (see *Used Ports*).

16.8 Chapter 6.4.1.1 How to Install the Communication Software

Prerequisites

- The SLES 11 SP4 64 bit operating system has been correctly installed and started on the Linux server.
- DVD with OpenScape Business communication software.
- DVD with the Linux operating system SLES 11 SP3 64 bit for any subsequent installation of software packages (RPM) that may be required.
- The root access data (user name and password) for logging into the Linux server is available.

> ***IMPORTANT:*** The OpenScape Business communication software overwrites any existing configuration files (e.g., for DHCP, FTP, Postfix, etc.) during the installation.

Step by Step

1. Log into the Linux server with root privileges.
2. Insert the OpenScape Business DVD into the DVD drive.
3. Confirm the message with **Run**. The "Welcome" window appears.
4. Select the desired setup language (e.g., **English**) and click **Start**. The rest of the installation is described here for the English language.
5. Select the desired product from the list and click on **Select**. A check is performed to determine whether the hardware meets all the requirements for the installation. A warning is displayed for minor shortfalls in meeting the requirements. After confirmation, the installation can then be continued. For severe shortfalls, the installation is canceled automatically.
6. A check is performed to determine whether additional RPM packages need to be installed. If yes, confirm this with **Confirm**. If this occurs, you will need to switch back to the SLES 11 DVD later.
7. A window with the terms of the license (i.e., the End User License Agreement or EULA) appears. Read the terms of the license and accept the license agreement with **Yes**.
8. If a DHCP server is already present in the customer LAN (e.g., the DHCP server of the Internet router), stop the configuration of the Linux DHCP server here with **No** and proceed to step 12 to continue.

> ***INFO:*** In order to ensure that the software of system telephones can be updated automatically even when using an external DHCP server, you have two options:
>
> a) The IP address of the Linux server must be entered as the DLS address at each system telephone.
>
> b) The network-specific data must be entered at the external DHCP server. The parameters for this can be found under `/var/log/OPTI.txt`.

9. If you want to use the Linux DHCP server, click on **Yes** to enable and configure the Linux DHCP server.

10. Enter the following values (preset with default values):

- **Default Route**: IP address of the default gateway; as a rule, the IP address for the Internet router, e.g., `192.168.5.1`.
- **Domain** (optional): the domain specified during the Linux installation, e.g., `<customer>.com`
- **DNS-Server** (optional): IP address of the DNS server specified during the Linux installation. If no DNS server is available in the internal network, you can enter the IP address of the Internet router (e.g., `192.168.5.1`) here.
- **SNTP Server**: IP address of the internal or external NTP server.
- **DLS/DLI Server**: IP address of DLS server, i.e., the IP address of the Linux server (e.g.: `192.168.5.10`).
- **Subnet**: appropriate subnet for the IP address range, e.g.: `192.168.5.0`.
- **Netmask**: Subnet mask of the Linux server that was specified during the Linux installation, e.g.: `255.255.255.0`.
- **IP range begin** and **IP range end**: IP address range from which the DHCP server may assign IP addresses, e.g.: `192.168.5.100` to `192.168.5.254`.

11. Click on **Continue**.

12. After the installation, the Linux operating system needs to be restarted. Select the check box **PC Reboot** and confirm with **Continue**.

13. If additional RPM packages need to be installed, you will be prompted to insert the SLES 11 DVD. Insert the DVD and confirm with **Continue**. Following the successful installation of the RPM packages, reinsert the OpenScape Business DVD and confirm this with **Continue**, followed by **Run**.

14. The OpenScape Business communication software is installed. The operating system then automatically performs a restart.

15. After the restart, log in with the user account that was set up earlier during the Linux installation.

16. Right-click on the DVD drive icon on the desktop and select the menu item **Eject**. Remove the OpenScape Business DVD from the DVD drive.

INFO: It takes a few minutes until all components of the OpenScape Business communication software are active. Using the OpenScape Observer, you can check when the OpenScape Business communication software is ready for use.

16.9 Chapter 25.1.3 Migration of a HiPath 3000 V9 Standalone System with OpenScape Office V3 HX

In order to upgrade a HiPath 3000 V9 standalone system with an attached OpenScape Office V3 HX to an OpenScape Business communication system with a UC Booster, the following migration steps must be completed as described below.

The UC functionality of an OpenScape Office V3 HX is mapped to the external OpenScape Business V2 UC Booster Server.

A prerequisite for the migration is a HiPath 3000 V9 system as of V9 R2.7.0 with an OpenScape Office V3 HX as of V3R3 FR6. Earlier HiPath 3000 V9 and OpenScape Office V3 HX versions must be upgraded to this status before the migration. For the OpenScape Business UC Booster Server, an upgrade to the OpenScape Business Software V1 R2.2 (Version 1, Minor Release 2, FixRelease 2) must be first performed. This must then be followed by an upgrade to the OpenScape Business Software V1 R3.3. It is only from this basic software version that an upgrade to the latest OpenScape Business V2 software can be performed.

The following UC configuration data and user data are transferred:

- Announcements
- Images
- Voicemail
- Faxes
- Journal
- Contact Center Data
- User settings
- User Profiles
- External directory
- Schedules

The following UC configuration data and user data are **not** transferred and must be reconfigured in the UC Booster Server:

- Web services (e.g., XMpp, Web Collaboration, Mobility)
- Open Directory Service
- OpenStage Gate View

Migration Steps

Perform the following steps in sequence:

1. **Record agent IDs** (only when using the Contact Center)
   Record the mappings of agent IDs to the stations of the UC Suite, since these assignments will not be migrated. The assignments must be reconfigured with the **UCD** wizard in the WBM of the OpenScape Business communication system.
2. **Update OpenScape Office V3 HX**
   First update the OpenScape Office V3 HX to the V3 R3FR6 software if this has not already been performed.

3. **Create an OpenScape Office V3 HX backup set**
   Create a backup set on an external device via the WBM of OpenScape Office V3 HX.
   More detailed information can be found in the online help of the OpenScape Office Assistant.
4. **Upgrade the HiPath 3000 V9**
   Perform the upgrade from HiPath 3000 V9 to OpenScape Business V1 as described in the migration procedure for a standalone system. The licenses of the OpenScape Office V3 HX are transferred to OpenScape Business during the license migration at the license server. The license file contains the license data for both OpenScape Business X3/X5/X8 and the UC Suite.
5. **Integrate the UC Booster Server in the customer LAN**
   The Linux operating system SLES 11 SP4 64 bit must be installed on the new server PC (Linux server), followed by the communication software (Version V1 R2.2). For details, please refer to the *OpenScape Business Linux Server Installation Guide*.
6. **Activate the UC Booster**
   Activate the UC Booster functionality in the WBM of the OpenScape Business communication system (Basic Installation - Initial Installation - Package with UC Suite on OSBiz UC Booster Server) and enter the IP address of the new server PC (using the same IP address as the old server PC if possible). Make sure that the UC Suite is active on the UC Booster Server.
   For more detailed information, see the section "Initial Installation of OpenScape Business X3/X5/X8" under *How to Define the UC Solution*.
7. **Configure the UC Booster**
   The IP address of the communication system must be specified in the WBM of the UC Booster Server.
   For more detailed information, see the section "Initial Installation of the OpenScape Business UC Booster" under *Announcing the IP Address of the Communication System*.
8. **Convert the OpenScape Office V3 HX backup set**
   The OpenScape Office V3 HX backup set saved on the external media must be converted via a Linux script to an OpenScape Business V1 backup set. To do this, you must be familiar with Linux. The converted backup set must then be loaded into the UC Booster Server via the WBM. The UC configuration data and user data mentioned above will then be available.
   More information on how to do this can be found in this section under *How to Convert an OpenScape Office V3 HX Backup Set*.
9. **Update the OpenScape Business UC Booster Server**
   First update the UC Booster Server to the Version V1 R3.3 and then to the latest OpenScape Business V2 software.

16.10 Chapter 25.1.4 Migrating a HiPath 3000 V9 System to OpenScape Business UC Booster

In order to upgrade a HiPath 3000 V9 communication system to an OpenScape Business communication system with UC Booster functionality, the following migration steps must be completed as described below.

Depending on the number of UC users, a UC Booster Card or an external UC Booster Server can be used for the UC Booster functionality.

Migration Steps

Perform the following steps in sequence:

1. **Upgrade the HiPath 3000 V9**
   Perform the upgrade from HiPath 3000 V9 to OpenScape Business as described in the migration procedure for a standalone system.
2. **Alternative 1: Insert the UC Booster Card into the housing of OpenScape Business**
   If you prefer the UC Booster Card, this card is plugged into the housing during the upgrade from HiPath 3000 V9.
   More details can be found in the *Service Documentation, Hardware Installation, under the section on "Boards - Description of the Boards - OCAB"*.
3. **Alternative 2: Integrate the UC Booster Server in the customer's LAN**
   If you prefer the external UC Booster Server, the Linux operating system SLES 11 SP4 64 bit must be installed on a server PC, followed by the communication software. For details, please refer to the *OpenScape Business Linux Server Installation Guide*.
4. **Enabling the UC Booster manually**
   The automatic activation of the UC Booster functionality is not possible a migration. Consequently, the UC Booster functionality must be activated manually in the WBM.
   More information on this can be found under *How to Activate the UC Booster Manually*.
5. **Configure the UC Booster**
   The UC Booster functionality is configured in the WBM.

16.11 Chapter 25.2 Migrating from OpenScape Office V3 MX/LX to OpenScape Business V2

The technical migration of OpenScape Business V3 MX/LX systems to OpenScape Business V2 systems is described here.

The following communication systems can be migrated to V2:

- OpenScape Office V1 MX (hardware model)
  This requires switching to an OpenScape Business V2 hardware model, as well as a new installation.
- OpenScape Office V3 LX (Softswitch)
  The Linux operating system SLES 11 SP4 64 Bit must be installed on the Linux server, followed by the OpenScape Business V2 communication software. Operation in a virtual environment is possible.

For both systems, it is possible to import some mass data such as phone numbers with names from the old system into the new system via a CSV file. Customer data such as saved voicemails, for example, cannot be transferred.

License Migration

The following preconditions must be satisfied for a successful license migration:

- An upgrade license to upgrade from OpenScape Office V3 MX/LX to OpenScape Business V2 was ordered.
- For the license migration of OpenScape Office V3 LX, a separate upgrade license to OpenScape Business V2 S and the OpenScape Business S/ Booster Server software on DVD (SLES 11 SP4 64 bit), incl. three years of free SLES upgrades, has been ordered.
- The LAC for the upgrade license, which is required to retrieve the new license from the license server, is available.

Using the upgrade license, the following licenses can be converted from the existing OpenScape Office V3 MX/LX license file into OpenScape Business V2 licenses:

- OpenScape Office V3 LX Base 5/10/20 Comfort Plus User
  1x OpenScape Business Base, 5/10/20x IP User, 5/10/20x myPortal for Desktop, 5/10/20x Voicemail, 5/10/20x Fax, 5/10/20x Conference
- OpenScape Office V3 MX Base 10/20 Comfort Plus User
  1x OpenScape Business Base, 10/20x IP User, 10/20x myPortal for Desktop, 10/20x Voicemail, 10/20x Fax, 10/20x Conference
- Per system: 1x AutoAttendant, 1x Web Collaboration
- Per OpenScape Office Comfort User: 1x IP User, 1x myPortal for Desktop, 1x Voicemail
- Per OpenScape Office Comfort Plus User: 1x IP User, 1x myPortal for Desktop, 1x Voicemail; 1x Fax, 1x Conference
- For the following other OpenScape Office V3 LX licenses, the corresponding number of OpenScape Business V2 licenses are generated: myPortal for Outlook, myAttendant, Application Launcher, Gate View cameras, OpenDirectory Connector, myAgent, Contact Center Fax, Contact Center Email, myReports
- Changes in the presence statuses for other users by myAgent users are bound in OpenScape Business to the myAttendant license. These must be ordered separately.

> ***INFO:*** Station licenses and user-oriented licenses are permanently assigned to subscribers. Please ensure that an adequate number of licenses are available for myAgent and myAttendant users.
>
> To use the Mobility features, additional user licenses must be purchased if required.

Subscription (Linux Software for OpenScape Business S)

For migrations from OpenScape Office V3 LX, an SLES subscription can be set up with OpenScape Business S. The required Novell registration key is provided as a LAC on purchasing the DVD with the OpenScape Business communication software.

> ***INFO:*** The registration key used for the OpenScape Office V3 LX (hosting via the Central Update Server) is no longer required.

16.12 Chapter 25.3.2 Migrating from OpenScape Business V1 S

The following migration steps must be performed to upgrade an OpenScape Business V1 S system to an OpenScape Business V2 S system:

> ***INFO:*** Before performing the migration, it must be checked whether the hardware and software properties of the Linux server are appropriate for OpenScape Business V2 S. An upgrade to the Linux server (e.g., more RAM) may be sufficient. The Linux operating system SLES 11 SP4 64 bit is a prerequisite.
>
> If a new Linux server is required, the OpenScape Business V1 S communication software must be installed after installing Linux. A V1 data backup can then be transferred and you can continue with step 1.

Perform the following migration steps in sequence:

1. **Update the OpenScape Business V1 software**
   Using the WBM, update the OpenScape Business V1 software to the version V1 R3.3 or higher (see *Updating the Communication System*).
2. **Load the OpenScape Business V2 license file**
   Load the OpenScape Business V2 license file into the OpenScape Business V1 system and activate the licenses (see *Activating Licenses (Standalone)*).
   The license for the free SLES upgrades can still be used.
3. **Load the current OS Biz V2 software**
   Using the WBM, load the current OpenScape Business V2 software into the communication system. The V1 data is automatically converted to V2 data in the process (see *Updating the Communication System*).
4. **Perform a data backup**
   Back up your V2 data (see *Immediate Backup*).

> ***IMPORTANT:*** If the system is upgraded from OpenScape Business V1 to OpenScape Business V2, then no ITSP activation/ deactivation can be done in Internet Telephony wizard until a reset to LCR is done. Already configured ITSPs in OpenScape Business V1 will continue to work also in OpenScape Business V2 even without resetting the LCR. It is possible to edit the already activated ITSP but not to deactivate it. In order to make any

activation/deactivation change in the wizard, the LCR reset is needed. This is to reflect the necessary changes for the increase of ITSPs from 4 to 8. To reset LCR, go to **Expert Mode> LCR> LCR Flags** and click the **Reset LCR Data** flag.

INFO: Up to sixty MEB channels are supported in OpenScape Business V2 S. The number of additional MEB channels must be manually configured after the system is upgraded from OpenScape Business V1 to OpenScape Business V2.

16.13 Chapter 25.3.3 Migrating an OpenScape V1 UC Business Booster Server

The following migration steps must be performed to upgrade an OpenScape Business V1 UC Booster Server to an OpenScape Business V2 UC Booster Server:

INFO: Before performing the migration, it must be checked whether the hardware and software properties of the Linux server are appropriate for the OpenScape Business V2 UC Booster Server. An upgrade to the Linux server (e.g., more RAM) may be sufficient. The Linux operating system SLES 11 SP4 64 bit is a prerequisite.

If a new Linux server is required, the OpenScape Business V1 UC Booster Server must be installed after installing Linux. A V1 data backup can then be transferred and you can continue with migration step 1.

Perform the following migration steps in sequence:

1. **Update the OpenScape Business V1 software**
   Using the WBM, update the OpenScape Business V1 software to the version V1 R3.3 or higher (see *Updating the Communication System*).
2. **Load the OpenScape Business V2 license file**
   Load the OpenScape Business V2 license file into the OpenScape Business V1 system and activate the licenses (see *Activating Licenses (Standalone)*).
   The license for the free SLES upgrades can still be used.
3. **Load the current OS Biz V2 software**
   Using the WBM, load the current OpenScape Business V2 software into the communication system. The V1 data is automatically converted to V2 data in the process (see *Updating the Communication System*).
4. **Perform a data backup**
   Back up your V2 data (see *Immediate Backup*).

V2R1.0: Support Suse SLES 11 SP4
Chapter 25.3.3 Migrating an OpenScape V1 UC Business Booster Server

17 V2R1.0: Support Google Chrome as web browser

Affected Documentation	Administrator Documentation
Issue	9
Reference No.	A31003-P3020-M100-09-76A9

17.1 Chapter 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

17.2 Chapter 4.1 Prerequisites for the Initial installation

Meeting the prerequisites for the initial installation ensures the proper operation of the communication system.

General

Depending on the existing hardware (boards, phones, ...) and infrastructure, the following general conditions apply:

- The infrastructure (LAN, TDM telephony network) is available and usable.
- The hardware is installed and connected properly.
- One LAN port each is required to integrate the mainboard and the UC Booster Card in the customer LAN.
- The communication system has not yet been connected to the LAN.
- If the UC Booster Card is used, it should be inserted prior to the initial installation.
- Internet access is available through an Internet Service Provider.
- An ISDN S_0 or ISDN Primary Rate Interface is required for using ISDN outside lines.
- A CAS trunk connection is required for using a CAS outside line.
- An analog trunk connection is required for using an analog outside line.
- An IP address scheme exists and is known (see *IP Address Scheme*).
- A dial plan (also called a numbering plan) is present and known (see *Dial Plan*).

Admin PC

The following prerequisites must be fulfilled for the Administration PC (Admin PC) that is used for initially setting up the system and for the subsequent administration of the communication system:

- Network interface:
  The admin PC requires an available LAN port.
- Operating system:
  Configuring the communication system with the Manager E is only possible on a Windows operating system (Windows XP and later).
  WBM configuration, however, is browser-based and therefore platform-independent.
- Web browser:
  The following web browsers are supported:
  - Microsoft Internet Explorer Version 10 and later.
  - Mozilla Firefox Version 17 and later.
  - Google Chrome

  If an older version of the Web browser is installed, you will need to install an up-to-date version before you can start setting up the system.
- Oracle Java:
  The latest version of Oracle Java must be installed. If an older version is installed, you will need to update it to the latest version before you can start setting up the system.

17.3 Chapter 5.1 Prerequisites for the Initial Setup

Meeting the prerequisites for the initial setup ensures the proper operation of OpenScape Business S.

General

Depending on the used hardware (phones, ...) and the existing infrastructure, the following general conditions apply:

- The LAN infrastructure (Internet routers, switches, etc.) is present and usable.
- The IP phones are connected to the customer LAN.
- The Linux server required for OpenScape Business S was installed as per the instructions in the *OpenScape Business Linux Server Installation Guide*, was integrated into the customer LAN, and is ready for use.
- All licenses required for OpenScape Business S are present (e.g., UC clients, Gate View, Directory Services, etc.).
- An IP address scheme exists and is known.
- A dial plan (also called a numbering plan) is present and known.

Software

The following software is required for the installation of OpenScape Business S:

- DVD with the OpenScape Business communication software
  Contains the OpenScape Business communication software. This DVD is included in the delivery package.
- DVD with Linux operating system SLES 11 SP3 64 bit
  The Linux DVD may be needed during the installation of the OpenScape Business communication software, since some software packages (RPM) required for the communication software may need to installed later from this DVD.

Administration

For the initial setup of OpenScape Business S with the OpenScape Business Assistant (WBM), the Linux server or the Admin PC can be used. The WBM is browser-based and is thus independent of the operating system.

- Web browsers:
  The following HTML 5-enabled web browsers are supported:
  - Microsoft Internet Explorer Version 10 and later (Admin PC).
  - Mozilla Firefox Version 17 and later (Linux server / Admin PC)
  - Google Chrome

  If an older version of the web browser is installed, you will need to install an up-to-date version before you can start the initial setup of the system.
- Oracle Java:
  The latest version of Oracle Java must be installed. If an older version is installed, you will need to update it to the latest version before you can start setting up the system for the first time.
- Screen resolution: 1024x768 or higher

Firewall

When connected to the Internet, a firewall is needed for the Linux server to prevent unauthorized access from outside. After installing Linux, the Linux firewall is enabled. The installer of the communication software adjusts the firewall settings so that the communication software can be operated properly. The ports for the communication software are opened, and all other ports are closed.

If an external firewall is used in the network, the Linux firewall must be disabled, and the addresses and ports required for the communication software must be opened (see *Used Ports*).

Internet Access

The Server PC must have broadband Internet access for:

- Security patches and general Linux software updates

OpenScape Business requires an Internet connection for:

- OpenScape Business software updates
- OpenScape Business features such as Internet telephony, for example
- OpenScape Business Mobility Clients such as myPortal to go, for example
- Remote Service (SSDP)

E-mail Server (Optional)

OpenScape Business requires access to an e-mail server in order to send e-mails. For this purpose, the access data to the E-mail server must be entered in OpenScape Business, and the relevant accounts (IP address, URL, login data of the E-mail server) must be set up in the E-mail server.

If the e-mail functionality is not used within OpenScape Business, this data need not be entered.

Internet Telephony, VoIP (Optional)

If Internet telephony is used within OpenScape Business, then OpenScape Business will require broadband access to the Internet and to an Internet Telephony Service Provider (ITSP, SIP Provider) for SIP telephony over the Internet. To do this, the appropriate accounts must be obtained from the ITSP, and the access data for the ITSP (IP address, URL, login data of the SIP Provider) must be set up in OpenScape Business.

Second LAN Port

If OpenScape Business S (or the Linux server) has a second LAN port, you can use this as a WAN interface for Internet access and Internet telephony via an ITSP. The first LAN port is used as usual as a LAN interface for the internal phones and PCs. The configuration of Internet access occurs in the external Internet router of the customer LAN. The setup of the second LAN port occurs directly during the initial setup of Linux or can be performed later using YaST. In the WBM, the second LAN port only needs to be activated as a WAN interface.

Fax as PDF

If faxes are to be saved in PDF format, the server PC requires at least 4 GB RAM. If OpenScape Business S is being operated in a virtual environment, the virtual machine must also be assigned 4GB RAM.

17.4 Chapter 6.1 Prerequisites for the Initial Setup

Meeting the requirements for the initial setup ensures the proper operation of the OpenScape Business UC Booster.

General

Depending on the used hardware (phones, ...) and the existing infrastructure, the following general conditions apply:

- The OpenScape Business X3/X5/X8 communication system is configured and ready for use.
- The LAN infrastructure (Internet routers, switches, etc.) is present and usable.
- The IP phones are connected to the customer LAN.
- A broadband Internet connection is recommended for software updates and remote access.

- All licenses required for the OpenScape Business UC Booster are present (e.g., UC clients, Gate View, Directory Services, etc.). When integrating in an already licensed communication system, there is no activation period.
- An IP address scheme exists and is known.
- A dial plan (also called a numbering plan) is present and known.

For UC Booster Card

The following requirements must be observed for the operation of the UC Booster Card.

- OpenScape Business Hardware:
  The UC Booster Card is installed.
- Switch:
  The switch through which the UC Booster Card is connected with the communication system should be IPv6-enabled for the UC Booster Card to receive an IP address during the initial setup.
  If the switch is not IPv6-enabled, the red LED of the communication system flashes. In this case, the Admin port of the system must be connected to the second LAN port of the UC Booster Card using an additional Ethernet cable. This causes the UC Booster Card to automatically receive an IPv4 IP address via the IPv6 protocol. As soon as the UC Booster Card is reachable over IP, the red LED of the communication system goes out. The desired IP address for the UC Booster Card can then be entered during the initial setup. Communication between the system and UC Booster Card now takes place through the IPv4 connection of the switch.

  > ***INFO:*** The additional Ethernet cable should be left connected in case a restart or a reload is required.

- Fan kit:
  The UC Booster Card requires an additional fan. The fan kit depends on the communication system.
- Housing cover:
  For the OpenScape Business X3W, a new housing cover is required for the UC Booster Card fan kit.
  When migrating from HiPath 3000 systems, new housing covers to accommodate the UC Booster Card fan kit are required for OpenScape Business X3W/X5W and X3R/X5R.
- Communication software:
  The software of the communication system must be upgraded to the latest released software version. Note that the image including the UC Booster Card software must be used for this purpose.
- Web browsers:
  The Admin PC is used for the initial setup of the UC Booster Card with the OpenScape Business Assistant (WBM). The WBM is browser-based and is thus independent of the operating system. A screen resolution of 1024 x 768 or higher is required.
  The following HTML 5-enabled web browsers are supported:
  - Microsoft Internet Explorer Version 10 and later.

  - Mozilla Firefox Version 17 and later
  - Google Chrome

  If an older version of the web browser is installed, you will need to install an up-to-date version before you can start the initial setup of the system.

For UC server Booster

The following requirements must be observed for the operation of the UC Booster Server.

- Linux server:
  The Linux server required for OpenScape Business S was installed as per the instructions in the *OpenScape Business Linux Server Installation Guide*, was integrated into the customer LAN, and is ready for use.
- OpenScape Business communication software:
  The installation DVD with the OpenScape Business communication software is available. After the software installation, the software of the communication system and communication software of the UC Booster Server must be updated separately to the same, latest released software version.
- DVD with Linux operating system SLES 11 SP3 64 bit
  The Linux DVD may be needed during the installation of the OpenScape Business communication software, since some software packages (RPM) required for the communication software may need to installed later from this DVD.
- Web browsers:
  For the initial setup of the UC Booster Server with the OpenScape Business Assistant (WBM), either the Linux server or the Admin PC can be used. The WBM is browser-based and is thus independent of the operating system. A screen resolution of 1024 x 768 or higher is required.
  The following HTML 5-enabled web browsers are supported:
  - Microsoft Internet Explorer Version 10 and later (Admin PC).
  - Firefox Version 17 and later (Linux server / Admin PC)
  - Google Chrome

  If an older version of the web browser is installed, you will need to install an up-to-date version before you can start the initial setup of the system.
- Firewall:
  When connected to the Internet, a firewall is needed for the Linux server to prevent unauthorized access from outside. After installing Linux, the Linux firewall is enabled. The installer of the communication software adjusts the firewall settings so that the communication software can be operated properly. The ports for the communication software are opened, and all other ports are closed.
  If an external firewall is used in the network, the Linux firewall must be disabled, and the addresses and ports required for the communication software must be opened (see *Used Ports*).

17.5 Chapter 11.2.3 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.

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
- 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:*** 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

17.6 Chapter 11.2.4 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

17.7 Chapter 12.2.6 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
- 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: 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 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

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.

17.8 Chapter 12.2.7 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

18 V2M1.0: Microsoft Office 16

Affected Documentation	my Portal for Outlook
Issue	17
Reference No.	A31003-P3010-U103-17-7619

18.1 My Portal for Outlook User Guide Chapter 6.17.5 How to Resolve the Problem: myPortal for Outlook is not Loading (Outlook 2010/2013/16)

Step by Step

1. Click in Microsoft Outlook 2010 or 2013 or 16 on the **File** tab.
2. Click on the menu item **Options**.
3. In the **Outlook Options** window, click on the menu item **Add-Ins**.
4. In the **Manage** drop-down list, select the entry **Disabled Items** and click on the **Go To...** button.
5. In the **Disabled Items** window, select the possibly listed entries **OLI2010** and **Redemption (VSL)** and then click on **Enable**.
6. Exit the window with **Close**. This will return you to the **Basic Configuration** window.
7. In the **Manage** drop-down list, select the entry **COM-Add-Ins** and click on the **Go To...** button.
8. In the **COM-Add-Ins** window, select the entries for **OLI2010** and **Redemption (VSL)** and confirm this with **OK**.

   With auto-login set, the myPortal for Outlook plugin will be immediately loaded. Otherwise, the login window of myPortal for Outlook appears, and myPortal for Outlook is loaded after a successful login.

V2M1.0: Microsoft Office 16

My Portal for Outlook User Guide Chapter 6.17.5 How to Resolve the Problem: myPortal for Outlook is not Loading (Outlook

19 V2R1.0: Device@Home

Affected Documentation	Administrator Documentation
Issue	9
Reference No.	A31003-P3020-M100-09-76A9

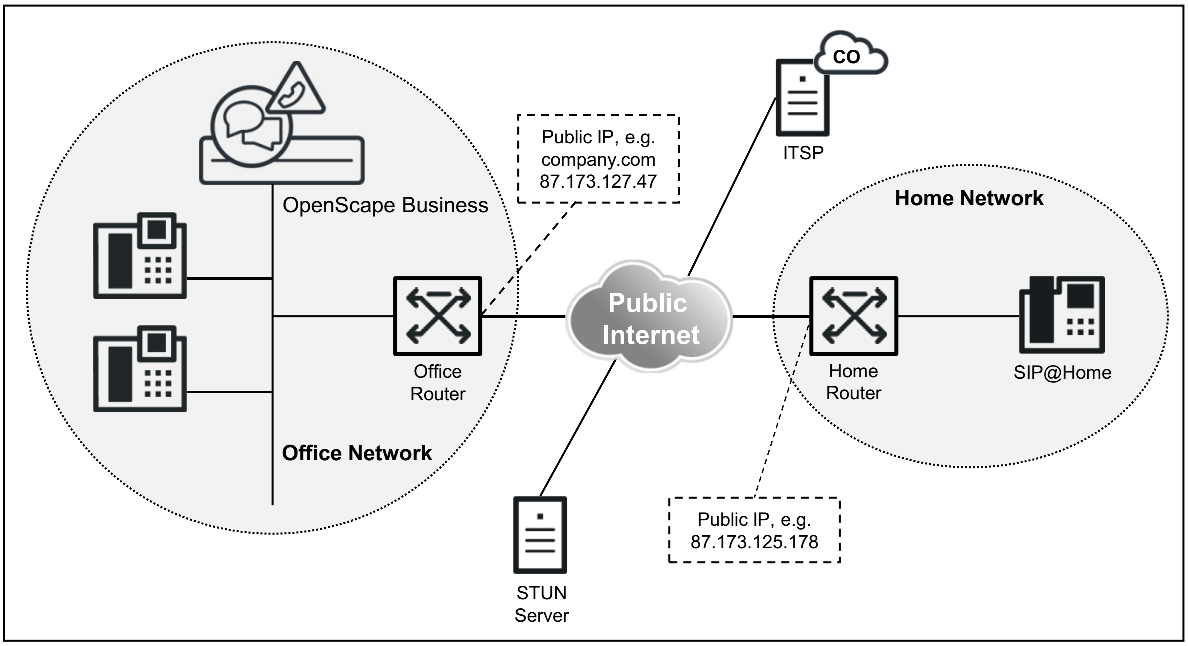
19.1 Chapter 18.4 Mobility at Home

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 HFA@Home stations
  STUN-enabled SIP phones (e.g., Yealink T19) (SIP@Home stations) or HFA phones (HFA@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@Home does not support the transmission of video signals.

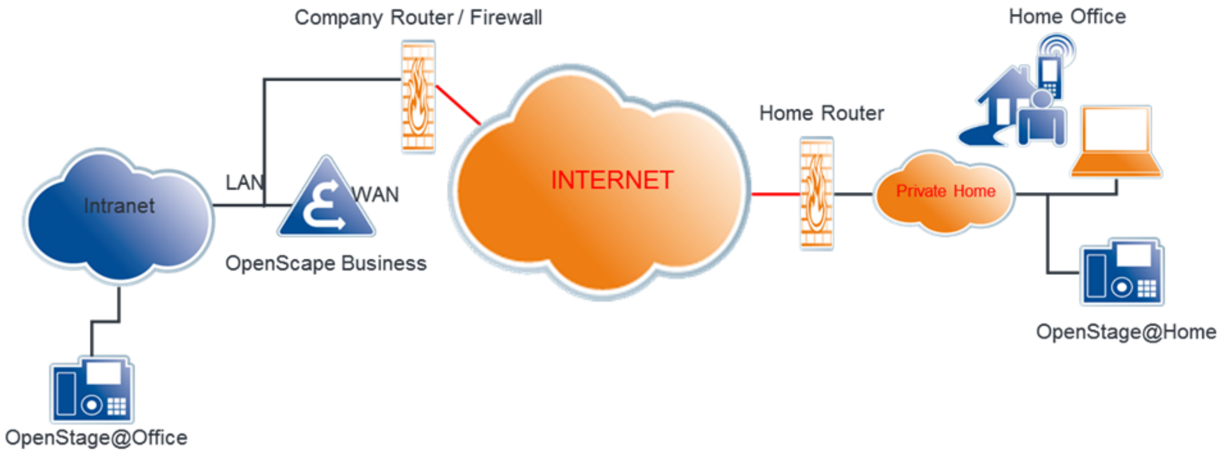
Figure: Device@Home (SIP@Home or HFA@Home) components



19.1.1 Chapter 18.4.3 Configuration for HFA@Home

In order to set up connections from a HFA phone to OpenScape Business over the Internet, certain configurations must be performed at OpenScape Business, the office Internet router and the HFA phone.

Figure: Example of HFA@Home use case



Configuring OpenScape Business

In order to enable a HFA@Home station to register at the communication system over the Internet, the integrated SBC function must be activated for the HFA@Home station (see How to Enable or Disable HFA@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 HFA@Home).

Configuring the Office Internet Router

In order to enable HFA@Home stations to reach the communication system over the Internet, port forwarding for the HFA 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:

- TCP/4060 (HFA)
- RTP port range in OpenScape Business X:30274-30259
- RTP port range in OpenScape Business S: 30528-30887
- 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 HFA@Home)

The transport protocol is set at the HFA@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 HFA@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 HFA password must also be set.

Restrictions

- TLS protocol is not supported.
- Depending on the home router, HFA mobility may not function. The home router must allow Internet access from the phone and support current standards regarding Network Address Translation and port mappings.
- 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 HFA@Home and installing them.
- It is not recommended to change the assigned ports and port ranges in the system configuration via the WBM.

19.1.1.1 Chapter 18.4.3.1 How to Enable or Disable HFA@Home

- You are logged into the WBM with the **Expert** profile.

Step by Step

1. In the navigation bar, click on **Expert Mode**.
2. In the navigation tree, click on **Telephony > Stations**.
3. In the menu tree, click **Stations > IP Clients > System Clients**.
4. Click on the desired HFA@Home station in the menu tree.
5. Click the **Edit Workpoint Client Data** tab.
6. Make sure that the **Authentication active** check box is selected and that a password is entered. The values specified here must also be entered on the HFA phone.

   INFO: A strong password should be used when connecting over the Internet (at least 8 characters including uppercase, numeric, and special characters).

7. Select one of the following options:
   - ***a)*** If you want to enable HFA@Home for the selected HFA@Home station, select the **Internet Registration with internal SBC** check box.
   - ***b)*** If you want to disable HFA@Home for the selected HFA@Home station, clear the **Internet Registration with internal SBC** check box.
8. If you want to enable or disable HFA@Home for further HFA@Home stations, repeat steps 4 through 7 accordingly.

19.1.1.2 Chapter 18.4.3.2 How to Specify a STUN Server for Device@Home (SIP@Home or HFA@Home)

- You are logged into the WBM with the **Expert** profile.

Step by Step

1. In the navigation bar, click on **Expert Mode**.
2. In the navigation tree, click on **Telephony > Voice Gateway**.
3. In the menu tree, click **Internet Telephony Service Provider**.
4. Click the **Edit STUN Configuration** tab.
5. Enter the IP address or the host name of the STUN server (e.g., `stun.serviceprovider.com`) under **IP Address / Host name** in the **Default STUN Server** area.
6. Enter the port of the STUN server (e.g., `3478`) under **Port** in the **Default STUN server** area.
7. Click **Apply**, followed by **OK**.

20 V2R1.0: Automatic Re-flashing

Affected Documentation	Administrator Documentation
Issue	9
Reference No.	A31003-P3020-M100-09-76A9

20.1 Chapter 24.3.3.6 How to Configure Automatic Re-flashing

Automatic re-flashing is an easy way to flash HFA software only for out of the box or factory reset OpenScape Desk Phone IP 35G Eco, using the system’s DLI server.

Prerequisites

- You are logged into the WBM with the **Expert** profile.

> ***INFO:*** Automatic re-flashing is valid only for out of the box devices (from the factory). Else, the factory settings must be restored on the device (“factory reset") before proceeding to automatic re-flashing.

Step by Step

1. Configure the device with a number and as system client:
   a) In the navigation bar, click on **Expert Mode**.
   b) In the navigation tree, click **Telephony Server> Station> IP Clients**.
   c) Enter the internal number in the **Callno** field.
   d) Enter the public number in the **DID** field.
   e) Enter a name for the device.
   f) Select **System Client** from the **Type** drop down menu.
   g) Click **Apply.**
2. Set up the DHCP server to send the IP address of the DLI via the DHCP option:
   a) In the navigation bar, click on **Expert Mode**.
   b) In the navigation tree, click **Telephony Server> Network Interfaces> DHCP> DHCP-Server> Edit Global Parameters**.
   c) Check the **Use Internal DLI** option at the **DNS Server** section.
3. Plug in the device and specify the terminal number once the phone is started.

4. The phone is also registered to the DLI database. To verify the device registration:

   a) Click on **Expert Mode** in the navigation bar.

   b) Click **Maintenance> Software Image** in the navigation tree.

   c) Click **Phone Images** in the menu tree.

   d) Click on **Deploy to Device**.

   The device should appear under **Device Type**.

5. Automatic re-flashing starts and loads the HFA software stored in the communication system to the device.

   IMPORTANT: Do not unplug the device during this process.

The device is now configured.

INFO: If the device is set to SIP (under **Telephony Server> Station> IP Clients**), it will update to the latest SIP software, only if the update is available in the corresponding software release.

INFO: If the re-flashing process is unsuccessful, the factory settings must be restored ("factory reset") on the device.

21 V2R1.0: Service log

Affected Documentation	Administrator Documentation
Issue	9
Reference No.	A31003-P3020-M100-09-76A9

21.1 Chapter 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.

V2R1.0: Service log
Chapter 3.1.6.11 Service Center – Diagnostics > Service log

22 V2R1.0: Progress Indicator and Basic Installation Wizard

Affected Documentation	Administrator Documentation
Issue	9
Reference No.	A31003-P3020-M100-09-76A9

22.1 Chapter 4.7 Basic Configuration

The **Basic Installation** wizard is used for basic configuration. Basic configuration includes the most important settings for operating the communication system.

The Basic Installation Wizard includes a progress indicator showing the current step, as well as the steps that follow.

23 V2R1.0: XML Improvements

Affected Documentation	Administrator Documentation
Issue	9
Reference No.	A31003-P3020-M100-09-76A9

23.1 Chapter 4.3 Dial Plan

A dial plan is a list of all phone numbers available in the communication system. It includes, among other things, the internal call numbers, DID numbers and group call numbers.

Default Dial Plan

The internal call numbers are preassigned default values. These values can be adapted to suit individual requirements as needed (e.g., to create individual dial plans).

Extract from the default dial plan:

Type of call numbers	X1	X3/X5/X8
Internal station numbers	11-30	100-742
User direct inward dialing numbers	11-30	100-742
Trunk station number	700-703	from 7801 onward
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
Call number for remote access	not preset	not preset
Call number for voicemail UC Smart UC Suite	 351 -	 351 not preset

Individual Dial Plan

An individual dial plan can be imported via an XML file during basic configuration.

The XML file contains several tabs. Besides the names and phone numbers of subscribers, the ~~"Stations"~~ "Customer" tab also includes additional subscriber data such as the subscriber types and e-mail addresses of the subscribers.

A sample XML file with the appropriate explanations can be found in the WBM under **Service Center > Documents > CSV Templates**. You can also use the XML file stored there as a template for your data. It can be edited with Microsoft Excel, for example.

23.2 Chapter 5.4 Dial Plan

A dial plan is a list of all phone numbers available in the communication system. It comprises internal phone numbers, DID numbers, and group station numbers.

Default Dial Plan

The internal call numbers are preassigned default values. These values can be adapted to suit individual requirements as needed (e.g., to create individual dial plans).

Extract from the default dial plan:

Type of call numbers	Default call numbers
Internal station numbers	100-349, 500-709
User direct inward dialing numbers	100-349, 500-709
Group station numbers	350-439
Voicemail call number	71
Announcement Player call number	72
Seizure codes (external codes): Central Office ITSP	 855-858
Call number for conferences	7400-7404
Call number for parking	7405
Call number for AutoAttendant	7410-7429
Call number for MeetMe conference	7430

Individual Dial Plan

An individual dial plan can be imported in the WBM via an XML file during the basic configuration.

The XML file contains several tabs. Besides the names and phone numbers of subscribers, the ~~"Stations"~~ "Customer" tab also includes additional subscriber data such as the subscriber types and e-mail addresses of the subscribers.

A sample XML file with the appropriate explanations can be found in the WBM under **Service Center > Documents > CSV Templates**. You can also use the XML file stored there as a template for your data. It can be edited with Microsoft Excel, for example.

24 V2R0.3: Security - Vulnerability Password/V2R1.0: Prohibit access with default passwords

Affected Documentation	Administrator Documentation
Issue	9
Reference No.	A31003-P3020-M100-09-76A9

24.1 Chapter 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.

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.

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 stars (*****), will not be accepted by the system for security reasons.

Profiles

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

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** wizard) 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.

24.2 Chapter 3.1.4.3 How to Change your Own Administrator Password

Prerequisites

- You are logged into the WBM with the **Expert** profile.

Step by Step

1. Click on **Administrators** in the navigation bar.
2. Enter the new password in the **Password** and **Retype Password** fields.

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

3. Click **OK & Next**.

24.3 Chapter 11.3.2 How to Change the Password for a UC Smart User

Prerequisites

- You are logged on to the WBM with the **Advanced** profile.
- The **Package with UC Smart** has been activated under **Application Selection** in Expert mode.

> ***INFO:*** Please note that a UC Smart user must change his or her password again by default after the administrator has changed it. If this is not desired, the flag "User must change the password" must be disabled after changing the password.

Step by Step

1. In the navigation bar, click on **Setup**.
2. In the navigation tree, click on **Wizards > UC Smart**.
3. Click on **Edit** to start the **UC Smart** wizard.
4. Click on **Administration > User Management** in the menu tree.
5. Select the relevant user in the **Users** area.

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

6. Enter the new password under **Password** in the **Settings** area.
7. Click on **Apply**.
8. If you want to reset the password of another user, repeat steps 5 through 7.

Next steps Notify the affected user(s) about the new password.

25 V2R1.0: UC Suite Enhancements: Directories

Affected Documentation	**Issue**	**Reference No.**
Administrator Documentation	9	A31003-P3020-M100-09-76A9
myPortal for Desktop	18	A31003-P3010-U102-18-7619

25.1 Administration Manual Chapter 27.4.3.13 OpenScape Business UC Suite > Server

Parameter Description of Tabs:

- **General Settings**
- **Live Record**
- Logging
- **Notifications**
- **Maintenance**
- **Voicemail**

Parameters	Description
Office Hours	
Start Time	Beginning of the daily office hours (business hours) Setting for the presence status of the UC clients Default value: 7.00 hours
End Time	End of the daily office hours (business hours) Setting for the presence status of the UC clients Default value: 19.00 hours
Length of Password	
Lengths	Length of the password for the UC clients ***NOTE:*** Changing the length of the password resets the passwords for all users. Default value: 6
Call number of intercept position	
Target Number	Call number of intercept position ***INFO:*** Enter the call number of the intercept position configured in the communication system.
Instant message	
Disable instant messaging	When this flag is activated, the sending of instant messages is impossible. Default value: Disabled
Analog Extensions	

Parameters	Description
Analog User Mode	Defines how analog stations are displayed in the internal directory Default value: Show All
Analog User Mode: Show All	All analog stations are displayed in the internal directory
Analog User Mode : Show named only	Only analog stations with a name are displayed in the internal directory.
Analog User Mode: Not shown	No analog station is displayed in the internal directory.
Extension	
Max. internal length	Maximum number of digits for internal call numbers To prevent toll fraud, the dialing of long internal call numbers is prohibited. Default value: 4
Min. external length	Minimum number of digits for external call numbers Default value: 3
Transfer	
Normal Auto Attendant SST	When this flag is activated, the call will be transferred, regardless of whether the destination is free, busy or unavailable. Default value: Enabled
Journal	
Allow deleting of journal entries	. Default value:
Fax Format	
Use PDF as fax format	. Default value:
External Provider	
Slow External Provider	. Default value:
Name Resolution	
Length of verification	A digit from 4 to 8 must be entered to define the length of CLI numbers for the search in LDAP in myPortal for Desktop and myPortal for Outloook. The highest number (8) can be configured for more exact search and imroved system performance Default value: 4
Dial by name search local extension only	
Dial by name search local extension only	. Default value:
TLS	
Using TLS for client connections	. Default value:
Live Record	

Parameters	Description
Live Record	When this flag is activated, the recording of calls and conferences is possible. Default value: Enabled
Play prompt before recording	When this flag is activated, an announcement is played before a recording starts. Default value: Disabled
Play pip tone during recording	When this flag is activated, a warning tone is played during the recording. Default value: Enabled
System Logging	
Log Trace Messages (Verbose)	When this flag is activated, trace messages are recorded in a log file on a daily basis. Default value: Disabled
Client Logs	
Client log path	Storage path for client log files (log files of the UC Suite)
Enable log upload	When this flag is activated, the client logs are stored on the hard disk of the UC Booster Card (OCAB), the UC Booster Server or the OpenScape Business S communication system. Default value: Enabled
VoiceMail Mode : No VoiceMail Menu	After the greeting announcement is played, the caller is directly taken to the voice recording.
Allow callback from VM to known number only	When this flag is activated, any callers whose numbers are not stored in the UC client will be prevented from accessing the voicemail box. Default value: Enabled

25.2 myPortal for Desktop User Guide Chapter 5.2.1.10 How to Export a Personal Directory

You can export your personal directory including all contact details in a .CSV file with ";" as field delimiter.

Step by Step

1. Click on the **Directories** tab.
2. Click on **Personal Directory**.
3. Click **Export.**
4. Select the directory in which the CSV file will be stored and click **Save.**

25.3 myPortal for Desktop User Guide Chapter 5.2.1.11 How to Import a Personal Directory

You can import a CSV or XML file into myPortal for Desktop. The imported contact details will be displayed in the personal directory. You can later edit the imported contacts details.

Prerequisites

- You have exported the existing personal directory by clicking on **Export** under **Directories> Personal Directories** and saving the exported file.
- You have included the contact details in the exported personal directory at the existing format, with ";" as field delimiter.
- You are working with the classic user interface.

> ***INFO:*** After importing the contact details, you can switch to the modern user interface if needed.

> ***INFO:*** The import will overwite the existing contacts in the personal directory.

Step by Step

1. Click on the **Directories** tab.
2. Click on **Personal Directory**.
3. Click **Import.**

   A pop up is displayed, indicating that the import will overwrite the existing personal directory.
4. Select the CSV file including your personal directory and click **Open**.

   The personal directory is uploaded to the system.

26 V2R1.0: UC Suite Enhancements: OLI

Affected Documentation	Issue	Reference No.
myPortal for Outlook	19	A31003-P3010-U103-19-7619
myPortal for Desktop	18	A31003-P3010-U102-18-7619
myAttendant	19	A31003-P3010-U105-19-19

26.1 myPortal for Outlook User Guide Chapter 5.2.2.12 How to Display the Favorites List in Outlook

You have the option to view your Favorites List in Outlok.

Prerequisites

- You must have Outlook 2010.

Step by Step

1. Click on the **Setup** symbol.
2. Click on **My Preferences> Appearance**.
3. Enable the **Show in Outlook** checkbox.
4. Click **Save**.

26.2 myPortal for Outlook User Guide Chapter 5.2.2.13 How to Call a Contact from the Favorites List

You can quickly call a contact who is in your Favorites List.

Prerequisites

- The contact’s phone number must be available in the directory.

Step by Step

1. Right-click in free area of the **Favorites List** to open the context menu.
2. Move your mouse over the corresponding contact.

   You see additional options.
3. Select ☎ to dial the contact’s number.

   The contact is being called.

26.3 myPortal for Outlook User Guide Chapter 5.2.2.14 How to View a Contact’s Phone Numbers in the Favorites List

You can view a contact’s phone numbers via the Favorites List.

Prerequisites

- The contact's phone number must be available in the directory.

Step by Step

1. Right-click in free area of the **Favorites List** to open the context menu.
2. Move your mouse over the corresponding contact.
   You see additional options.
3. Select ☎ to view the contact's phone numbers.
   The contact's phone numbers are displayed.

26.4 myPortal for Outlook User Guide Chapter 5.2.2.15 How to E-Mail a Contact from the Favorites List

You can quickly e-mail a contact via the Favorites List.

Prerequisites

- The contact's e-mail address must be available in the directory.

Step by Step

1. Right-click in free area of the **Favorites List** to open the context menu.
2. Move your mouse over the corresponding contact.
   You see additional options.
3. Select ✉ to send an e-mail to the selected contact.

26.5 myPortal for Outlook User Guide Chapter 5.2.2.16 How to Chat with a Contact from the Favorites List

You can quickly chat with a contact via the Favorites List.

Prerequisites

- The contact must have activated instant messaging.

Step by Step

1. Right-click in free area of the **Favorites List** to open the context menu.
2. Move your mouse over the corresponding contact.
   You see additional options.
3. Select 💬 to send an instant message to the selected contact.

26.6 myPortal for Outlook User Guide Chapter 5.2.2.17 How to Display recent Contacts in the Favorites List

You can view the last contacts or teams you communicated with in the Favorites List. Up to ten entries of inbound and outbound calls including internal and external calls are displayed.

Prerequisites

- The checkbox **Show recent contacts in Favorites** must be enabled (**Setup> Preferences> Appearance> Show recent contacts in Favorites**).

Step by Step

1. Right-click in free area of the **Favorites List** to open the context menu.
2. Click on **Recent Contacts**.

   The ten most recent contacts or teams are displayed.

26.7 myPortal for Outlook User Guide Chapter 5.2.2.18 How to View a Contact’s Presence in the Favorites List

You can view a contact’s presence in the Favorites List.

Step by Step

1. Right-click in free area of the **Favorites List** to open the context menu.
2. Move your mouse over the corresponding contact.

   The contact’s presence and XMPP states are displayed in a tooltip.

26.8 myPortal for Outlook User Guide Chapter 5.18 How to Undock the Toolbar from Outlook 2010

myPortal for Outlook toolbar can be undocked and placed on the top of your Windows user interface. The toolbar automatically hides. It is displayed by moving your mouse to the top of the screen.

Prerequisites

- You must have Outlook 2010.

Step by Step

1. Click on the **Setup** symbol.
2. Click on **My Preferences> Appearance**.
3. Select **Floating** from the **Display Toolbar** drop-down list.
4. Click **Save**.

26.9 myPortal for Outlook User Guide Chapter 5.4.1.2 How to Initiate am Ad-hoc Conference in Outlook

You initiate an ad-hoc conference directly from an Outlook Appointment.

Prerequisites

- You must have initited an Outlook appointment and selected attendees.

Step by Step

1. Within the corresponding Outlook appointment, click New onference onference to create a new ad-hoc conference.
2. In the conference creation window, you can select to **Add** or **Remove** attendees if needed.

3. You enable the checkbox **Start this conference now** and instantly initiate the conference if applicable.
4. Click **Finish**.

   The conference is created with all Outlook settings, such as duration, time and date, recurrence, etc. The conference settings may be later edited via the advanced options of the **AdHoc Conference** window after starting the conference.

26.10 myAttendant Chapter 7.10/ myPortal for Desktop Chapter 6.19 / myPortal for Outlook User Guide Chapter 6.17 How to Allow others to See your Call Details

You can allow directory users to see information about your current active call, such as who you are talking to, whether it is an inbound or outbound call and the call duration. This option is disabled by default.

Prerequisites

- The option of enabling this feature is activated by your system dminisstrator.

Step by Step

1. Click on the **Setup** symbol.
2. Click on **Sensitivity> Security and Access**.
3. Select the option **Allow others to see who I am talking to**.
4. Click **Save**.

26.11 myPortal for Outlook User Guide Chapter 5.2.1 Quick Action Toolbar for Directories and Journal

You can quickly communicate with your contacts via the quick action toolbar on the bottom right of the user interface. The following actions can be performed for the selected contact on your journal or directory:

Symbol	Meaning
☎	Dial
△	Start conference
🔔	Call pickup
@	Send E-Mail
🗨	Send instant message
🕒	Schedule outbound call

26.12 myPortal for Outlook User Guide Chapter 5.6.1 Quick Action Toolbar for Messages

You can quickly perform actions related to your messages, such as moving a message to another folder, or playing a voicemail message through your speaker. The following actions can be performed via the quick action toolbar, which is displayed on the bottom right of your Messages user interface:

Symbol	Meaning
📁	Move message to folder (e.g. Saved)
▶	Play through speaker
☎	Call through phone
→	Forward voicemail
@	Send in E-Mail
💾	Save voicemail message
▨	Copy to Outlook

Related Topics

- How to Send a Fax Message to a Fax Number
- How to Change your Sender Fax Number
- How to Change Users
- Fax Cover Editor

27 V2R1.0: UC Suite Enhancements: Journal

Affected Documentation	Issue	Reference No.
myPortal for Outlook	19	A31003-P3010-U103-19-7619
Administrator Documentation	9	A31003-P3020-M100-09-76A9
myPortal for Desktop	18	A31003-P3010-U102-18-7619
FaxPrinter	18	A31003-P3010-U108-18-7619

27.1 myPortal for Outlook User Guide Chapter 5.2.3 Journal

The Journal is the list of all your inbound and outbound calls. You can use it to quickly and easily call your contacts again or to respond to missed calls.

Folder for Call Types

The calls are arranged on the following tabs:

- **Open**
  Contains the unanswered missed calls for which a call number was transmitted. As soon as you answer one of these calls, all associated entries with that call number are dropped from the list.
- **All calls**
- **Missed**

> ***INFO:*** If you want to be notified about missed calls via screen pops, disable the "close tray pop on call termination" function.

- **Answered**
- **Internal**
- **External**
- **Inbound**
- **Outbound**
- **Scheduled**
  Contains all the calls that you 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 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 communication system defers the scheduled call until you are free again. myPortal for Outlook informs you of any pending scheduled calls on exiting the program. On starting the application, 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.

Grouped by time period

The calls in all folders are grouped by the same criterion, as selected by you:

- Date (for example: **Today**, **Yesterday**, etc., **Last Week**, **2 Weeks Ago**, **3 Weeks Ago**, **Last Month** and **Older**)
- Phone number
- Last Name,First Name
- First Name, Last Name
- Company

The number of Journal entries contained in the group is displayed on the right of the group designation in parentheses.

Call Details

Every call is shown with the start **Date**, the start **Time** and, if available, the **CLI** (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**, **Call Complete**, **Domain** and **Call Info** columns are also displayed in most folders. Missed calls, forwarded calls and group calls are also displayed together with user pick up information.

Symbol	Meaning
■	Inbound
■	Outbound
■	The call was successful or was answered
🌐	External
🏠	Internal
☎	Missed call forwarded to <User>
☎	Missed call picked up by <User>
☎	Group call answered by <User>
☎	Group call by caller <User>
✉	Voicemail

~~Call Complete~~	~~Meaning~~
■	~~The call was successful or was answered.~~

Sorting

You can sort the calls in the Journal by any column (except **Direction**) in ascending or descending alphanumeric order. The direction in which the triangle at a column header is pointing indicates the ascending or descending order. The sorting of the Journal is retained even after it is closed.

Zooming in on an Entry

You can zoom in on a specific entry one character at a time in the column by which the entries are sorted. For example, you could jump to the first Last Name starting with "Sen" one letter at a time. This method can also be used in the results of a search.

Retention Period

The communication 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 communication system automatically deletes all associated entries.

Export

You can export the log data for the current day manually or automatically to a CSV file. The storage location of the CSV file can be freely selected. Once a manual export is completed, a window appears with a link to the generated CSV file containing the exported journal data.

The automatic export is performed:

- on exiting
- at midnight, provided is active

The file is named according to the scheme <phone number>-<yyyymmdd>.csv. If the file already exists, the data is appended to it. The file contains the journal data of all call types except **Open** and **Scheduled** in the following fields: **Start Date**, **Start Time**, **End Date**, **End Time**, **From**, **To**, **First Name**, **Last Name**, **Company, Direction, Duration, Status and Domain.**

27.2 myPortal for Outlook User Guide Chapter 5.2.3.11 How to Call back a Contact from the Journal

It is possible to call back a journal entry by double-clicking on it.

Step by Step

1. Click on the **Journal** symbol.
2. Click on one of the groups: **Open**, **All Calls**, **Missed**, **Answered**, **Internal**, **External**, **Inbound** or **Outbound**.
3. If required, double-click on the triangle on the left of the relevant group to expand the associated Journal entries.
4. Double-click on the required journal entry.

   The selected contact is being called.

27.3 myPortal for Outlook User Guide Chapter 5.2.3.12 How to Search Journal Entries

Step by Step

1. Click on the **Journal** symbol.
2. Click on one of the groups: **Open**, **All Calls**, **Missed**, **Answered**, **Internal**, **External**, **Inbound** or **Outbound**.
3. Enter the last four digits of the required number (CLI) or a keyword in the available search field.

   INFO: Should you need to search for a number, you may enter from four up to eight digits according to the configuration set by the system administrator.

4. The search results will be displayed underneath.

   INFO: The system retrieves results from all journal sections.

28 V2R1.0: UC Suite Enhancements: Fax

Affected Documentation	Issue	Reference No.
FaxPrinter	18	A31003-P3010-U108-18-7619

28.1 FaxPrinter User Guide, Chapter 5.2 How to Send a Fax Message to an E-Mail Address

You can send a fax in pdf format to an e-mail address.

Prerequisites

- The contact’s e-mail address is included in the directory.

Step by Step

1. Select the menu item for printing in the relevant application, e.g., **File > Print** in Microsoft Word.
2. Select **CommunicationsClients Fax Printer** as the printer. The **Fax Printer** window opens.
3. Select the header line for the fax message:
   a) Click on **Setup**.
   b) Click on the **Fax Headlines** tab.
   c) Click in the list of header lines on the desired header.
   d) Click on **Save**.
4. If you want to send the fax message with a cover page, proceed as follows:
   a) Click on **Setup**.
   b) Click on the **Cover Page** tab.
   c) Click on the desired cover page.
   d) If you want to display the selected cover page, click on **Preview**.
   e) Click on **Save**.
5. If you want to insert a comment in the **Note** field in the cover page, proceed in the following steps:
   a) Click on **Comment**.
   b) Enter the **Cover Page Comment**.
   c) Click on **Comment**.

6. If you are a member of a fax group, proceed as follows to specify whether you are sending the fax on behalf of yourself or the fax group:

a) Click on **Setup**.

b) Click on the **Fax Ph.** tab.

c) In the **Sending documents on behalf of** drop-down list, select either the desired Fax Group or **Myself**.

d) Click on **Save**.

7. Enter the complete recipient’s e-mail address or the first part of the e-mail address in the search field.

The contact details are displayed underneath.

8. Click on the available e-mail address in order to add it in the Recipients list. The selected e-mail address is displayed under the phone number column.

9. Click on **Send**.

The system converts the fax in pdf format and sends it to the selected contact's e-mail address.

28.2 FaxPrinter User Guide, Chapter 5.3 How to Send a Fax Message to Recipients Found by Searching Directories

Prerequisites

- The document to be sent contains only TrueType fonts.
- You have changed your password in a UC client or at the phone menu of the voicemail box to at least 6 digits.

Step by Step

1. Select the menu item for printing in the relevant application, e.g., **File > Print** in Microsoft Word.

2. Select **CommunicationsClients Fax Printer** as the printer. The **Fax Printer** window opens.

3. Select the header line for the fax message:

a) Click on **Setup**.

b) Click on the **Fax Headlines** tab.

c) Click in the list of header lines on the desired header.

d) Click on **Save**.

4. If you want to send the fax message with a cover page, proceed as follows:

a) Click on **Setup**.

b) Click on the **Cover Page** tab.

c) Click on the desired cover page.

d) If you want to display the selected cover page, click on **Preview**.

e) Click on **Save**.

5. If you want to insert a comment in the **Note** field in the cover page, proceed in the following steps:
   a) Click on **Comment**.
   b) Enter the **Cover Page Comment**.
   c) Click on **Comment**.
6. If you are a member of a fax group, proceed as follows to specify whether you are sending the fax on behalf of yourself or the fax group:
   a) Click on **Setup**.
   b) Click on the **Fax Ph.** tab..
   c) In the **Sending documents on behalf of** drop-down list, select either the desired Fax Group or **Myself**.
   d) Click **Save**.
7. If relevant, click on the **Search Options** icon to display the selection options of the directories to be searched.
8. Select which directories are to be included in the search by enabling or clearing the **Internal Directory**, **Personal Directory**, **External Directory** and **External Offline Directory** check boxes as required. If myPortal for Outlook has been started, even fax numbers in Outlook contacts can be included in the search.
9. You can enter a company name, an e-mail address, a contact's name or fax number partially or fully in the input panel and click on the **Search** icon. If your search returns a result, Fax Printer will display a hit list.
10. Select the check box with the fax number of the desired recipient in the **Search Results** list to add that recipient to the fax message.
11. If you want to send the fax message to further recipients, click in the input field and repeat steps 9 through 10 accordingly.

> ***INFO:*** You can also add further recipients by entering their fax numbers directly.

12. If you want to remove a recipient, proceed in the following steps:
    a) Click in the list of **Recipients** on the desired entry.
    b) Press the `Del` key.
13. Click on **Send**.

> ***INFO:*** If myPortal for Desktop or myPortal for Outlook is already open, a screen pop informs you whether the transmission succeeded or failed.

Related Topics

- How to Send a Fax Message to a Fax Number
- How to Change your Sender Fax Number
- How to Change Users
- Fax Cover Editor

29 V2R1.0: Caller Number Transfer at Mobile Device if Transferred by System Device

Affected Documentation	Administrator Documentation
Issue	9
Reference No.	A31003-P3020-M100-09-76A9

29.1 Chapter 27.3.1.3 Basic Settings > System > Display

Parameter Description of Tabs:

- **Edit Display**

Parameters	Description
Display name / call number	It is possible to configure which of the following data is displayed for calls on the screens of all connected telephones: Calling ID only, Name (if present), or both Name and calling ID at the same time. If a telephone does not support one of these settings, instead of displaying the name and the calling ID at the same time, only the calling ID may be shown, for example. OpenStage telephones support the simultaneous display of the name and calling ID. Default value: Name and calling ID
Transfer before answer	If a call is transferred before it has been answered, either the number of the party transferring the call or the number of the party placing the call can be displayed at the receiving station. A call which was switched by "Transfer before answer" cannot be rejected by the called party. If Transferred by is selected, the display will show the transferring party before the connection is established and after the call is released. If Transferred to is selected, the display will show the transferring party as long as the transferring party is connected to the receiving station. After the transferring party releases the call and there is a connection, the display will change from the transferring party to the transferred party. Default value: Transferred to
Automatic recall	If a call is transferred and then recalled, either the number of the party transferring the call or the number of the party recalling the call can be displayed at the receiving station. An internal B station displays the call transfer. C receives a ring tone until either B answers or A recalls. This item can be used to configure what is to be shown on the display of transfer destination B: either station A (caller) or C (transferred destination). If an automatic recall is started from station A, both stations receive the display no reply. Default value: Transferred destination
Date/Time format	The date can be displayed in various formats. Default value: Europe - 24 hour format

Parameters	Description
Caller list, mode	If Internal and external calls or Only external calls is activated, all calls that were not accepted are saved in a list whose contents can then later be retrieved using a system procedure. If All external calls whether answered or not is activated, then calls that have been accepted are also saved in the caller list. No call numbers are removed from the caller list, either for incoming or outgoing calls. If all of the memory locations in the caller list have already been used, the oldest entry is overwritten when an additional call number is saved. Calls that have not been accepted are displayed in the manner already described in the Missed Calls List feature. Calls that have been accepted are displayed in the same manner as for the "Save call number" functionality of the caller list. If an external incoming call is routed via the AutoAttendant to an internal station and the station is currently busy or has call forwarding activated, no entry is made to the missed calls list. Default value: External calls only
Call number suppression	When this flag is activated, the calling number is not displayed in ISDN, i.e., the called party does not see the calling number (this feature also needs to be activated at the telephone company). Similarly, the name of the calling party is suppressed in networks with additional communication systems. There are call scenarios in which a caller may have been set to "presentation restricted" by the Central Office. If this flag is enabled, the caller's number is displayed to the called party. If this flag is disabled, the text "Number unknown" appears. The flag always depends on the CO settings of each provider. Default value: disabled
Directory (phone book)	Users can access a system-wide online directory (phone book) that includes names and call numbers for all internal extensions. System-specific display terminals allow users to scroll through the directory, to display all available internal stations with their names and call numbers, and then dial any of the stored numbers. Terminal devices with alphanumeric keypads can use this to search for a specific number. Select the appropriate option from the list: no: No access to the directory is possible; internal: Access to the internal directory (stations, groups and speed-dial destinations) is possible; LDAP: Access to the directory information of the LDAP server. LDAP access must be configured via LDAP for this purpose; all: Users can choose between accessing the internal directory or the LDAP directory. Default value: Internal
Switches	
Call timer display	No call charge information is displayed for outgoing external calls. For UP0/E devices with a display, the current call duration is displayed. For analog lines, time recording is started by a timer (five seconds after the end-of-dialing) and for digital trunks with CONNECT. The communication system does not support call duration display for S0 devices. Default value: disabled
DTMF closed display	When PIN codes are entered on system telephones with a display, only asterisks (*) are shown on the display. Default value: enabled

Parameters	Description
Display for info message	Info messages are shown on the display of system telephones. Default value: enabled
Outreach call number transparent	If a call is forwarded to an external station, the number of the calling station is displayed at the called station. In a networked system, the option must be set in the node at which a trunk connection is activated. This feature is contingent on the explicit release of the chargeable function Clip No Screening in the CO. This flag works as a toggle with the flag Suppress station number under Routes. Default value: disabled
SST with transfer option (transfer caller's number)	When this flag is activated, Single Step Transfer is enabled in desk phones. In case of blind transfer, the calling number is displayed at the external destination when the mobile device rings , i.e. the called party sees the calling number and not the number of the transferring party when the call is transferred by a system device. The flag "Outreach call number transparent" must be also activated. Default value: enabled IMPORTANT: If the transferred party is an external device, then the function CLIP no screening must be supported by the Network Provider and activated. Otherwise, the default DID of the system will be used from CO, or the call will be rejected from CO.

30 V2R1.0: Network Dial by Name

Affected Documentation	Administrator Documentation
Issue	9
Reference No.	A31003-P3020-M100-09-76A9

30.1 Chapter 12.5.2.2 How to Enable or Disable Searching the Internal Directory only

When dialing by name, you can configure either limiting the search only in the internal directory, or searching all directories in the network environment. The system is configured by default to search only in the internal directory.

Prerequisites

- You are logged into the WBM with the **Expert** profile.

Step by Step

1. In the navigation bar, click on **Expert Mode**.
2. In the navigation tree, click on **Applications> OpenScape Business UC Suite**.
3. Click **Servers** in the menu tree.
4. Click on the **General Settings** tab.
5. To enable searching only in the internal directory, select the check box **Dial by Name Search Local Extension only**.

   INFO: The check box **Dial by Name Search Local Extension only** is enabled by default.

   The system now searches only the internal directory when dialing by name. When the local extension is reached, the system plays the receiver’s name, as long as it has been previously recorded.
6. To disable searching only in the internal directory, clear the check box **Dial by Name Search Local Extension only**.

   The system now searches all directories in the network environment when dialing by name.

31 V2R1.0: Improve Configuration of LCR

Affected Documentation	Administrator Documentation
Issue	9
Reference No.	A31003-P3020-M100-09-76A9

31.1 Chapter 15.2.3.1 How to Edit Routing Tables

Prerequisites

- You are logged into the WBM with the **Expert** profile.

Step by Step

1. In the navigation bar, click on **Expert Mode**.
2. In the navigation tree, click **Telephony > LCR**.
3. Click on **Route table**.
4. All routing tables are displayed for you:
   - **1-Table**
   - **2-Table**
   - **nn-Table**

   INFO: Routing tables 1 to 15 are intended for default entries or for configuration using wizards. During a migration, the existing entries are automatically entered into these routing tables.

   However, this mechanism does not prevent any duplicates in the entries. Manual post-processing of the routing tables is therefore recommended.
5. Click on the desired routing table. The selected table with the **Change Routing table** tab is displayed.
6. The individual routing tables are listed under **Change Routing table** and you can edit the following fields:
   - **Route**
   - **Dial Rule**

   INFO: By clicking on the blue arrow next to the desired rule, you can view and edit the dial rule properties.

   - **min. COS (LCR Class of Service)**
   - **Warning**
   - **Dedicated Gateway**

- **GW Node ID**

7. Click on **Apply** followed by **OK**.

31.2 Chapter 27.3.5.4 LCR > Routing Table

Parameter Description of Tabs:

- **Change Routing Table**

Parameters	Description
Route tables	Call numbers defined in the dial plan are assigned an action (choice) here via the route tables. Value range: 254 route tables
Index	The route 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 in accordance the outdial rule and schedule entered in the route table. Value range: 1 to 16
Dedicated Route	The fixed route that was assigned to the subscriber (e.g., via the route assignment of the multisite management) is used.
Route	For details on the route to be assigned, see "Trunks/Routing > Routes" Default value: Route name configured in the system
Dial Rule	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. Definition under "Dial Rule". Value range: 254 dial rules
min. COS	COS describes the minimum LCR class-of-service needed by a station in order to use the associated route. It is thus possible to stipulate, for example, that one station is only permitted to place calls via a specific carrier or during certain times, while other stations have the option of using alternative routes. The value for the maximum class of service is 15. Value range: 1 to 15
Warning	If the first route selection in the route table is busy, the LCR function advances 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. Value range: None, Tone, Display, Display + Tone
Dedicated Gateway	This parameter defines the way in which the destination partner node is identified in an IP internetwork. Value range: No, Forced, Multi-location
Dedicated Gateway: **No**	The partner node is identified by the destination call number.
Dedicated Gateway: **Forced**	Routed is forced via the gateway that is defined by its node ID in the **GW Node ID** column.

Parameters	Description
Dedicated Gateway: **Multi-location**	Caller-based determination of the partner node: Routing occurs via the gateway that was assigned to the respective caller via the Multigateway wizard or in the **Stations > Edit workpoint client data > Secondary system ID** input mask. For callers without a related entry, routing occurs via the gateway that is defined by its node ID in the **GW node ID** column (default).
GW Node ID	Specifies the gateway node ID for the **Forced** or **Multi-location** options of the **Dedicated Gateway** parameter.
Buttons	
Blue arrow in the **Dial Rule** column	Displays the page with the **Dial Rule** parameters.

32 V2R1.0: Circuit Integration

Affected Documentation	Administrator Documentation
Issue	9
Reference No.	A31003-P3020-M100-9-76A9

32.1 How to Configure the Circuit Connectivity

- You have entered the value **Upstream up to (Kbps)** under **Setup > Wizards > Network/Internet > Internet Configuration**, in order to conduct simultaneous calls. For example, enter '256' for 2 simultaneous calls.

Step by Step

1. In the navigation bar, click on **Setup**.
2. In the navigation tree, click **Wizards > Circuit**.
3. Click on **Edit** next to **Circuit Connectivity**, to configure the basic connectivity settings.
4. Select the checkbox **Enable Circuit** to activate the Circuit connectivity.
5. Under **Tenant Credentials**, enter the following details:

   a) In case checkbox **Use Api key** is selected:

   Insert the Api Key which is generated for your tenant.

   b) In case checkbox **Use Api key** is not selected:
   The username in the **Tenant Admin** text box.
   The tenant password in the **Password** field.
   The Circuit URL.

6. Under **Simultaneous Circuit Calls**, select the number of simultaneous Circuit calls from the available drop-down list. This number depends on the upstream value previously configured.

   INFO: If the call quality deteriorates, the number of simultaneous calls must be reduced.

7. Click **OK & Next**.
8. Click **Execute function** to proceed with the automatic configuration.

   The system adds the trunks to Circuit, completes the UTC configuration and checks the connectivity.

9. When the function is executed, click **OK & Next**.

10. Click **Finish**.

INFO: It is suggested to save the configuration data, by selecting **Data Backup > Backup - Immediate** from the main menu.

Related Topics

32.2 How to Add Circuit Users

Step by Step

1. In the navigation bar, click on **Setup**.
2. In the navigation tree, click **Wizards > Circuit**.
3. Click on **Edit** next to **Circuit User Instance**.
4. Click on **Add** next to **New Circuit User**.
5. At the **Circuit User Allocation** page, enter the following details:
   - *a)* The **trunk access code + Circuit user call number**.
   - *b)* The **Circuit user call number**.
   - *c)* The **Circuit user DID**.
   - *d)* The Circuit User. The available users are displayed as icons.
   - *e)* The Circuit user **Name** is filled automatically.
6. Click **OK & Next**.
7. Perform steps 4- 6 to add more Circuit users.

32.3 How to Edit Circuit User Details

Step by Step

1. In the navigation bar, click on **Setup**.
2. In the navigation tree, click **Wizards > Circuit**.
3. Click on **Edit** next to **Circuit User Instance**.
4. Click on **Edit** next to the corresponding Circuit user.
5. You can edit the following details:
   - *a)* The **trunk access code + Circuit user call number**.
   - *b)* The **Circuit user call number**.
   - *c)* The **Circuit user DID**.
   - *d)* The Circuit user **Name**.

INFO: The Selected Circuit User field which contains the e-mail address of the user is not editable.

6. Click **OK & Next**.

32.4 Chapter 27.3.7.15 Station > Station > Circuit User

Circuit users can be added only via the **Setup > Wizards > Circuit: Edit - Circuit user instance**

Parameter Description of Tabs:

- **Edit Subscriber**

Parameters	Description
Callno	Input of the internal extension number of the Circuit User (e.g., 777). This internal call number must not have already been assigned.
DID	Direct inward dialing number of the Circuit User.
First Name	Freely selectable first name for the station. Value range: max. 16 characters, no umlauts or special characters.
Last Name	Freely selectable last name for the station. Value range: max. 16 characters, no umlauts or special characters.
Display	Freely selectable name for the station. By default, is created using the First Name and Last Name parameters depending on display name algorithm. Value range: max. 16 characters, no umlauts or special characters.
Type	Displays the type of Circuit User.
Circuit Call Number	The Circuit User call number.

33 V2R1.0: Unified Directory Improvements

Affected Documentation	Administrator Documentation
Issue	9
Reference No.	A31003-P3020-M100-09-76A9

33.1 Chapter 11.5.1 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:

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.

33.1.1 Chapter 11.5.1.1 How to Configure Directories for System Telephones

Prerequisites

- You are logged into the WBM with the **Expert** profile.

You can select which directories are to be made available on system telephones with displays.

Step by Step

1. In the navigation bar, click on **Expert Mode**.
2. Click **Telephony Server > Basic Settings** in the navigation tree.
3. In the menu tree, click on **System > Display**.
4. Select one of the following options in the **Directory (phone book)** drop-down list:
   - If both the personal contacts, the internal, external and networking directory and the LDAP directory are to be made available, select **All**.
   - If only the personal contacts, the internal, external and networking directory is to be made available, select **Internal**.
   - If only the LDAP directory is to be made available, select **LDAP**.
   - If no directory is to be made available, select **No**.
5. Click **Apply**.

Next steps If you have selected **All** or **LDAP**, make sure that an appropriate LDAP directory (e.g., Open Directory Service) is available for the system telephones.

33.2 Chapter 12.5.1 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:

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.

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.

33.2.1 Chapter 12.5.1.1 How to Configure Directories for System Telephones

Prerequisites

- You are logged into the WBM with the **Expert** profile.

You can select which directories are to be made available on system telephones with displays.

Step by Step

1. In the navigation bar, click on **Expert Mode**.
2. Click **Telephony Server > Basic Settings** in the navigation tree.
3. In the menu tree, click on **System > Display**.
4. Select one of the following options in the **Directory (phone book)** drop-down list:
   - If both the personal contacts, the internal, external and networking directory and the LDAP directory are to be made available, select **All**.
   - If only the personal contacts, the internal, external and networking directory is to be made available, select **Internal**.
   - If only the LDAP directory is to be made available, select **LDAP**.
   - If no directory is to be made available, select **No**.
5. Click **Apply**.

Next steps If you have selected **All** or **LDAP**, make sure that an appropriate LDAP directory (e.g., Open Directory Service) is available for the system telephones.

33.3 Chapter 27.3.1.3 Basic Settings > System > Display

Parameter Description of Tabs:

- **Edit Display**

Parameters	Description
Display name / call number	It is possible to configure which of the following data is displayed for calls on the screens of all connected telephones: Calling ID only, Name (if present), or both Name and calling ID at the same time. If a telephone does not support one of these settings, instead of displaying the name and the calling ID at the same time, only the calling ID may be shown, for example. OpenStage telephones support the simultaneous display of the name and calling ID. Default value: Name and calling ID
Display name / algorithm	Full name support is done with three fields, one for the first name, one for the last name and a third for the display name. Each field is able to store up to sixteen characters. One of the following options of the display name algorithm can be used: • <last name>, <first name> • <last name>, <first name initial.> • <first name> <last name> • <first name initial.> <last name> • <last name> Default value: <last name>, <first name>
Transfer before answer	If a call is transferred before it has been answered, either the number of the party transferring the call or the number of the party placing the call can be displayed at the receiving station. A call which was switched by "Transfer before answer" cannot be rejected by the called party. If Transferred by is selected, the display will show the transferring party before the connection is established and after the call is released. If Transferred to is selected, the display will show the transferring party as long as the transferring party is connected to the receiving station. After the transferring party releases the call and there is a connection, the display will change from the transferring party to the transferred party. Default value: Transferred to
Automatic recall	If a call is transferred and then recalled, either the number of the party transferring the call or the number of the party recalling the call can be displayed at the receiving station. An internal B station displays the call transfer. C receives a ring tone until either B answers or A recalls. This item can be used to configure what is to be shown on the display of transfer destination B: either station A (caller) or C (transferred destination). If an automatic recall is started from station A, both stations receive the display no reply. Default value: Transferred destination
Date/Time format	The date can be displayed in various formats. Default value: Europe - 24 hour format

Parameters	Description
Caller list, mode	If Internal and external calls or Only external calls is activated, all calls that were not accepted are saved in a list whose contents can then later be retrieved using a system procedure. If All external calls whether answered or not is activated, then calls that have been accepted are also saved in the caller list. No call numbers are removed from the caller list, either for incoming or outgoing calls. If all of the memory locations in the caller list have already been used, the oldest entry is overwritten when an additional call number is saved. Calls that have not been accepted are displayed in the manner already described in the Missed Calls List feature. Calls that have been accepted are displayed in the same manner as for the "Save call number" functionality of the caller list. If an external incoming call is routed via the AutoAttendant to an internal station and the station is currently busy or has call forwarding activated, no entry is made to the missed calls list. Default value: External calls only
Call number suppression	When this flag is activated, the calling number is not displayed in ISDN, i.e., the called party does not see the calling number (this feature also needs to be activated at the telephone company). Similarly, the name of the calling party is suppressed in networks with additional communication systems. There are call scenarios in which a caller may have been set to "presentation restricted" by the Central Office. If this flag is enabled, the caller's number is displayed to the called party. If this flag is disabled, the text "Number unknown" appears. The flag always depends on the CO settings of each provider. Default value: disabled
Directory (phone book)	Users can access a system-wide online directory (phone book) that includes names and call numbers for all internal extensions. System-specific display terminals allow users to scroll through the directory, to display all available internal stations with their names and call numbers, and then dial any of the stored numbers. Terminal devices with alphanumeric keypads can use this to search for a specific number. Select the appropriate option from the list: no: No access to the directory is possible; internal: Access to the internal directory (stations, groups and speed-dial destinations) is possible; LDAP: Access to the directory information of the LDAP server. LDAP access must be configured via LDAP for this purpose; all: Users can choose between accessing the internal directory or the LDAP directory. Default value: Internal
Switches	
Call timer display	No call charge information is displayed for outgoing external calls. For UP0/E devices with a display, the current call duration is displayed. For analog lines, time recording is started by a timer (five seconds after the end-of-dialing) and for digital trunks with CONNECT. The communication system does not support call duration display for S0 devices. Default value: disabled

Parameters	Description
DTMF closed display	When PIN codes are entered on system telephones with a display, only asterisks (*) are shown on the display. Default value: enabled
Display for info message	Info messages are shown on the display of system telephones. Default value: enabled
Outreach call number transparent	If a call is forwarded to an external station, the number of the calling station is displayed at the called station. In a networked system, the option must be set in the node at which a trunk connection is activated. This feature is contingent on the explicit release of the chargeable function Clip No Screening in the CO. This flag works as a toggle with the flag Suppress station number under Routes. Default value: disabled

33.4 Chapter 27.3.7.1 Station > Stations > UP0 Stations

Parameter Description of Tabs:

- **Change Station**

Parameters	Description
Call no	Internal call number of the station.
DuWa	DID number of the station.
First Name	Freely selectable first name for the station. Value range: max. 16 characters, no umlauts or special characters
Last Name	Freely selectable last name for the station. Value range: max. 16 characters, no umlauts or special characters
Display	Freely selectable name for the station. By default, it is created using the First Name and Last Name parameters depending on display name algorithm. Value range: max. 16 characters, no umlauts or special characters
Clip/Lin	Sequence of digits to be displayed at the called party instead of the actual number for outgoing external calls (e.g., for E911 emergency services in the USA) Value range: max. 16 digits
Active	Indicates whether the station is operational.
Device type	Displays the device associated with the subscriber.
Fax Call no.	If a fax box has been set up (e.g., with the UC clients myPortal for Desktop or myPortal for Outlook), the fax number at which fax messages from internal locations can be received by the subscriber should be entered here.
Fax DID	If a fax box has been set up (e.g., with the UC clients myPortal for Desktop or myPortal for Outlook), the fax number at which fax messages from external locations can be received by the subscriber should be entered here.
Access	Displays the physical interface at which the device is connected.

Parameters	Description
Search	You can also have selected subscribers displayed by entering a search term in the **Search** fields and pressing the Return key. The subscribers who match the search term are displayed. If you leave all the **Search** fields empty and press the Enter key, all subscribers will be listed again.
Items per page	Selection to determine whether 10, 25, 50 or 100 items are to be displayed per page.
Buttons	
Blue arrow in the **Call no** column	Brings up the page with the **Edit station parameters**, **Edit station flags**, **Edit workpoint client data** and **Edit Group/CFW** tabs.
>	Moves one page forward.
<	Moves one page back.
>|	Moves to the end of the list.
|<	Moves to the beginning of the list.

Parameter Description of Tabs:

- **UP0 Master/Slave**
  This tab appears only for OpenScape Business X8, since the slave ports are managed dynamically in this system. For OpenScape Business X1/X3/X5, the slave ports are assigned statically (i.e., are fixed)

Parameters	Description
Call no	Internal call number of the station.
DuWa	DID number of the station.
Name	Freely selectable name for the station. Value range: max. 16 characters, no umlauts or special characters
Access	Displays the physical interface at which the device is connected.
Add Slave Zone	If this check box is selected, a slave port is preassigned to the selected master port. After saving the selection with **Apply** the call number, DID number and name of the slave system telephone can be configured in advance. When the slave system telephone is then connected to the slave adapter of the master system telephone, it is assigned the previously selected slave port. If the slave system telephone is connected without a predefined slave port, the next available port (as of port 384) is automatically used.
Delete Slave Zone	If this check box is selected, the preconfiguration of the slave system telephone is deleted. If a slave system telephone is already connected to the slave adapter of the master system telephone, the check box is grayed out, and the preconfiguration cannot be deleted.
Search	You can also have selected subscribers displayed by entering a search term in the **Search** fields and pressing the Return key. The subscribers who match the search term are displayed. If you leave all the **Search** fields empty and press the Enter key, all subscribers will be listed again.
Items per page	Selection to determine whether 10, 25, 50 or 100 items are to be displayed per page.
Buttons	

Parameters	Description
>	Moves one page forward.
<	Moves one page back.
>|	Moves to the end of the list.
|<	Moves to the beginning of the list.

Parameter Description of Tabs:

- **Device Info**

Parameters	Description
Call no	Internal call number of the station.
Name	Station name.
Device type	Displays the device type associated with the station.
Current SW version	Software version of the associated device (if available).
HW version	Hardware version of the associated device (if available).
Items per page	Selection to determine whether 10, 25, 50 or 100 items are to be displayed per page.
Buttons	
>	Moves one page forward.
<	Moves one page back.
>|	Moves to the end of the list.
|<	Moves to the beginning of the list.

33.5 Chapter 27.3.7.2 Station > Stations > IP Clients

Parameter Description of Tabs:

- **Change Station**

Parameters	Description
Call no	Internal call number of the station.
DuWa	DID number of the station.
First Name	Freely selectable first name for the station. Value range: max. 16 characters, no umlauts or special characters
Last Name	Freely selectable last name for the station. Value range: max. 16 characters, no umlauts or special characters
Display	Freely selectable name for the station. By default, it is created using the First Name and Last Name parameters depending on display name algorithm. Value range: max. 16 characters, no umlauts or special characters
Type	Type of the station.

Parameters	Description
Type: **Free**	This call number is not yet assigned to any station.
Type: **System Client**	A system client is an IP station that can use all the features of the communication system via CorNet-IP (formerly called HFA system client)
Type: **RAS User**	A RAS user (Remote Access Service user) is granted Internet access to the IP network via the ISDN connection. This allows the communication system to be remotely serviced and licensed.
Type: **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.
Type: **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).
Clip/Lin	Sequence of digits to be displayed at the called party instead of the actual number for outgoing external calls (e.g., for E911 emergency services in the USA)
Active	Indicates whether the station is operational.
Fax Call no.	If a fax box has been set up (e.g., with the UC clients myPortal for Desktop or myPortal for Outlook), the fax number at which fax messages from internal locations can be received by the subscriber should be entered here.
Fax DID	If a fax box has been set up (e.g., with the UC clients myPortal for Desktop or myPortal for Outlook), the fax number at which fax messages from external locations can be received by the subscriber should be entered here.
Search	You can also have selected subscribers displayed by entering a search term in the **Search** fields and pressing the Enter key. The subscribers who match the search term are displayed. If you leave all the **Search** fields empty and press the Enter key, all subscribers will be listed again.
Items per page	Selection to determine whether 10, 25, 50 or 100 items are to be displayed per page.
Buttons	
Blue arrow in the **Call no** column	Brings up the page with the **Edit station parameters**, **Edit station flags**, **Edit workpoint client data** and **Edit Group/CFW** tabs.
>	Moves one page forward.
<	Moves one page back.
>|	Moves to the end of the list.
|<	Moves to the beginning of the list.

Parameter Description of Tabs:

- **Device Info**

Parameters	Description
Call no	Internal call number of the station.
Name	Station name.
Device type	Displays the device type associated with the station.
IP Address	IP address of the associated device; direct link to the WBM of the IP telephone
MAC Address	MAC address of the associated telephone
Current SW version	Software version of the associated device (if available).

Parameters	Description
HW version	Hardware version of the associated device (if available).
Items per page	Selection to determine whether 10, 25, 50 or 100 items are to be displayed per page.
Buttons	
>	Moves one page forward.
<	Moves one page back.
>|	Moves to the end of the list.
|<	Moves to the beginning of the list.

33.6 Chapter 27.3.7.3 Station > Stations > Analog Stations

Parameter Description of Tabs:

- **Change Station**

Parameters	Description
Call no	Internal call number of the station.
DuWa	DID number of the station.
First Name	Freely selectable first name for the station. Value range: max. 16 characters, no umlauts or special characters
Last Name	Freely selectable last name for the station. Value range: max. 16 characters, no umlauts or special characters
Display	Freely selectable name for the station. By default, it is created using the First Name and Last Name parameters depending on display name algorithm. Value range: max. 16 characters, no umlauts or special characters
Clip/Lin	Sequence of digits to be displayed at the called party instead of the actual number for outgoing external calls (e.g., for E911 emergency services in the USA) Value range: max. 16 digits
Active	Indicates whether the station is operational.
Device type	Displays the device associated with the subscriber.
Fax Call no.	If a fax box has been set up (e.g., with the UC clients myPortal for Desktop or myPortal for Outlook), the fax number at which fax messages from internal locations can be received by the subscriber should be entered here.
Fax DID	If a fax box has been set up (e.g., with the UC clients myPortal for Desktop or myPortal for Outlook), the fax number at which fax messages from external locations can be received by the subscriber should be entered here.
Access	Displays the physical interface at which the device is connected.

Parameters	Description
Search	You can also have selected subscribers displayed by entering a search term in the **Search** fields and pressing the Return key. The subscribers who match the search term are displayed. If you leave all the **Search** fields empty and press the Enter key, all subscribers will be listed again.
Items per page	Selection to determine whether 10, 25, 50 or 100 items are to be displayed per page.
Buttons	
Blue arrow in the **Call no** column	Brings up the page with the **Edit station parameters**, **Edit station flags**, **Edit workpoint client data** and **Edit Group/CFW** tabs.
>	Moves one page forward.
<	Moves one page back.
>|	Moves to the end of the list.
|<	Moves to the beginning of the list.

33.7 Chapter 27.3.7.4 Station > Stations > ISDN Stations

Parameter Description of Tabs:

- **Change Station**

Parameters	Description
Call no	Internal call number of the station.
DuWa	DID number of the station.
First Name	Freely selectable first name for the station. Value range: max. 16 characters, no umlauts or special characters
Last Name	Freely selectable last name for the station. Value range: max. 16 characters, no umlauts or special characters
Display	Freely selectable name for the station. By default, it is created using the First Name and Last Name parameters depending on display name algorithm. Value range: max. 16 characters, no umlauts or special characters
Clip/Lin	Sequence of digits to be displayed at the called party instead of the actual number for outgoing external calls (e.g., for E911 emergency services in the USA) Value range: max. 16 digits
Active	Indicates whether the station is operational.
Device type	Displays the device associated with the subscriber.
Fax Call no.	If a fax box has been set up (e.g., with the UC clients myPortal for Desktop or myPortal for Outlook), the fax number at which fax messages from internal locations can be received by the subscriber should be entered here.

Parameters	Description
Fax DID	If a fax box has been set up (e.g., with the UC clients myPortal for Desktop or myPortal for Outlook), the fax number at which fax messages from external locations can be received by the subscriber should be entered here.
Access	Displays the physical interface at which the device is connected.
Search	You can also have selected subscribers displayed by entering a search term in the **Search** fields and pressing the Return key. The subscribers who match the search term are displayed. If you leave all the **Search** fields empty and press the Enter key, all subscribers will be listed again.
Items per page	Selection to determine whether 10, 25, 50 or 100 items are to be displayed per page.
Buttons	
Blue arrow in the **Call no** column	Brings up the page with the **Edit station parameters**, **Edit station flags**, **Edit workpoint client data** and **Edit Group/CFW** tabs.
>	Moves one page forward.
<	Moves one page back.
>|	Moves to the end of the list.
|<	Moves to the beginning of the list.

33.8 Chapter 27.3.7.5 Station > Station > DECT Stations > SLC Call number

Parameter Description of Tabs:

- **Change Station**

Parameters	Description
Call no	Internal call number of the station.
DuWa	DID number of the station.
First Name	Freely selectable first name for the station. Value range: max. 16 characters, no umlauts or special characters
Last Name	Freely selectable last name for the station. Value range: max. 16 characters, no umlauts or special characters
Display	Freely selectable name for the station. By default, it is created using the First Name and Last Name parameters depending on display name algorithm. Value range: max. 16 characters, no umlauts or special characters
Clip/Lin	Sequence of digits to be displayed at the called party instead of the actual number for outgoing external calls (e.g., for E911 emergency services in the USA) Value range: max. 16 digits
Active	Indicates whether the station is operational.
Device type	Displays the device associated with the subscriber. Base stations are shown as S0 stations.

Parameters	Description
Access	Displays the physical interface at which the device is connected.
Parameters	Default view for all stations; do not change the settings
Search	You can also have selected subscribers displayed by entering a search term in the **Search** fields and pressing the Return key. The subscribers who match the search term are displayed. If you leave all the **Search** fields empty and press the Enter key, all subscribers will be listed again.
Items per page	Selection to determine whether 10, 25, 50 or 100 items are to be displayed per page.
Buttons	
Blue arrow in the **Call no** column	Brings up the page with the **Edit station parameters**, **Edit station flags**, **Edit workpoint client data** and **Edit Group/CFW** tabs.
>	Moves one page forward.
<	Moves one page back.
>|	Moves to the end of the list.
|<	Moves to the beginning of the list.

33.9 Chapter 27.3.7.6 Station > Station > DECT Stations > DECT Stations

Parameter Description of Tabs:

- **Change Station**

Parameters	Description
Call no	Internal call number of the station.
DuWa	DID number of the station.
First Name	Freely selectable first name for the station. Value range: max. 16 characters, no umlauts or special characters
Last Name	Freely selectable last name for the station. Value range: max. 16 characters, no umlauts or special characters
Display	Freely selectable name for the station. By default, it is created using the First Name and Last Name parameters depending on display name algorithm. Value range: max. 16 characters, no umlauts or special characters
Clip/Lin	Sequence of digits to be displayed at the called party instead of the actual number for outgoing external calls (e.g., for E911 emergency services in the USA) Value range: max. 16 digits
Active	Indicates whether the station is operational.
Device type	Displays the device associated with the subscriber.. DECT stations are shown as Comfort-PP.

Parameters	Description
Fax Call no.	If a fax box has been set up (e.g., with the UC clients myPortal for Desktop or myPortal for Outlook), the fax number at which fax messages from internal locations can be received by the subscriber should be entered here.
Fax DID	If a fax box has been set up (e.g., with the UC clients myPortal for Desktop or myPortal for Outlook), the fax number at which fax messages from external locations can be received by the subscriber should be entered here.
Access	Displays the physical interface at which the device is connected.
Search	You can also have selected subscribers displayed by entering a search term in the **Search** fields and pressing the Return key. The subscribers who match the search term are displayed. If you leave all the **Search** fields empty and press the Enter key, all subscribers will be listed again.
Items per page	Selection to determine whether 10, 25, 50 or 100 items are to be displayed per page.
Buttons	
Blue arrow in the **Call no** column	Brings up the page with the **Edit station parameters**, **Edit station flags**, **Edit workpoint client data** and **Edit Group/CFW** tabs.
>	Moves one page forward.
<	Moves one page back.
>|	Moves to the end of the list.
|<	Moves to the beginning of the list.

33.10 Chapter 27.3.7.7 Station > Stations > IVM/EVM Ports > IVM

Parameter Description of Tabs:

- **Change Station**

Parameters	Description
Call no	Internal call number of the IVM port.
DuWa	DID number of the IVM port, if present.
First Name	Freely selectable first name for the station. Value range: max. 16 characters, no umlauts or special characters
Last Name	Freely selectable last name for the station. Value range: max. 16 characters, no umlauts or special characters
Display	Freely selectable name for the station. By default, it is created using the First Name and Last Name parameters depending on display name algorithm. Value range: max. 16 characters, no umlauts or special characters
Clip/Lin	Sequence of digits to be displayed at the called party instead of the actual number for outgoing external calls (e.g., for E911 emergency services in the USA).
Active	Indicates whether the IVM port is operational.

Parameters	Description
Device type	For IVM, S0 stations are displayed.
Access	Displays the internal port for the IVM.
Station type	"PhoneMail" must be selected for IVM; "Standard" should be set for the announcement function.
Parameters	Default view for all stations; do not change the settings (e.g., the "language" is not the language of voicemail announcements).
Search	You can also have selected IVM ports displayed by entering a search term in the **Search** fields and pressing the Return key. The IVM ports that match the search term are displayed. If you leave all the **Search** fields empty and press the Return key, all IVM ports will be listed again.
Items per page	Selection to determine whether 10, 25, 50 or 100 items are to be displayed per page.
Buttons	
Blue arrow in the **Call no** column	Brings up the page with the **Edit station parameters**, **Edit station flags**, **Edit workpoint client data** and **Edit Group/CFW** tabs.
>	Moves one page forward.
<	Moves one page back.
>|	Moves to the end of the list.
|<	Moves to the beginning of the list.

33.11 Chapter 27.3.7.8 Stations > Station > IVM/EVM Ports > EVM

Parameter Description of Tabs:

- **Change Station**

Parameters	Description
Call no	Internal call number of the voicemail port.
DuWa	DID number of the voicemail port, if present.
First Name	Freely selectable first name for the voicemail port. Value range: max. 16 characters, no umlauts or special characters
Last Name	Freely selectable last name for the voicemail port. Value range: max. 16 characters, no umlauts or special characters
Display	Freely selectable name for the voicemail port. By default, it is created using the First Name and Last Name parameters depending on display name algorithm. Value range: max. 16 characters, no umlauts or special characters
Clip/Lin	Sequence of digits to be displayed at the called party instead of the actual number for outgoing external calls (e.g., for E911 emergency services in the USA).
Active	Indicates whether the voicemail port is operational.
Device type	For EVM, S0 stations are displayed.

Parameters	Description
Access	Displays the internal port for the voicemail.
Station type	"PhoneMail" must be selected for EVM; "Standard" should be set for the AutoAttendant.
Parameters	Default view for all voicemail ports; do not change the settings (e.g., the "language" is not the language of voicemail announcements).
Search	You can also have selected voicemail ports displayed by entering a search term in the **Search** fields and pressing the Return key. The voicemail ports that match the search term are displayed. If you leave all the **Search** fields empty and press the Return key, all voicemail ports will be listed again.
Items per page	Selection to determine whether 10, 25, 50 or 100 items are to be displayed per page.
Buttons	
Blue arrow in the **Call no** column	Brings up the page with the **Edit station parameters**, **Edit station flags**, **Edit workpoint client data** and **Edit Group/CFW** tabs.
>	Moves one page forward.
<	Moves one page back.
>|	Moves to the end of the list.
|<	Moves to the beginning of the list.

33.12 Chapter 27.3.7.9 Station > Stations > Virtual Stations

Parameter Description of Tabs::

- **Change Station**

Parameters	Description
Call no	Internal call number of the virtual station.
DuWa	DID number of the virtual station.
First Name	Freely selectable first name for the station. Value range: max. 16 characters, no umlauts or special characters
Last Name	Freely selectable last name for the station. Value range: max. 16 characters, no umlauts or special characters
Display	Freely selectable name for the station. By default, it is created using the First Name and Last Name parameters depending on display name algorithm. Value range: max. 16 characters, no umlauts or special characters
Type	Empty or virtual station (fixed display for Mobility Entry)
Clip/Lin	Sequence of digits to be displayed at the called party instead of the actual number for outgoing external calls (e.g., for E911 emergency services in the USA)
Active	Indicates whether the virtual station is operational.

Parameters	Description
Search	You can also have selected subscribers displayed by entering a search term in the **Search** fields and pressing the Return key. The subscribers who match the search term are displayed. If you leave all the **Search** fields empty and press the Enter key, all subscribers will be listed again.
Items per page	Selection to determine whether 10, 25, 50 or 100 items are to be displayed per page.
Buttons	
Blue arrow in the **Call no** column	Brings up the page with the **Edit station parameters**, **Edit station flags**, **Edit workpoint client data** and **Edit Group/CFW** tabs.
>	Moves one page forward.
<	Moves one page back.
>|	Moves to the end of the list.
|<	Moves to the beginning of the list.

33.13 Chapter 27.3.7.10 Stations > Station > Station Parameters

Parameter Description of Tabs:

- **Edit station parameters**

Parameters	Description
Stations - ...	
Type	Type of the station.
Call number	Internal call number of the station.
First Name	Freely selectable first name for the station. Value range: max. 16 characters, no umlauts or special characters
Last Name	Freely selectable last name for the station. Value range: max. 16 characters, no umlauts or special characters
Display	Freely selectable name for the station. By default, it is created using the First Name and Last Name parameters depending on display name algorithm. Value range: max. 16 characters, no umlauts or special characters
Direct inward dialing	DID number of the station.
Device type	Displays the device associated with the subscriber.
Clip/Lin	Sequence of digits to be displayed at the called party instead of the actual number for outgoing external calls (e.g., for E911 emergency services in the USA) Value range: max. 16 digits
Access	Displays the physical interface at which the device is connected.
Fax	

Parameters	Description
Call number	If a fax box has been set up (e.g., with the UC clients myPortal for Desktop or myPortal for Outlook), the fax number at which fax messages from internal locations can be received by the subscriber should be entered here.
Direct inward dialing	If a fax box has been set up (e.g., with the UC clients myPortal for Desktop or myPortal for Outlook), the fax number at which fax messages from external locations can be received by the subscriber should be entered here.
Mobility	
Mobile phone number	Only for SIP clients and mobile users: For the One Number Service, this number is used for the authentication of DISA access via the mobile service. Enter the mobile phone number associated with the subscriber together with the dialout prefix (i.e., the CO code), e.g., 0017312345678).
Web Feature ID	The Web Feature ID defines how the subscriber should log in at the mobile web client (user name). Choice between "no" (Mobility Entry only) and "automatic" (internal call number of the subscriber) or selection of the station number of the client or phone from the drop-down list.
Parameters	
Station type	Type of the connected device (drop-down list)
Station type: **Standard**	System telephones or analog telephones
Station type: **Fax**	Fax machine, e.g., no override possible
Station type: **Loudspeaker**	For paging via the a/b port
Station type: **Answering Machine**	Only for analog: if an answering machine is connected to this interface, this setting enables a call to be taken over from the answering machine from any device even though the answering machine has already accepted the call. To do this, the terminal must be programmed with the internal call number of the analog station. Besides being selected for answering machines, this entry should also be selected for virtual ports where no physical equipment has been set up. This prevents the communication system from checking the operating status of the port. Only for virtual ports: If a station without access was configured as a type of answering machine in Manager E, the port must be additionally configured as a virtual port. Otherwise, it will not be visible as a station in the WBM.
Station type: **P.O.T. MW LED**	For standard analog telephones (P.O.T = Plain Old Telephone) with a message-waiting LED Not for U.S.
Station type: **Door station with pulsed loop**	When using a pulsed loop device with the door opener function
Station type: **Modem**	Call override is not possible with this setting. It is intended for modems.
	When a fax or modem station is deleted (i.e., the call number and DID are deleted), the extension type must also be reset to the default (standard).
Language	Language for the menu control of the device (system telephone).
Call signaling internal	Every station can be assigned one of a total of eight possible internal ringing tones here. This means that in addition to the external ringing tone, an internal ringing tone is assigned here and subsequently transmitted for internal calls. Default value: Ring type 1

Parameters	Description
Call signaling external	Three different ring types for signaling external calls can be selected here: – System Phones: Ring type 1 = External call (e.g., double ring), Ring type 2 = External call CO 2 (e.g., triple ring), Ring type 3 = External call CO 3 (e.g., short/long/short) – Analog telephones for Germany: Ring type 1 = External call, Ring type 2 = Automatic recall, Ring type 3 = Door bell ring – Analog telephones for other countries: Ring type 1 = External call, Ring type 2 = External call, Ring type 3 = External call Default value: Ring type 1
Class of Service (LCR)	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). Default value: 15
Hotline Mode	Selection of the hotline options
Hotline Mode: **off**	Disables the hotline feature.
Hotline Mode: **Off-hook alarm after timeout**	The call to the hotline takes place after a predefined delay (off-hook alarm time), see Telephony/Basic Settings/System/Intercept-Attendant-Hotline
Hotline, Mode: **Hotline**	Enables the hotline feature. On lifting the handset, the connection to the hotline destination is established immediately, see Telephony/Basic Settings/System/ Intercept-Attendant-Hotline
Hotline	For details on selecting hotline destinations, see Telephony/ Basic Settings/System/ Intercept-Attendant-Hotline
Hotline: **none**	No destination defined
Hotline: **Digits 1 to 6**	For details on hotline destinations, see Telephony/ Basic Settings/System/ Intercept-Attendant-Hotline
Payload Security	Only for IP system clients: enable or disable the encryption of phone conversations (SPE). To do this, all stations involved must have SPE enabled.
Buttons	
>	Moves to the next station. If the stations matching the search term entered in the **Search** fields were previously filtered, it is possible to move between only those specific stations.
<	Skips back one station.

Parameter Description of Tabs:

- **Edit station flags**

Parameters	Description
Stations - ...	
Type	Type of the station.
Call number	Internal call number of the station.
Name	Station name.
Station flags	

Parameters	Description
Override class of service on	When this flag is activated, the subscriber can break into (i.e., override) an internal subscriber's ongoing connection. The subscribers involved are notified of the busy override by a warning tone and a display message. Default value: Disabled
Override Do Not Disturb	When this flag is activated, the following applies: when the subscriber calls a station for which Do Not Disturb has been activated, he or she can override Do Not Disturb. After five seconds, the call is signaled at the called station. If the flag is disabled, the Do Not Disturb function cannot be overridden. Subscribers who call a station for which Do Not Disturb has been activated receive the busy tone. Default value: Disabled
FWD external permitted	When this flag is activated, the subscriber can activate call forwarding to an external destination. Charges incurred for the execution of an external call forwarding are allocated to the subscriber who activated the call forwarding. Default value: Enabled
Prevention of voice calling off	When this flag is activated, the station can be called directly. This enables an internal call to be set up without lifting the handset. The loudspeaker on the called station is activated automatically in the process. Default value: Enabled
DISA class of service	When this flag is activated, external subscribers can activate or deactivate functions of the communication system via DISA (Direct Inward System Access) and set up outbound external connections just like any other internal subscribers. This also includes activating and deactivating call forwarding, the Do Not Disturb feature and the lock code, for example. Default value: Disabled
Transit allowed via Hook-on	When this flag is activated, the subscriber can transfer an external call to another external subscriber by hanging up. Example: The subscriber is the conference controller and hangs up: if there are other internal subscribers still in the conference, the longest participating internal subscriber automatically becomes the conference controller. If there are only external participants remaining in the conference, the conference is terminated, and all connections are cleared. Default value: Disabled
System telephone lock reset	When this flag is activated, the subscriber can reset the individual lock code of other internal subscribers to the default code. Default value: Disabled
CLIP analog (only for analog devices)	When this flag is activated, the caller's phone number is shown on the phone display of the analog station. As a prerequisite, the analog phone of the subscriber must support CLIP (Calling Line Identification Presentation). Default value: Enabled

Parameters	Description
MCID access	When this flag is activated, the subscriber can have malicious external callers identified via the ISDN Central Office. As a prerequisite, the "Trace call" (Malicious Call Identification, MCID) feature must have been applied for and activated by the network provider. After the "Trace call" feature has been activated by the network provider, the following must be noted: for each incoming call from the ISDN CO, the release of the connection to the called station is delayed for a specific timeout period after the caller hangs up. This timeout enables the called station to activate the "Trace call" feature. The ISDN trunk availability is somewhat reduced as a result. Default value: Disabled
Entry in telephone directory	When this flag is activated, the name and number of the subscriber will be displayed in the system directory. Default value: Enabled
Editing the Telephone Number	When this flag is activated, the subscriber can edit the digits of the call number entered via the keypad before the digit transmission. This requires a system phone with a display. Default value: Disabled
No group ringing on busy	When this flag is enabled, the following applies: The status of the station with group ringing programmed (i.e., the primary station) determines whether or not group ringing occurs. If the primary station is free, all stations included in the group are called immediately. If call waiting is enabled at the primary station: all stations included in the group are called after a delay of 5 seconds. If the primary station cannot receive a call or if call waiting is inactive: group ringing does not take place. Default value: Disabled
Associated dialing/services	Associated dialing: when this flag is activated, the subscriber can dial a number on behalf of another internal subscriber as if that station itself were dialing. Associated services: When this flag is activated, the subscriber can control features on behalf of another internal subscriber as if that station itself were controlling these features. This includes activating and deactivating call forwarding, group ringing and the lock code, for example. Default value: Disabled
Call waiting rejection on	When this flag is activated, subscribers who are conducting a call are not informed about other incoming calls via a call waiting tone or a display message. Default value: Enabled
Discreet call	When this flag is activated, the subscriber can discreetly join an existing voice call of another internal subscriber. He or she can silently monitor the call and speak with the internal subscriber without the other party hearing this conversation. This is only possible in the case of a two-party call. Discreet calling is not possible with consultation calls or conferences. Default value: Disabled
Discreet Call Lock	When this flag is activated, the station cannot be called discreetly. Default value: Disabled
DTMF-based feature activation	Only relevant for Mobility Entry stations: This flag must be set in order to be able to activate features during a call (i.e., in the talk state). The code receiver remains active. (Attention: limited resources) Default value: Disabled

Parameters	Description
Headset	When this flag is activated, the station can be equipped with a headset that plugs into the handset connection. Setting the flag enables the user to accept a call by pressing a headset button on the system telephone without lifting the handset. When a headset is connected to the system telephone connection, it is recognized automatically by the communication system; an authorization enable is not necessary in this case. When this flag is set, calls cannot be released by pressing the speaker key; a disconnect key must be programmed so that calls can be released. Default value: Disabled
Last destination mailbox active	If this flag is activated and the called party is not available, the call is forwarded to the substitute mailbox, and the caller's number is displayed on the substitute telephone. Default value: Disabled
Call prio./immed. tone call wait.	When this flag is activated (Call priority/immediate tone call waiting), calls through this station are signaled with a higher priority to partners. The priority is set to be the same as the priority of external calls. In other words, the prioritized calls are thus queued before existing internal calls, but after existing external calls. Note that existing first calls (not waiting calls) are usually never displaced, regardless of their ring type. If the same priority is also to be set for an internal call in another node, then the station flag "Call prio./immed. tone call wait." (Area: Circuit flags, Call prio./immed. tone call wait.) must be likewise set for the corresponding trunk. If this flag is set, the caller receives a ring tone immediately instead of a busy tone. This has no impact on the acoustic signaling. The prioritized calls are still signaled like an internal call. This feature is important for phonemail connections. Default value: Disabled
Voice recording	If the flag is activated, the subscriber can activate voice recording during a call. In addition, the "Warning tone during voice recording" switch under Flags can be used to specify whether or not a warning tone should be output on starting the voice recording. Furthermore, a suitable Live Recording device must be configured under PhoneMail. If the IVM is to be used for voice recording, then the maximum length of the voice recording can be set via "IVM | Additional Settings/General", and the appropriate signaling method to be used before starting a voice recording (if any) can be defined. Default value: Disabled
Compress display data	When this flag is enabled, the display outputs are compressed for improved performance. If the display on a UP0/E terminal changes, the communication system only updates the data that differs from the previous display. If an application (e.g., Smartset/TAPI) is connected via an RS 232 adapter (data or control adapter), this feature must be deactivated. The flag must be deactivated for applications that obtain the call number information from the telephone's display, (i.e., uncompressed output with call number instead of compressed output with name). Names are generally displayed only when the flag "Calling ID only" under "Display name/call number" is deactivated. Default value: Enabled
Door release DTMF	If this flag is enabled, the station can open a door with the DTMF/MFV code signaling when a door relay is connected to the relevant port. Default value: Disabled

Parameters	Description
Autom. connection, CSTA (only for OpenStage SIP telephones)	When the flag is enabled, the following applies: speakerphone mode is activated on the associated SIP telephone when dialing or answering calls via myPortal or myAttendant. The information contained in the documentation of the SIP telephone must be observed, since additional settings on the SIP phone may be required for the proper use of the feature. When the flag disabled, the call setup occurs only after lifting the handset. Default value: Enabled
Call Monitoring (for specific countries only)	When this flag is activated, the subscriber can silently monitor (i.e., listen in on) the conversation of any internal subscriber. The microphone of the party listening in is automatically muted. The monitored subscriber is not notified via a signal tone or display message. When you start and end call monitoring, you may encounter a lapse of up to two seconds of the conversation. Default value: Disabled
Disable handsfree microphone	If this flag is activated, the handsfree microphone cannot be used. This flag is only supported by OpenStage phones. Default value: Disabled
Forced Number Presentation	If this flag is activated, the caller's phone number appears on the display of the called party instead of his or her name. Default value: Disabled
Usage (for specific countries only)	This drop-down list can be used to configure the output current of the interfaces of an analog board (in mA, e.g., 27 mA for China).
Operating Mode	In this drop-down list, an operating mode can be selected for the subscriber line.
Payload Security (only for TDM system telephones)	If this flag and the **SPE Support** system flag are activated, the Signaling & Payload Encryption (SPE) feature is supported for the selected subscriber(s). The signaling and payload data for this/these subscriber/s is encrypted. An option can be set to indicate in the display whether or not a part of a connection path to an IP station is encrypted (off = no information is displayed). The payload security setting does not work for any other telephones. Default value: Disabled
Missed Calls List	When this flag is activated, the missed calls list is activated for the subscriber at his or her telephone (only for phones with a display). Calls that were not answered by the subscriber are provided with a time stamp (time and date) and added to a chronologically sorted list. Only the calls which also contain a phone number or name are recorded. If a subscriber calls more than once, only the time stamp for the entry is updated, and a call counter for that caller is incremented.
Central busy signaling	This flag must be set (see also QSIG features) for subscribers who have busy signaling on a centralized communication system. Does not apply to the USA. The implementation of central busy signaling is contingent on a maximum number of 100 stations per node.
Display of Emergency text	If this flag is activated, a configurable Emergency text is shown on the phone's display in emergency mode.
Priority for outbound calls	
Call Supervision	

Parameters	Description
Buttons	
>	Moves to the next station. If the stations matching the search term entered in the **Search** fields were previously filtered, it is possible to move between only those specific stations.
<	Skips back one station.

Parameter Description of Tabs:

- **Edit workpoint client data**

Parameters	Description
Stations - ...	
Type	Type of the station.
Call number	Internal call number of the station.
Name	Station name.
Parameters	
Status message	For system clients only: this flag activates the "keep-alive" mechanism for system telephones. If a system phone fails, for example, it is flagged as inactive after four minutes. The flag must not be enabled when setting up a system telephone as a home client or when using the "Short-Hold" feature. Disabling this flag reduces the message traffic between the communication system and the system telephones.
Authentication active	If you want the IP client to be able to identify himself/herself at the communication system with a password, authentication must be activated and a password set. This is an advantage especially for clients that are not connected to the internal LAN, but that dial in from outside.
New password	Password for authentication.
Confirm password	Password to repeat the authentication.
SIP User ID / Username	Only for SIP clients: freely selectable user name for authentication of the SIP subscriber, e.g., "SIP-120". The value defined here must also be entered at the SIP telephone.
Realm	Only for SIP clients: freely selectable names for the associated zone, e.g., "OSBIZ-SIP". This value must be the same for all SIP clients. The value defined here must also be entered at the SIP telephone.
Fixed IP address	For SIP clients only: entering a fixed IP address ensures that only one SIP client can log on to the system with this IP address. If this flag is activated, the IP address and the call number are verified. If this flag is not activated, only the call number is verified.
IP Address	Only for SIP clients: IP address of the SIP client (e.g., the IP address of the SIP telephone)
Type	Only for system clients: A mobile IP client (Mobile option) is not permanently assigned to any IP phone. The call no. of a mobile IP client can be used by a subscriber to log on to any IP terminal (that permits this) via the logon procedure (*9419) (provided the option Mobile blocked is not activated).
Type: **Mobile**	Only for system clients: No IP device is permanently assigned to the subscriber. The feature is only supported from the third station port onwards.
Type: **Non-mobile**	Only for system clients: The call number is permanently assigned to the IP device of the subscriber. When using a WLx phone, the option Non mobile must be set before registering the WLx phone with the communication system.

Parameters	Description
Type: **Non-mobile and blocked**	Only for system clients: A subscriber cannot log into this IP device with a mobile system client.
Blocked for Deskshare User	Only for system clients: This system phone can be shared by multiple subscribers (Desksharing).
Secondary system ID	This parameter has two different functions: 1. For all stations: defines the multi-location gateway assigned to the station. 2. Only for system clients: If the "Emergency" flag has been set (under the "Stations/ IP Clients/Secondary Gateway") for networked systems, the node ID of the failover system for system clients can be entered here.
Internet registration with internal SBC	Enables the SIP@Home feature. This makes it possible for an external STUN-enabled SIP phone to register at OpenScape Business over the Internet and thus be used as an internal telephone.
Buttons	
>	Moves to the next station. If the stations matching the search term entered in the **Search** fields were previously filtered, it is possible to move between only those specific stations.
<	Skips back one station.

Parameter Description of Tabs:

- **Edit Group/CFW**

Parameters	Description
Stations - ...	
Type	Type of the station.
Call number	Internal call number of the station.
Name	Station name.
Call forwarding	
Day destination	Displays the call forwarding destinations for incoming external calls during the day (see the wizard User Telephony/Call Forwarding)
Night destination	Displays the call forwarding destinations for incoming external calls during the night (see the wizard User Telephony/Call Forwarding).
Internal destination	Displays the call forwarding destinations for incoming internal calls (see the wizard User Telephony/Call Forwarding).
Class of Service	
Day	Every subscriber can be assigned a class of service for day. There are 15 classes of service to choose from (see Telephony/Classes of Service).
Night	Every subscriber can be assigned one class of service for night. There are 15 classes of service to choose from (see Telephony/Classes of Service).
Call Pickup	
Group	Every station can be assigned to a call pickup group. You can choose between 32 call pickup groups (120 with OSBiz S; see also Incoming Calls / Call Pickup).

Parameters	Description
Buttons	
>	Moves to the next station. If the stations matching the search term entered in the **Search** fields were previously filtered, it is possible to move between only those specific stations.
<	Skips back one station.

33.14 Chapter 27.3.7.11 Station > Station > UC Applications

The functions of the UC solutions UC Smart and UC Suite are shown here. It is recommended that the basic settings be configured under "Setup > Basic Installation> Basic Installation> Change preconfigured call and functional numbers".

Depending on the UC solution being used, different functions are displayed.

Parameter Description of Tabs:

- **Change Station**

Parameters	Description
Call no	Call number of the service
DuWa	DID number of the service
First Name	Freely selectable first name for the service. Value range: max. 16 characters, no umlauts or special characters
Last Name	Freely selectable last name for the service. Value range: max. 16 characters, no umlauts or special characters
Display	Freely selectable name for the service. By default, it is created using the First Name and Last Name parameters depending on display name algorithm. Value range: max. 16 characters, no umlauts or special characters
Type	Depending on the UC solution: UC Smart: MeetMe / Conference UC Suite: Auto-Attendant / Fax / Contact Center Fax / Park / MeetMe / Conference / Fax Group
Clip/Lin	Sequence of digits to be displayed at the called party instead of the actual number for outgoing external calls (e.g., for E911 emergency services in the USA)
Active	Indicates whether the service is operational.
Search	You can also have selected services displayed by entering a search term in the **Search** fields and pressing the Return key. The services that match the search term are displayed. If you leave all the **Search** fields empty and press the Return key, all services will be listed again.
Items per page	Selection to determine whether 10, 25, 50 or 100 items are to be displayed per page.
Buttons	

Parameters	Description
Blue arrow in the **Call no** column	Brings up the page with the **Edit station parameters**, **Edit station flags**, **Edit workpoint client data** and **Edit Group/CFW** tabs.
>	Moves one page forward.
<	Moves one page back.
>|	Moves to the end of the list.
|<	Moves to the beginning of the list.

33.15 Chapter 27.3.7.14 Station > Stations > Mobility Entry

It is recommended to set up mobile users via the "User Telephony > Mobile Phone Integration" wizard.

Parameter Description of Tabs::

- **Change Station**

Parameters	Description
Call no	Input of the internal extension number of the Mobility user (e.g., 777). This internal call number must not have already been assigned.
DuWa	Input of the internal DID number of the Mobility user. This internal DID number must not have already been assigned.
First Name	Freely selectable first name for the Mobility user. Value range: max. 16 characters, no umlauts or special characters
Last Name	Freely selectable last name for the Mobility user. Value range: max. 16 characters, no umlauts or special characters
Display	Freely selectable name for the Mobility user. By default, it is created using the First Name and Last Name parameters depending on display name algorithm. Value range: max. 16 characters, no umlauts or special characters
Type	Displays the type of Mobility user.
Mobile Callno	Input of the mobile phone number. The entry must include the leading dialout prefix (i.e., the CO code), e.g., 0016012345678.
Web Feature ID	The Web Feature ID defines how the subscriber should log in at the mobile web client (user name). Choice between "no" (Mobility Entry only) and "automatic" (internal call number of the subscriber) or selection of the station number of the client or phone from the drop-down list.
Search	You can also have selected subscribers displayed by entering a search term in the **Search** fields and pressing the Return key. The subscribers who match the search term are displayed. If you leave all the **Search** fields empty and press the Enter key, all subscribers will be listed again.
Items per page	Selection to determine whether 10, 25, 50 or 100 items are to be displayed per page.
Buttons	

Parameters	Description
Blue arrow in the **Call no** column	Brings up the page with the **Edit station parameters**, **Edit station flags**, **Edit workpoint client data** and **Edit Group/CFW** tabs.
>	Moves one page forward.
<	Moves one page back.
>|	Moves to the end of the list.
|<	Moves to the beginning of the list.

Parameter Description of Tabs:

- **Secondary Gateway**
  Only for networked systems (multi-location)

Parameters	Description
Call number	Internal call number of the Mobility User.
Name	Name of the Mobility User.
Node ID	Input of the node ID via which the mobile subscriber is externally accessible.

33.16 Chapter 27.3.7.15 Station > Stations > Overview of Stations

Lists all stations of the communication system sorted by call number (default). Clicking on a different column heading sorts the list by the selected column in ascending order; a second click sorts it in descending order.

Parameter Description of Tabs:

- **Change Station**

Parameters	Description
Call no	Internal call number of the station.
DuWa	DID number of the station.
First Name	Freely selectable first name for the station. Value range: max. 16 characters, no umlauts or special characters
Last Name	Freely selectable last name for the station. Value range: max. 16 characters, no umlauts or special characters
Display	Freely selectable name for the station. By default, it is created using the First Name and Last Name parameters depending on display name algorithm. Value range: max. 16 characters, no umlauts or special characters
Device type	Displays the type of station.
Active	Indicates whether the station is operational.
Access	Displays the physical interface at which the device is connected.

Parameters	Description
Search	You can also have selected subscribers displayed by entering a search term in the **Search** fields and pressing the Return key. The subscribers who match the search term are displayed. If you leave all the **Search** fields empty and press the Enter key, all subscribers will be listed again.
Items per page	Selection to determine whether 10, 25, 50 or 100 items are to be displayed per page.
Buttons	
Blue arrow in the **Call no** column	Brings up the page with the **Edit station parameters**, **Edit station flags**, **Edit workpoint client data** and **Edit Group/CFW** tabs.
>	Moves one page forward.
<	Moves one page back.
>|	Moves to the end of the list.
|<	Moves to the beginning of the list.

33.17 Chapter 27.3.9.1 Incoming Calls > Groups/Hunt groups

For the initial configuration of group calls and hunt groups, it is recommended that the **Group Call / Hunt Group** wizard be used.

Parameter Description of Tabs::

- **Edit Group Call Numbers**
- **Display Used Groups**
- **Display all group members**
- **Add group**
- **Delete group**
- **Edit group parameters**
- **Display members**
- **Add member**
- **Edit member order**
- **Check Basic MULAPs**
- **Check MULAP Preference**

Parameters	Description
Index	Consecutive number that is assigned by the communication system.
Call no. **Phone number**	Phone number of the group call, hunt group, basic MULAP, executive MULAP or voicemail group
DuWa **MSN**	DID number of the group call, hunt group, basic MULAP, executive MULAP or voicemail group
First Name	Freely selectable first name for the group call, hunt group, basic MULAP, executive MULAP or voicemail group. Value range: max. 16 characters, no umlauts or special characters

Parameters	Description
Last Name	Freely selectable last name for the group call, hunt group, basic MULAP, executive MULAP or voicemail group. Value range: max. 16 characters, no umlauts or special characters
Name	Name of the group call, hunt group, basic MULAP, executive MULAP or voicemail group By default, it is created using the First Name and Last Name parameters depending on display name algorithm.
Type	Definition of the group type Default value: Group
Type: Linear hunt group	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.
Type: Cyclical hunt group	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.
Type: Group	Group call of type 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.
Type: RNA	Group call of type 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.
Type: Basic MULAP	Incoming calls are indicated visually at all phones associated with the basic MULAP (Multiple Line Appearance). 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.
Type: Executive MULAP	You can configure Executive MULAPs if you want to use restricted executive and secretary functions. 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.
Type: Call waiting	Group call of type 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.
Type: Answering machine	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.
Ring type	Defines the acoustic signaling of incoming external calls to the group Default value: 1 Only the default setting is possible for analog phones. Changes have no effect.

Parameters	Description
Ring type: 1	Two rings
Ring type: 2	Three rings
Ring type 3	short-long-short ring
Tel. directory	When this flag is activated (Display Yes), the call number of the group appears in the internal directory. Default value: Enabled
Group member	
Group	Number (index) of the group
Member	Number (index) of the member within the group
Phone number	Call number of the group member
Name	Name of the group member
Parameters	Enabled parameters of the group member
Parameter: M	Master (M): Basic MULAP: The member is master of the basic MULAP. Executive MULAP: The member has Executive functions.
Parameter: R	Acoustic call (R): Basic MULAP and Executive MULAP: Incoming calls are signaled acoustically.
Parameter: A	Automatic seizure outgoing (A): Basic MULAP: The Basic MULAP trunk is automatically selected for a call when you lift the handset. Executive MULAP: The Executive MULAP trunk is automatically selected for a call when you lift the handset.
Parameter: K	No automatic incoming call acceptance (K): Basic MULAP and Executive MULAP: An incoming call must be accepted by pressing the MULAP key.
Parameter: P	Automatic privacy release (P): Basic MULAP and Executive MULAP: You can release the seized MULAP line for a conference by pressing the MULAP key.
MULAP key set up	Indicates whether or not a MULAP key has been configured the group member.
Route	For an external member of the group, the route is displayed.
Group	
Consistency Check	Possible collisions due to the overlapping of masters of basic MULAPs or in the automatic outgoing seizure of basic MULAPs are displayed.

33.18 Chapter 27.3.9.2 Incoming Calls > Group Members

Parameter Description of Tabs::

- **Edit member**

- **Delete member**

Parameters	Description
Group	Number (index) of the group
Group member	Number (index) of the group member
Phone number	Call number of the group member
First Name	Freely selectable first name for the group member. Value range: max. 16 characters, no umlauts or special characters
Last Name	Freely selectable last name for the group member. Value range: max. 16 characters, no umlauts or special characters
Name	Name of the group member By default, it is created using the First Name and Last Name parameters depending on display name algorithm.
MULAP name	MULAP (Multiple Line Appearance) group
MULAP call no.	MULAP group number
Master (M)	Basic MULAP: Activating this flag 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. Executive MULAP: Activating this flag assigns 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.
Acoustic call (R)	Basic MULAP and Executive MULAP: When this flag is activated, incoming calls are signaled acoustically. Default value: Enabled for all masters of a Basic MULAP. Activated for all members with the Secretary function of an Executive MULAP.
Automatic seizure outgoing (A)	Basic MULAP: When this flag is activated, the Basic MULAP trunk is automatically called when the subscriber lifts the handset. Executive MULAP: When this flag is activated, the Executive MULAP trunk is automatically called when you lift the handset. Default value: Enabled for all masters of a Basic MULAP. Activated for all members with the Secretary function of an Executive MULAP.
No automatic incoming call acceptance (K)	Basic MULAP and Executive MULAP: When this flag is activated, you cannot answer an incoming call by lifting the handset. Answering an incoming call is possible only by pressing the MULAP key. Default value: Disabled
Automatic privacy release (P)	Basic MULAP and Executive MULAP: When this flag is activated, 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 value: Disabled

Parameters	Description
MULAP key set up	Basic MULAP: When this flag is activated, 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. Executive MULAP: When this flag is activated, 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 value: Enabled
Route	For an external member of the group, the route is displayed.
Type	Definition of the group type

33.19 Chapter 27.3.9.3 Incoming Calls > Team/top

For the initial configuration of Team and Top groups, it is recommended that the **Team Configuration** and **Executive / Secretary** wizards be used.

Parameter Description of Tabs::

- **Display All Team/top**
- **Display Used Team/top**
- **Add Team/top Group**
- **Edit Team/top Group**
- **Delete Team/top Group**
- **Edit Team/top Group**
- **Display Team/top Members**
- **Add Team/top Member**
- **Edit Team/top Member**
- **Delete Team/top Member**
- **Display Fax Boxes**
- **Add Fax Box**

Parameters	Description
Index	Consecutive number that is assigned by the communication system.
First Name	Freely selectable first name for the Team/Top group. Value range: max. 16 characters, no umlauts or special characters
Last Name	Freely selectable last name for the Team/Top group. Value range: max. 16 characters, no umlauts or special characters
Name	Name of th Team/Top group By default, it is created using the First Name and Last Name parameters depending on display name algorithm.
Type	Definition of the group type

Parameters	Description
Type: Team	A 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.
Type: Top	A Top Group offers convenient Executive and Secretary functions (Top function) for up to three executives and up to three secretaries.
Key assignment to team	Definition for the setup of MULAP keys of Team Group members
Key assignment to team: to first/second console	When this flag is activated, an automatic setup of MULAP keys occurs on the first or second add-on device (key module or BLF) of the Team telephone.
Key assignment to team: to first free key	When this flag is activated, an automatic setup of MULAP keys occurs on the first free key of the Team telephone.
Key assignment to top	Definition for the setup of MULAP keys of Top Group members
Key assignment to top: to first/ second console	When this flag is activated, an automatic setup of MULAP keys occurs on the first or second add-on device (key module or BLF) of the Top telephone.
Key assignment to top: to first free key	When this flag is activated, an automatic setup of MULAP keys occurs on the first free key of the Top telephone.
Group member	
Group	Number (index) of the group
Members	Number (index) of the member within the group
Type	Definition of the member type
Call no.	Call number of the group member (changes in a MULAP group to ** Call no and is internally accessible under this ** Call no.)
Name	Name of the group member
MULAP call no.	MULAP group number
MULAP DID	DID number of the MULAP group
MULAP name	MULAP group name
Ring type	Defines the acoustic signaling of incoming external calls to the group Default value: 1 Only the default setting is possible for analog phones. Changes have no effect.
Ring type: 1	Two rings
Ring type: 2	Three rings
Ring type 3	short-long-short ring
Tel. directory	When this flag is activated (Display Yes), the call number of the group appears in the internal directory. Default value: Enabled

Parameters	Description
Master (M)	Team group: Activating this parameter turns a member of the Team group into a master of the group. If a master activates call forwarding, this feature applies to all members (phones) in the Team group. Top group: Enabling this flag 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.
Acoustic call (R)	Team group and Top group: When this flag is activated, incoming calls are signaled acoustically. Default value: Enabled for all members of a Team group. Activated for all members with the Secretary function of a Top group.
Automatic seizure outgoing (A)	Team group and Top group: When this flag is activated, a call is automatically made via the MULAP trunk of this member on lifting the handset. Default value: Enabled
No automatic incoming call acceptance (K)	Team group and Top group: When this flag is activated, you cannot answer an incoming call by lifting the handset. Answering an incoming call is possible only by pressing the MULAP key. Default value: Disabled
Automatic privacy release (P)	Team group and Top group: When this flag is activated, 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 value: Disabled
MULAP key set up	Team group: When this flag is activated, 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. Top group: When this flag is activated, 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 value: Disabled for all members of a Team group. Enabled for all members of a Top group.
MULAP type	Definition of the MULAP type
MULAP Type: Basic MULAP	Incoming calls are indicated visually at all phones associated with 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.
MULAP type: Executive MULAP	All members of an Executive MULAP can be reached at the Executive MULAP phone number as well as at their personal station numbers.
Fax Call no.	Call number of the group member's fax box
Fax DID	Direct inward dialing number of the group member's fax box

34 V2R1.0: Version dependent TDM license migration from H3k Vx to OSBiz V2

Affected Documentation	Administrator Documentation
Issue	9
Reference No.	A31003-P3020-M100-09-76A9

34.1 25 Migration

HiPath 3000 V5 and above systems and OpenScape Business V1 systems can be migrated to OpenScape Business V2 systems.

34.2 25.1 Migrating from HiPath 3000 V5 and above to OpenScape Business V2

This section describes the technical migration of HiPath 3000 standalone systems and HiPath 3000 internetworks to OpenScape Business V2.

The following communication systems and internetworks can be migrated:

- HiPath 3000 V5 and above standalone system
- HiPath 3000 V5 and above standalone system with OpenScape Office V3 HX
- HiPath 3000 V5 and above Internetwork
- HiPath 3000 V5 and above internetwork with HiPath 5000 RSM

~~It is also possible to migrate from HiPath 3000 V7 and HiPath 3000 V8 to OpenScape Business V2. In such cases, an upgrade to HiPath 3000 V9 must be performed before migrating to OpenScape Business V2.~~

INFO: Before migrating to OpenScape Business V2, the HiPath 3000 V5 and above system, including all the connected devices, needs to first made fully operational once.

If an OpenScape Office V3 HX is additionally connected to the HiPath 3000 communication system, this can be upgraded to an external UC Booster Server.

The upgrading of a HiPath 3000 V5 and above communication system occurs by replacing the mainboard, converting the CDB and subsequently migrating the license.

> ***INFO:*** All of the steps listed below to install the new hardware are described in detail in the Hardware Installation chapter of the Service Documentation.

The following points must be observed prior to migration:

- **Hardware compatibility check**
  Please verify whether the existing hardware can still be used. Discontinued components or devices which are no longer supported must be removed and replaced by their respective successors if required. A list can be found here *Non-Supported Boards and Devices*
- **Determining the power requirements**
  Since an OpenScape Business mainboard requires more power than a HiPath 3000 mainboard, the power requirements must be determined for the following scenarios (see the Appendix "Power Requirements of a Communication System" in the Service Documentation), and the OpenScape Business Powerbox should be used if required:
  - For HiPath 3000 systems without HG1500
  - when using the UC Booster Card (OCAB)

  When migrating a HiPath 33xx/35xx to OpenScape Business X3/X5, the original power supply unit (PSU) which may still be in use must be replaced by a newer UPSC-D/-DR power supply.
- **Slot verification with X8**
  To ensure optimal ventilation of the base box, the following slot restrictions apply to a few boards:
  - **Analog subscriber line modules**
    Analog subscriber line modules must not be inserted in slot 7 directly to the right of the OCCL mainboard. Similarly, if possible, no analog subscriber line modules should be inserted in slot 5 immediately to the left of the OCCL mainboard.
  - **LUNA2 power supply unit**
    If possible, there should be at least one free slot between two LUNA2 boards.
- **Function compatibility check**
  Please inform yourself about which features are longer supported or have changed as compared to HiPath 3000 V5 and above. A list can be found here: *Changed Features and Interfaces*.
- **License migration**
  Please note the information on the license migration so that all existing features can be correctly identified and applied to the new system (see *License Migration*).
- **Protective Grounding**
  Protective grounding via an additional ground wire is mandatory for all OpenScape Business communication systems!

- **EVM module**
  The EVM module is no longer needed. The functionality is integrated on the new mainboard in the form of UC Smart (voicemails, announcements, AutoAttendant). The voice messages and announcements of the EVM module cannot be migrated.
- **HG1500**
  The HG1500 board is no longer required. The functionality is integrated on the new mainboard.
  - **DSP channels**
    Please determine the number of DSP channels required. DSP channels are required to implement network transitions from TDM telephony to VoIP. With HiPath 3000, the DSP channels were provided by the HG1500 and its PDM modules. OpenScape Business has eight integrated DSP channels on the mainboard. For additional DSP channels, the DSP module OCCB1 (up to 40 channels) or OCCB40 (up to 100 channels) can be used.
    For more detailed information on DSP and T.38 resources, refer to chapter *System-Specific Capacity Limits*.
  - **S_0 ports**
    All S_0 ports configured on mounted HG 1500 boards are automatically registered again on slot 0 of the communication system after the CDB conversion.
- **Dial plan in the internetwork**
  In a pure voice network, open and closed numbering are possible. When using the UC Suite, closed numbering is required in the internetwork (network-wide UC functionality). When using UC Smart, open and closed numbering are possible (node-wide UC functionality).
- **Multi-SLC**
  If multiple SLCN boards are inserted in the HiPath 3800, these are synchronized via SLC networking lines (multi-SLC). For each SLC networking line, an internal S_0 station is set up. After the migration, it should be verified that the station flag **Call waiting rejection on** is disabled for this S_0 station. Otherwise, problems may occur when a DECT phone attempts roaming to a base station that is connected to another SLCN board.

34.3 License Migration

The license migration is required to upgrade from HiPath 3000 V5 and above to OpenScape Business V2. Any OpenScape Office V3 HX systems connected to HiPath 3000 can also be migrated.

Prerequisites for License Migration

The following preconditions must be satisfied for a successful license migration:

- The latest version of the Manager E should always be used.
- An upgrade license to upgrade from HiPath 3000 V5 and above to OpenScape Business V2 was ordered. This license can also be used to upgrade an OpenScape Office V3 HX, if present.

- ~~In order to migrate from HiPath 3000 V7 or HiPath 3000 V8 to OpenScape Business V2, it is necessary to first upgrade to a running HiPath 3000 V9 system with all terminal devices connected to ensure that all TDM stations are transferred correctly.~~
- The LAC for the upgrade license, which is required to retrieve the new license from the license server, is available.

Upgrade License for HiPath 3000 / OpenScape Office V3 HX

Using the upgrade license, the following licenses can be transferred from the existing HiPath 3000 license file to OpenScape Business:

- IP stations (ComScendo)
- S_{2M}/T1 channels
- Mobility Entry (for the DISA-based mobility function)
- Xpressions Compact Announcements, Conferencing, Mobility

The following applies to the OpenScape Office V3 HX connections:

- Per OpenScape Office Standard User: 1x myPortal for Desktop, 1x Voicemail; 1x Fax applies to Standard User licenses in the HX base licenses 5/10 and individual licenses
- Per system: 1 x Company AutoAttendant
- For the following other OpenScape Office HX licenses, the corresponding number of OpenScape Business licenses are generated: myPortal for Outlook, myAttendant, Application Launcher, Gate View cameras, OpenDirectory Connector, myAgent, Contact Center Fax, Contact Center Email, myReports.
  Station licenses and user-oriented licenses are permanently assigned to subscribers. A sufficient number of licenses must be available for myAgent and myAttendant users.
- In the case of an OpenScape Office HX Voicemail license (voicemail functionality for all users), 500x OpenScape Business Voicemail licenses are generated.

License Migration of TDM Stations (only for HiPath 3000)

In OpenScape Business, subscriber licenses of type "TDM User' are required for all TDM stations (UP0, a/b, S0, DECT). No new licenses need to be purchased for existing TDM stations.

During the CDB conversion, the number of active TDM stations in the HiPath 3000 system is determined automatically. The required TDM User licenses are automatically transferred to the newly generated license file during the license migration at the CLS.

Calculation for TDM licences:

- Upgrade from H3k V7 or older to OSBiz V2:
  70% of TDM users are calculated for cheaper / free of charge OSBiz upgrade licenses
- Upgrade from H3k V8 to OSBiz V2:
  80% of TDM users are calculated for cheaper / free of charge OSBiz upgrade licenses

- Upgrade from H3k V9 to OSBiz V2:
  100% of TDM users are calculated for cheaper / free of charge OSBiz upgrade licenses

The number of TDM user licenses is determined as follows:

- 1x TDM User license per active UP0 port - Phone ready, call number available
- 1x TDM User license per registered DECT phone - Call number available
- 1x TDM User license per configured a/b port (call number) for inserted boards
- 1x TDM User license per configured S0 port (call number) for active boards

CDB conversion can be performed only once. The steps for the technical migration must hence be followed precisely. It is not possible to subsequently alter the data determined.

License activation is performed offline at the CLS via a license file. The license activation procedure is described here: *Activating Licenses (Standalone)*.

Products and Features without License Migration

No license migration is performed for the following HiPath 3000 V5 and above and OpenScape Office V3 LX products and features:

- OpenStage Gate View on the Plug PC: OpenStage Gate View can continue to be operated with OpenScape Business.
- HG1500 B-channels: The board is dropped, since the functionality is integrated on the new mainboard.
- optiClient Attendant V8: does not run on OpenScape Business.
  Follow-up product: OpenScape Business Attendant
- optiClient BLF V1/V2: does not run on OpenScape Business.
  Follow-up product: OpenScape Business BLF
- HiPath TAPI 120/170 V2: does not run on OpenScape Business.
  Follow-up product: OpenScape Business TAPI 120/170
- Entry VoiceMail: The module is dropped, since it is integrated on the new mainboard
- myPortal entry web services communications clients on the plug PC.
- Base stations: licenses for base stations are no longer required.
- ITSP trunk access: licenses must be purchased to use ITSP channels for Internet telephony in OpenScape Business.
- As in the past, no licenses are required for S_0, Analog and CAS trunks.
- For networking and the connection of external systems via tie lines, one network license per node must be purchased in OpenScape Business.

Additional Notes

Please note the following additional information:

- In OpenScape Business systems, all user-oriented licenses are permanently assigned to call numbers via the Administration (WBM) and are thus bound to these numbers. This requires the appropriate licenses.
- The Deskshare User (IP Mobility) feature requires a license in OpenScape Business as opposed to HiPath 3000. Additional licenses of the type "Deskshare User" must be purchased.

Licensing Procedure for Migration of an Internetwork

An existing HiPath 3000/5000 internetwork with a shared network license file must be split into standalone systems with individual license files at the CLS. After this, each node is upgraded and licensed as a standalone system. If necessary, the OpenScape Business systems can then be recombined into an internetwork with a single network license file at the CLS.

OpenScape Office V3 LX with HiPath 3000 gateways are upgraded and licensed as stand-alone systems. If necessary, the OpenScape Business systems can then be recombined into an internetwork with a single network license file at the CLS.

Subscription (Linux Software for OpenScape Business Server)

For migrations from OpenScape Office V3 HX, an SLES subscription can be set up with OpenScape Business S. The required Novell registration key is provided as a LAC on purchasing the DVD with the OpenScape Business communication software.

> ***INFO:*** The registration key used for the OpenScape Office V3 HX (hosting via the Central Update Server) is no longer required.

34.4 How to Convert the HiPath 3000 V5 and above CDB

Prerequisites

- HiPath 3000 communication system (HiPath 3300, HiPath 3350, HiPath 3500, HiPath 3550 and HiPath 3800), Version 5 and above, is available.
- The admin PC is connected to the HiPath 3000 communication system.

Step by Step

1. Click on **File > Convert customer database** in the menu bar.
2. Select the CDB previously stored on the admin PC and click **OK**.
3. Enter your **Name** and your **Contract number** as your customer data and click **Next**.
4. Select **OpenScape Business V2** as the **Version** and click **Next**.
5. Click **OK** to confirm the unsupported boards advisory messages.
6. Click **Yes** to confirm the window which informs you about the number of TDM users to perform the migration and proceed with the migration. The number of TDM user which will be migrated is calculated automatically.
7. Click **Next** to confirm the window which informs you about which boards are plugged.
8. Click in the menu bar on **File > Save customer database as** and save the CDB under a different name on the admin PC in a folder of your choice.
9. Close Manager E.

Next steps How to Replace the Hardware for HiPath 3300/3500 or

How to Replace the Hardware for HiPath 3350/3550 or

How to Replace the Hardware for HiPath 3800

35 MR_I51416: No speech in OSBiz network cordless w/o CMA module

Affected Documentation	Issue	Reference No.
Administration Documentation	9	A31003-P3020-M100-09-76A9
OpenScape Business X3/X5/X8 Service Documentation	5	A31003-P3020-S100-05-7620

35.1 Administration Documenation Chapter 18.3.2.2 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 $U_{P0/E}$, a CMA module is needed on the control board in case of an osbiz network with cmi roaming over the nodes.

35.2 Administration Documenation Chapter 25.1 Migrating from HiPath 3000 V9 to OpenScape Business V2

This section describes the technical migration of HiPath 3000 V9 standalone systems and HiPath 3000 V9 internetworks to OpenScape Business V2.

The following communication systems and internetworks can be migrated:

- HiPath 3000 V9 standalone system
- HiPath 3000 V9 standalone system with OpenScape Office V3 HX
- HiPath 3000 V9 Internetwork
- HiPath 3000 V9 internetwork with HiPath 5000 RSM

It is also possible to migrate from HiPath 3000 V7 and HiPath 3000 V8 to OpenScape Business V2. In such cases, an upgrade to HiPath 3000 V9 must be performed before migrating to OpenScape Business V2.

INFO: Before migrating to OpenScape Business V2, the HiPath 3000 V9 system, including all the connected devices, needs to first made fully operational once.

If an OpenScape Office V3 HX is additionally connected to the HiPath 3000 V9 communication system, this can be upgraded to an external UC Booster Server.

The upgrading of a HiPath 3000 V9 communication system occurs by replacing the mainboard, converting the CDB and subsequently migrating the license.

INFO: All of the steps listed below to install the new hardware are described in detail in the Hardware Installation chapter of the Service Documentation.

The following points must be observed prior to migration:

- **Hardware compatibility check**
  Please verify whether the existing hardware can still be used. Discontinued components or devices which are no longer supported must be removed and replaced by their respective successors if required. A list can be found here *Administrator Documentation, Migration.*
- **Determining the power requirements**
  Since an OpenScape Business mainboard requires more power than a HiPath 3000 mainboard, the power requirements must be determined for the following scenarios (see the Appendix "Power Requirements of a Communication System" in the Service Documentation), and the OpenScape Business Powerbox should be used if required:
  - For HiPath 3000 systems without HG1500
  - when using the UC Booster Card (OCAB)

  When migrating a HiPath 33xx/35xx to OpenScape Business X3/X5, the original power supply unit (PSU) which may still be in use must be replaced by a newer UPSC-D/-DR power supply.
- **Slot verification with X8**
  To ensure optimal ventilation of the base box, the following slot restrictions apply to a few boards:
  - **Analog subscriber line modules**
    Analog subscriber line modules must not be inserted in slot 7 directly to the right of the OCCL mainboard. Similarly, if possible, no analog subscriber line modules should be inserted in slot 5 immediately to the left of the OCCL mainboard.
  - **LUNA2 power supply unit**
    If possible, there should be at least one free slot between two LUNA2 boards.

- **Function compatibility check**
  Please inform yourself about which features are longer supported or have changed as compared to HiPath 3000 V9. A list can be found here: *Administrator Documentation, Migration*.
- **License migration**
  Please note the information on the license migration so that all existing features can be correctly identified and applied to the new system (see *Administrator Documentation, Migration*).
- **Protective Grounding**
  Protective grounding via an additional ground wire is mandatory for all OpenScape Business communication systems!
- **EVM module**
  The EVM module is no longer needed. The functionality is integrated on the new mainboard in the form of UC Smart (voicemails, announcements, AutoAttendant). The voice messages and announcements of the EVM module cannot be migrated.
- **HG1500**
  The HG1500 board is no longer required. The functionality is integrated on the new mainboard.
  - **DSP channels**
    Please determine the number of DSP channels required. DSP channels are required to implement network transitions from TDM telephony to VoIP. With HiPath 3000, the DSP channels were provided by the HG1500 and its PDM modules. OpenScape Business has eight integrated DSP channels on the mainboard. For additional DSP channels, the DSP module OCCB1 (up to 40 channels) or OCCB40 (up to 100 channels) can be used.
    For more detailed information on DSP and T.38 resources, refer to chapter *Administrator Documentation, Configuration Limits and Capacities*.
  - **S_0 ports**
    All S_0 ports configured on mounted HG 1500 boards are automatically registered again on slot 0 of the communication system after the CDB conversion.
- **Dial plan in the internetwork**
  In a pure voice network, open and closed numbering are possible. When using the UC Suite, closed numbering is required in the internetwork (network-wide UC functionality). When using UC Smart, open and closed numbering are possible (node-wide UC functionality).
- **Multi-SLC**
  If multiple SLCN boards are inserted in the HiPath 3800, these are synchronized via SLC networking lines (multi-SLC). For each SLC networking line, an internal S_0 station is set up. After the migration, it should be verified that the station flag **Call waiting rejection on** is disabled for this S_0 station. Otherwise, problems may occur when a DECT phone attempts roaming to a base station that is connected to another SLCN board.
  If there are not SLCN or SLC16N boards and BS is plugged on $U_{P0/E}$, a CMA module is needed on the control board in case of an osbiz network with cmi roaming over the nodes.

35.3 Openscape Business X3/X5/X8 Chapter 5.1.5 Multi-SLC

Multi-SLC offers the full mobility of DECT stations across all Cordless boards within a communication system (OpenScape business X8) and across all communication systems in a network (OpenScape business X3/X5/X8).

Multi-SLC within a communication system

You can install up to four SLCN Cordless boards in OpenScape Business X8. For the total DECT station mobility (roaming and seamless connection handover) within a communication system, the radio areas of these cordless boards are synchronized.

If there are not SLCN or SLC16N boards and BS is plugged on $U_{P0/E}$, a CMA module is needed on the control board in case of an osbiz network with cmi roaming over the nodes.

Each DECT phone is seen as a corded phone by the communication system. During administration, a fixed port on the system's "home cordless board" is assigned to the DECT phone; this is used for addressing the DECT phone.

As soon as a DECT phone moves into the area of a different radio switching location ("current-location cordless board"), an extension connection is switched using a DSS1 connection initiated by the cordless board. The home and current-location cordless boards exchange a networking protocol (User-to-User Signaling UUS) over this extension connection to support full mobility.

Multi-SLC in a network

Multi-SLC can also be used across systems (across nodes) because the SIP-Q protocol used for networking supports the UUS protocol. That means full mobility across the radio areas of the different Cordless systems. All DECT phone features (callback, team functions, Voicemail, etc.) remain intact. The network-wide handover feature is the only exception here, since it is not supported.

As a precondition, the radio areas of the networked communication systems must not overlap.

Required B Channels for Multi-SLC

DECT phone has set up a connection	Required B channels	Required B channels for the home cordless board	Required B channels on the transitional cordless board
In the home cordless board range	1	1	–
In the transitional cordless board range	3	2	1

DECT phone has set up a connection	Required B channels	Required B channels for the home cordless board	Required B channels on the transitional cordless board
Handover from home to home cordless boards	1	1	–
Handover from home to transitional cordless board	3	2	1
Handover from transitional to transitional cordless board	5 (temporary)	3	2 (one for each cordless board)

Additional B channels using fixed connection paths (SIP-Q) may be required for the system-wide extension connections (Multi-SLC in a network).

36 MR_I52084: BS5 LEDs

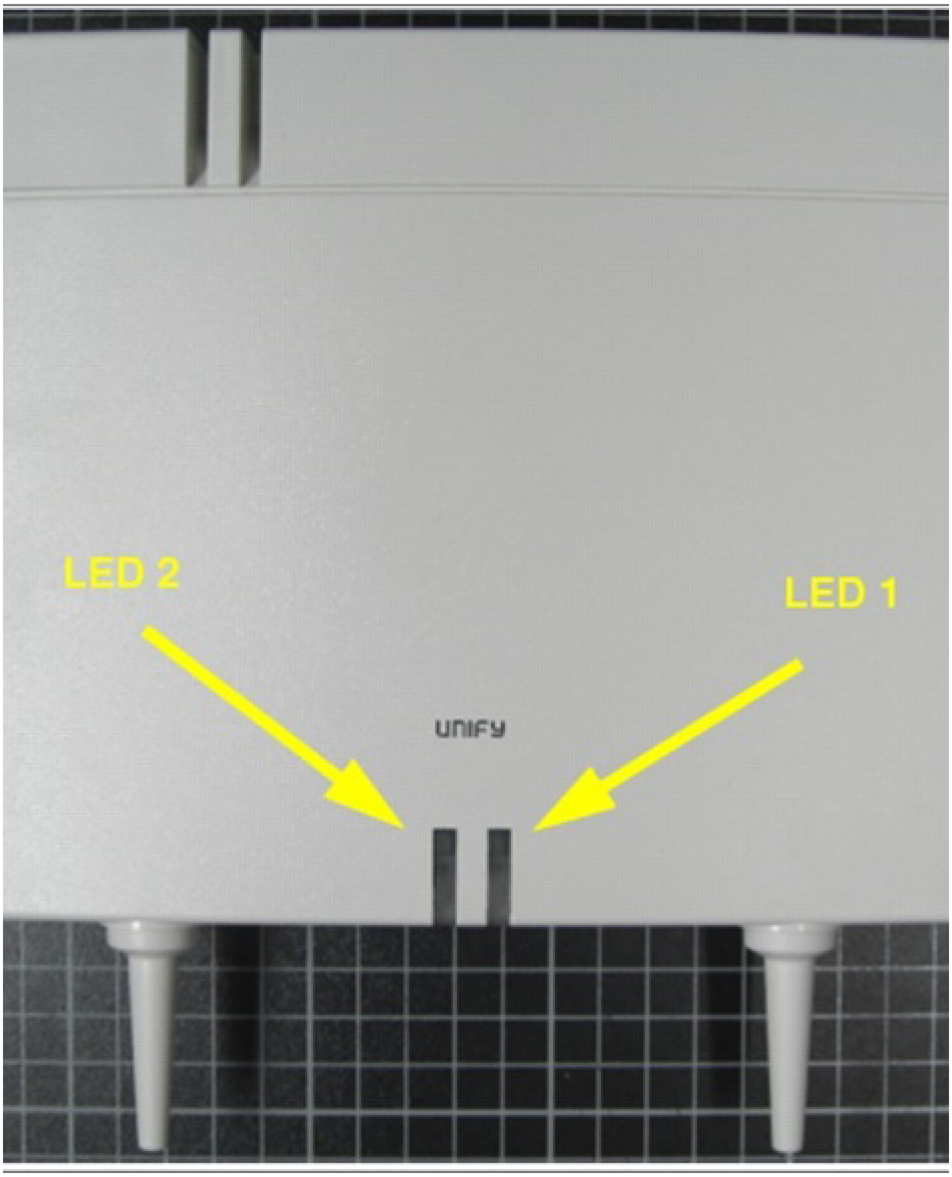
Affected Documentation	Service Documentation
Issue	5
Reference No.	A31003-P3020-S100-05-7620

36.1 Chapter 5.2.1 Technical Data

The technical data provides information on the operating conditions for the BS5 base station.

	BS5
Power supply voltage range	42 to 54 V
Maximum power consumption	3.0 W
Housing dimensions (length x width x depth)	202 x 172 x 43 mm
Weight	Approx. 0.5 kg
Temperature range	- 5 to + 45 °C (when operating indoors)
	- 20 to 50 °C (when operating outdoors with the outdoor housing)
Maximum humidity	95 %
Direct connection	1 x $U_{P0/E}$
Board connection	1 x or 2 x or 3 x $U_{P0/E}$

Figure: Base Station BS5



36.2 Chapter 5.2.3 LEDs

The front panel of the BS5 base station features two LEDs that indicate the operating states.

Author: te000004

Table: Information on LED displays for BS5

LED 1	LED 2	State	Comment
red	red	Board is in reset state	During boot-up
blue	off	FPGA is loaded, boot starts	During boot-up
white	white	BIST is running	During boot-up

LED 1	LED 2	State	Comment
Blinking yellow: Encryption on Blinking red: Encryption off	blue	Parameter download	
	light dimly violet	T-Bit request	
	brightly violet	T-Bit received	Switch to normal operation, if phase difference < 50ppm
red	off	Selftest of base station	
		(at major error BS remains in this condition)	
blinking red	off	Boot-Firmware is running	
		-no loadware in BS	
		-waiting for loadware download	
		-download of new LW is currently underway	
blinking red	blue	-BS ready (working with LW), but parameter download and synchronization is missing	
twice flashing red	blue	-BS ready, but all frequencies are blocked (RFP does not send)	
off	blue	-BS synchronized and sends Dummy bearer, but no slot active	
off	blinking blue	-BS synchronized and one slot active at least	
red	blinking blue	-BS in overload	
off	twice flashing blue	-DNS, slave BS is searching for master BS (not synchronous to master system)	
blinking red	blinking blue (synchronous to other LED)	CTR6 testmode	
		Note: Layer 1 has to be established at port 0	
blinking	blinking blue (alternatingly with other LED)	Loopback # 2 (2B+D) for biterror-measurement	
	dark blue	1x UP0E connected	During operational mode
	white	2x UP0E connected	During operational mode
	light blue	3x UP0E connected	During operational mode

MR_I52084: BS5 LEDs
Chapter 5.2.3 LEDs

37 MR_I52121: BS Feature Amount

Affected Documentation	Issue	Reference No.
Administration Documentation	9	A31003-P3020-M100-09-76A9
OpenScape Business X3/X5/X8 Service Documentation	5	A31003-P3020-S100-05-7620
Service Documentation X1		A31003-P3010-U105-19-19

37.1 Administrator Documention Chapter 18.3.2.3 and Openscape Business X3/X5/X8 Chapter 5.1.1 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.

OpenScape Business	Cordless board	CMA required?	Maximum number of base stations with connection via 1 x $U_{P0/E}$				Maximum number of simultaneous calls per base station, depending on the $U_{P0/E}$ connection				Max. number of DECT phones	Analog trunk access is possible
			BS3/1	BS3/S	BS3/3	BS4/ BS5	BS3/1	BS3/S	BS3/3	BS4/ BS5		
X1	–	no	7	1	–	7	2 (1 x $U_{P0/E}$)	2 (1 x $U_{P0/E}$)	–	2 (1 x $U_{P0/E}$)	16	no
	–	yes	7	–	–	7	4 (1 x $U_{P0/E}$)	–	–	4 (1 x $U_{P0/E}$)	16	no
X3/X5	–	no	15	15	–	15	2 (1 x $U_{P0/E}$)	2 (1 x $U_{P0/E}$)	–	2 (1 x $U_{P0/E}$)	32	no
	–	yes	15	–	–	15	4 (1 x $U_{P0/E}$)	–	–	4 (1 x $U_{P0/E}$)	32	yes
X5W	1 x SLC16N	no	16	–	16	16	4 (1 x $U_{P0/E}$)	–	12 (3 x $U_{P0/E}$)	12 (3 x $U_{P0/E}$)	64	Yes
X8	4 x SLCN	no	64	–	64	64	4 (1 x $U_{P0/E}$)	–	12 (3 x $U_{P0/E}$)	12 (3 x $U_{P0/E}$)	250	yes

37.2 Openscape Business X1 Chapter 4.1.1 System Configuration

Up to 7 base stations can be connected, and up to 16 DECT phones can be used.

The following table shows the maximum possible system configuration of the integrated Cordless solution.

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 X1.

In the event of a failure, the current base stations should be used.

OpenScape Business	CMA required?	Maximum number of base stations with connection via 1 x $U_{P0/E}$				Maximum number of simultaneous calls per base station, depending on the $U_{P0/E}$ connection				Maximum number of DECT phones
		BS3/1	BS3/S	BS3/3	BS4/ BS5	BS3/1	BS3/S	BS3/3	BS4/ BS5	
X1	no	7	1	–	7	2 (1 x $U_{P0/E}$)	2 (1 x $U_{P0/E}$)	–	2 (1 x $U_{P0/E}$)	16
	yes	7	–	–	7	4 (1 x $U_{P0/E}$)	–	–	4 (1 x $U_{P0/E}$)	16

Index