

OpenScape Cordless IP V2

Administrator Documentation

P31003C1020M1000276A9

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

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

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

Copyright © Unify Software and Solutions GmbH & Co. KG 01/2018
Mies-van-der-Rohe-Str. 6, 80807 Munich/Germany

All rights reserved.

Reference No.: P31003C1020M1000276A9

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.

Unify, OpenScape, OpenStage, Circuit and HiPath are registered trademarks of Unify Software and Solutions GmbH & Co. KG. All other company, brand, product and service names are trademarks or registered trademarks of their respective holders.

Contents

1 OpenScope Cordless IP V2 – Introduction	5
1.1 Planning your DECT wireless network	7
1.2 OpenScope Cordless IP V2 – overview	8
2 First steps	9
2.1 Package content	9
2.2 Preparing to use the telephone system	9
2.3 Mounting the device	10
2.4 Defining the device role	12
2.5 Wall mounting	12
3 Operation hints	14
3.1 Light emitting diodes (LED)	14
3.2 Resetting base stations to factory settings via power procedure	15
4 Configuring the system	17
4.1 The web configurator	17
5 Network administration	23
5.1 IP settings	23
5.2 Local network setting – VLAN	25
6 Base stations	27
6.1 Base stations administration	27
6.2 Base station synchronisation	31
7 Provider and PBX profiles	39
7.1 Configuring telephony server profiles	40
8 Mobile devices	49
8.1 Mobile devices	49
8.2 Registering/de-registering handsets	50
8.3 Handset Registration Centre	57
9 Telephony settings	59
9.1 General VoIP settings	59
9.2 Audio quality	61
9.3 Call settings	62
10 Online directories	65
10.1 Corporate online directory (LDAP)	65
11 System settings	73
11.1 Web configurator access rights	73
11.2 Loading the web security certificate	75
11.3 Capacity licensing	75
11.4 Provisioning and configuration	78
11.5 Security	79
11.6 Date and time	81
11.7 Firmware	82
11.8 Save and restore	84
11.9 Reboot and reset	85

Contents

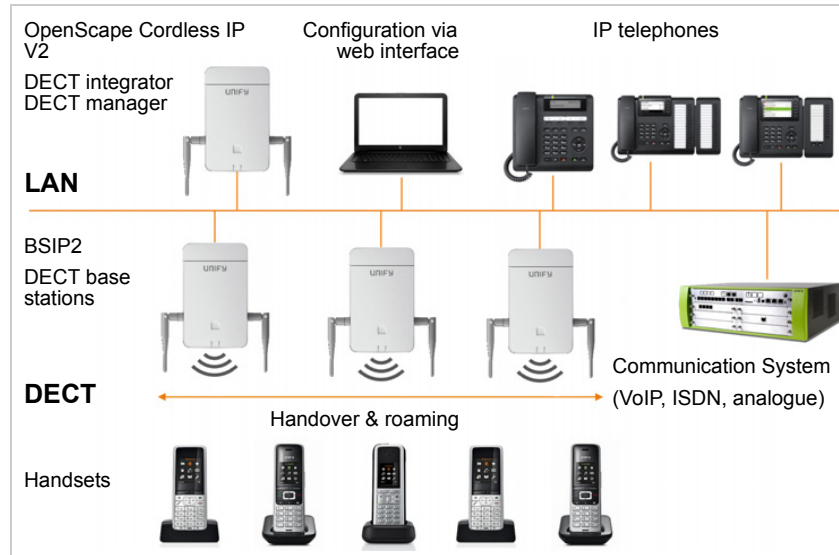
12 Diagnostics and troubleshooting	87
12.1 Status information	87
12.2 Base station events	88
12.3 Incidents	89
12.4 System log and SNMP manager	90
13 Using handset connected to a BSIP2 base	93
13.1 Making calls	93
13.2 Accepting calls	95
13.3 Conversation with three participants	95
13.4 Message indication	97
13.5 Using directories	97
13.6 Using the network mailbox	98
14 LDAP directory – configuration example	99
14.1 Access to the LDAP server	99
14.2 Filters	101
14.3 Attributes	104
14.4 Display on the handsets	105
A Appendix	107
A.1 Safety precautions	107
A.2 Service	107
A.3 Authorisation	107
A.4 Disposal	107
B Technical data	109
B.1 Specifications	109
Index	110

1 OpenScape Cordless IP V2 – Introduction

OpenScape Cordless IP V2 is a DECT multicell system for connecting DECT base stations to a VoIP Communication System. It combines the options of IP telephony with the use of DECT telephones.

Components

The following illustration shows the components of the OpenScape Cordless IP V2 and the way the system is embedded in the IP telephone environment:



- **DECT integrator**

Central management and configuration unit of the DECT multicell system.

The DECT integrator

- Integrates the handover domains managed by multiple DECT managers to one roaming domain
- Contains the central DECT subscriber database
- Provides a web user interface for subscriber configuration
- Provides access to the configuration for all DECT managers and the base station synchronisation hierarchy
- Acts as provisioning server for DECT registration and IP registration
- Integrates multiple DECT managers to one roaming domain (future installation)

In small and medium installations the integrator and DECT manager are located on the same device.

Configuring the DECT network using the web user interface → p. 17

- **OpenScape Cordless IP V2 DECT manager**

Management unit for a group of base stations. At least one DECT manager must be used for each installation.

The DECT manager

- Enables division into subnets (**Cluster** formation)
- Manages bases station synchronisation within the clusters
- Provides application gateway between SIP signalling and DECT signalling
- Controls the media path from Communication System to relevant base stations

The current version only supports the use of one DECT manager.

- **BSIP2 DECT base stations**

OpenScape Cordless IP V2 – Introduction

- Provide cell site DECT functions
- Provide media processing from handset directly towards Communication System
- Provide up to 12 DECT full slot pairs (zero blind slot)
- Provide up to 6 DECT long slot pairs (wideband)

Configuring the base stations → p. 27

• Handsets (mobile devices)

- Per DECT manager 250 handsets can be connected by roaming and 60 DECT calls could be made simultaneously for VoIP calls, network directory sessions and info center sessions.
- Subscribers can accept or initiate calls in all DECT cells with their handset (**Roaming**), and can also switch between the DECT cells during a call (**Handover**). A handover is only possible if cells are synchronised.

Configuring handsets → p. 49

• Communication System

You can connect your DECT telephone system to a Communication System for VoIP, ISDN or analogue telephony, e.g.,

- OpenScape Business
- OpenScape 4000
- OpenScape Voice

The Communication System

- Establishes the connection to a public telephone network
- Enables central management of telephone connections, directories, network mailboxes

• Forming clusters

A cluster defines a set of base stations of a DECT manager that shall synchronise in order to perform handover, roaming and overload balancing.

Handover means to switch a handsets DECT connection to a new base station during a call.

Roaming means to connect a handset in idle mode via a new base.

Overload balancing is the process to setup a DECT connection (for a call or other administrative or customer purpose) not at the current base station, which is fully loaded with active DECT or media connections, but via a neighbour base station, which has free resources to setup/accept the new DECT connection.

Handover and overload balancing could only be provided by synchronised base stations. In some cases, not all base stations connected to one DECT manager can be synchronised for location specific reasons. To organize synchronisation just within a subset of base stations connected to one DECT manager, you can form clusters, within a DECT manager.

A DECT manager can offer multiple clusters with base stations synchronised within the cluster, but not synchronised along different clusters.

In future multiple DECT manager integrations, DECT managers could be synchronised by defining synchronisation between clusters of different DECT managers.

Deployments

The current OpenScape Cordless IP V2 deployment can be used for small to medium DECT networks.

	Small	Medium
Base stations	Up to 10 BS functionality can be activated on the Integrator/DM device.	Up to 60
Handsets	Up to 50	Up to 250 per DM

DECT manager	Integrator and DECT manager on the same device
Integrator	

Number of parallel calls depending of device role

Base	10
Base + DECT manager	8
Base + DECT manager + Integrator	5

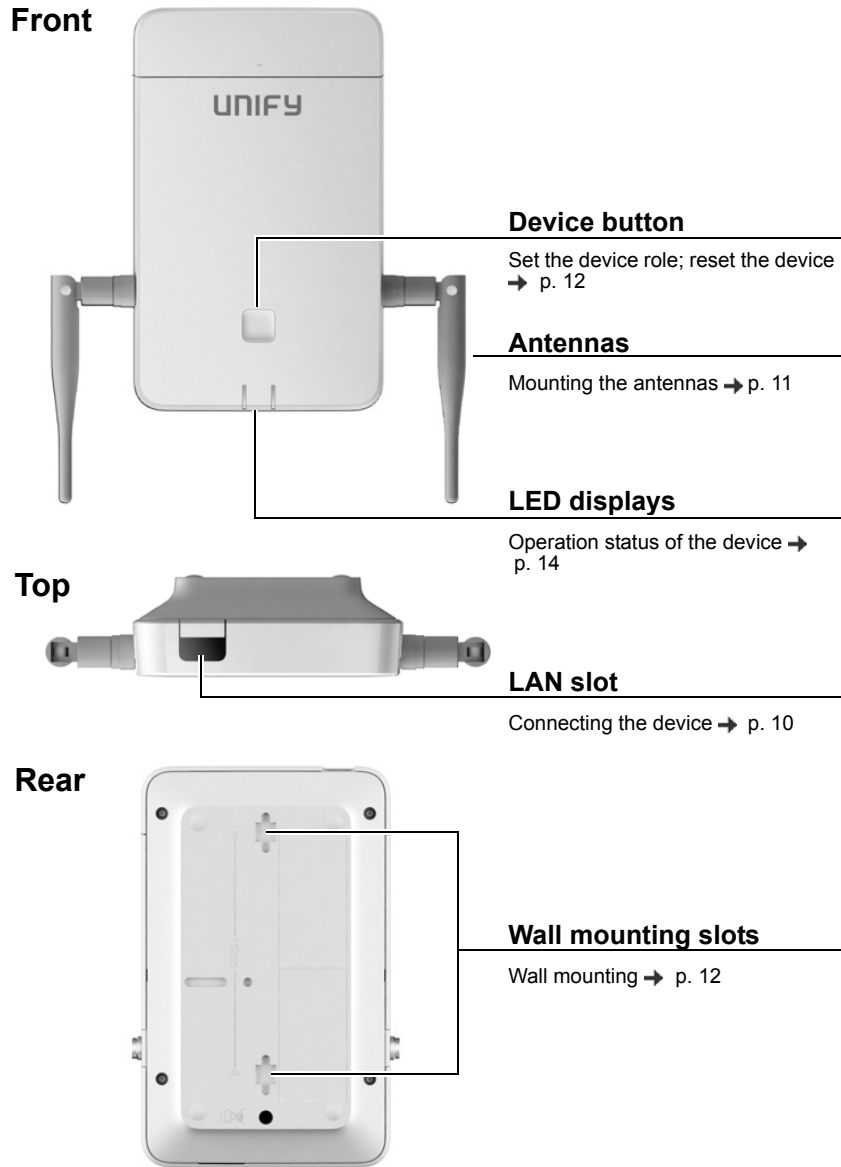
Number of parallel calls per base station depending on the bandwidth: → p. 45

1.1 Planning your DECT wireless network

Careful planning of your DECT wireless network is the prerequisite for successful operation of the OpenScape Cordless IP V2 with good call quality and adequate call options for all subscribers in all the buildings and areas belonging to the Communication System. When deciding how many base stations are needed, and where these should be positioned, both the requirements for the capacity of the Communication System and its wireless coverage, as well as many ambient conditions, must be taken into consideration.

- ▶ For detailed information on planning your DECT network please refer to the service documentation for OpenScape Cordless IP V2.

1.2 OpenScape Cordless IP V2 – overview



2 First steps

2.1 Package content

- One BSIP2
It can be used as DECT management system or as base station
- Two antennas
- Security leaflet



2.2 Preparing to use the telephone system

To use the telephone system the following steps must be performed:

- 1 Perform DECT measurement and site planning
During the planning phase of your DECT network you should have created an installation plan for the DECT managers and base stations.
- 2 Connect the devices to the local network → p. 11
- 3 Configure one device as Integrator/DECT manager → p. 12
- 4 Mount the devices at the planned locations → p. 12
Note: For each location please note down the MAC address of the device you are going to install.
- 5 Configure the local network settings via web configurator → p. 23
You need a PC connected to the local network, so that you can configure your telephone system via the web configurator.
- 6 Perform a firmware update → p. 82
Note: To ensure that the latest, best default initialisation of customer settings come into effect, proceed as follows:
 - Once again, reset the DECT manager device as Integrator/DECT manager via web configurator (→ p. 85) or key procedure (→ p. 15). This will apply the default initialisation of customer settings.
 - If applicable, configure the local network settings via web configurator.
 - Then perform the firmware update. This should be done
 - not to update the device again (it is already up to date)
 - but to provide the update software (or URL) for base stations to be added in the next step. That information was lost by the previous reset procedure.
- 7 Register the base stations to the DECT manager → p. 27
Note: The base stations will go offline for the time of firmware update, i.e., that you may have to wait a short time until you can continue with step 8.
- 8 Configure the base station synchronization → p. 31
- 9 Configure VoIP Communication System or provider → p. 39

First steps

Mounting the device

10 Register handsets and perform handset configuration → p. 49

All the handsets to be used for making calls over the OpenScape Cordless IP V2 must be registered on the telephone system. Any handset must get assigned an individual SIP account at the SIP Communication System. When registering, the handset is permanently assigned a VoIP connection as the receive and send connection.

11 Create a backup to save your configuration → p. 84



Information and support for our products can be found on the Internet at:

<http://www.unify.com/>

Select the product to open the relevant product page for your base, where you will find a link to the user guides.

Technical notes, current information about firmware updates, frequently asked questions and lots more can be found on the Internet at:

<http://wiki.unify.com/>

Select the product to open the relevant product page for your base, where you will find a link to the user guides.

To find out which version of the Integrator/DECT manager firmware is currently loaded, see → p. 82 and/or p. 87.

2.3 Mounting the device

- When installing the base stations, please take into account the technical conditions for positioning and the installation guidelines, which are described in the "HiPath Cordless IP – Service Documentation".
- Install the base stations at the positions you determined when planning or measuring your DECT wireless network.
- The OpenScape Cordless IP V2 device acting as Integrator/DECT manager can be installed anywhere within the range of the local network. It does not need to be installed in the coverage area of the DECT wireless network. Exception: the device comprising the DECT manager also acts as base station.
- The OpenScape Cordless IP V2 devices are intended for wall mounting (→ p. 12).



The devices are designed for indoor use or for outdoor use, in case it is mounted in an outdoor case.

Indoor use:

- The devices are designed for use in dry rooms with a temperature range of +5°C to +45°C.
- Never expose the devices to heat sources, direct sunlight or other electrical appliances.
- Protect your device from moisture, dust, corrosive liquids and fumes.

Outdoor use:

- Base station protection at ambient temperature between -20°C and +50°C.

2.3.1 Connecting to the LAN



DECT manager and base stations must be connected to the same Ethernet or virtual LAN sharing a common broadcast domain.

If you intend to use DECT-LAN synchronisation, please consider the requirements mentioned in section "LAN-based synchronisation" (→ p. 32).

You can connect the devices to your local network via a router, switch, or hub. A VoIP Communication System is required for Internet telephony. This must be accessible via the local network and must have network access (to the Internet and/or the analogue or ISDN telephone network). Otherwise it will only be possible to make calls within the LAN.

You also need a PC connected to the local network, so that you can configure your telephone system via the web configurator.

For each device to be connected to the local network an Ethernet cable is required.



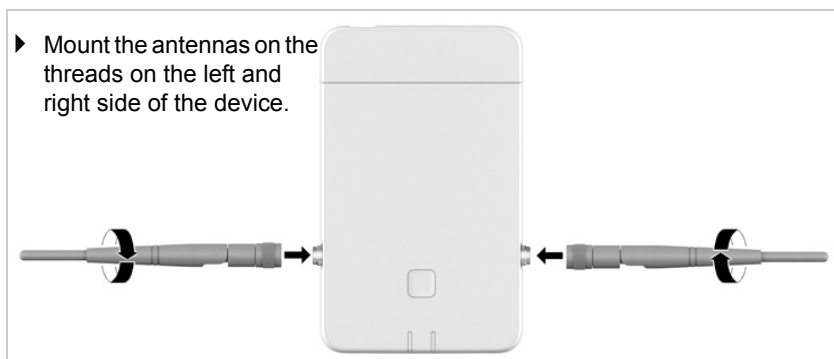
The OpenScope Cordless IP V2 is supplied with power via PoE (Power over Ethernet). It must be connected to an Ethernet device with PoE functionality (PoE class IEEE802.3af).



- ▶ Pull up the upper part of the housing and fold it forwards **1**.
- ▶ Insert a plug from an Ethernet cable into the LAN connection socket at the top of the device **2**.
- ▶ Insert the second Ethernet cable plug into a LAN socket for your local network or on the PoE switch **3**.
- ▶ Close the flap.

2.3.2 Mounting the antennas

Devices that are intended to be used as base station should be equipped with the external antennas supplied.



First steps

Defining the device role



In case you connect other external antenna models or types please take care that the maximum allowed transmission power is not exceeded. If in doubt, you can lower the transmitting power by the web interface option **Reduce TX power by 8dB for external antenna operation** for this device (→ p. 30).

2.4 Defining the device role

On delivery all OpenScape Cordless IP V2 devices are configured as base station. To set up the DECT multicell system at least one device must be configured as Integrator/DECT manager. Detailed information on device roles: → p. 5.

You use the device button on the front side to change the role of the device. The following settings are possible: base station, Integrator/DECT manager with dynamic IP address, Integrator/DECT manager with fixed IP settings.

- ▶ Press the device button for at least 10 seconds until all LEDs switch off. ▶ Release the button . . . the device is now in programming mode.
- ▶ Select the device role by pressing the device button.

Integrator/DECT manager with dynamic IP settings:

- ▶ Short press the device button until both LEDs light blue. . . . The IP address will be assigned by a DHCP server in your network.



Integrator/DECT manager with fixed IP settings:

- ▶ Short press the device button until the right LED lights blue. . . . The following IP settings are set:
IP address: 192.168.143.1
Subnet mask: 255.255.0.0



Base station:

- ▶ Short press the device button until the right LED lights green.



Once the desired role is selected:

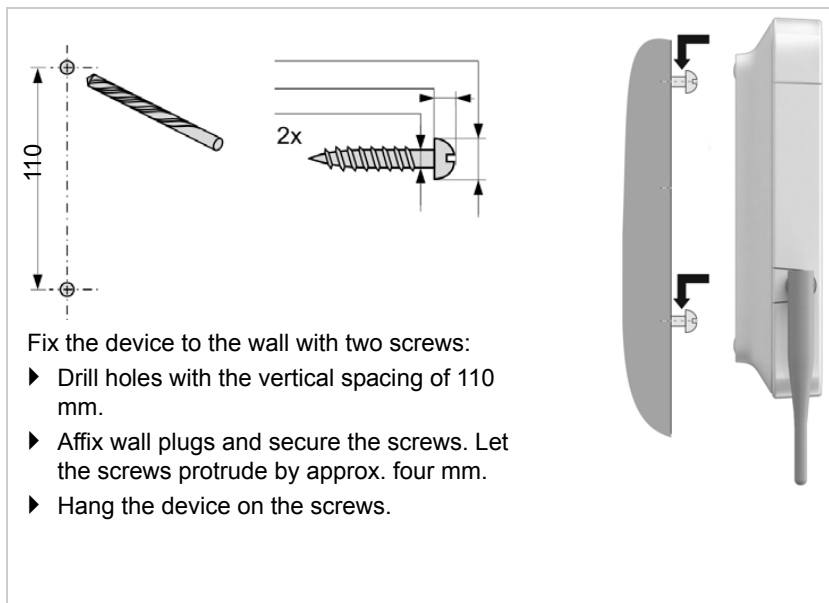
- ▶ Press the device button at least three seconds but less than 10 seconds . . . the previously selected role is assigned to the device . . . the device is reset and rebooted.



When changing the device role the system is reset to factory setting. This means, that existing configuration and user data will be lost.

2.5 Wall mounting

BSIP2 is intended for wall mounting. After connecting the LAN cable and setting the device role you can place it to the destined location.



For outdoor use the device can also be mounted in an outdoor case. Detailed information on installing the outdoor case can be found in the "HiPath Cordless IP – Service Documentation".

Operation hints

Light emitting diodes (LED)

3 Operation hints

3.1 Light emitting diodes (LED)

Depending on the device role the LEDs on the front side show different operational states. The LEDs can have three different colours (red, blue, green) or can be off.

3.1.1 DECT manager and base stations

LED 1 (left)				LED 2 (right)				Description
0.5 s	0.5 s	0.5 s	0.5 s	0.5 s	0.5 s	0.5 s	0.5 s	
[Grey]				[Grey]				Power off
[Red]				[Red]				Device is booting
[Blue]		[Grey]		[Grey]		[Blue]		Firmware update in progress
[Red]		[Grey]		[Grey]		[Red]		No connection to LAN or no IP address available/assigned
[Green]		[Grey]		[Grey]				Connecting to DECT manager or no connection to DECT manager

3.1.2 Base station operational states

LED 1 (left)				LED 2 (right)				Description
0.5 s	0.5 s	0.5 s	0.5 s	0.5 s	0.5 s	0.5 s	0.5 s	
[Green]				[Grey]				Successful connection to DM, synchronising
[Green]				[Green]				Synchronised, DECT ready
[Green]				[Green]		[Grey]		Synchronised, DECT traffic
[Green]				[Green]	[Grey]			Synchronised, DECT overload

3.1.3 DECT manager (without DECT)

LED 1 (left)				LED 2 (right)				Description
0.5 s	0.5 s	0.5 s	0.5 s	0.5 s	0.5 s	0.5 s	0.5 s	
[Blue]				[Grey]				No DECT base inside active
[Blue]		[Grey]		[Grey]				System traffic / ongoing calls

3.1.4 DECT manager (with DECT)

LED 1 (left)				LED 2 (right)				Description
0.5 s	0.5 s	0.5 s	0.5 s	0.5 s	0.5 s	0.5 s	0.5 s	
								Not synchronised, DECT ready
								Synchronised, DECT ready
								Synchronised, system traffic, no DECT traffic
								Synchronised, DECT traffic
								Synchronised, DECT overload

3.2 Resetting base stations to factory settings via power procedure

The following describes the procedure to reset base stations to factory settings via power procedure. You can use it, if it is not possible to reset the device

- via the web configurator (→ p. 85), for instance because you have forgotten the password for the web configurator or you are experiencing problems accessing the LAN
- via the key procedure (→ p. 12), for instance because the devices are mounted in places that are difficult to access.



The following procedure only applies to base stations. For DECT manager/Integrator you need to use one of the above procedures.

Resetting the device to factory settings is performed by interrupting the boot process.

- ▶ Remove the power supply from the device (unplug the LAN cable).
- ▶ Replug the LAN cable . . . the reboot starts. If the boot process is not interrupted, the standard reboot is performed.
- ▶ Interrupt the boot procedure after 30 sec. at the earliest and 40 sec. at the latest.
 - Once The device is reset as Integrator/DECT manager with a dynamic IP settings.
 - Three times The device is reset as base station.
 - Five times The device is reset as Integrator/DECT manager with fixed IP settings.



This procedure resets all the settings you have made for the device. The procedure deletes the saved data from the base stations and handsets. The base station's assignment to the DECT manager is cancelled. Ongoing calls are cancelled. In the case of an Integrator/DECT manager the whole configuration is reset.

To enable the restoration of your system configuration after a reset, you should regularly save the configuration data to a file (→ p. 84).

Operation hints

Resetting base stations to factory settings via power procedure

4 Configuring the system

System settings are made via the web configurator of the OpenScape Cordless IP V2 (→ p. 17) and cannot be changed using the handsets.

This applies in particular for:

- Registering and de-registering the handset to the telephone system, handset name.
- All settings for the VoIP account used by a handset for calls.
- Configuration of online directories.

Handset-specific settings are preset on your handset. You can change these settings.

This applies, for example, for Display settings, such as language, colour, backlight etc.

- Settings relating to ringtones, volume, speaker profiles etc.

Information about this can be found in the user guide for the relevant handset.

4.1 The web configurator

Use the web configurator to set up your OpenScape Cordless IP V2 and configure your DECT network.

- Set up the DECT network, register and synchronise the base stations.
- Make basic settings for the VoIP connections and register and configure the handsets you wish to use in the DECT network.
- Save data required to access specific services on the Internet. These services include access to online directories, as well as synchronising the date/time with a time server.
- Save your DECT network's configuration data as files on your PC and reload these in the event of an error. Upload new firmware, if available, and plan firmware updates at a specific date.

4.1.1 Starting



At least one OpenScape Cordless IP V2 device is installed as Integrator/DECT manager (→ p. 12).

A standard web browser is installed on the PC/tablet.

The device housing the Integrator/DECT manager and the PC/tablet are directly connected to one another in a local network. The settings of any existing firewall installed on your PC allow the PC/tablet and Integrator/DECT manager to communicate with each other.



While you are connected to the web configurator, it is blocked to other users. Simultaneous access is not possible.

- ▶ Launch the web browser on your PC/tablet.
- ▶ Enter the current IP address for the Integrator/DECT manager in the address field of the web browser (for example: `http://192.168.2.10`).

Configuring the system

The web configurator

IP address of the device

If the IP address is assigned dynamically via your local network's DHCP server, you can find the current IP address on the DHCP server in the list of registered DHCP clients. The MAC address can be found on the rear of the device. If necessary, contact the network administrator for your local network.

Your DECT manager's IP address may change occasionally depending on the DHCP server settings (→ p. 23).

4.1.2 Logging into/off the web configurator

Once you have successfully established the connection, the login screen is displayed in the web browser.

- ▶ Enter **admin** in the **Username** text field.
- ▶ Enter the password in the **Password** text field. Default: **admin**
- ▶ Click on **Login**.

You will be asked to change the default password.

- ▶ Enter a new password in the **New password (Admin)** field and repeat it in the **Repeat password** field
- ▶ Click on **Change password**.



If you do not make any entries for a lengthy period (approx. 10 minutes), you are automatically logged off. The next time you try to make an entry or open a web page, the login screen is displayed again. Enter the password again to log back in.

Any entries that you did not save on the telephone system before automatic logoff will be lost.

Logging off

You will find the log off function at the top right of each web page, below the product name.

- ▶ Click on  Logout



The session is automatically terminated after ten minutes of inactivity.

Always use the logout function to end the connection to the web configurator. If, for example, you close the web browser without logging off beforehand, access to the web configurator may be blocked for a few minutes.

4.1.3 Showing/hiding the navigation menu

On each web configurator page a side menu on the left allows you to navigate through the available functions. The menu currently used is unfolded and the currently selected menu entry is coloured green.

The navigation menu can be displayed permanently or can be hidden in the case the pointer is moved out of the menu area.

- ▶ Use the **Auto-hide menu** check box beneath the menu list to show/hide the menu.



unchecked The navigation menu is shown permanently. (Default)



checked

The menu is hidden as soon as you move the pointer out of the menu area. Only the upper menu level symbols are shown on the left.

To redisplay the menu: ▶ Move the pointer to the area the menu symbols are shown.

4.1.4 Help function

Parameter description

- ▶ Click on the question mark next to the parameter for which you need information. A popup window is opened displaying a short description for the selected parameter.

Function description for the entire web configurator page

- ▶ Click on the question mark in the upper right corner of the page. The online help is opened in a separate window. It provides information about the functions and tasks that can be performed via this page.

You have access to the total online help:

Browse through the online help: ▶ Use the ◀ ▶ buttons.

Open the table of contents: ▶ Click on the ☰ button.

Open the index to search for specific keywords: ▶ Click on the 🔍 button.

4.1.5 Applying/discarding changes

Applying changes

- ▶ Select the **Set** button as soon as you have completed your change on a page . . . the new settings are saved and activated on the DECT manager configuration.



Changes that have not been saved are lost if you move to another web page or the connection to the web configurator is lost, e.g., due to exceeding the time limit (→ p. 18).

Discarding changes

- ▶ Select the **Cancel** button . . . changes made on the web page are rejected and the settings that are currently saved in the telephone system configuration are reloaded.

4.1.6 Working with lists

Changing the appearance of the list

Filtering the list:

- ▶ Enter a search item (full field content) in the text field . . . Only entries containing text matching the search item in any column are shown in the table.

Filtering the list by column content:

- ▶ In the **Search in** option menu select the columns which should be searched for the entered search item . . . Only entries containing text matching the search item in the selected column are shown in the table.

Sorting the list:

Configuring the system

The web configurator

- ▶ Click on the arrows next to the column header to sort the table on the column content in ascending or descending order.

Displaying/ hiding columns:

- ▶ Click on the **View** option menu on the right ▶ Select the columns you want to be displayed in the table (👁 / 👁 = displayed/hidden).

Names of columns which cannot be hidden are greyed out.

Browsing through the list

If there is not enough space to display all entries you can browse through the whole table. The number of pages is shown below the list. The current page is highlighted.

- ▶ Click on **Previous** or **Next** to scroll through the list page by page.
- ▶ Click on a specific page number, to go to the desired page directly.

4.1.7 Web configurator menu overview

Settings	Network	IP	→ p. 23
		LAN	→ p. 25
	Base stations	Administration	→ p. 27
		Synchronization	→ p. 31
	Provider or PBX profiles		→ p. 39
	Mobile devices	Administration	→ p. 49
		Registration Center	→ p. 57
	Telephony	VoIP	→ p. 59
		Audio	→ p. 61
		Call settings	→ p. 62
	Online directories	Corporate	→ p. 65
	System	Web configurator	→ p. 73
		Capacity licensing	→ p. 75
		Provisioning and configuration	→ p. 78
		Security	→ p. 79
		System log	→ p. 90
		Date and time	→ p. 81
		Firmware	→ p. 82
		Save and restore	→ p. 84
	Reboot and reset	→ p. 85	
Status	Overview		→ p. 87
	Statistics	Base stations	→ p. 88
		Incidents	→ p. 89

Configuring the system

The web configurator

5 Network administration

5.1 IP settings

This page is used to integrate the DECT multicell system into your company's local network.

► **Settings** ► **Network** ► **IP**

Device name	
Device name in the network ?	<input type="text" value="einstein"/>
Address Assignment	
Network type ?	<input type="text" value="IPv4"/>
IP address type ?	<input type="text" value="Dynamic"/>
IP address ?	<input type="text" value="192.168.250.168"/>
Subnet mask ?	<input type="text" value="255.255.255.0"/>
Standard gateway ?	<input type="text" value="192.168.250.53"/>
Preferred DNS ?	<input type="text" value="192.168.250.53"/>
Alternate DNS ?	<input type="text"/>



If you change the IP address of the device or an error occurs when you are changing the IP settings, the connection to the web User Interface may be lost.

- IP address changed: ► Re-establish the connection with the new address.
- An error occurred: ► Reset the device to the factory settings.

Defining the device role (→ p. 12)

Device name in the network

- Enter a label for the device. It is used to identify the device in network communication.

Network type

- Select the IP protocol used in your local network: Currently only **IPv4** is supported.

Network administration

IP settings

IP address type

- ▶ Select **Dynamic**, if your device receives the IP address via a DHCP server.
- ▶ Select **Static**, if you want to assign a fixed IP address to the device.

If the **Dynamic** setting is selected, all further settings are automatically configured. They are displayed and cannot be changed.

If you have selected **Static** as the address type, you must create the following settings.

IP address

- ▶ Enter an IP address for your device. This IP address allows your device to be reached by other subscribers in your local network.

The IP address comprises four individual groups of numbers with decimal values from 0 to 255 that are separated by a dot, e.g., 192.168.2.1.

The IP address must be included in the address block used by the router/gateway for the local network. The valid address block is defined by the IP address for the router/gateway and the **Subnet mask**.



The IP address must be unique across the network, which means that it must not be used by another device connected to the router/gateway.

The fixed IP address must not belong to the address block that is reserved for the DHCP server for the router/gateway.

Check the settings on the router or ask your network administrator.

Subnet mask

The Subnet mask specifies how many parts of an IP address the network prefix must comprise. For example, 255.255.255.0 means that the first three parts of an IP address must be the same for all devices in the network, while the last part is specific to each device. In subnet mask 255.255.0.0, only the first two parts are reserved for the network prefix.

- ▶ Enter the subnet mask that is used by your network.

Standard gateway

The Standard gateway is generally the router/gateway of the local network. Your Integrator/DECT manager device requires this information to be able to access the Internet.

- ▶ Enter the local (private) IP address for the standard gateway through which the local network is connected to the Internet (e.g., 192.168.2.1).

Preferred DNS

DNS (Domain Name System) allows you to assign public IP addresses to symbolic names. The DNS server is required to convert the DNS name into the IP address when a connection is being established to a server.

- ▶ Enter the IP address for the preferred DNS server. You can specify the IP address for your router/gateway here. This forwards address requests from the Integrator/DECT manager to its DNS server. There is no default setting for a DNS server.

Alternate DNS

- ▶ Enter the IP address for the alternate DNS server that should be used in situations where the preferred DNS server cannot be reached.

5.2 Local network setting – VLAN

Details in this page are only required if you connect your phone system to a local network that is divided into virtual subnetworks (VLAN – Virtual Local Area Network). In a tagged VLAN, data packets are assigned to the individual subnetworks via tags (markings) that consist of a VLAN identifier and the VLAN priority, amongst others.

▶ **Settings ▶ Network ▶ LAN**

VLAN

VLAN tagging ?

VLAN identifier ?

VLAN priority ?

You will need to save the VLAN identifier and VLAN priority on the phone system configuration. Your VLAN provider will supply you with this data.

VLAN tagging

▶ Select the check box next to **VLAN tagging**, if you want the phone system to use VLAN tagging.

VLAN identifier

▶ Enter the VLAN identifier that uniquely identifies the subnetwork. Value range: 0–4094.

VLAN priority

The VLAN priority allows voice data transport to take priority, for example.

▶ From the option menu select the priority for the phone system data.
Value range: 0–7 (0 = lowest, 7 = highest priority)



Ensure that the details in **VLAN identifier** or **VLAN priority** are set correctly. Incorrect settings can cause problems when connecting the DECT manager for configuration purposes. Internal connections between DECT manager and base stations are not tagged and therefore phone functions are not concerned.

If required, you must carry out a hardware reset via power procedure (→ p. 15). This means that all settings are lost.

Network administration

Local network setting – VLAN

6 Base stations

The Integrator/DECT manager automatically recognises the base stations within the network. Base stations need to be confirmed, activated and synchronised.

6.1 Base stations administration

Use the following web configurator page to assign base stations to the DECT manager.

▶ **Settings** ▶ **Base stations** ▶ **Administration**

Connected base stations

Q Search in ▾

👁 View ▾

<input type="checkbox"/>	MAC address	Base station	RPN	DECT manager	FW	Status
	<input type="checkbox"/> 7c2f80c6e273	LocalBS	0x2	local	V2R0.13.0 (V1.13.0+build.34a799c)	Sync
	<input type="checkbox"/> 7c2f80c6e5cd	Base station 7c2f80c6e5cd	0x3	local	V2R0.13.0 (V1.13.0+build.34a799c)	Sync

Previous 1 Next

🗑 Delete

Pending base stations

Q Search in ▾

MAC address	DECT manager

Previous 1 Next

There are two tables:

- **Connected base stations** lists all base stations which are already connected to the DECT manager.
- **Pending base stations** lists all base stations which are not yet connected to a DECT manager.

6.1.1 Connected base stations

The page shows the connected base stations with the following information:

- MAC address** Hardware address of the base station. With this address the device is uniquely identified within the LAN.
- Base station** Name of the base station. When added to the list the MAC address is used as name. The base station located at the same device as the DECT manager is shown as **LocalBS**.
The name can be edited (→ p. 29)

Base stations

Base stations administration

RPN	(Radio Fixed Part Number) Part of the RFPI. Identifies the base station on the air interface. It also enumerates the base station within a DECT manager. Each DECT manager gets a group of RPN to assign to its base stations. So it is possible to identify the DECT manager the base station belongs to.															
DECT manager	Name of DECT manager the base station belongs to. Currently always: local															
FW	Version of the currently installed firmware.															
Status	Synchronization status of the base station: <table><tr><td>0</td><td>Offline</td><td>Not available</td></tr><tr><td>1</td><td>Deactivated</td><td>Available but not activated</td></tr><tr><td>2</td><td>No Sync</td><td>Activated but not synchronised</td></tr><tr><td>3</td><td>Sync</td><td>Activated and synchronised,</td></tr><tr><td>4</td><td>Sync Overload</td><td>Synchronised but DECT overload</td></tr></table>	0	Offline	Not available	1	Deactivated	Available but not activated	2	No Sync	Activated but not synchronised	3	Sync	Activated and synchronised,	4	Sync Overload	Synchronised but DECT overload
0	Offline	Not available														
1	Deactivated	Available but not activated														
2	No Sync	Activated but not synchronised														
3	Sync	Activated and synchronised,														
4	Sync Overload	Synchronised but DECT overload														

6.1.2 Actions

Edit base station data

▶ Click on  next to the base station you want to edit . . . the data page for the base station is opened (→ p. 29).

Delete base station

▶ Select the check box of one or more base stations ▶ Click on **Delete** ▶ Confirm with **Yes** . . . All selected base stations are deleted. They are shown in the list of pending base stations again.

6.1.3 Pending base stations

The **Pending base stations** list shows the automatically recognised DECT base stations in the network that have not yet been registered. To integrate them into your DECT multicell system, they need to be confirmed and activated.

The base stations are identified by their MAC address.

Assigning a base stations to your DECT manager

▶ Click on in the row of the base station you want to add to your system . . . the data page for the base station is opened.



The relation to a DECT manager cannot be edited and changed. To assign a base station to another DECT manager:

- ▶ Delete it from the **Connected base stations** list.
- ▶ Open a connection to the intended DECT manager.
- ▶ Assign the base station from the base stations pending list to the DECT manager.

Adding/Editing base stations

On this page you enter the data for a base station to be added to the DECT manager or edit the data for a base station that is already assigned to the DECT manager.

Own Base Station Data

MAC address ?	7c2f80c6e273
Name / Location ?	LocalBS
DECT manager ?	local
Status ?	Sync
IP address type ?	Dynamic
IP address ?	192.168.250.168
	To change network settings for local base station go to IP configuration page.
RFPI = PARI + RPN (hex) ?	102D95AF 0x2
Current firmware version ?	V2R0.13.0 (V1.13.0+build.34a799c)
Reduce TX power by 8dB for external antenna operation ?	<input type="radio"/> Yes <input checked="" type="radio"/> No
Activate base station ?	<input checked="" type="radio"/> Yes <input type="radio"/> No

The following information is displayed and cannot be changed:

MAC address

Hardware address of the base station. With this address the device can be uniquely identified within the Ethernet. It cannot be changed

DECT manager

Name of DECT manager the base station belongs to. Currently always **local**: The base station belongs to the configuring device.

Base stations

Base stations administration

Status

Synchronization status of the base station:

0	Offline	Not available
1	Deactivated	Available, but not activated
2	No sync	Activated, but not synchronised
3	Sync	Activated and synchronised
4	Sync overload	Synchronised, but DECT overload

IP address

Current IP address of the Base station.

RFPI = PARI + RPN (hex)

(RFPI = Radio Fixed Part Identity) unique name of the base station in a multicell DECT network. It consists of:

- PARI (Primary Access Rights Identity): unique system ID of a base station
- RPN (Radio Fixed Part Number): base station number within the DECT network

Current firmware version

Firmware version currently installed.

The following data can be edited

Name / Location

This name should make it easier to assign the base station within the logical and spatial structure of the DECT network.

- ▶ In the text field enter a descriptive name or description for the base station. Value: max. 32 characters

IP address type

The IP address type is copied from the setting for the DECT manager on the **Network – IP** page (→ p. 23). You can change the IP address type. The settings for the DECT manager and the base stations do not have to match. For example, the DECT manager could receive a fixed IP address so that it will always be able to access the web configurator with the same address, while the base stations receive their IP addresses dynamically.

- ▶ Select the desired IP address type from the option menu.

If the IP address type is **Static**, you have to enter the IP address.

IP address

- ▶ Enter an IP address for the base station.

Reduce TX power by 8dB for external antenna operation

The transmitting power of the external antennas can be reduced. This may be needed in order not to violate emission regulations, in case the device is equipped with external antennas (→ p. 11).

- ▶ Click on **Yes/No** to reduce/not reduce the transmitting power by 8 dB.

Activating/deactivating the base station

A base station must be active to manage the calls of the connected handsets. If it is deactivated, it will no longer connect handsets but it still stays in the list of connected base stations.

- ▶ Select **Yes/No** to activate/deactivate the base station.



Please ensure that the base station you want to deactivate is not on sync level 1. Check your sync settings before deactivating a base station. Otherwise your system may no longer work properly

Adding a base station to the Connected Base Stations list

- ▶ Click on **Confirm**

Delete the base station

- ▶ Click on **Delete base station** ▶ Confirm with **Yes** . . . the base station is deleted. It is shown in the list of pending base stations again.

Reboot the base station

- ▶ Click on **Reboot base station** ▶ Confirm with **Yes** . . . the base station is rebooted. All existing connections managed by the base station are terminated.

6.2 Base station synchronisation

Synchronisation and the logical structuring of the base stations in clusters are prerequisites for the functioning of the multicell system, intercell handover, and (over)load balancing. Overload balancing means that a handset can roam to a free base, when current base is fully loaded and cannot accept further handset connections.

Base stations can be synchronised "over the air", meaning that they are synchronised via DECT. If the DECT connection between specific base stations seems to be not reliable enough, synchronisation can also take place via LAN. To carry out the synchronisation you will need the plan of the clusters with the synchronisation level for each base station.



Synchronisation always refers to a cluster. In case you set up several clusters that are not synchronised with one another, there will be no possibility of a handover or (over)load balancing between them.

For detailed information on DECT network planning, please refer to the "HiPath Cordless IP – Service Documentation".



A base station shows its synchronisation status with an LED (→ p. 14).

6.2.1 Synchronisation planning

Base stations that combine to form a DECT wireless network must synchronise with one another to ensure a smooth transition of the handsets from cell to cell (handover). No handover and no (overload) balancing is possible between cells that are not synchronised. In the event of loss of synchronisation, the base station stops accepting calls once all ongoing calls that were being conducted on the asynchronous base station have ended and then it re-synchronises the asynchronous base station.

The synchronisation within a cluster takes place in a master/slave procedure. This means that one base station (sync master) defines the synchronisation cycle for one or more other base stations (sync slaves).

Base stations

Base station synchronisation

The synchronisation needs a some kind synchronisation hierarchy with the following criteria:

- 1 There must be one single and common root source for the synchronisation in the hierarchy (sync level 1).
- 2 With synchronisation over LAN there are just two levels needed (LAN-Master and LAN-Slave).
- 3 DECT synchronisation usually needs more than two levels and just one hop, because most base stations won't be able to receive the DECT signal from the root source of the synchronisation (sync level 1). DECT signal providing reference timer synchronisation is relayed along a chain of multiple base stations, until it finally synchronises the last base station in a sync chain.
- 4 The number of hops along any branch of DECT synchronisation tree should be minimised, because any hop can introduce jitter in the synchronisation timer and could so lower the quality of the synchronisation.

DECT-based synchronisation

To relay DECT synchronisation signals from base station A to base station B, base station B must be able to receive signals from base station A in a sufficient signal quality.



DECT manager and base stations must be connected to the same Ethernet or virtual LAN sharing a common broadcast domain.

A base station can synchronise with each base station on a higher sync level. The sync level concept allows base stations to automatically select the best suitable base station to receive synchronisation signal from. Simultaneously, it guarantees a strictly limited number of hops a long any branch in the synchronisation tree and to prevent circles between automatically optimised synchronisation chains.

During configuration, assign one level in the synchronisation hierarchy (sync level) to each base station. Sync level 1 is the highest level; this is the level of the sync master and appears only once in each cluster. A base station always synchronises itself with a base station that has a better sync level. If it sees several base stations with a better sync level, it synchronises itself with the base station that provides the best signal quality. If it does not see any base station with a higher sync level, it cannot synchronise.

LAN-based synchronisation

If the DECT connection between base stations seems to be not reliable enough to permanently guarantee a stable DECT over the air synchronization, e.g., because they are separated by iron doors or a firewall, you can determine that synchronisation should take place via LAN. In this case the base station with the higher sync level will act as LAN master, the base station with the lower sync level is a LAN slave. One base station must be explicitly be defined as LAN master. Currently, it must be on DECT sync level 1.

Advantages of LAN synchronisation compared with DECT synchronisation:

- Higher flexibility in the arrangement of the base stations as no synchronisation chains need to be formed.
- Fewer base stations required as the overlapping area of the base stations is smaller. The overlapping area for handset handover can be smaller, because neighbored base stations do not need to receive each other in stable error free quality, but they must still be able to detect each other for the process of dynamic channel selection.
- Configuration of the system is simplified as all base stations can be synchronised on one synchronization master.

Requirements for LAN synchronisation

Minimum packet delay jitter is crucial for successful synchronisation over LAN. As multiple LAN traffic parameters could have an impact on packet delay and its jitter, specific switches and maximum number of switch hops are required, to guarantee sufficient maximum packet delay jitter.

Consider the following:

- The less switch hops, the lower the transmission delay and its jitter will be.
- The higher the bandwidth or quality of used switches is regarding packet delay and its jitter, the lower the packet delay and the lower the packet delay jitter will be.
- Enhanced packet processing logics (like L3 switching or packet inspection) could have significant negative impact on the resulting packet delay jitter. If possible, they should be deactivated for UNIFY BSIP2 base stations connected switch ports.
- Significantly increased traffic load on a switch, in the range of the maximum throughput, could have significant negative impact on the packet delay jitter.
- VLAN based prioritisation of LAN packets could be a fruitful measure to minimize packet delay and its jitter for UNIFY BSIP2 base stations.

Hints regarding PTP deviation

LAN synchronisation is based on a two layer design:

- Native PTPv2 is used to synchronise a common reference timer along all base stations involved.
Target quality benchmark to provide sufficient PTP synchronisation along the base stations, is to have a **PTP deviation lower than 500 ns** (rms). For this PTP synchronisation a few single deviations > 500 ns are accepted and might just generate first warnings. If the PTP sync packet deviation does continuously exceed this limit of 500 ns, the PTP synchronisation is considered broken and will lead to new start synchronisation procedure.
- Based on the PTP synchronisation LAN master and LAN slave adjust their DECT reference timer to one common offset to the common PTP reference timer. This common offset will be permanently monitored by an proprietary communication.
The target quality benchmark for this synchronisation level is to see reference timer deviation by this DECT reference timer sync packets: **DECT-LAN-Sync deviation lower than 1000 ns**. A good mean value would be 500 ns (rms).

To meet this criteria the switches themselves do not necessarily need to be PTP aware. But the network should consider the above mentioned guidelines to meet this criteria.

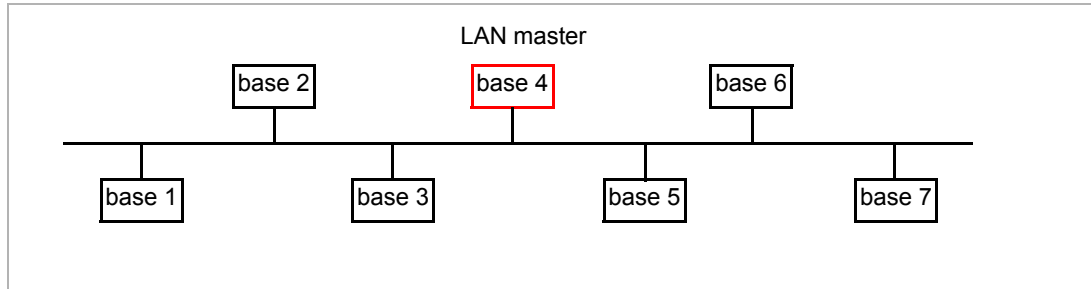
Base stations

Base station synchronisation

Scenarios for LAN/DECT synchronisation hierarchy

Scenario 1: Pure LAN synchronisation

Use such a configuration, if all requirements for LAN synchronisation are fulfilled and the radio coverage is not stable enough to ensure reliable synchronisation.



Configuration: Simple LAN synchronisation with base station 4 as LAN master. The DECT level has no relevance for this configuration.

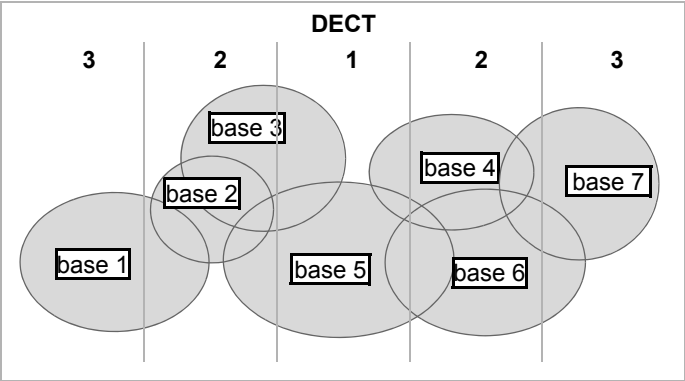
Base station	Cluster	DECT Level	LAN Master	Sync Slave
1	1	1		LAN
2	1	2		LAN
3	1	2		LAN
4	1	2	<input checked="" type="checkbox"/>	
5	1	2		LAN
6	1	2		LAN
7	1	2		LAN

Scenario 2: Pure DECT synchronisation

Use such a configuration if your environment ensures a stable DECT over the air synchronisation or your LAN does not fulfil the requirements for LAN synchronisation.



Prior to installation of base stations for DECT synchronisation, you should have an idea, where in the centre to plan the level 1 base station and in which distances around the centre to place the next sync level's base station. To proof and optimise this idea into a plan you should use a coverage measurement kit.



Configuration: Pure DECT synchronisation. Each base station can synchronise with a base station on a higher level. If more than one base station is possible the base station with the better signal is used. The base station in the centre of the cluster is on DECT level 1. That reduces the amount of necessary sync levels.

Base station	Cluster	DECT Level	LAN Master	Sync Slave
1	1	3		DECT
2	1	2		DECT
3	1	2		DECT
4	1	2		DECT
5	1	1		
6	1	2		DECT
7	1	3		DECT

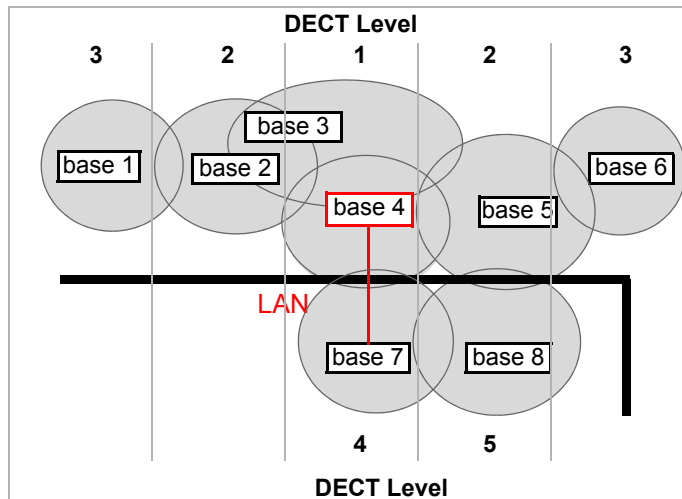
Base stations

Base station synchronisation

Scenario 3: Mixed

Use such a configuration, if your environment is mainly able to synchronise via DECT but there are particular circumstances which cannot always guarantee reliable DECT synchronisation, e.g., a passage through a fire door.

For all base stations on levels lower than the LAN master you can individually decide whether it should be synchronised via DECT or LAN.



Configuration: Mixed scenario. The base stations of the cluster are separated by a firewall. The overlap area may be large enough for handover and dynamic channel selection but not for synchronisation. Therefore the synchronisation between one base station on each side of the firewall takes place via LAN. The other base stations are synchronised via DECT. As the LAN master must be on DECT level 1 the base station 4 is used as LAN master.

Base station	Cluster	DECT Level	LAN Master	Sync Slave
1	1	3		DECT
2	1	2		DECT
3	1	2		DECT
4	1	1	<input checked="" type="checkbox"/>	
5	1	2		DECT
6	1	3		DECT
7	1	4		LAN
8	1	5		DECT

6.2.2 List of synchronised base stations

All activated base stations contained in the **Connected base stations** list (→ p. 27) appear in the **Base station synchronization** list.

► Settings ► Base stations ► Synchronization

Base station synchronization							
Search		Q Search in ▾		View ▾			
MAC address ↕	Base station ↕	DECT manager ↕	Cluster ↕	DECT Level ↕	LAN Master ↕	Sync Slave ↕	Status ↕
7c2f80c6e273	LocalBS	local	1 ▾	1 ▾	<input type="checkbox"/>		Sync
7c2f80c6e5cd	BS 7c2f80c6e5cd	local	1 ▾	2 ▾	<input type="checkbox"/>	DECT ▾	Offline

For each registered base station the following information is shown:

MAC address	Hardware address of the base station. With this address the device is uniquely identified within the LAN.	
Base station	Name of the base station.	
DECT manager	Name of DECT manager the base station belongs to. Currently always local : The base station belongs to the configuring device.	
Cluster	Number of the cluster to which the base is assigned.	
DECT Level	Synchronisation level within the sync hierarchy.	
LAN Master	The base station acting as LAN master is marked by a ✓.	
Sync Slave	Indicates if the base station is synchronised via DECT or via LAN. For the Sync master there is no entry in this column.	
Status	Synchronisation status of the base station:	
0	Offline	Not available
1	Deactivated	Available but not activated
2	No sync	Activated but not synchronised
3	Sync	Activated and synchronised
4	Sync Overload	Synchronised but DECT overload

6.2.3 Actions

Setting up the base station synchronisation

- Select the cluster to which the base should be assigned to from the **Cluster** option menu.
Base stations only synchronise within the same cluster, meaning that a handover of a handset from one cluster to a neighbouring cluster is not possible. The DECT multicell system can manage up to nine clusters.
- Select the synchronisation level for the base station from the **DECT Level** option menu.

Base stations

Base station synchronisation

DECT level 1 is the highest level and may appear only once in each cluster. A base station always synchronises itself with a base station that has a better sync level. If it sees several base stations with a better sync level, it synchronises itself with the base station that has the strongest signal. If it does not see any base station with a higher sync level, it cannot synchronise.

- ▶ Mark the **LAN Master** check box, if the base station should act as LAN master.

If synchronisation via LAN is used, there must be one base station acting as LAN master.
Currently the LAN master can only be configured on DECT level 1.











- ▶ From the **Sync Slave** option menu select whether the base station is to be synchronised via DECT or via LAN. For the Sync master leave this column empty.

7 Provider and PBX profiles

You can use up to ten different VoIP PBX (Telephony Server) or VoIP provider profiles, e.g.

- OpenScape Business (1 profile)
- OpenScape 4000 (1 profile per IP GWY)
- OpenScape Voice (1 profile)

► **Settings** ► **Provider or PBX profiles**


Provider or PBX profiles		
	Name	Domain
1	 IP1	Not configured
2	 IP2	Not configured
3	 IP3	Not configured
4	 IP4	Not configured
5	 IP5	Not configured
6	 IP6	Not configured
7	 IP7	Not configured
8	 IP8	Not configured
9	 IP9	Not configured
10	 IP10	Not configured

The page lists the available VoIP connections.

Name The name that you have defined for the connection is displayed, or the default name (IP1 - IP10). It can be edited (→ p. 40).

Domain Domain part of the user address. In the case that a connection is not used **Not configured** is displayed.

Configuring provider and/or PBX profiles

- Click on  next to the name of the VoIP connection you want to edit . . . the provider/PBX configuration page is opened (→ p. 40).

Provider and PBX profiles

Configuring telephony server profiles

7.1 Configuring telephony server profiles

On this page you can edit the data for the selected telephony server profile.

1. VoIP Provider

Connection name or number ?

General data of your service provider

Domain ?

Proxy server address ?

Proxy server port ?

Registration server ?

Registration server port ?

Registration refresh time ?

Transport protocol ?

SRTP options ?

Secure Real Time Protocol

Accept non-SRTP calls

Connection name or number

- ▶ Enter a name for the provider or PBX profile. This name is shown in the Provider/PBX list. To distinguish between different connections it should specify the respective VoIP service provider.

General provider data

Domain

- ▶ Enter the domain part of the user address (SIP URI). Together with the phone's user name it is used to build the Address Of Record (AOR) or to build a destination out of the dialed number.

Examples:

sip.domain. for john.smith@sip.domain.net
net

10.100.0.45 for 02871913000@10.100.0.45

Proxy server address

The SIP proxy is your VoIP provider's gateway server and the first SIP server, where the device should send SIP requests and expects to receive requests.

- ▶ Enter the IP address or the (fully qualified) DNS name of your SIP proxy server (max. 74 characters, 0 - 9, a - z, A - Z, -, ., _,).

Examples: **10.100.0.45** or **sip.domain.net** or **sipproxy01.domain.net**

Proxy server port

- ▶ Enter the port number of the first SIP server, where the device should send SIP requests and expects to receive requests.

Range: 1-65535; Default: **5060** (for UDP/TCP), **5061** (for TLS)

DNS SRV SIP server redundancy lookup might provide a different server port which is used then.

Registration server

The registration server assigns the public IP address/port number that was used by the phone on registration to your SIP address (username@domain). With most VoIP providers, the registrar server is identical to the SIP server. But it is also possible to address another service for registration of this account.

- ▶ Enter the IP address or the (fully qualified) DNS name of the registration server. (max. 74 characters, 0 - 9, a - z, A - Z, -, ., _,)

Examples: **10.100.0.45** or **sip.domain.net** or **sipproxy01.domain.net**

Registration server port

- ▶ Enter the communication port used on the registrar.

Range: 1-65535; Default: **5060** (for UDP/TCP), **5061** (for TLS)

Registration refresh time

- ▶ Enter the time intervals (in seconds) at which the phone should repeat the registration with the VoIP server (SIP proxy). A request will be sent to establish a session. The repeat is required so that the phone's entry in the tables of the SIP proxy is retained and the phone can therefore be reached. The repeat will be carried out for all enabled VoIP connections.

Values: 1 - 5 digits, > 0; Default: **180** seconds

Transport protocol

- ▶ Select between UDP, TCP and TLS.

UDP (User Datagram Protocol) UDP is a non session-based protocol. UDP does not establish a fixed connection. The data packets ("datagrams") are sent as a broadcast. The recipient is solely responsible for making sure the data is received. The sender is not notified about whether it is received or not.

TCP (Transmission Control Protocol) TCP is a session-based transmission protocol. It sets up, monitors and terminates a connection between sender and recipient for transporting data.

TLS (Transport Layer Security) TLS is a protocol for encrypting data transmissions on the Internet. TLS is a superordinate transport protocol.

SRTP options

Only available if TLS is selected. SRTP (Secure Realtime Protocol) is a security profile to ensure confidentiality, integrity, replay protection and message authentication for audio-visual data transmission over IP-based networks.

Provider and PBX profiles

Configuring telephony server profiles

► Select which calls should be accepted:

Secure Real Time Pro-Security is activated for voice connections.

toctol

Accept non-SRTP calls Insecure calls are accepted even when SRTP is activated.

Redundancy settings

Redundancy

Redundancy - DNS query ?

Failover Server

Enable registration Yes No

Registration server ?

SIP server port ?

Redundancy - DNS query

VoIP providers provide SIP server redundancy for load balancing and service reliability. SIP servers can be identified by DNS using different queries:.

A Records just the specified IP addresses and the related port numbers.

SRV + A Finds an available server port for the specified proxy and registration server. DNS SRV allows a client to only have to know what type of service it is looking for instead of the actual server.

Failover server

If **Redundancy - DNS query** = A

In case your provider supports a failover server you can enter the data here.

► Enable/disable the use of a failover server via the radio boxes next to **Enable registration**.

Registration server

► Enter the IP address or the (fully qualified) DNS name of the failover registration server.


SIP server port


► Enter the communication port used on the failover registrar.

Range: 1-65535; Default: **5060** (for UDP/TCP), **5061** (for TLS)


Network data of the service provider

Network data of your service provider

Outbound proxy mode 

Outbound server address 

Outbound proxy port 

SIP SUBSCRIBE for Net-AM MWI  Yes No

Outbound proxy mode

The DECT IP multicell system allows you to configure an outbound proxy. Despite of any other SIP protocol rules, if activated (**Always**), the system will always send all outgoing requests towards this outbound proxy. It can be an outbound proxy in the local network provided by the local network provider or in the public network provided by the network/VoIP provider.

► Specify when the outbound proxy should be used.

Always: All signalling and voice data sent by the system is sent to the outbound proxy.

Never: The outbound proxy is not used.

If the further outbound proxy configuration is identical to the proxy and registrar configuration it is useless and will be ignored.



The DHCP option 120 "sip server" sent by a SIP phone would internally overrule the outbound proxy address and port setting. **Outbound proxy mode** is still and exclusively in the hands of the local device administrator. By setting **Outbound proxy mode** to **Never**, you can prevent any usage of DHCP option 120 by the DECT VoIP phone. To allow for DHCP option 120, you should set **Outbound proxy mode** to **Always**.

Outbound server address

This is the address, where the device should send all SIP requests to and where (in case of successful registration) it expects to receive requests from.

► Enter the (fully qualified) DNS name or the IP address of your provider's outbound proxy.

Example: **10.100.0.45** or **sip.domain.net** or **sipproxy01.domain.net**

If the **Outbound server address** field is empty, the system behaves independently of the selected mode, as with **Outbound proxy mode = Never**.

Outbound proxy port

This is the port number of the outbound proxy server, where the device should send all SIP requests to (and where it in case of successful registration expects to receive requests from)

► Enter the communication port used by the outbound proxy.

Range: 1-65535; Default: **5060** (for UDP/TCP), **5061** (for TLS)

Outbound proxy port is empty and **Outbound server address** is a name:

Provider and PBX profiles

Configuring telephony server profiles

The RFC3263 rules will be used to locate SIP servers and select them for load balancing and redundancy.

Outbound proxy port is a fixed number:

The usage of DNS SRV records according to RFC3263 is blocked.

SIP SUBSCRIBE for Net-AM MWI

When activated a subscription is established for the purpose of receiving notifications about new messages on the network mailbox.

▶ Enable/disable SIP subscription via the radio boxes next to **SIP SUBSCRIBE for Net-AM MWI**.

DTMF over VoIP Connections

DTMF signalling (Dual Tone Multi Frequency) is required, for example, for querying and controlling certain network mailboxes via digit codes, for controlling of automatic directory enquiries or for remote operation of the local answering machine.

To send DTMF signals via VoIP, you must define how key codes should be converted into and sent as DTMF signals: as audible information via the speech channel or as a "SIP Info" message.

Ask your VoIP provider which type of DTMF transmission it supports.

DTMF over VoIP Connections

Automatic negotiation of DTMF transmission Yes No

Send settings of DTMF transmission Audio RFC 2833 SIP info

When using G.722 codecs (wideband connection). DTMF signals cannot be transmitted over audio

Automatic negotiation of DTMF transmission

▶ For each call, the phone attempts to set the appropriate DTMF signalling type for the codec currently being negotiated: select **Yes**.

The system will use the transmission method matching best the received capabilities from the peer based on the following priority order:

- send via RFC2833, if PT for telephone event is provided by the peer
- send via SIP INFO application/dtmf-relay, if SIP INFO method is supported by the peer
- send in-band audio

▶ Specify the DTMF signalling type explicitly: select **No** ▶ Select the send settings for DTMF transmission.

Send settings of DTMF transmission

▶ Make the required settings for sending DTMF signals:

Audio or RFC 2833 DTMF signals are to be transmitted acoustically (in voice packets).

SIP Info DTMF signals are to be transmitted as code.

Settings for codecs

The voice quality of VoIP calls is mainly determined by the codec used for the transmission and the available bandwidth of your network connection. A "better" codec (better voice quality) means more data needs to be transferred, i.e. it requires a network connection with a larger bandwidth. You can change the voice quality by selecting the voice codecs your phone is to use, and specifying the order in which the codecs are to be suggested when a VoIP connection is established. Default settings for the codecs used are stored in your phone; one setting optimised for low bandwidths and one for high bandwidths.

Both parties involved in a phone connection (caller/sender and recipient) must use the same voice codec. The voice codec is negotiated between the sender and the recipient when establishing a connection.

Active codecs / Available codecs

The following voice codecs are supported:

G.722 Outstanding voice quality. The G.722 wideband voice codec works at the same bit rate as PCMA/PCMU (64 kbit/s per voice connection) but at a higher sampling rate (16 kHz).

To enable wideband connections via G.722 you have to activate the codec explicitly on the **Telephony – VoIP** page (→ p. 61)

PCMA/(Pulse Code Modulation) Excellent voice quality (comparable with ISDN). The required bandwidth is 64 PCMU kbit/s per voice connection.

PCMA (G.711 a law): Used in Europe and most countries outside of USA.

PCMU (G.711 μ law): Used in USA.

G.729 Average voice quality. The necessary bandwidth is less than or equal to 8 kbit/s per voice connection.
A

Activate/deactivate a codec:

- ▶ Select the required codec from the **Available codecs/Active codecs** list and click on \leftarrow / \rightarrow .

Define the sequence in which the codecs should be used:

- ▶ In the **Active codecs** list select the required codec and click on \uparrow / \downarrow to move it up/down.



Selection of codecs G.722 and G.729 influence the system capacity in direction to lower amount of parallel calls per base station.

Number of parallel calls per base station depending on bandwidth

Codec	Narrow band / wide band	Number of calls
G711	Narrow band	10

Provider and PBX profiles

Configuring telephony server profiles

G729 or G711	Narrow band	8
G722 or G729 or G711	Wide band	5

RTP Packetisation Time (ptime)

Length of time in milliseconds represented by the audio data in one packet.

- ▶ Select the size of RTP packets to send. Select between 10 / 20 / 30 ms.

Signalling options for 'Hold' in Session Description Protocol (SDP)

Call hold means that a user request to put an active call on hold. The holding part sends a re-INVITE request to the held client with an SDP offer (Session Description Protocol). This SDP offer contains the attribute line a=inactive or a=sendonly.

- ▶ Select which attribute should be send in the SDP offer:

inactive The SIP endpoint would neither send nor receive data.

sendonly The SIP endpoint would only send and not receive data.

Hold towards Transfer-Target

The device enables call transfer after consultation or without consultation.

- ▶ Define whether a consultation call with transfer target is put on-hold prior to the execution of the call transfer (**Yes**) or not (**No**).

Display of caller information

Display of Caller Information

Calling Party (User Part) ⊕ PAI+PPI+FROM

- ▶ From the **Calling Party (User Part)** option menu select which information is allowed to be transferred to the receiving part within the SIP header. Which information is actually transferred is determined by the provider.

FROM Only the FROM information can be added.

Caller identity in the form number@server, e.g.:12345678@192.168.15.1

PPI+FROM P-Preferred-Identity (PPI) or FROM can be added

The P-Preferred-Identity header field is used from a user agent to a trusted proxy to carry the identity the user sending the SIP message wishes to be used for the P-Asserted-Header field value that the trusted element will insert.

PAI+PPI+FROM P-Asserted-Identity (PAI) or PPI or FROM can be added

The P-Asserted-Identity header field is used among trusted SIP entities (typically intermediaries) to carry the identity of the user sending a SIP message as it was verified by authentication.

Service Codes

Service Codes

Call Completion on (CCBS, CCNR) *6

Call Completion off (CCBS, CCNR) #6

Service codes are key sequences provided by the provider or PBX in order to activate/deactivate specific functions on the handset. You can set the adequate service codes for activating/deactivating CCBS and CCNR.

CCBS (Completion of Call to busy Sub- Ringback if busy
scriber)

CCNR (Completion of Calls on No Reply) Ringback if no answer
R

- ▶ In the text fields **Call Completion on (CCBS, CCNR)/Call Completion off (CCBS, CCNR)** enter the key sequence for activating/deactivating CCBS and CCNR.
- ▶ Click on **Set** to save the settings of this page.

Provider and PBX profiles

Configuring telephony server profiles

8 Mobile devices

You can use the web configurator to register all handsets on the DECT network and for a VoIP connection. Use the add function of the **Administration** page to register single handsets or use the **Registration Center** to register groups of handsets in one process.

You can edit the settings for handsets, deactivate or delete them and make further settings e.g., for using directories and network services.

8.1 Mobile devices

► Settings ► Mobile devices ► Administration

The screenshot shows the 'Mobile devices' administration interface. It features a search bar with a 'Search in' dropdown and a 'View' button. Below this is a table with the following columns: IPUI, Username, Display name, Location, DECT, SIP, Type, and FW. The table is currently empty. Below the table, there are navigation buttons: 'Previous', '1' (highlighted), and 'Next'. At the bottom of the interface, there are three buttons: '+ Add', 'Copy', and 'Delete'.

The currently registered handsets and place holders for handsets that could be registered are listed on the page with the following information:

IPUI	International Portable User Identity used in order to uniquely identify a handset within the DECT network.										
Username	User name from the SIP account that is assigned to the handset, usually the phone number. The name is displayed on the handsets when they are in idle status.										
Display name	Display name from the SIP account that is assigned to the handset. The display name indicates the originator of the request when the user initiates a call.										
Location	Name of the DECT manager the handset belongs to. Currently, always local										
DECT	DECT registration state of the handset: <table border="0" style="margin-left: 20px;"> <thead> <tr> <th>Status</th> <th>Meaning</th> </tr> </thead> <tbody> <tr> <td>ToReg</td> <td>System ready to register a handset</td> </tr> <tr> <td>NotReg</td> <td>Registration not possible</td> </tr> <tr> <td>InReg</td> <td>Registration in progress</td> </tr> <tr> <td>Registered</td> <td>Handset is registered</td> </tr> </tbody> </table>	Status	Meaning	ToReg	System ready to register a handset	NotReg	Registration not possible	InReg	Registration in progress	Registered	Handset is registered
Status	Meaning										
ToReg	System ready to register a handset										
NotReg	Registration not possible										
InReg	Registration in progress										
Registered	Handset is registered										
SIP	Indicates, if the handset has a working VoIP connection. <table border="0" style="margin-left: 20px;"> <tr> <td>✓</td> <td>A VoIP connection is registered for the handset and a connection has been established successfully.</td> </tr> <tr> <td>✗</td> <td>There is no VoIP connection configured or it is not possible to establish a connection to the configured VoIP provider.</td> </tr> </table>	✓	A VoIP connection is registered for the handset and a connection has been established successfully.	✗	There is no VoIP connection configured or it is not possible to establish a connection to the configured VoIP provider.						
✓	A VoIP connection is registered for the handset and a connection has been established successfully.										
✗	There is no VoIP connection configured or it is not possible to establish a connection to the configured VoIP provider.										
Type	Model designation of the handset.										

Mobile devices

Registering/de-registering handsets

FW Current firmware version of the handset.

8.1.1 Actions

Adding a handset to the list

▶ Click on **Add** . . . the mobile devices data page is opened (→ p. 50).


Copying handset data for another configuration

▶ Select the check box next to the handset whose settings you want to copy. ▶ Click on **Copy** . . . the mobile devices data page is opened (→ p. 50). The settings of the selected mobile device except personal data are taken over for the new handset configuration.

Deleting a handset from the list

▶ Select the check box next to the handset you want to delete. Multiple choice is possible. ▶ Click on **Delete** ▶ Confirm with **Yes** . . . all selected handsets are deleted.

Editing the data of a handset

▶ Click on  next to the handset you want to edit . . . the mobile devices data page is opened (→ p. 50).

8.2 Registering/de-registering handsets

The page allows you to register a handset with the DECT multicell network or to prepare the registration of numerous handsets via the Registration Center. You can assign a VoIP account, enable online directories, and make further settings for the handsets.

8.2.1 Registering handsets

- ▶ Enter an IPUI, if you want to restrict the registration to a specific handset.
- ▶ Enter an authentication code manually or generate it via the **Generate random PIN** button.
- ▶ Enter all configuration data for the handset.
- ▶ Click on **Register now**.

The handset with the matching IPUI is now allowed to register. If no IPUI is defined all handsets within range can register.



The system stays in registration mode as long as it is defined via the **Registration duration** parameter on the **Registration Center** page (→ p. 57). Default: 3 min.

On the handset

- ▶ Start the registration procedure as described in the appropriate documentation. ▶ When prompted, enter the PIN that has been entered or generated.

Registering a set of handsets

You can register a set of handsets without restarting the registration mode. Prepare registration for new mobile devices as follows:

- ▶ Enter the actual IPUI and maybe an individual PIN

or

- ▶ Use wildcards as IPUI (0_1, 0_2, 0_3 ...) and preferably the same PIN for all handsets.
- ▶ Set the **RegStatus** of the handsets to **To register**
- ▶ Open the registration window for a desired time and register all handsets without further Web UI interaction via the **Registration Center** (→ p. 57).

Parameters

Mobile device

IPUI ?

RegStatus ? Not registered ▼

Authentication Code (PIN) ? Entry is required

🔀 Generate random PIN

IPUI

(International Portable User Identity) Unique identifier of a handset within the DECT network. If you edit an existing handset registration entry, the IPUI is shown and cannot be changed.

For a new entry:

- ▶ Enter the IPUI of the handset that should be allowed to register with the DECT network in the text field.

If the field is empty, any handset will be allowed to register.

RegStatus

DECT registration status of the handset entry. The option menu allows you to change the status.

Status	Meaning / possible action to change the status
To register	The system is ready to register a handset using these settings. ▶ Select Not registered to disable registration.
Not registered	No registration possible. ▶ Select To register to allow a handset to register using these settings.
In registration	Registration in progress. ▶ Select Not registered to cancel the running registration process.
Registered	The handset is registered. ▶ Select To deregister to de-register the handset.

Authentication Code (PIN)

This PIN must be used on the handset to register with the DECT network.

- ▶ Enter a PIN in the text field. Value: min. 1, max. 4 digits


or

- ▶ Click on **Generate random PIN** . . . a four-digit PIN is generated and shown in the text field.

Mobile devices

Registering/de-registering handsets

8.2.2 De-registering handsets

- ▶ In the handset list click on  next to the handset you want to de-register. The status is **Registered**.
- ▶ From the **RegStatus** option menu select **To deregister**. ▶ Click on **Set . . .** the handset is de-registered.

DECT de-registration successful: The handset is deleted from the **Mobile devices** list.

DECT de-registration not successful: The handset stays in the **Mobile devices** list with status **To deregister**.

In the handset list an empty entry in **To register** status is shown. As long it is not deleted, you can re-register the handset (or any handset if no IPUI is given) via the **Mobile devices** the edit page or the Registration Center.


8.2.3 Settings for the handset


When registering a handset you can define important settings and assign functions at the same time.


Personal provider data


Personal provider data

A separate SIP connection must be assigned to each handset.


Authentication name 

Authentication password 

Username 

Display name 

VoIP provider

Configure the VoIP account for the handset. If the handset is successfully registered,  will be shown in the **SIP** column in the **Mobile devices** list.



The VoIP/PBX account must be set-up beforehand (→ p. 40).

VoIP provider

- ▶ Choose a configured VoIP PBX/provider from the option menu.
The connection must be configured on the **Provider or PBX profiles** page (→ p. 40).
- ▶ Enter the access data for the VoIP account in the relevant fields. These fields may vary depending on the PBX/provider profile.

Authentication name

- ▶ Specify the SIP authentication (HTTP digest) name. The **Authentication name** acts as access ID when registering with the SIP proxy/registrar server. It is usually identical to the phone number for the VoIP account. Value: max. 74 characters

Authentication password

- ▶ Enter the password for SIP authentication (HTTP digest). The phone needs the password when registering with the SIP proxy/registrar server. Value: max. 74 characters

Mobile devices

Registering/de-registering handsets

Username

- ▶ Enter the caller ID for the VoIP provider account. It is usually identical to the phone number for the VoIP account.
Value: max. 74 characters

Display name

The display name is used for presentation of the caller's name. In rare cases SIP networks check the display name for any local policy of the SIP network.

Usually, the display name is optional.

- ▶ Enter any name that should be shown for the caller on the other participant's display.
Value: max. 74 characters

If **Display name** is empty, the **Username** or the phone number will be used.

Online directories

The user can call up various directories using the handset control or INT key.

Online directories	
Directory for direct access ⓘ	Online directories ▼
Corporate directory for INT key ⓘ	▼
Automatic look-up ⓘ	Deactivated ▼

Directory for direct access

The user can press and hold the directory key (bottom of the control key) to open either the list of online directories or the local directory of the handset.

- ▶ Choose which directory is called up with the directory key.

Online directories A list of online directories is opened via the directory key.
The online directories must be set-up beforehand (→ p. 63)

Local directory The local directory is opened via the directory key..

Corporate directory for INT key

If a corporate directory is available and configured the user can open it by pressing the INT key (left on the handset's control key).

- ▶ Choose from the list which corporate directory is opened with the INT key.

Automatic look-up

- ▶ Select an online directory from the list for **Automatic look-up** or deactivate this option. When there is an incoming call, the caller's name is read from this directory and shown in the display (the availability of this function depends on the online directory provider).

LDAP authentication

Up to 10 directories in LDAP format can be provided by the phone system. The access to a corporate directory can be provided individually for specific handsets.

LDAP authentication

To authenticate mobile devices individually, activate this function in online directory settings.

Selected LDAP book

Show other LDAP servers Yes No

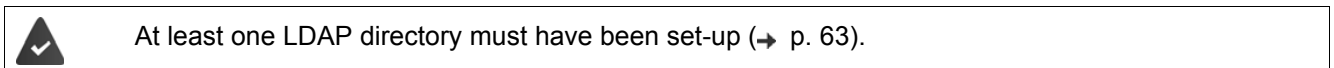
LDAP authorization type

Username

Password

Selected LDAP book

- ▶ Select the LDAP directory to be provided on the handset from the option menu.



Show other LDAP servers

- ▶ Select **Yes** if directories of other LDAP servers should be shown.

LDAP authorization type

- ▶ Select how the user authentication should be performed:

Global Credentials are set for all handsets during the LDAP directory set-up.

User Individual credentials are used.

- ▶ Enter **Username** and **Password** in the appropriate text fields.

SIP The credentials for the user's SIP account are used (**Authentication name** and **Authentication password**).

Network mailbox configuration

If a network mailbox is available for the VoIP account assigned to the handset, you have to activate this function.

Network mailbox configuration

Call number or SIP name (URI)

Activate network mailbox

Mobile devices


Registering/de-registering handsets

- ▶ Enter the **Call number or SIP name (URI)** for the network mailbox.
- ▶ Activate the function via the check box.

Group pick-up

Group pick-up enables a user to accept a call for another subscriber, e.g., a pick-up group. Users belonging to the same call pick-up group can accept all calls for the group. A pick-up group must be established during SIP account registration. The call number or the SIP URI of a pick-up group can be assigned to the mobile device.

Group pick-up


Call number or SIP name (URI) 

 Activate group pick-up

- ▶ Enter the **Call number or SIP name (URI)** of the pick-up group.
- ▶ Activate the function via the check box.

Call manager

Call manager


Accept calls directly via Call Manager 


- ▶ From the **Accept calls directly via Call Manager** option menu select whether calls that are transferred via the PBX call manager are to be accepted directly **via Headset, via Handsfree** or not at all (**No**).


Missed calls and alarms


You can define if missed and accepted calls should be counted and if new messages of specific types should be indicated via the MWI LED on the handset's message key.

Missed calls and alarms

Missed/accepted calls count  Yes No

Flashing LED (MWI) for missed calls  Yes No

Flashing LED (MWI) for missed alarms  Yes No

Flashing LED (MWI) for network mailbox  Yes No

- ▶ Select **Yes/No** next to **Missed/accepted calls count**, to activate/deactivate the call counter for missed and accepted calls. The information is displayed in the handset's call lists, missed calls are also shown on the handset's idle display.

- ▶ Select **Yes/No** next to the message type (missed calls, missed alarms, new message on the network mailbox), to activate/deactivate the MWI LED for the message type.

If **Yes** is selected, the message key will flash, if a new message of the selected types is received.

8.3 Handset Registration Centre

The registration centre allows you to register groups of handsets in one registration process. All handsets which are listed in the mobile devices list and have the registration status **To register** or **Registering** can be registered together.

- ▶ **Settings** ▶ **Mobile devices** ▶ **Registration Center**

Mobile devices

with RegStatus: "To register" ?	0
with RegStatus: "Registering" ?	0
Total ?	0

DECT managers

with Registrations Window open	0
Total	1

Current time ? 2017-08-30 16:05:26

Registration start time ?

Registration duration ?

d

h

min

s

The page shows the number of mobile devices in registration status **To register**, **Registering** and the total number of entries in the mobile devices list, including those in registration status **Registered** and **Not registered**.

Mobile devices

Handset Registration Centre



The page also shows the DECT managers that currently are ready to register handsets. As this version only supports the use of one DECT manager, the information is not meaningful at present.

8.3.1 Registering handsets time-controlled

Shows the current system time. Time settings: → p. 81

- ▶ In the **Registration start time** field enter the time when the next registration process should be started. Format: YYYY-MM-DD HH:mm.
- ▶ Click on **Start now**. . . . the DECT manager starts a registration process at the given time. If no time is set, the DECT manager will start registration at once.

Setting the registration duration

- ▶ In the **Registration duration** fields determine how long (days, hours, minutes and seconds) the DECT manager should stay in registration mode. Default: 3 min.

Closing the window and resetting the timers

- ▶ Click on **Close** . . . the registration window is closed, the time settings are reset.



When the first handset tries to register, the base closes the registration window and finalises the registration within a very few seconds. During this time any second handset registration attempt would be rejected. When the first handset is fully registered the base re-opens the registration window as long as defined with the **Registration start time** and **Registration duration** parameters. If all handsets try to register in parallel, a lot of them will enter the base one by one and so will be successfully registered, but others might enter while another registration is not yet completed and so they will be rejected. Single handsets that are rejected have to be registered by a new registration procedure or manually.

9 Telephony settings

9.1 General VoIP settings

► Settings ► Telephony ► VoIP

SIP

SIP port [?](#)

Secure SIP port [?](#)

SIP timer T1 [?](#) ms

SIP session timer [?](#) s

Failed registration retry timer [?](#) s

Subscription timer [?](#) s

PRACK [?](#)

SIP security certificate [?](#) File not uploaded

» Certificate

» Private key

SIP security password [?](#)

Quality of Service (QoS)

SIP ToS / DiffServ [?](#)

RTP ToS / DiffServ [?](#)

Telephony settings

General VoIP settings

This page allows you to make some general settings for the VoIP connections.

SIP port

- ▶ Enter the SIP port used for VoIP connections.

Range: 1-65535; Default: 5060

Secure SIP port

- ▶ Enter the SIP port used for secure VoIP connections (TLS).

Range: 1-65535; Default: 5061

SIP timer T1

- ▶ Enter the estimated round trip time of an IP packet between a SIP client and a SIP server (the time it takes between sending out the request to the point of getting a response).

Default: 500 ms

SIP session timer

- ▶ Defines a session expiry interval: If the session isn't refreshed within the interval, the session is released. Session refresh is started after half of the interval by a re-INVITE message, which the peer side has to confirm to get the session refreshed.

Values: max. 4 digits, min. 90 sec; Default: 1800 sec;

Failed registration retry timer

- ▶ Specify after how many seconds the phone should attempt to reregister when the initial registration has failed.

Values: max. 4 digits, min. 10 sec; Default: 300 sec;

Subscription timer

- ▶ Defines the expiration time (in seconds) of a subscription. In order to keep subscriptions effective, subscribers need to refresh subscriptions on a periodic basis.

Default: 1800 s

PRACK

- ▶ (Provisional Response Acknowledgement) SIP provisional responses do not have an acknowledgement system so they are not reliable. The PRACK method guarantees a reliable and ordered delivery of provisional responses in SIP.

Security settings

The phone system supports the establishment of secure voice connections over the internet via TLS certificates. Thereby, public and private keys are used to encrypt and decrypt the messages that are exchanged between SIP entities. The public key is contained within the certificate of an IP entity and is available for everyone. The private key is kept secret and is never revealed to anyone. The server certificate and the private key must be uploaded to the base stations.

- ▶ Click on **Browse...** and choose the file containing the certificate or the private key from the file system of your computer or network ▶ click on **Upload** . . . the file is uploaded and shown in the appropriate list.

SIP security password

- ▶ If your private key is protected by a password, enter it here.

Quality of Service (QoS)

The voice quality depends on the priority of the voice data in the IP network. Prioritising the VoIP data packets is done using the QoS protocol DiffServ (Differentiated Services). DiffServ defines a number of classes for the quality of service and, within these classes, various priority levels for which specific prioritisation procedures are defined.

You can specify different QoS values for SIP and RTP packets. SIP packets contain the signalling data, while RTP (Real-time Transport Protocol) is used for the voice transfer.

▶ Enter your chosen QoS values in the **SIP ToS / DiffServ** and **RTP ToS / DiffServ** fields. Value range: 0 - 63.

Common values for VoIP (default setting):

SIP	34	High service class for fast switching of the data flow (Expedited Flow)
RTP	46	Highest service class for fast forwarding of data packets (Expedited Forwarding)



Do not change these values without consulting your network operator first. A higher value does not necessarily mean a higher priority. The value determines the service class, not the priority. The prioritisation procedure used in each case meets the requirements of this class and is not necessarily suitable for transferring voice data.

9.2 Audio quality

The phone system allows the user to make calls with excellent voice quality using the wideband codec G.722. One base station enables a maximum of five wideband calls.

▶ **Settings** ▶ **Telephony** ▶ **Audio**

Audio

Enabling or disabling the G.722 codec will restart the system. Connections with mobile devices will be terminated.

One base station enables a maximum of 5 wideband calls.

Wideband with codec G.722

The page allows you to enable/disable the use of the wideband codec G.722 for the telephone system.

- ▶ Mark/unmark the check box to enable/disable wideband calls
- ▶ Click on **Set** to save the settings of this page.



To allow users to make wideband calls, the codec G.722 must have been activated for the provider profile that is used for the connection (→ p. 45).

Telephony settings

Call settings

9.3 Call settings

On this page you can make advanced settings for VoIP connections.

► **Settings** ► **Telephony** ► **Call settings**

9.3.1 Call transfer

Participants can transfer a call to another participant as long as the PBX/provider supports this function. The call is transferred using the handset menu (via the display key) or using the R key. You can expand or change the settings for call transfer.

Call Transfer

Call transfer via R key ? Yes No

Transfer call by on-hook ? Yes No

Determine target address ? From transfer target's AOR
 From transfer target's transport address

Call transfer via R key

Activated: Users can connect two external callers with each other by pressing the R key. The connections with both parties are terminated.

Transfer call by on-hook

Activated: The two participants are connected with one another when the user presses the end call key. The intermediary's connections with the participants are terminated.

Determine transfer target address

► Select how the transfer target address (Refer-To URI) is to be derived:

From transfer target's AOR (Address of Record)

From transfer target's transport address (Contact URI)

Most common PBX platforms show good results by using the AOR as transfer target address.

In case there are problems with transfer especially via transparent proxies, rather than call switching PBX, it might be worth to test with transfer target address derived from transfer target's transport address.

9.3.2 Access Code

You may have to enter an access code for external calls (external prefixes e.g., "0"). You can save this access code in the DECT manager configuration. These settings apply to all registered handsets.

Access Code

Access Code ?

is added to numbers ?

From incoming calls list

From network directory

Always

- ▶ Enter an access code in the **Access Code** text field. Value: max. 3 digits (0 – 9, *, R, #, P)
- ▶ Select when the phone numbers should be automatically prefixed with the digits, e.g. when dialling from a call list or a directory.

9.3.3 Area Codes

If you use VoIP to make a call to the fixed line, you may also have to dial the area code for local calls (depending on the provider).

Area Codes

Country ?

International

Prefix ?

Area code ?

Local

Prefix ?

Area code ?

You can set your telephone system so that the access code is automatically predialled when any VoIP call is made in the same local area, and also for national long-distance calls. This means that the access code is set before all phone numbers that do not start with 0 – even when dialling numbers from the directory and other lists.

Telephony settings

Call settings

You can change these settings if required.

Country

- ▶ From the option menu select the country or region where your telephone system is to be used . . . the international and national prefix is then entered in the **Prefix** and **Area code** fields.

International settings

Prefix Prefix of the international area code. Value: max. 4 digits, 0-9

Area code International area code. Value: max. 4 digits, 0-9

Example „Great Britain“: **Prefix** = 00, **Area code** = 44

Local settings

Prefix Prefix of the local area code. Value: max. 4 digits, 0 - 9. These digits are placed in front of the local area code for national long-distance calls.


Area code Local area code for your town/city (depending on country/provider). Value: max. 8 digits, 0-9

Example „London“: **Prefix** = 0, **Area code** = 171

9.3.4 Tone Selection

Tones (e.g., dialling tone, ring tone, busy tone or call waiting tone) vary from one country or region to another. You can choose from various tone groups for your telephone system.

Tone Selection

Tone scheme  Austria ▼

Tone scheme

- ▶ Select the country or region whose ring tones are to be used for your phone from the option menu.

10 Online directories











You can set up up to ten corporate directories in LDAP format for the phone system and make one of them available to the registered handsets.

Use the handset settings (→ p. 52) to specify which keys are to call up the directory.

10.1 Corporate online directory (LDAP)

If you wish to use a company directory on the telephone system, you must activate it on the Web configurator.

► **Settings** ► **Online directories** ► **Corporate**


LDAP directory		
	Name	Server url
1	 LDAP 1	
2	 LDAP 2	
3	 LDAP 3	
4	 LDAP 4	
5	 LDAP 5	
6	 LDAP 6	
7	 LDAP 7	
8	 LDAP 8	
9	 LDAP 9	
10	 LDAP 10	

The page lists the available LDAP directories.

Name The name that you have defined for the directory is displayed, or the default name (LDAP1 - LDAP10). It can be edited (→ p. 65).

Server url If the directory is configured, the server URL is displayed.

Configuring LDAP directories

► Click on  next to the name of the LDAP directory you want to edit . . . the LDAP configuration page is opened (→ p. 65).

Configuring an LDAP directory

On this page you can edit the data for the selected LDAP directory.







Online directories

Corporate online directory (LDAP)

Access to the LDAP data server

The directory is provided via an LDAP server. You need the server address, the server port and the access data for the directory that you wish to use.

Access to the LDAP data server

Directory name 	<input type="text" value="LDAP 1"/>
	<input checked="" type="checkbox"/> Enable directory
Server address 	<input type="text"/>
Server port 	<input type="text" value="389"/>
LDAP Search base (BaseDN) 	<input type="text" value="0"/>
Username 	<input type="text"/>
Password 	<input type="password"/>

- ▶ Enter a name in the **Directory name** field (max. 20 characters). This is the name under which the directory will be displayed on the handsets.
- ▶ Mark the **Enable directory** option, so that the directory is displayed on the telephones.

Server address / Server port

- ▶ Enter the URL of the LDAP server and the port the LDAP server expects database requests (Default: 389)

LDAP Search base (BaseDN)

- ▶ The LDAP database is hierarchical in design. With the **LDAP Search base (BaseDN)** parameter, stipulate in which area the search should begin.
Default: 0, the search starts at the upper area of the LDAP database.

User access data

If you want to define access data that have to be used by all users:

- ▶ Enter the access data for the LDAP directory in the **Username** and **Password** fields (max. 254 characters each).

If you want to use individual access data for each handset, the access data is to be set during the handset configuration (→ p. 52).

10.1.1 Settings for searching the LDAP database and displaying the result

Search in LDAP database

Enable list mode ?

Name filter ?

Number filter ?

Additional filter #1 name ?

Additional filter #1 value ?

Additional filter #2 name ?

Additional filter #2 value ?

Display format ?

Max. number of search results

Enable list mode

► Define what should be initially shown, when the user opens the LDAP directory.

Activated: A list of all entries of the LDAP directory is shown.

Not activated: An editor is opened first that allows the user to select a specific search area within the LDAP database and thereby to reduce the number of entries.

Filters

Using the filters, you can define criteria against which specific entries can be searched in the LDAP database. One filter consists of one or more search criteria. A search criterion contains the query for an LDAP attribute.

Example: sn=%

The **sn** attribute stands for surname. The percent sign (%) is a place holder for the user entry.

Rules for defining filters:

- Multiple criteria can be connected using logical AND (&) and/or OR (|) operators.
- The logical operators "&" and "|" are placed before the search criteria.
- The search criterion must be placed in brackets and the whole expression must be terminated with a bracket again.
- AND and OR operations can be combined.

Online directories

Corporate online directory (LDAP)

Examples:

AND operation: (& (givenName=%) (mail=%))

Searches for entries in which the first name **and** mail address begin with the characters entered by the user.

OR operation: (| (displayName=%) (sn=%))

Searches for entries in which the display name **or** surname begins with the characters entered by the user.

Combined operation: ((& (displayName=%) (mail=%))(& (sn=%) (mail=%)))

Searches for entries in which the display name **and** mail address **or** the surname **and** mail address begin with the characters entered by the user.

Information on attributes → p. 69

Name filter

The name filter decides which attribute is used for the search.

Example:

(displayName=%). The percent sign (%) is replaced by the name or part of the name entered by the user.

If a user enters the letter "A", for example, all entries in which the attribute **displayName** begins with "A" are searched for in the LDAP database. If the user then enters a "b", entries are searched in which the **displayName** begins with "Ab".

Number filter

The number filter stipulates the criteria for the automatic completion of telephone numbers.

Example:

((telephoneNumber=*)(mobile=*)). The percent sign (%) is then replaced by the part of the telephone number entered by the user.

When dialling, if a user enters the numbers "123", for example, all telephone numbers that begin with "123" are searched for in the LDAP database. The telephone number is completed with the addition of information from the database.

Additional filters

You can set two additional filters that will be offered to the user in order to specify the search more detailed.

- ▶ In the additional name fields enter the attribute name.
- ▶ In the corresponding value fields enter the attribute values.

Example:

Additional filter #1 name	City
Additional filter #1 value	((l=*))
Additional filter #2 name	Street
Additional filter #2 value	((street=*))

In addition to the fields defined in the **Name filter** parameter, the **City** and the **Street** fields are provided to the user. The user input for **City** is passed to the LDAP server in the **l** attribute, the user input for **Street** is passed in the **street** attribute.

Display format

In the **Display format** field you can stipulate how the search result is to be displayed on the handset.

- ▶ Enter combinations of different name and number attributes and special characters. You can select common formats from the attributes that are listed in the **Configuration of directory items** section of the page.

For the attribute values to be shown for the required attribute, the attribute name must be preceded by a percent sign (%).

Example:

Data of an directory entry on the LDAP server:

displayName	Peter Black	telephoneNumber	0891234567890
givenName	Peter	mobile	012398765432
sn	Black		

...

Attribute definition in the Web configurator:

Display format %sn, %givenName; %telephoneNumber/%mobile

The entry is shown on the handset as follows:

Black, Peter; 0891234567890/012398765432

Max. number of search results

- ▶ Enter the maximum number of search results that is to be returned by one search operation.

10.1.2 Attributes

A range of attributes are defined in the LDAP database for a directory entry, e.g. surname, first name, telephone number, address, company, etc. The quantity of all attributes which can be saved in one entry is stored in the relevant LDAP server scheme. In order to be able to access attributes or define search filters, you must know the attributes and their designation in the LDAP server. The majority of attribute designations are standardised, however specific attributes can also be defined.

Online directories

Corporate online directory (LDAP)

Configuration of directory items

First name	<input type="text"/>
Surname	<input type="text"/>
Phone (home)	<input type="text"/>
Phone (office)	<input type="text"/>
Phone (mobile)	<input type="text"/>
E-mail	<input type="text"/>
Fax	<input type="text"/>
Company	<input type="text"/>
Street	<input type="text"/>
City	<input type="text"/>
Zip	<input type="text"/>
Country	<input type="text"/>
Additional attribute	<input type="text"/>

Additional attribute can be dialled 

► For each field of a directory entry that should be displayed on the handsets enter the name of the corresponding LDAP attribute. Multiple attributes can be separated by commas.

Examples:

Field of a directory entry	Attribute name in the LDAP database
First name	givenName
Surname	sn, cn, displayName
Phone (home)	homePhone, telephoneNumber
Phone (office)	telephoneNumber
Phone (mobile)	mobile

Field of a directory entry	Attribute name in the LDAP database
E-mail	mail
Fax	facsimileTelephoneNumber
Company	company, o, ou
Street	street
City	l, postalAddress
Zip	postalCode
Country	friendlyCountryName, c
Additional attribute	user-defined

- ▶ Mark the check box **Additional attribute can be dialed**, if an additional attribute is defined and it is a phone number.

Online directories

Corporate online directory (LDAP)

11 System settings

11.1 Web configurator access rights

On this page you define the access rights for the web configurator user interface.

▶ **Settings** ▶ **System** ▶ **Web configurator**

11.1.1 Changing the web configurator password


For security reasons, you should frequently change the admin password for web configurator access.

Change password

New password (Admin) ?

Repeat password ?

Show password ?

 If you have forgotten the password, you will have to reset the device to the factory settings (→ p. 15).

New password (Admin)

▶ Enter a new password for the administrator access to the web configurator. Default: **admin**

Repeat password

▶ Repeat the new password entered in the **New password (Admin)** field.

Show password

▶ To view the entered characters mark the check box near **Show password**.


System settings


Web configurator access rights

11.1.2 Enabling CLI access to the device configuration


It is possible to perform the device configuration via CLI (Command Line Interface) using SSH from a remote system. Secure Shell (SSH) is a program for logging into a remote machine and for executing commands on a remote machine. It provides secure encrypted communications between two untrustworthy hosts over an insecure network.

CLI access via ssh

Activated if password is longer than 7 characters 

CLI Password (Admin) 

Repeat password

Show password 

Detailed information on CLI commands can be found in the online help of the web configurator.


Activated if password is longer than 7 characters

The CLI access is automatically enabled if you have entered a valid password that has more than seven characters and click on the **Set** button. ✓ = enabled; ✗ = disabled

CLI Password (Admin)

- ▶ Enter a password for the administrator access to the configuration via SSH. Value: min. 8, max. 74 characters

Repeat password

 The user name for the CLI access is **cli**.

- ▶ Repeat the new password entered in the **CLI Password (Admin)** field.

Show password

- ▶ To view the entered characters mark the check box next to **Show password**.

11.2 Loading the web security certificate


The web configurator is protected by SS L/TLS security mechanism. That means that data transfer is encrypted and that the website is identified to be who it claims to be. The Internet browser checks the security certificate to determine that the site is legitimate. The certificate may be updated from time to time. If a new certificate is available you can download it to your computer or network and then upload it to the device.

Web security certificate

Web security certificate

File not uploaded

 Delete


 Browse...

- ▶ Click on **Browse...** next to **Web security certificate** and select the local certificate file from your computer's file system ▶ click on **Upload...** the selected certificate file is loaded and added to the certificate lists.

11.3 Capacity licensing

- ▶ **Settings** ▶ **System** ▶ **Capacity licensing**

Capacity licensing				
Product Name	Item under Licensing	Available Licenses	Used Licenses	Status
OpenScape Cordless IP V2	Base License	-	1	Grace period. Days left: 30
OpenScape Cordless IP V2	Dect Managers	1	1	Grace period. Days left: 30

 Refresh

Deployment

Licensing type

Address

The page shows the licences that currently are used from the system with the following information:

Product Name	Name of the product that is licensed
Item under Licensing	Base License: License for one DECT manager in a small deployment Further DECT manager licenses can be added. In case of a small deployment the DECT manager line is greyed out.
Available Licenses	Number of licenses that can temporarily be used. If a system is booted the first time, a grace period of 30 days enters into force in which the license must be activated.
Used Licenses	Number of licenses that are currently used. This can be activated licenses or licenses in grace period.
Status	SIEL-ID: % % stands for the license ID of an activated license.

System settings
Capacity licensing

Grace period. Days left: %	License in grace period. % stands for the number of days that are still left to activate the license.
Grace period - expired	The grace period has expired. Making calls is no longer possible.

11.3.1 Renewing licenses

You can request for a new license during the grace period or change the request after licenses are already uploaded.

Deployment

- ▶ Select the desired deployment for the license (**Small, Medium**)



If the deployment is changed from **Small** to **Medium**:

- The local base station of the DECT manager will be deactivated.



If the local base station is on sync level 1, you should change your synchronisation configuration at first. If the base station on sync level 1 is deactivated, your system may no longer work properly.

If the deployment is changed from **Medium** to **Small**:

- The capacity is limited to maximum 9 base stations and 50 handsets.
- The local base station of the DECT manager will be reactivated.

Changing from **Medium** to **Small** is not possible, if

- the number of connected external base stations is greater than 9
the number of handsets is greater than 50.

Licensing type

The license is provided by a remote license server.

- ▶ Select **Remote CLA** (CLA = Contributor License Agreement).
- ▶ Enter the address (URI) of the remote license server.

At present, **Local CLA** is not supported.

Updating the license

- ▶ Click on **Refresh** . . . the license is updated based on the license server

11.4 Provisioning and configuration

Provisioning is the process for uploading the necessary configuration and account data to the VoIP phones (here the DECT bases). This is done by means of profiles. A profile is a configuration file that contains VoIP phone-specific settings, VoIP provider data as well as user-specific content. It has to be available on an HTTP provisioning server which is accessible in the public (Internet) or local network.

Auto-configuration is defined as the mode of operation by which the telephone system connects automatically to a server and downloads both provider-specific parameters (such as the URL of the SIP server) and user-specific parameters (such as the user name and password) and stores them in its non-volatile memory. Auto-configuration is not necessarily limited to the parameters required for doing VoIP telephony. Auto-configuration can also be used to configure other parameters, e.g. settings for online service, if the VoIP phones support these features. However, for technical reasons auto-provisioning is not possible for all configuration parameters of the phone.

► Settings ► System ► Provisioning and configuration

Provisioning and configuration

Provisioning server

Auto configuration file

This page allows you to define the provisioning server for the telephone system or download a configuration file and to start an auto-configuration process.

Provisioning server

► Enter the URL of your provisioning server in the text field. Value: max. 255 characters

Auto configuration file

If you have received a configuration file from your provider, you download it to the phone system.

► Click **Browse...** and select the configuration file from your computer's file system ► click on **Upload** . . . the selected configuration file is loaded.

Start auto configuration

► Click on the button . . . the provisioning profile is downloaded and installed on the system.



The process will take some time and requires a system restart. Connections with mobile devices will be terminated.

For security reasons you should save the configuration before you start an auto-configuration process (→ p. 84).

11.5 Security

The page allows you to organise the certificates used for secure internet communication and to define the credentials for HTTP authentication.

► **Settings** ► **System** ► **Security**

Certificates

The phone system supports the establishment of secure data connections on the Internet with the TLS security protocol (Transport Layer Security). With TLS, the client (the phone) uses certificates to identify the server. These certificates must be stored on the base stations.

The screenshot shows the 'Certificates' configuration interface. At the top, there's a section for 'Accept all certificates' with two radio buttons: 'Yes' and 'No' (which is selected). Below this are three main sections: 'Server certificates', 'CA certificates', and 'Invalid certificates'. Each section contains a list of certificates. In the 'Server certificates' list, one certificate is visible: 'Unify Production Default Certificate', which has a green 'Accepted' label. To the right of each list are 'Remove' and 'Details' buttons. At the bottom of the page, there is an 'Import local certificate' section with a 'Browse...' button.

Accept all certificates

► Mark the **Yes** radio button, If you want to accept all certificates.

Server certificates / CA certificates

The lists contain the server certificates or CA certificates that have been certified by a certification authority (CA). The certificates in both lists have already been implemented by default or have been downloaded via the Web configurator and are classed as valid, i.e., have been accepted.

If one of the certificates becomes invalid, e.g., because it has expired, it is transferred to the **Invalid certificates** list.

Invalid certificates

The list contains the certificates that have been received from servers but have not passed the certificate check, and certificates from the **Server certificates / CA certificates** lists that have become invalid.

System settings

Security

Accepting / rejecting invalid certificates

Accepting a certificate:

- ▶ Select the certificate and click on the **Accept** button . . . depending on its type, the certificate is transferred to one of the **Server certificates** / **CA certificates** lists (even if it has already expired). If a server responds again with this certificate, this connection is accepted immediately.

Reject a certificate:

- ▶ Select the certificate and click on the **Reject** button . . . the certificate is transferred to the **Server certificates** list with the label **Rejected**. If a server responds again with this certificate, this connection is rejected immediately.

Checking information about a certificate

- ▶ Select the certificate and click on the **Details** button. . . . a new web page appears, displaying the properties of the certificate.

Deleting a certificate from one of the lists

- ▶ Select the certificate and click on the **Remove** button. The certificate is deleted from the list immediately.

Import local certificate


You can make available further certificates to your phone system. The certificates must have been downloaded to your computer before.


- ▶ Click **Browse...** and select the local certificate file from your computer's file system ▶ click on **Upload** . . . the selected certificate file is loaded and, depending on its type, added to one of the certificate lists.

HTTP authentication

Define the credentials (user name and password) for HTTP authentication. The credentials are to be used by a user's web browser for secure communication with web server.

HTTP Authentication

HTTP digest username 

HTTP digest password 

HTTP digest username

- ▶ Enter the user name for HTTP authentication. Value: max. 74 characters

HTTP digest password

- ▶ Enter the password for HTTP authentication. Value: max. 74 characters

11.6 Date and time

By default, the system is configured so that the date and time are transferred from a time server on the internet. The page allows you to change the time servers, to set your time zone, and to make arrangements in case the internet time servers are not available.

▶ Settings ▶ System ▶ Date and time

Date and time

Time server ⓘ	0.europe.pool.ntp.org,1.europe.pool.ntp.org,2
Time Zone ⓘ	Europe/Berlin ▼
System time	2017-08-30 16:55
Act as Local Time Server ⓘ	<input type="radio"/> Yes <input checked="" type="radio"/> No

Time server

There are some common time servers preset in the field.

- ▶ Enter your preferred time server in the text field. Multiple time servers can be entered separated by commas. Value: max. 255 characters

Time Zone

- ▶ Select the time zone for your location from the option menu.

System time

Shows the time currently set for the phone system. It is updated every minute.

Fallback option

In case the internet time servers are not available you can set the time manually.

- ▶ Enter the time in the **System time** text field. Once you have started editing the automatic time update stops.

Act as Local Time Server

You can determine the internal time server to act as local time server for your network.

- ▶ Click on **Yes/No** to determine the internal time server to act/not to act as local time server.
- ▶ Click on **Set** to save the settings on this page.

System settings

Firmware



Date and time are synchronised system-wide on all base stations and handsets. It can take up to one hour until the manually changed time is visible on every handset.

Synchronisation is carried out in the following cases:

- If the date or time has been changed on the DECT manager.
- If a handset is registered to the telephone system.
- If a handset is switched off and switched back on again, or is outside the wireless range of the telephone system for more than 45 seconds and then comes back into range.
- Automatically every night at 4.00 am.

You can change the date and time on the handset. This setting only applies for that handset and will be overwritten when the next synchronisation takes place.

The date and time are displayed in the format set for that handset.

11.7 Firmware

Regular updates to the firmware for the Integrator/DECT manager and base stations are provided by Unify via SWS (Software Supply Server). You can upload these updates onto the Integrator as required.



The base stations' firmware is updated automatically by the DECT manager.

► Settings ► System ► Firmware

System firmware

Current version ⓘ V2R0.20.0 (V1.20.0+build.a922f5e)

URL to firmware file ⓘ

Planned schedule ⓘ
 Immediately

Confirmed schedule ⓘ 2017-11-28 16:59

DECT manager's firmware

Identifier ⓘ	Current version ⓘ	Confirmed schedule ⓘ	URL to firmware file ⓘ
<input type="button" value="edit"/> local	V2R0.20.0 (V1.20.0+build.a922f5e)	2017-11-28 16:59	.../192.168.250.168/swupdate/.....update.bin

11.7.1 Firmware of the local system

Current version

Shows the current firmware version of the Integrator/DECT manager on which you are logged in.

- ▶ Click **Browse...** and select the firmware file from your computer's file system.

Starting the firmware update

At a specific date: ▶ Deselect the check box **Immediately** ▶ Enter the exact start time in the format: YYYY-MM-DD HH:mm

Immediately: ▶ Select the check box next to **Immediately** (default) . . . the firmware update is started when you click on the **Set** button.

Confirmed schedule

Shows **Immediately** or the date for the next planned firmware update.

- ▶ Click on **Set** to save the settings and to start the firmware update.

Once the update process starts, the system updates the DECT manager and all subordinate base stations automatically. No action is needed. The handsets lose their connection to the bases during the download and updating process. You can tell that the update has been successful when the handsets re-establish the connection to the base.



The firmware update may take up a longer period. Do not disconnect the devices from the local network during this time.


11.7.2 Firmware of all DECT managers

The DECT managers used in the multicell system are listed with their identifier, name, the current firmware and protocol version, and if applicable, the settings for planned firmware updates.



Currently, only one DECT manager is supported.

Editing the data of a DECT manager

- ▶ Click on  next to the DECT manager you want to edit . . . the DECT manager firmware page is opened.

Firmware update configuration is carried out analogous to the configuration for the local system.

11.8 Save and restore

This page allows you to save and restore the system configuration.

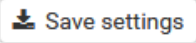
► **Settings** ► **System** ► **Save and restore**

Once you have configured the DECT manager and after making any changes to the configuration, particularly registering or de-registering handsets, you should save the latest settings in a file on the computer so that the current system can be restored quickly if problems occur.

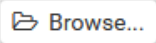
If you change the settings accidentally or you need to reset the DECT manager due to a fault, you can reload the saved settings from the file on your computer to your telephone system.

The configuration file contains all system data including the DECT registration data of the handsets, but not the calls list on the handsets.

Save settings

 Save settings

Restore settings

Settings file  Browse...

Saving configuration data

- Click on **Save settings** ► Select the location where the configuration file should be stored using the system file selection dialogue. Enter a name for the configuration file.

Restoring configuration data

- Click on **Browse...** ► Select the previously saved configuration file from the file system of your computer. ► Click on **Upload** . . . the selected configuration file is loaded.



The secure configuration file can also be loaded onto a new device.

Prerequisites:

- The old device must no longer be in operation.
- The firmware version of the new device must correspond, at least, with the version of the device from which the data is saved, including the set patches.

11.9 Reboot and reset

This page allows you to reboot the devices and to reset the system to factory settings.

► **Settings** ► **System** ► **Reboot and reset**

11.9.1 Manual reboot

- From the **Reboot of** option menu select the devices you want to reboot: the **DECT manager** only or the **DECT manager and base stations**.
- Click on **Reboot now** ► Confirm with **Yes** . . . the reboot starts immediately.



All existing connections managed by the affected base stations are terminated.
To reboot one single base station: → p. 29

11.9.2 Reset to factory settings

All settings of the DECT manager can be reset to the factory settings. This will delete all settings, disconnect all connections, and terminate all calls managed by the connected base stations!



Factory reset can also be performed by using the device key (→ p. 12) or via power procedure (→ p. 15).

Defining the role

- From the **Reset to device** option menu select the role the device should have after the reset.

Base only

The device acts as base station.

All in one - dynamic IP

The device is a Integrator/DECT manager. The network configuration is set to dynamic IP.

All in one - static IP

The device is a Integrator/DECT manager. The network configuration is set to the following static IP settings:

System settings

Reboot and reset

IP address:	192.168.143.1
Subnet mask:	255.255.0.0
Gateway:	192.168.1.1

Resetting the device

► Click on the **Reset to** button to reset the DECT manager to factory condition according to the selection made in **Reset to device**. . . . a confirmation dialogue is opened ► confirm with

Yes The **Save and restore** page is opened allowing you to save the current configuration on your computer (→ p. 84).

No The reset procedure starts at once. The current configuration will be lost.

Cancel The reset procedure is interrupted.

12 Diagnostics and troubleshooting

12.1 Status information

The web configurator provides a status page with important information on the multicell system operation and the connected devices.

► **Status** ► **Overview**

Integrator status	
Device name	OpenScape Cordless IP V2
Device role	Integrator+DECT-Manager+Base
MAC address	7c:2f:80:c6:e2:73
IP address	192.168.250.168
Firmware version	V2R0.13.0 (V1.13.0+build.34a799c)
Date and time	2017-09-04 15:26:28
Last backup	Never
DECT managers	
Number of DECT managers	1
Number of DECT managers with deviating Firmware Version	0
Base stations	
Number of active base stations	2
Number of pending base stations	0
Mobile devices	
Number of registered mobile devices	0
Number of mobile devices to register	0
Number of mobile devices with SIP registration	0

Diagnostics and troubleshooting

Base station events

The following information is provided:

- Integrator status**
 - Device name
 - Device role
 - MAC address
 - IP address
 - Firmware version
 - Date and time
 - Last backup
- DECT managers**
 - Number of DECT managers
 - Number of DECT managers with deviating Firmware Version
- Base stations**
 - Number of active base stations
 - Number of pending base stations
- Mobile devices**
 - Number of registered mobile devices
 - Number of mobile devices to register
 - Number of mobile devices with SIP registration

12.2 Base station events

This page displays counters for diagnostic purposes relating to various events that affect the base stations, e.g. active radio connections, handovers, unexpectedly terminated connections, etc.

► Status ► Statistics ► Base stations

SNMP								
Choose column ▾	Condition	Filter ▾	Clear ✕			View ▾		
[-] DECT manager: local				Ho setup	Ho release	Call drops	Async	E
[-] Cluster: 1								
[-] Base station: LocalBS				0	0	0	0	0
[-] Base station: Base station 7c2f80c6e5cd				0	0	0	0	0

The following information is given:

- DECT manager** Name of the DECT manager responsible for the base station
 - Click on next to the **DECT manager** entry to display the clusters of the DECT manager.
- Cluster** Cluster number
 - Click on next to the **Cluster** entry to display the base stations of the cluster.
- Base station** Name of the base station
- MAC address** MAC address of the base station
- RPN** Radio Fixed Part Number, identifying the radio-entity
- Cluster** Group identifier of the synchronised DECT modules
- DECT Level** Synchronisation level, synchronisation allowed with any lower sync level
- From / To** Time period of the statistical data collection for this base station
- Conn** Number of connections, i.e. calls made

Ho setup	Number of incoming handovers
Ho releasee	Number of outgoing handovers
Call drops	Number of lost connections, i.e. interrupted calls
Async	How often the base station has lost on-air DECT synchronisation
Busy	How often the maximum number of possible connections of the module was achieved. The base station has entered busy-state and pointed to other modules for load balancing.
Conn. drops	How often the LAN connection to the base station was interrupted

12.2.1 Actions

Filtering the list

- ▶ From the **Choose column** option menu select the column for which you want to set a filter.
- ▶ In the text field enter the filter criteria ▶ Click on **Filter** . . . only the entries matching the filter are shown.

Deleting the filter: ▶ Click on **Clear**

Displaying/ hiding columns

- ▶ Click on the View option menu on the right ▶ Select the columns you want to be displayed in the table (👁 / 🚫 = displayed/hidden).

Names of columns which cannot be hidden are greyed out.

12.3 Incidents

- ▶ **Status** ▶ **Statistics** ▶ **Incidents**

Incidents			
<input type="checkbox"/> Timestamp ▾	DECT manager	Incident Type	Info
<input type="checkbox"/> 2017-09-04 14:16:01	local	Crash	lighttpd terminated
<input type="checkbox"/> 2017-09-04 14:15:37	local	Reboot	Reboot occurred
<input type="checkbox"/> 2017-08-31 08:58:03	local	Crash	lighttpd terminated
<input type="checkbox"/> 2017-08-31 08:57:40	local	Reboot	Reboot occurred
<input type="checkbox"/> 2017-08-30 12:29:14	local	Crash	lighttpd terminated
<input type="checkbox"/> 2017-08-30 12:28:30	local	Reboot	Reboot occurred
<input type="checkbox"/> 2017-08-30 09:43:45	local	Crash	lighttpd terminated
<input type="checkbox"/> 2017-08-16 22:21:56	local	Crash	fake-hwclock terminated

1

Diagnostics and troubleshooting

System log and SNMP manager

The page contains the following information on incidents concerning DECT manager operation.

Timestamp	Date and time of the incident
DECT manager	DECT manager affected
Incident Type	e.g. Crash, Reboot, Reset
Info	Detailed information, e.g., the component producing the problem

12.3.1 Actions

Downloading detailed information to a file

To get detailed information about the circumstances causing the error, you can download the incident information to a file. If required, you can pass it to the responsible service personnel.

- ▶ Mark the check box next to one or more incidents you want to download or next to **Timestamp**, if you want to download all incidents.
- ▶ Click on **Download** and select the desired file location for the log files in the file system . . . for each selected incident a log file is created. All log files are taken into a tar file.

Deleting entries

- ▶ Mark the check box next to one or more incidents you want to delete or next to **Timestamp**, if you want to delete all incidents.
- ▶ Click on **Delete**.

Refreshing the list

- ▶ Click on **Refresh**, to update the information in the table.

Browsing through the list

If there is not enough space to display all entries you can browse through the whole table. The number of pages is shown below the list. The current page is highlighted.

- ▶ Click on **Previous** or **Next** to scroll through the list page by page.
- ▶ Click on a specific page number, to go to the desired page directly.

12.4 System log and SNMP manager

The system report (SysLog) gathers information about selected processes performed by the DECT manager and base stations during operation and sends this to the configured SysLog server.

- ▶ **Settings** ▶ **System** ▶ **System log**

System log

Activate system log ?

Server address ?

Server port ?

Log level ?

Info

Debug

Warning

Error

Test

Activate system log

- ▶ Mark/unmark the check box to activate/deactivate the logging function.

Server address

- ▶ Enter the IP address or the (fully qualified) DNS name of your Syslog server. Value: max. 240 characters

Server port

- ▶ Enter the port number, where the Syslog server expects to receive requests.

Range: 1-65535; Default: 514

Log level

- ▶ Mark/unmark the check boxes next to the log information that should be included/not included in the system log.

12.4.1 SNMP manager

To gather management and statistic information concerning base station events via an SNMP manager you have to enter the address information.

SNMP manager address

- ▶ Enter the IP address of the SNMP manger.

SNMP manager port

- ▶ Enter the port number.

Diagnostics and troubleshooting

System log and SNMP manager

13 Using handset connected to a BSIP2 base

The functions of your OpenScape Cordless IP V2 are available on the registered handsets. The functions of the telephone system are added to the handset menu. Handset-specific functions, e.g., local directory or organiser, are not described here. Information about this will be found in the relevant handset user guide. The availability of functions or their designations may differ on individual handsets.

13.1 Making calls

You can make calls using any handset registered to your OpenScape Cordless IP V2.

Prerequisite: You are located in the cell of at least one of the base stations registered to the telephone system.

The cells of the base stations together form the DECT wireless network of the telephone system. You can initiate or answer calls on a handset across the whole wireless network and change cells during a call (handover).

Prerequisite for handover: The base stations involved must be assigned to the same cluster and must be synchronised (→ p. 31).

Each handset is assigned a send and receive connection (→ p. 52).



If your OpenScape Cordless IP V2 is connected to a PBX that permits the formation of groups, VoIP connections can also be assigned to groups. In this case, you will also receive calls on your handset that have been sent to your group number.

The OpenScape Cordless IP V2 uses a VoIP PBX Communication System or the services of a VoIP provider for Internet telephony. The availability of some phone functions depends on whether they are supported by the PBX/provider and whether they have been enabled. If necessary, you can obtain a description of the services from the operator of your PBX.





Depending on the specifications of your PBX, you may need to dial an access code for calls outside the area covered by your VoIP PBX (→ p. 63).

13.1.1 Calling

▶ ... use  to enter a number ▶ **Briefly** press the Talk key 

or

▶ Press and **hold** the Talk key  ▶ ... use  to enter a number

The connection is established using the SIP connection assigned to the handset (→ p. 52).






If you make a call to the fixed line network, you may also have to dial the area code for local calls (depending on the PABX/provider). This is not necessary if the area code is entered in the configuration on the DECT Manager (→ p. 63).

13.1.2 Dialling from the redial list



The redial list contains the numbers last dialled with the handset.

Using handset connected to a BSIP2 base

Making calls







▣ **Briefly** press the Talk key  . . . the redial list is opened ▶ . . . use  to select an entry ▶ Press the Talk key 

If a name is displayed:


▶ **View** . . . the number is displayed ▶ . . . use  to browse numbers if necessary ▶ . . . when the desired number is reached press the Talk key 

Dialling from the call list

The call lists contain the most recent accepted, outgoing and missed calls.

 ▶ . . . use  to select  **Call Lists** ▶ **OK** ▶ . . . use  to select a list ▶ **OK** ▶ . . . use  to select an entry ▶ Press the Talk key 



The **Missed calls** list can also be opened by pressing the Message key .

13.1.3 Initiating ringback

If the number you have called is engaged or the participant called does not reply, you can arrange a ringback if your PBX/provider supports the CCBS and CCNR services.

CCBS (Completion of Call to busy Subscriber) Ringback if busy

CCNR (Completion of Calls on No Reply) Ringback if no answer

The service code for activating/deactivating CCBS, CCNR must be configured on the DECT manager (→ p. 46).

Activating ringback:

▶ Enter the service code defined for the PBX/provider, e.g., *6

If you decide you do not want a ringback, you can switch the function off again:

▶ Enter the service code defined for the PBX/provider, e.g., #6

13.2 Accepting calls

Incoming calls for the connection assigned to your handset are signalled.

▶ Press the Talk key  to accept the call.

Switch off ringtone: ▶ **Silence** . . . the call can be accepted for as long as it is shown on the display

Reject a call: ▶ Press the End call key 

Information about the caller

The caller's phone number is displayed, if provided. If the caller's number is saved in the directory, the name is displayed.

Using a PBX call manager

In case a PBX call manager is used it is possible to define that incoming calls are accepted directly via headset or handsfree. This has to be configured for the handset via web configurator in the **Call manager** section (→ p. 56).



13.2.1 Group pickup

You can also accept incoming calls for the group.

Group pickup must be activated and the call number or SIP URI of the group must be entered. This has to be configured for the handset via web configurator in the **Group pick-up** section (→ p. 56).

13.2.2 Accepting/rejecting call waiting


A call waiting tone indicates a call during an external call. The number or the name of the caller is displayed if the phone number is transferred.

- Reject a call: ▶ **Options** ▶  **Reject waiting call** ▶ **OK**
- Accept a call: ▶ **Accept** ▶ . . . speak to the new caller. The previous call is placed on hold.
- End the call, resume the on-hold call: ▶ Press the End call key .

13.3 Conversation with three participants


13.3.1 Consultation calls

Make another external call during an external call. The first call is placed on hold.


▶ **Ext. Call** ▶ . . . use  to enter the number of the second participant . . . the active call is placed on hold and the second participant is called

If the second participant does not answer: ▶ **End**

Ending a consultation call

▶ **Options** ▶  **End active call** ▶ **OK** . . . the connection to the first caller is reactivated

or


▶ Press the End call key  . . . a recall to the first participant is initiated

Using handset connected to a BSIP2 base


Conversation with three participants

13.3.2 Call swapping


Switching between two calls. The other call is placed on hold.

- ▶ During an external call, dial the number of a second participant (consultation call) or accept a waiting caller . . . the display shows the numbers and/or names of both call participants
- ▶ Use the control key  to switch back and forth between participants

Ending a currently active call

- ▶ **Options** ▶  **End active call** ▶ **OK** . . . the connection to the other caller is reactivated

or

- ▶ Press the End call key  . . . a recall to the first participant is initiated

13.3.3 Conference

Speaking to both participants at the same time.

- ▶ During an external call, dial the number of a second participant (consultation call) or accept a waiting caller . . . then


Initiate conference call:


- ▶ **Conf.** . . . all callers can hear one another and hold a conversation with one another

Return to call swapping:

- ▶ **End Conf.** . . . You will be reconnected to the participant with whom the conference call was initiated



End call with both participants:

- ▶ Press the End call key 

Each of the participants can end their participation in the conference call by pressing the End call key  or hanging up.

13.3.4 Call transfer

Connecting an external call with a second external participant.

- ▶ Use the display key **Ext. Call** to establish an external consultation call ▶ . . . use  to enter the number of the second participant . . . the active call is placed on hold . . . the second participant is called ▶ press the End call key  (during a conversation or before the second participant has answered) . . . the call is transferred



Call transfer options must be set correctly for the PBX/provider (→ p. 44).

13.4 Message indication

Notifications about accepted and missed calls, missed alarms and messages on the network mailbox are saved in messages list and can be displayed on the handset display.


Which messages are displayed on the handset is defined during handset configuration in the **Missed calls and alarms** section (→ p. 56).

Missed/accepted calls count

If the option is activated, the number of missed and accepted calls will be shown on the handset display in idle mode.

Message Waiting Indication (MWI)

For each message type (missed call, missed alarm, new message the network mailbox) the MWI option can be activated or deactivated via the web configurator.

If activated, the LED on the message key  flashes, in the case a **new message** arrives indicating missed calls, a missed alarms or new messages on the network mailbox.

13.5 Using directories


The options are:

- The (local) directory for your handset (see handset user guide)
- Corporate directories provided by an LDAP server (→ p. 99).

The directories available are defined by the web configurator of the telephone system (→ p. 65).

Opening directories

Opening the corporate directory using the INT key

The INT key  (press left on control key) on the handsets opens a corporate directory, provided that this is set up via the web configurator using the **Corporate directory for INT key** option and can be accessed by the telephone system. The directory to be opened can be set for each handset (→ p. 49).

Opening directories using the directory key

The directory key  (press down on the control key) for the handset is normally set as follows:







- Press **briefly** to open the local directory
- Press and **hold** to open the selection of available network directories.

This assignment can be changed for each handset via the web configurator using the **Directory for direct access** option (→ p. 54). Direct access can be assigned to a specific online directory. In this case, open the local directory by pressing and holding the directory key.

The description below assumes the default assignment.

Opening directories via the menu

Depending on the handset used you can access all available directories also via the handset's menu:

-  ▶ ... use  to select  **Directory** ▶ **OK** Local directory
-  ▶ ... use  to select  **Net Directories** ▶ **OK** List of all online directories set up on the telephone system

Using handset connected to a BSIP2 base

Using the network mailbox

The directories are displayed with the names specified in the web configurator.

Example for handling a corporate directory on the handset (→ p. 105).



If handsets are connected to a OpenScape Cordless IP V2, it is not possible to transfer entries from the local directory to another handset.

13.6 Using the network mailbox

The network mailbox accepts incoming calls made via the corresponding line (corresponding VoIP phone number).

In order to record calls, a network mailbox must be set up for the VoIP connection assigned to the handset. This is done during handset configuration in the **Network mailbox configuration** section (→ p. 55).

Playing back messages

▶ Press and hold (if key 1 has been assigned to the network mailbox)

or

▶ Press the Message key ▶ ... use to select the network mailbox ▶ **OK**

or

▣ ▶ ... use to select **Answer Machine** ▶ **OK** ▶ **Play Messages** ▶ **OK**

Listen to announcement out loud: ▶ Press the handsfree key

14 LDAP directory – configuration example


To allow the entries of an LDAP directory to be displayed on the handsets, you will need to configure the phone's LDAP client. This involves the following:

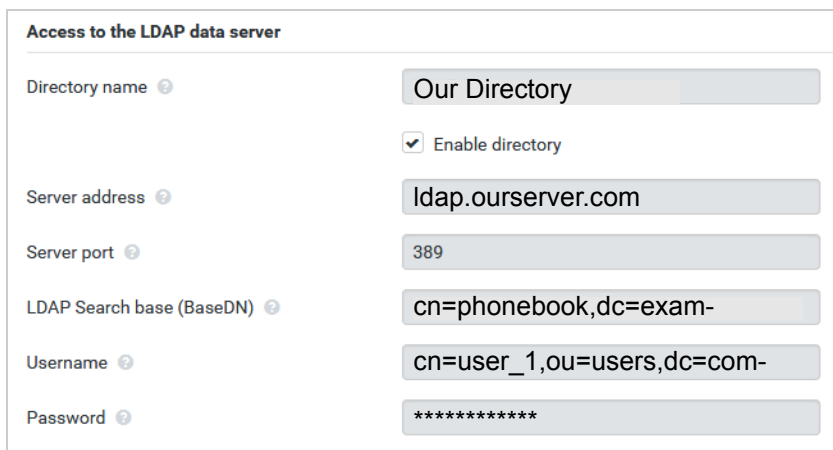
- Setting up access to the LDAP server and database
- Specifying the attributes to be displayed (→ p. 101)
- Defining search criteria (filters) (→ p. 101).

14.1 Access to the LDAP server


To ensure that entries from the LDAP database are displayed on the phones, enter the access data via the web configurator.

▶ Settings ▶ Online directories ▶ Corporate


- ▶ Click on  next to the name of the LDAP directory you want to edit . . . the LDAP configuration page is opened.





Access to the LDAP data server


Directory name  Our Directory


Enable directory

Server address  ldap.ourserver.com

Server port  389

LDAP Search base (BaseDN)  cn=phonebook,dc=exam-

Username  cn=user_1,ou=users,dc=com-

Password  *****

- ▶ Enter a name for the directory in the **Directory name** field.

This is the name under which the directory will appear in the list of network directories on the telephones (→ p. 105).

- ▶ Select the option **Enable directory**, so that the directory will be displayed on the telephones.

- ▶ Enter the access data for the LDAP server

Server address IP address or domain name of the LDAP server, e.g. 10.25.62.35 or ldap.example.com

Server port Port on which the LDAP server expects queries from the clients. Normally the port number 389 is used (default).

Username / Password Credentials for access to the LDAP server.



It is also possible to use individual access data for each handset (→ p. 52).

LDAP Search base (BaseDN)

The **LDAP Search base (BaseDN)** parameter specifies the starting point for the search in the LDAP directory tree. This starting point must be defined on the LDAP server and entered here for the LDAP client according to the

LDAP directory – configuration example

Access to the LDAP server

server configuration. BaseDN is a special LDAP name which represents an object including its position in a hierarchical directory.

BaseDN is used to define which section of the hierarchical LDAP database is to be searched. Access to the entire directory can be enabled (e.g. to the corporate directory) or only to a subdirectory (e.g. the directory of a particular organisational unit).

BaseDN is created from series of RDNs (Relative Distinguished Names) found by walking up the directory information tree.

The BaseDN is specified as follows:

- The directory hierarchy is specified from left to right from the lowest level to the highest, e.g. object, organisational unit, organisation, domain.
- A hierarchical level has the following format: keyword=object, e.g. cn=PhoneBook.
- Hierarchical levels are separated by commas.
- It must be unique in the directory information tree.

The following objects are often used as hierarchical levels:

cn: common name
ou: organisational unit
o: organisation
c: country
dc: domain component

But other objects can also be used. For this parameter you require information on the structure of the LDAP server.

For the meaning of the objects, see section Filters (→ p. 101).

Examples:

Starting point: Object PhoneBook, in the domain example.com

Definition: cn=PhoneBook,dc=example,dc=com

Starting point: Object PhoneBook in the subdirectory sales/support, in the domain example.sales.com.

Definition: cn=PhoneBook,o=support,ou=sales,dc=example,dc=sales,dc=com

14.2 Filters

With filters you define criteria by which the phone searches for certain objects in the LDAP database

- The name filter determines which attributes are used in the search for directory entries.
- The number filter specifies which attributes are used for the automatic search in the LDAP database when phone numbers are entered.
- Additional filters can be defined to enable detailed search

Search in LDAP database

Enable list mode ?

Name filter ?

Number filter ?

Additional filter #1 name ?

Additional filter #1 value ?

Additional filter #2 name ?

Additional filter #2 value ?

Display format ?

Max. number of search results



The LDAP protocol offers various setting options for filters and search functions, e.g. wildcards, fixed character strings and further operators. For full details see the [RFC 4515](#).

14.2.1 Filter format

A filter consists of one or more criteria. A criterion defines the LDAP attribute in which the entered string is to be searched for, e.g. sn=%. The percent sign (%) is a placeholder for the user input.

Operators

Following operators can be used to create filters:

Operator	Meaning	Example
=	Equality	(attribute1=abc)
!=	Negation	(!(attribute1=abc))
>=	Greater than	(attribute1>=1000)
<=	Less than	(attribute1<=1000)
~	Proximiy (LDAP server dependent)	(attribute1~=abc)
*	Wildcard	(attr1=ab*) or (attr1=*c) or (attr1=*b*)

Multiple criteria can be connected with logical AND (&) and/or OR operators (|). The logical operators "&" and "|" are placed in front of the criteria. The criterion must be placed in brackets and the whole expression must be bracketed again. AND and OR operations can also be combined.

Examples

AND operation: (&(givenName=*)(mail=*))

Searches for entries in which the first name **and** e-mail address begin with the characters entered by the user.

OR operation: ((displayName=*)(sn=*))

Searches for entries in which the display name **or** surname begins with the characters entered by the user.

Combined operation: ((&(displayName=*)(mail=*))(&(sn=*)(mail=*)))

Searches for entries in which the display name **and** e-mail address **or** the surname **and** e-mail address begin with the characters entered by the user.

Special characters

It is also possible to find entries containing special characters. If you want to compare these characters within an attribute string use backslash (\) and a 2-digit hex ASCII code as follows:

Special character	ASCII code
(\28
)	\29
<	\3c
>	\3e
/	\2f
\	\2a

Special character	ASCII code
=	\3d
&	\26
~	\7e
*	\2a
	\7c

Example

(givenName=James \28Jim\29)

will find any entry with givenName attribute's value equal to "James (Jim)"

14.2.2 Name filter

The name filter determines which attributes are used for the search in the LDAP database.

Examples:

- (displayName=%) The attribute **displayName** is used for the search.
The percent sign (%) is replaced with the name or part of the name entered by the user. If you enter e.g. the character "A", the phone searches the LDAP database for all entries in which the attribute **displayName** begins with "A". If you then enter a "b", it searches for entries in which the **displayName** begins with "Ab".
- ((cn=*)(sn=*)) The attributes **cn** or **sn** are used for the search.
If you enter e.g. the character "n", the phone searches the LDAP database for all entries in which the attribute **cn** or **sn** begins with "n". If you then enter an "o", it searches for entries in which the attribute **cn** or **sn** begins with "no".



LDAP does not distinguish between upper and lower case in the search request.

14.2.3 Number filter

The number filter defines which attributes are used in the automatic search for a directory entry. The automatic search is performed when a phone number is entered and in the case of an incoming call with calling line identification. If an entry is found for a phone number, the display shows the name instead of the number.

Entries are only found and displayed if the stored phone number matches the entered phone number exactly.

Examples:

- (homePhone=%) The attribute **homePhone** is used for the search.
The percent sign (%) is replaced with the phone number entered by the user. If you enter the numbers "1234567" when dialling, the phone searches the LDAP database for entries with the private phone number "1234567".
- ((telephoneNumber=*)(mobile=*)(homePhone=*))
The attributes **telephoneNumber**, **mobile** and **homePhone** are used for the search. If you enter the numbers "1234567" when dialling, the phone searches the LDAP database for entries with the private **or** mobile **or** work number "1234567".

14.3 Attributes

For a directory entry (an object), a series of attributes are defined in the LDAP database, e.g. surname, first name, phone number, address, company etc. The set of all attributes that can be stored for an entry is stored in the schema of the relevant LDAP server. To access attributes or define search filters, you must know the attributes and their names in the LDAP server. Most attribute names are standardised, but there can also be specific ones defined.

Which attributes can actually be displayed on a phone depends on

- which attributes are defined for an entry in the LDAP database,
- which attributes are set in the web configurator for display on the phone,
- which attributes can be displayed on the phone or handset.

14.3.1 Available attributes on handsets or phones

The following table shows the attributes that could be used for a directory entry on a handset or phone. Of course, the set of attributes that are actually shown depends on the specific handset used.

Attributes of a directory entry	Attribute name in the LDAP database
First name	givenName
Surname	sn, cn, displayName
Phone (home)	homePhone, telephoneNumber
Phone (office)	telephoneNumber
Phone (mobile)	mobile
E-mail	mail
Fax	facsimileTelephoneNumber
Company	company, o, ou
Street	street
City	l, postalAddress
Zip	postalCode
Country	friendlyCountryName, c
Additional attribute	can be freely defined

14.3.2 Specifying attributes for display on the phone

In the web configurator (→ p. 69) you specify which of the available attributes from the LDAP database are to be queried and displayed on the phone.

- ▶ For each attribute of a directory entry, select the appropriate attribute from the LDAP database. There are pre-defined settings at choice. Alternatively you can enter manually a different attribute defined in the LDAP database for this field.
- ▶ If an attribute is not to be displayed, select the option **none**.

In the **Additional attribute** field, you can enter an additional attribute that is available in the LDAP database and should be displayed. If the attribute is a number to be dialled, the option **Additional attribute can be dialled** must be checked.

The attributes **First name** and **Surname** will be used for the following functions:

- Display in the list of directory entries in the form **Surname, First name**
- Alphabetical sorting of the directory entries on the phone
- Name display of a caller or call participant

If the database query only produces one of the attribute values (e.g. because a contact is only stored with their first name), only this one will be displayed.

14.4 Display on the handsets

If one or more LDAP directories are set up in the web configurator, they will be available on the handsets with the following functions:


- Scroll through directory or search for directory entries,
- Display directory entries with detailed information (no edit or delete),
- Dial phone numbers directly from the directory,
- Add directory entries to the local directory.

When a phone number is entered or a call comes in, the directory is automatically searched for an entry that matches the phone number. If an entry is found, the name is displayed instead of the phone number.

To display the corporate directory on the telephone screen

The corporate directory is assigned to the INT key: ▶ press 



Depending on the settings for the handset in the web configurator (→ p. 54), you may also be able to access a corporate directory via the directory key .

Some handsets provide access also via the display menu. For details, see the user guide for your phone.

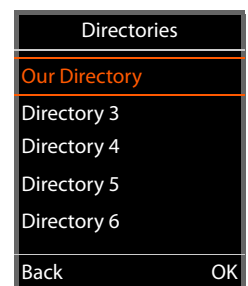
14.4.1 Entries in the directory

The following description shows an example for the display of an LDAP directory on a handset.

The menu shows all directories that have been set up and activated on the **Online directories** page in the web configurator. Each one appears with the name entered under **Directory name** in the web configurator (→ p. 99). In the example on the right, the LDAP directory is shown as **Our Directory**.

▶ . . . use  to select the directory ▶ **OK**

The phone initiates a query to the LDAP server defined in the web configurator.

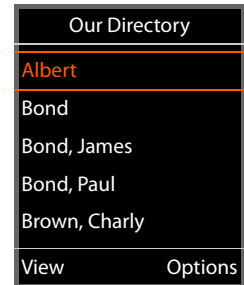


LDAP directory – configuration example

Display on the handsets

The LDAP directory is displayed according to the following rules:

- The search begins in the directory/subdirectory which is defined as the search base on the LDAP server and specified with the **LDAP Search base (BaseDN)** parameter in the web configurator (→ p. 99).
- The entries are listed in alphabetical order.
- The entries are displayed with **Surname** and **First name** if both attributes are available in the LDAP database. Otherwise only the surname or first name is displayed.



14.4.2 Searching the directory

- ▶ Use to scroll through the directory

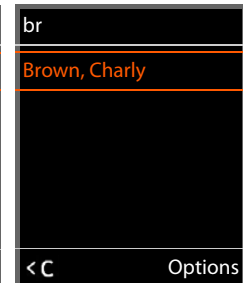
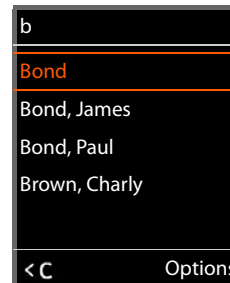
or

- ▶ Use to enter a name (or the first few letters).

As soon as you press a key on the keypad, the telephone goes into search mode. You can enter up to 15 characters. All entries in the LDAP directory that match your input are displayed.

- ▶ Use to delete the last character you entered.

The current search string is shown in the top line.



14.4.3 Displaying a directory entry

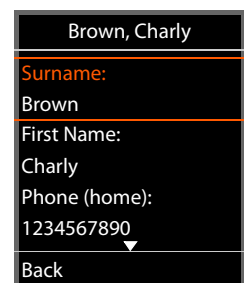
- ▶ Use to select the entry you want.
- ▶ Press the display key **View** or the navigation key .

or

- ▶ Press the display key **Options** ▶ **View**

The directory entry is displayed with its detailed information. Only attributes for which a value is stored are shown (→ p. 101).

- ▶ Use to scroll through the entry.
- ▶ Press the End call key or the **Back** display key to close the entry.

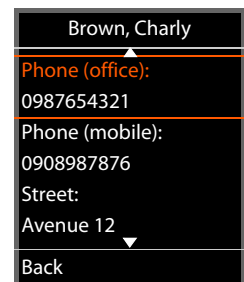


14.4.4 Dialling a number from the directory

- ▶ Use to select the entry you want in the directory.
- ▶ Press the Talk key . If only one phone number is stored, it is dialled. If there are several phone numbers, they are displayed in a selection list.







or

- ▶ Use to select the phone number you want in the detailed view of an entry: **Phone (home)**, **Phone (office)** or **Phone (mobile)**.
- ▶ Press the Talk key . The number is dialled.



A Appendix

A.1 Safety precautions

	Read the safety precautions and the user guide before use. Comprehensive user guides for all telephones and telephone systems as well as for accessories can be found online at www.unify.com in the Support category. We thereby help to save paper while providing fast access to the complete up-to-date documentation at any time.
	Do not use the devices in environments with a potential explosion hazard (e.g. paint shops).
	The devices are not splashproof. For this reason do not install them in a damp environment such as bathrooms or shower rooms.
	Use only the power adapter indicated on the device. Use only the cable supplied for LAN connection and connect it to the intended ports only.
	Remove faulty devices from use or have them repaired by our Service team, as these could interfere with other wireless services.
	Using your telephone may affect nearby medical equipment. Be aware of the technical conditions in your particular environment, e.g. doctor's surgery. If you use a medical device (e.g. a pacemaker), please contact the device manufacturer. They will be able to advise you regarding the susceptibility of the device to external sources of high frequency energy (for the specifications of your Unify product see "Specifications" →p. 109).

A.2 Service

Information and support for our products can be found on the Internet at:

<http://www.unify.com/>.

Technical notes, current information about firmware updates, frequently asked questions and lots more can be found on the Internet at:

<http://wiki.unify.com/>.

A.3 Authorisation

The device conforms to the EU directive 1999/5/EC as attested by the CE marking.

A.4 Disposal

All electrical and electronic products should be disposed of separately from the municipal waste stream via designated collection facilities appointed by the government or the local authorities.

Appendix

Disposal



Proper disposal and separate collection of your old appliance will help prevent potential damage to the environment and human health. It is a prerequisite for reuse and recycling of used electrical and electronic equipment.

For more detailed information about disposal of your old appliance, please contact your city office, waste disposal service, the shop where you purchased the product or your sales representative.

The statements quoted above are only fully valid for equipment which is installed and sold in the countries of the European Union and is covered by the directive 2002/96/ EC. Countries outside the European Union may impose other regulations regarding the disposal of electrical and electronic equipment.

B Technical data

B.1 Specifications

B.1.1 Power consumption

Operation as OpenScape Cordless IP V2 (DECT Manager)	< 4 W
Operations as BSIP2 (Base station)	< 4 W

B.1.2 General specifications

DECT Manager and base stations	
Power over Ethernet	PoE IEEE 802.3af < 4 W
LAN interface	RJ45 Ethernet, 10/100 Mbps Protection class IP20
Ambient conditions for operation	+5°C to +45°C indoors; 20% to 75% relative humidity
Protocols	IPv4, SNTP, DHCP, DNS, TCP, UDP, VLAN, HTTP, TLS, SIP, STUN, RTP, MWI, SDP, SRTP
Base stations	
DECT standard	DECT EN 300 175-x
Transmission power	10 mW average power per channel, 250 mW pulse power
No. of channels	120 channels
Number of connections	10 simultaneous connections per base station (G.726, G711, G.729ab codec), 5 connections in wideband operation (G.722)
Range	Up to 300 m outdoors, up to 50 m indoors
Codec	G.711, G.722, G.729ab
Quality of Service	TOS, DiffServ

Index

- A**
- Access code 63
- Access data for LDAP server 99
- Activating base station 31
- Additional attributes 104
- Address of LDAP server 99
- AND operator 102
- Answer machine, playing back messages 98
- Antenna
 - mounting 11
- Antennas 8
- Area code 93
 - local 64
 - prefix 64
- Area codes 63
- Attribute 104
 - c 71, 104
 - cn 104
 - company 104
 - displayName 104
 - facsimileTelephoneNumber 104
 - friendlyCountryName 104
 - givenName 104
 - homePhone 104
 - l 104
 - mail 104
 - mobile 104
 - o 104
 - ou 104
 - postalAddress 104
 - postalCode 104
 - sn 104
 - street 104
 - telephoneNumber 104
 - user-defined 104
- Attributes
 - defining for display 104
 - in LDAP database 104
- Attributes in the LDAP database 69
- Attributes, LDAP
 - cn 70
 - company 71
 - displayName 70
 - facsimileTelephoneNumber 71
 - friendlyCountryName 71
 - givenName 70
 - homePhone 70
 - l 71
 - mail 71
 - mobile 70
 - o 71
 - ou 71
 - postalAddress 71
 - postalCode 71
 - sn 70
 - street 71
 - telephoneNumber 70
 - user-defined 71
- Audio quality 61
- Authentication code for handset registration 51
- Automatic search 105
- B**
- Base station
 - activating 31
 - administration 27
 - assign to a DECT manager 28
 - belonging cluster 37
 - connected 27
 - deleting 31
 - events 88
 - firmware 28
 - IP address type 30
 - LED display for operational states 14
 - LED display for synchronisation status 14
 - LED display, DECT traffic 14
 - MAC address 27
 - name 27
 - number 88
 - organising clusters 31
 - pending 28
 - rebooting 31
 - resetting 15
 - responsible DECT manager 28
 - sync level 37
 - sync slave 37
 - synchronisation status 28
- Base stations
 - synchronised 37
 - synchronising 31
- BSIP2 DECT base station 5

C

- Call
 - external 93
- Call list
 - dialling 94
- Call manger, accepting call directly 56
- Call on hold settings 46
- Call swapping
 - two external calls 96
- Call transfer settings 62
- Call waiting, external
 - accepting/rejecting 95
- Calling
 - external 93
- Calling party information 46
- Certificate 60
- Certificates 79
- CLI (Command Line Interface) 74
- CLI access to the device configuration 74
- Cluster 6, 37
 - configuring 31
- cn, attribute 70, 104
- Codecs 44
- Column
 - displaying/hiding 20, 89
- company, attribute 71, 104
- Conference 96
- Conference call
 - end 96
 - two external calls 96
- Connected base stations 27
- Connecting
 - to the LAN 11
- Connecting the PC to the web configurator 17
- Connection name 39
- Consultation call
 - ending 95
- Consumption of electricity, see Power consumption
- Customer Care 107

D

- Database access 99
- Date
 - synchronisation 82
- Date, setting 81
- DECT integrator 5
- DECT Level 37
- DECT manager 5
 - LED display DECT traffic 15
 - number 88
 - reseting 15
- DECT manager operation, incidents 90

- DECT registration state
 - handset 49
- DECT traffic
 - base station 14
 - DECT manager 15
- Deployments 6
- Device button 8
- Device role
 - setting 12
- Device roles 12
- DHCP server 24
- Diagnostics
 - base stations 88
 - DECT manager incidents 90
- Dialling
 - from the call list 94
 - from the redial list 93
- DiffServ (Differentiated Services) 61
- Directory
 - accessing 97
 - attributes 104
 - configuring 65
 - configuring handset access 54
 - displaying attributes 104
 - opening 105
 - searching 106
 - using 97
- Directory entry
 - attributes 70
 - searching 106
- Directory
 - name 99
- Display format, LDAP 68
- Display name
 - handset 49
- displayName, attribute 70, 104
- DNS (Domain Name System) 24
- DNS redundancy method 42
- Domain name 99
- Domain part of the user address 39
- Download log files 90
- Dynamic IP address
 - base station 30

E

- Entering the number
 - of the network mailbox 98
- Environment 107

F

- facsimileTelephoneNumber, attribute 71, 104
- Factory settings see Reset 12, 13

Index

Failed registration retry timer 60
Filter 101

- criteria 102
- format 102
- name 103
- number 103

Filter, LDAP 67
Firmware

- base station 28
- current version 83
- handset 50
- update 82

Firmware update

- LED display 14
- scheduled 83

friendlyCountryName 71
friendlyCountryName, attribute 104

G

G.711 45
G.722 45

- enabling 61

G.729A 45
givenName, attribute 70, 104
Grace period for licenses 75
Group pick-up 56

H

Handover 6
Handset 6

- belonging DECT manager 49
- configuring mailbox access 55
- DECT registration state 49
- de-registering 52
- directory assignment 54
- display name 49
- Firmware 50
- LDAP authentication 55
- menu 93
- MWI settings 56
- PIN for DECT registration 51
- registering 49, 50
- registration centre 57
- settings 52
- time-controlled registration 58
- type 49
- user name 49
- VoIP account registration data 52

Handsets

- administration 49
- registered 49

Help function, web configurator 19

homePhone, attribute 70, 104
HTTP authentication 80

I

Incidents 90
Installing 10
INT key 97

- assigning directory 54

Integrator 5

- status 88

IP Address

- IPv4 24, 30

IP address of LDAP server 99
IP address type 24

- base station 30

IP configuration 23
IPII (International Portable User Identity) 49
IPv4 23

L

LAN master 37
LAN master/slave 32
LAN port 11
LAN slot 8
LAN synchronisation 32

- advantages 32
- requirements 33

LDAP

- display format 68
- name filter 68
- number filter 68
- search base 66

LDAP attributes 69, 104
LDAP authentication for handset 55
LDAP directory

- configuring 65
- name 66
- server access data 66

LDAP filter 67
LDAP filter see Filter
LDAP name 65
LDAP search base 100
LDAP server

- address 99
- domain name 99
- IP address 99
- port 99
- User ID 99

LDAP server scheme 69
LDAP server, URL 65
LED displays 8
LEDs 14

- Licence 75
- List
 - browse 20, 90
 - filtering 19
 - sorting 19
- Local area code 64
- Local network 23
- Local Time Server 81
- Log file
 - download 90
- Log level 91
- Logical operators see Operator

M

- MAC address, base station 27
- mail, attribute 71, 104
- Mailbox configuration 55
- Making calls
 - external 93
- Medical equipment 107
- Menu overview
 - handsets 93
- Mobile devices 6
 - number 88
- mobile, attribute 70, 104
- Mounting the antennas 11
- Multicell system 5
- MWI settings 56

N

- Name filter 101, 103
- Name filter, LDAP 68
- Network mailbox
 - entering number 98
- Network MB, see Network mailbox
- Network protocol 23
- Non-SRTP calls, accepting 42
- Number 70
- Number filter 101, 103
- Number filter, LDAP 68

O

- OpenScape Cordless IPV2 DECT manager 5
- OpenScape Cordless IPV2 DECT multicell system 5
- Operator
 - AND 102
 - OR 102
- OR operator 102
- ou, attribute 71, 104
- Outbound proxy mode 43
- Outbound proxy port 43
- Outbound server address 43

P

- Package content 9
- Packet delay jitter 33
- P-Asserted-Identity (PAI) 46
- Password 99
- Password, web configurator 18
 - changing 73
- PBX access code 63
- PBX profile 39
- PCMA/ PCMU 45
- Pending base stations 28
- Phone number
 - dialling 106
- Phone number in directory 104
- Place holder for user input 102
- PoE (Power over Ethernet) 11
- Port 99
- postalAddress, attribut 104
- postalAddress, attribute 71
- postalCode, attribute 71, 104
- Power adapter 107
- Power consumption 109
- P-Preferred-Identity (PPI) 46
- PRACK (Provisional Response Acknowledgement) 60
- Priority of voice data 61
- Profile 78
- Profile, VoIP provider/PBX 40
- Provider profile 39
- Provisioning 78
- Provisioning server 78
- Proxy server
 - address 41
 - port 41
- PTP deviation 33

Q

- QoS (Quality of Service) 61

R

- Reboot
 - base station 31
 - LED display 14
 - manually 85
- Redial list 93
- Registering a set of handsets 50
- Registering handsets 49, 50
 - time-controlled 58
- Registering, with web configurator 18
- Registration centre 57
- Registration refresh time 41
- Registration server 41
- Registration server port 41

Index

Reset

- to factory settings 15
- using the device button 12, 13
- via power procedure 15
- via web configurator 85

Restore configuration 84

Ringback

- switching function off if busy 94
- when the number is busy 94

Roaming 6

RPN 28

RTP (Realtime Transport Protocol) 61

RTP packetisation time (ptime) 46

S

Safety precautions 107

Save configuration 84

SDP (Session Description Protocol) 46

Search base 100

Search mode 106

Search start point 99

Secure Real Time Protocol 42

Secure Shell (SSH) 74

SIP port 60

SIP redundancy 42

SIP server port 42

SIP session timer 60

SIP timer T1 60

sn, attribute 70, 104

Specifications 109

SRTP options 41

Standard gateway 24

Status information 87

street, attribut 104

street, attribute 71

Subnet mask 24

Subscription timer 60

Sync level 32, 37

Sync master/slave 31

Sync Slave 37

Synchronisation 31

- over LAN 31
- over the air 31, 32
- via LAN 32

Synchronisation hierarchy 32

- examples 34

Synchronisation planning 31

Synchronisation status

- base station 14, 28

SysLog 90

System configuration 17

System report (SysLog) 90

T

Telephone system

- overview 5
- preparing to use 9

telephoneNumber, attribute 70, 104

Time

- synchronisation 82
- zone 81

Time server 81

Time, setting 81

Timer

- failed registration retry 60
- SIP session 60
- SIP timer T! 60
- subscription 60

Tone scheme 64

Transport protocol 41

TX power, reduce 30

U

Update 82

user ID 99

User input, place holder 102

User name

- handset 49
- web configurator 18

V

Voice quality 61

VoIP provider, configure profile 40

VoIP settings 60

W

Wall mounting 12

Wall mounting slots 8

Web configurator

- applying/discarding changes 19
- changing password 73
- connecting with PC 17
- logging in 18
- logging off 18
- online help function 19
- password 18
- starting 17
- working with lists 19