V05 10/2021

COMfortel WS-500S

DECT Base Station
FW V2.42

Advanced Information

Content

Configuring the system

System settings are made via the web configurator of the COMfortel WS-500S and cannot be changed using the handsets.

This applies in particular for:

- Registering and deregistering the handset at the telephone system, handset name.
- All settings for the VoIP provider 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.

The web configurator

Use the web configurator to set up your device and configure your DECT network.

- Make basic settings for the VoIP connections and register and configure the handsets you wish to use in the DECT network.
- Make additional settings, e.g., meet particular prerequisites for connecting the handsets to a corporate network or adjust the voice quality on VoIP connections.
- 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.

Starting

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

The device 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 the device to communicate with each other.

ℹ Depending on your VoIP PBX/VoIP provider, it is possible that you will be unable to change individual settings in the web configurator.

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).

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 (→ page 10).

Logging into/off the web configurator

Once you have successfully established the connection, the login screen is displayed in the web browser. There are two user roles with different user IDs:

admin has unlimited access to all functions of the web configurator.

user has only limited access to some settings and system information, e.g., handset registration and some system settings. The **user** role must be activated before it can be used (→ page 58).

By changing the language, the information entered for user name and password are deleted and must be entered again. If you want to change the language, first choose the language and enter user name and password afterwards.

- Enter the user ID in the **Username** text field (**admin**/**user**).
- Enter the password in the **Password** text field. Default **admin**/**user**
- From the options menu **Language** select the desired language.
- Click on **Login**.

Logging in the first time

You will be asked to change the default password and to set the appropriate radio frequency band.

- Enter a new password in the **New password** field and repeat it in the **Repeat password** field

  The password must contain:
  - at least one uppercase
  - at least one number
  - at least one special character
  - from 8 to 74 characters
- Select the radio frequency band used in your region from the list (→ page 68).
- Click on **Set** to save the settings and to open the administrator interface.

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**

ℹ 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.

Changing language

You can change the language at any time.

- From the option menu **Language ▾** at the top right of any web page select the desired language.

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 bold.

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 re-display the menu: ▶ Move the pointer to the area the menu symbols are shown.

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.

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 (➜ page 5).

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.

Working with lists

In some menus you can generate a filtered list.

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:

- 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.

Changing the number of list entries

- On the right side below the list select the maximum number of entries that should be displayed on a page (10, 25, 50, 100).

Browsing through the list

If there are more list entries than the selected number, you can browse through the whole table page by page. 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.

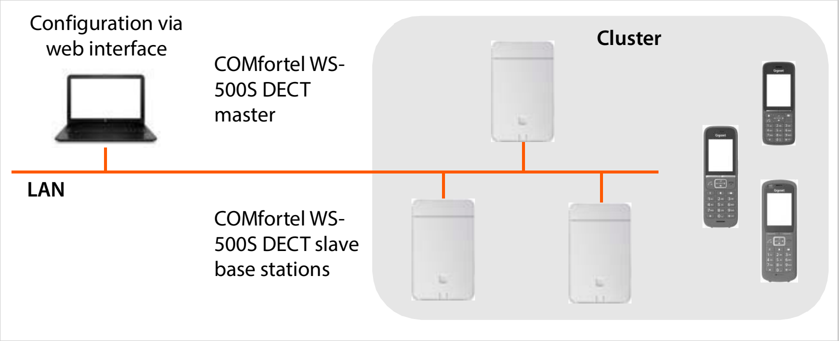
Web configurator menu overview

Settings	Network	IP/LAN	➜ page 10
	Base stations	Administration	➜ page 12
		Synchronisation	➜ page 16
	Provider or PBX profiles		➜ page 29
	Mobile devices	Administration	➜ page 36
		Registration Centre	➜ page 43
	Telephony	VoIP	➜ page 46
		Audio	➜ page 44
		Call settings	➜ page 44
	Online directories	Corporate	➜ page 48
		XML	➜ page 52
		XSI	➜ page 54
		Central phonebook	➜ page 53
	Online services	XHTML	➜ page 55
		Application-Server	➜ page 56
	System	Web configurator	➜ page 58
		Licensing	➜ page 59
		Provisioning and configuration	➜ page 60
		Security	➜ page 61
		System log	➜ page 63
		Date and time	➜ page 64
		Firmware	➜ page 65
		Save and restore	➜ page 66
		Reboot and reset	➜ page 66
		DECT settings	➜ page 67
Status	Overview		➜ page 70
	Statistics	Base stations	➜ page 71
		Incidents	➜ page 73

The **user** role has only restricted access to the user interface. If you login as **user**, most of the menus entries are hidden.

Creating a mini multi-cell system with COMfortel WS-500S devices

To expand the range of the DECT network, a COMfortel WS-500S device can be installed in a network where another COMfortel WS-500S is already present. One of these devices acts as a master, the second device is changed to a slave. Two slave base stations are supported. The master device contains, in addition to the local base station, the components (Integrator/DECT manager) for managing the mini multi-cell system.


Configuration via web interface
COMfortel WS-500S DECT master
Cluster
LAN
COMfortel WS-500S DECT slave base stations

All COMfortel WS-500S devices build a cluster and synchronise in order to perform handover, roaming and overload balancing for handsets. Synchronisation takes place via DECT or LAN. Up to eight simultaneous calls are possible.

Handover A handset switches to a new base station during a call.

Roaming A handset in idle mode is connected to the DECT network via a new base.

Overload balancing A DECT connection (for a call or other administrative or customer purpose) is not set up 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.

- Install one or two additional COMfortel WS-500S as slave base stations.
- Change the role of the slave base stations to **Base**.
  Via device button: → Manual of the COMfortel WS-500S
  Via the web configurator: → page 67
- On the master device add the slave base stations to the DECT network (→ page 12).

Network administration

IP and VLAN settings

This page is used to integrate the device into your company‘s local network.

It is only available for the user role **admin**.

▶ **Settings** ▶ **Network** ▶ **IP/LAN**

> 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.
> No connection set up: ▶ Reset the device to the factory settings.

Device name in the network

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

Address assignment

Network type

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

IP address type

▶ Select **Dynamic**, if your device receives the IP address via a DHCP server.

▶ Select **Static**, if your 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 in the same network.
>
> The fixed IP address must not belong to the address block used by the DHCP server for assigning IP addresses.
>
> 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, if it also works as DNS server. 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.

VLAN

Details in this area 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.

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 device for configuration purposes.
>
> If required, you must carry out a hardware reset via device button (→ page 82). This means that all settings are lost.

Base stations

This chapter is only to be used in the case that the device is used as master in a mini multi-cell system or it has been upgraded to the functions of a multi-cell.

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

Base stations administration

The page allows you to assign base stations to the DECT managers.

It is only available in the Integrator user interface for the user role **admin**.

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

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

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.

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.

The symbol ⚠ indicates that the base station function is disrupted.

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.

DM Name Name of DECT manager the base station belongs to.

The symbol ⚠ indicates that the DECT manager is currently disconnected.

FW Version of the currently installed firmware.

The turning symbol ⟳ indicates that currently a firmware update is in progress.

Status Synchronization status of the base station:

Offline	Not available
Deactivated	Available but not activated
No sync	Activated but not synchronised
Sync	Activated and synchronised,
Sync overload	Synchronised, but DECT overload; attempts were made at this base station to initiate more than the permitted simultaneous calls..

Actions

Editing base station data

- Click on ✎ next to the base station you want to edit . . . the data page for the base station is opened.

Deleting 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.

Exporting/Importing the base station configuration

You can export the base station configuration and import it into another DECT manager, in order to change the DECT manager assignment.

Exporting:

- Select all base stations you want to be transferred via the check mark ✓ next to the MAC address.
- Click on **Export** ▶ Select the location where the export file should be stored using the system file selection dialogue.

Preferably, you want to export and import base stations DECT manager by DECT manager:

- Filter the base station list by **DM Name**. So you can easily export base stations of this specific DECT manager.

Importing:

- Click on **Import** ▶ Select the previously exported base station configuration file from your computer's file system.
- Select the DECT manager into which base station export should be imported from the **DM Name** list and the **IP address type** from the corresponding list. ▶ Click on **Import**.

> ! The export contains all data. The import does not contain the data of the local base station, because the local base station is physically bound to the (potential) new DECT manager.
>
> Please review your sync settings after a base station import.

Enabling/Disabling LED status display at the base station

LED displays are enabled by default on all base stations.

- Select **Yes**/**No** to enable/disable the LED display on all base stations.

Pending base stations

The **Pending base stations** list shows the automatically recognised DECT base stations in the network that have not yet been registered. If a base station is detected by several DECT manages, there are several entries for one base station. To integrate them into your DECT network, 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.

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.

It is only available in the Integrator user interface for the user role **admin**.

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

DM Name

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

Status

Synchronization status of the base station:

Offline	Not available
Deactivated	Available, but not activated
No sync	Activated, but not synchronised
Sync	Activated and synchronised
Sync overload	Synchronised, but DECT overload; attempts were made at this base station to initiate more than the permitted simultaneous calls.

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 multi-cell 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
  The two most significant bits in the RPN represent the RPN group of the DECT manager.

Current firmware version

Firmware version currently installed.

Sync Level

Base station synchronisation level.

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/LAN** page (→ p. 28). 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.

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

Act as Sync Master redundancy

If the DECT sync master or the LAN sync master fails, the base station can take over its role.

▶ Click on **Yes**/**No** to define the base station to act/not to act as redundancy sync master.

If you select **Yes**, the **Sync Level** is automatically set to 2⟶1 to indicate that level 2 is able to become level 1.

> ! The base station must been seen by all level 2 base stations with good quality to assure that the network can still be synchronised in case of a take-over.

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.

Base station synchronisation

Synchronisation and the logical structuring of the base stations in clusters are prerequisites for the functioning of the multi-cell system, inter-cell 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.

For detailed information on DECT network planning, please refer to the "COMfortel WS-500M - Site Planning and Measurement Guide".

A base station shows its synchronisation status with an LED (→ p. 19).

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 additional base stations (sync slaves).

The synchronisation needs some kind of 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 with 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 (having a lower sync level number) to receive synchronisation signal from. Simultaneously, it guarantees a strictly limited number of hops along 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 along the synchronisation path

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.

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 neighboured 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 synchronisation master.

Network requirements

- The devices must be connected to a switch port of minimum 100 Mbit/s with corresponding cabling.
- PoE IEEE 802.3af < 3.8 W (Class 1) for an alternatively external power supply.
- The DECT manager and all its base stations must be in the same layer 2 segment (common broadcast domain).

Base station synchronisation

Requirements for LAN synchronisation

- Minimum number of switch hops between master and all slave base stations.
- For internally and uplink switching use Enterprise class switches >= 1Gbit/s.
- VLAN based QoS could be fruitful to minimise packet delay and its jitter. Switch port based VLAN can isolate base stations from other devices' traffic.
- DSCP (Differentiated Services Codepoint) based QoS could be even more efficient.

  Settings for DSCP tagging:

Sync via LAN:	PTPv2, DLS (proprietary): DSCP=CS7=56
RTP:	DSCP=EF=46
SIP:	DSCP=AF41=34

- Synchronisation via LAN makes intensive use of IP multicasts which have to be supported by the switches.

  Multicast destination address and ports:

PTPv2:	224.0.1.129	UDP via ports 319/320
Proprietary DLS protocol:	239.0.0.37	UDP via ports 21045/21046

  Cascaded switches might need uplink switching of these multicast packets to allow inter-switch LAN synchronisation. Otherwise you need isolated LAN-sync clusters, inter-cluster-synchronized via DECT.
- IGMP snooping is supported and shall be supported by the switch, to configure and minimise multicast distribution only to the LAN synchronising base stations.

Packet delay jitter

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 COMfortel WS-500S 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 COMfortel WS-500S base stations.

Acceptable Network Jitter for LAN-synchronisation

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 a 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.

Cluster selective LAN synchronisation

LAN synchronisation consists of two layers:

- Standard PTP which is shared within a multicast IP domain between all DECT managers
- Proprietary DLS (DECT over LAN Sync) which synchronises the clusters isolated within one DECT manager

Multiple DLS domains are possible per DECT manager as DECT manager clusters. A cluster forming an isolated PTP domain needs to have one LAN master of its own. Maximum one LAN master is allowed per cluster.

DLS sync master and slave do care for matching DECT manager and cluster numbers.

Cluster numbers

For LAN synchronisation a cluster needs to be assigned to a PTP domain. This assignment takes place via the cluster number.

Cluster numbers from 1-c to 7-c (c = common)	Build up one **common** PTP sync domain
Clusters numbers 8-i to 15-i (i = isolated)	Build up an **isolated** PTP sync domain per each such cluster number

- Inter-DM-LAN sync is only possible with matching cluster number (independent from the PTP domain).
- DECT managers forming one common LAN synchronisation domain need to use a cluster number from common domain (1..7) or an identical cluster number of isolated domain (8..15).
- DECT managers using different PTP domains (cluster numbers 8..15) cannot be synchronised by inter-DECT manager LAN synchronisation rule (Reference=**LAN Master of DM x**), but only by inter-DM DECT synchronisation rule.

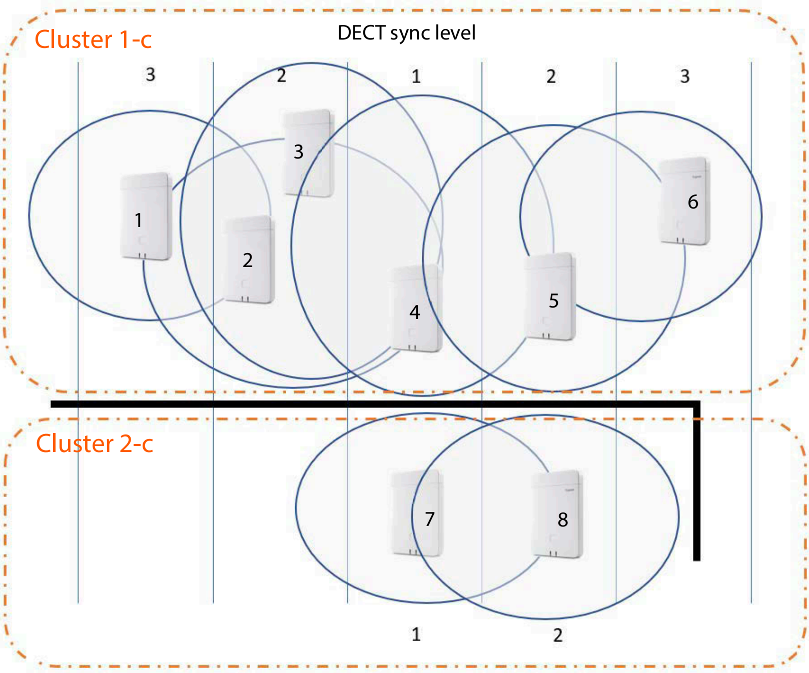
The mentioned PTP domain in aspect of cluster numbers is only relevant for LAN master and LAN slave base stations. For DECT synchronisation, cluster numbers do not have any additional relevance beside just identifying different clusters.

Example scenarios for small/medium systems (single DECT manager clusters)

Synchronisation for handovers between base stations in clusters managed by one DECT manager are configured via the base station administration using the web configurator. Below are some example scenarios.

Scenario 1: Pure DECT

- Your environment ensures a stable DECT over the air synchronisation
- Cluster 1-c is created to insure handover, roaming and load balancing
- The base station in the centre is DECT level 1 to reduce the amount of sync levels
- Environment blocks DECT signal (e.g., a passage through a fire door)
- Second cluster 2-c is created to cover the area that can't be reached by cluster 1-c
- No handover (active calls are disconnected when switch over between clusters)
- Roaming between clusters is possible (handsets in idle mode can switch between clusters)

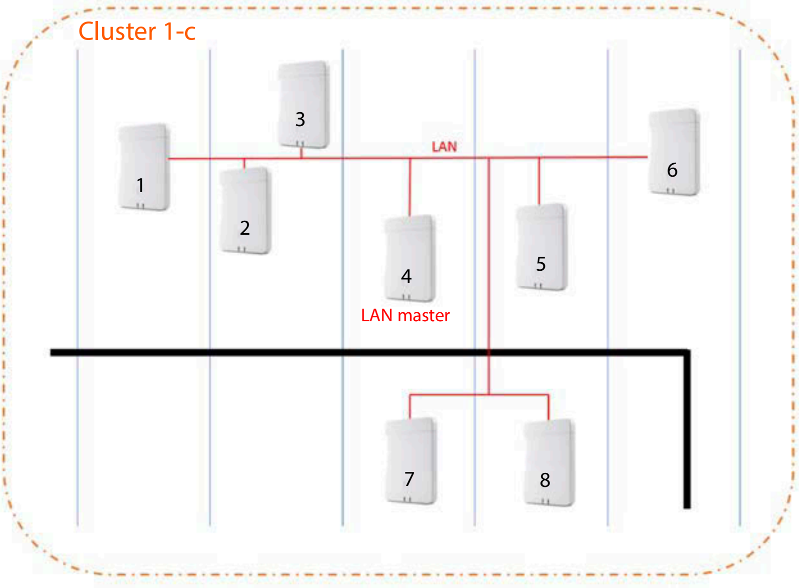


Configuration:

Base station	Cluster	Sync Level	LAN Master	Sync Slave
1	1-c	3		DECT
2	1-c	2		DECT
3	1-c	2		DECT
4	1-c	1		DECT
5	1-c	2		
6	1-c	3		DECT
7	2-c	1		DECT
8	2-c	2		DECT

Scenario 2: Pure LAN

- Use such a configuration, if all requirements for LAN synchronisation are fulfilled
- Cluster 1-c is created to insure handover, roaming and load balancing
- Base 4 is configured as LAN master
- DECT level has no relevance for pure LAN synchronisation
- Handover and roaming is possible within the whole DECT environment
- That LAN sync is used, does not mean that DECT signal range is not important

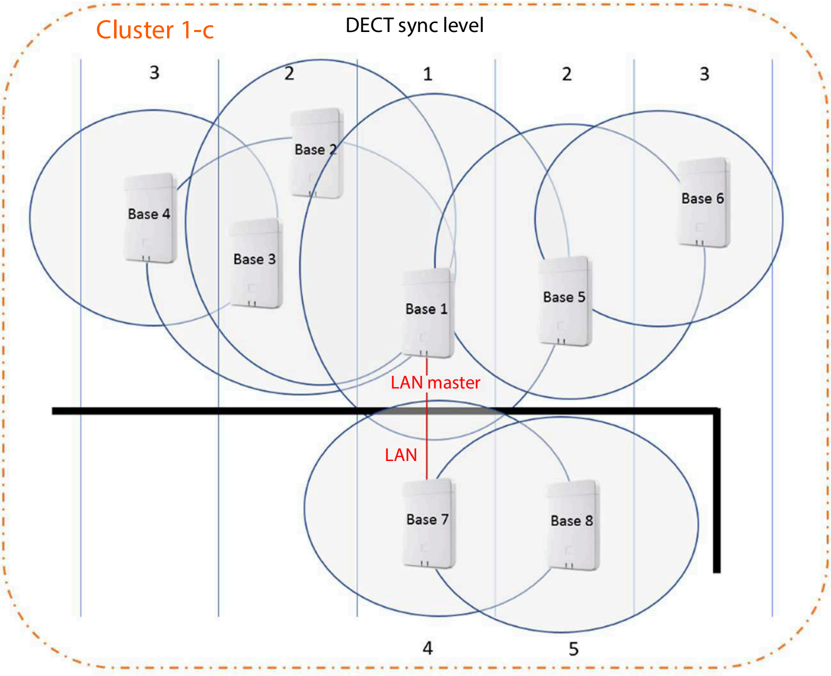


Configuration:

Base station	Cluster	Sync Level	LAN Master	Sync Slave
1	1-c	2		LAN
2	1-c	2		LAN
3	1-c	2		LAN
4	1-c	1	☑	
5	1-c	2		LAN
6	1-c	2		LAN
7	1-c	2		LAN
8	1-c	2		LAN

Scenario 3: DECT-LAN 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
- Cluster 1-c is created to insure handover, roaming and load balancing
- Base station 1 in the centre is DECT level 1 to reduce the amount of sync levels
- Base 1 with DECT level 1 is configured as LAN master
- For each base lower than the LAN master you can individually decide whether it should be synchronised via DECT or LAN
- Base 7 is synchronised via LAN and has DECT sync level 4
- Base 8 is synchronised via DECT and will synchronise with Base 7 via DECT, therefore the DECT sync level 5



Configuration:

Base station	Cluster	Sync Level	LAN Master	Sync Slave
1	1-c	1	✓	
2	1-c	2		DECT
3	1-c	2		DECT
4	1-c	3		DECT
5	1-c	2		DECT
6	1-c	3		DECT
7	1-c	4		LAN
8	1-c	5		DECT

Example scenarios for large systems (multiple DECT manager clusters)

Synchronisation for handovers between base stations in clusters managed by different DECT managers are configured via the DECT manager administration using the web configurator. Below are some examples based on two DECT managers.

Base station synchronisation

Scenario 1: DECT – DECT – DECT

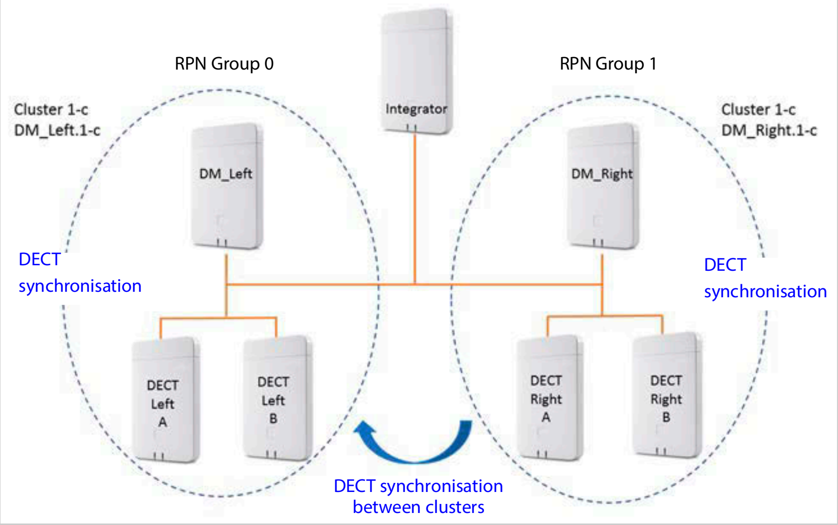
- Integrator (virtual or embedded)
- Two devices with role of DECT manager only
- Every DECT manager has two DECT base stations
- Cluster 1-c on the left side uses DECT synchronisation
- Cluster 1-c on the right side uses DECT synchronisation too (even if the name is the same, it is a different cluster as it is part of another DECT manager)
- Between the clusters also DECT synchronisation is used

Advantage:

- Users can move within the system with handover and roaming.
- DECT synchronisation, no network requirements for LAN sync.

Attention:

- Enough DECT signal quality should be available within the complete system, also between the clusters.
- Every DECT manager must have a different RPN group.



Configuration:

Base station	DM Name	Cluster	Sync Level	LAN Master	Sync Slave
DECT_Left_A	DM_Left	1-c	1		
DECT_Left_B	DM_Left	1-c	2		DECT
DECT_Right_A	DM_Right	1-c	1		
DECT_Right_B	DM_Right	1-c	2		DECT

Scenario 2: DECT – DECT – LAN

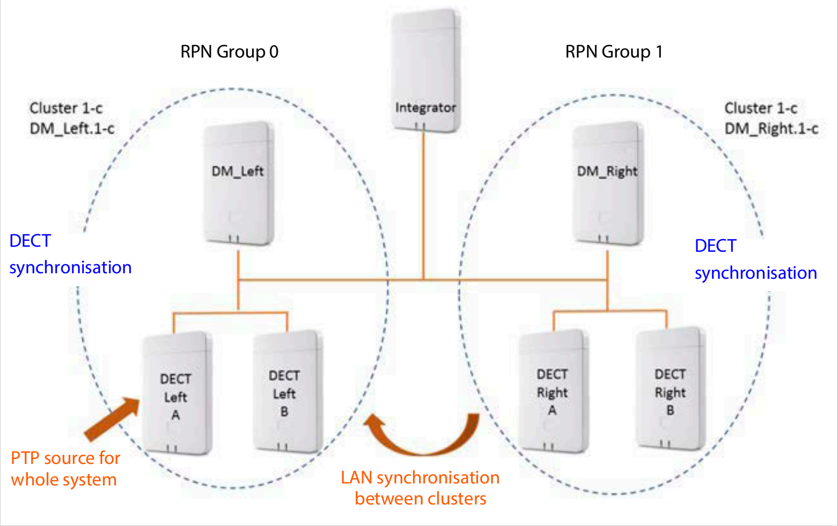
- Integrator (virtual or embedded)
- Two devices with role of DECT manager only
- Every DECT manager has two DECT base stations
- Cluster 1-c on the left side uses DECT synchronisation
- Cluster 1-c on the right side uses DECT synchronisation too (even if the name is the same, it is a different cluster as it is part of another DECT manager)
- Between the clusters LAN synchronisation is used
- Base station **DECT_Left_A** is the PTP source (LAN master)

Advantage:

- Users can move within the system with handover and roaming.
- Synchronisation between the two clusters was not possible due to DECT signal range was not enough. LAN sync is the solution.

Attention:

- The customer network between the clusters must be capable to be used for LAN synchronisation. This needs more configuration in the customer network then using DECT synchronisation.



Configuration:

Base station	DM Name	Cluster	Sync Level	LAN Master	Sync Slave
DECT_Left_A	DM_Left	1-c	1	☑	
DECT_Left_B	DM_Left	1-c	2		DECT
DECT_Right_A	DM_Right	1-c	1		
DECT_Right_B	DM_Right	1-c	2		DECT

Scenario 3: LAN – LAN with isolated PTP domain – DECT

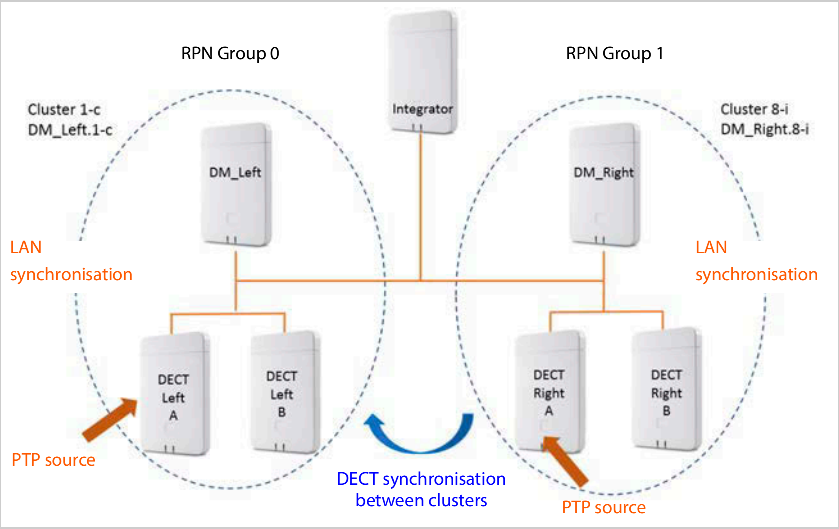
- Integrator (virtual or embedded)
- Two devices with role of DECT manager only
- Every DECT manager has two DECT base stations
- Cluster 1-c on the left side uses LAN synchronisation
- Cluster 8-i on the right side uses LAN synchronisation (cluster 8-i is the first isolated cluster)
- Between the clusters DECT synchronisation is used
- DECT base **Left A** is the PTP source for cluster 1-c
- DECT base **Right A** is the PTP source for cluster 8-i

Advantage:

- Users can move within the system with handover and roaming.

Attention:

- The customer network must be capable to be used for LAN synchronisation. This needs more configuration in the customer network then using DECT synchronisation.
- Every DECT manager must have a different RPN group.



Configuration:

Base station	DM Name	Cluster	Sync Level	LAN Master	Sync Slave
DECT_Left_A	DM_Left	1-c	1	✓	
DECT_Left_B	DM_Left	1-c	2		LAN
DECT_Right_A	DM_Right	1-c	1	✓	
DECT_Right_B	DM_Right	1-c	2		LAN

List of synchronised base stations

All activated base stations contained in the **Connected base stations** list appear in the **Base station synchronisation** list.

It is only available in the Integrator user interface for the user role **admin**.

▶ **Settings** ▶ **Base stations** ▶ **Synchronisation**

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.

DM Name Name of DECT manager the base station belongs to.

Cluster Number of the cluster to which the base is assigned.

Sync Level Synchronisation level within the sync hierarchy.

A base station that is defined as redundancy sync master is automatically set to sync level 2→1 to indicate that level 2 is able to become level 1.

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 Synchronization status of the base station:

Offline	Not available
Deactivated	Available but not activated
No sync	Activated but not synchronised
Sync	Activated and synchronised,
Sync overload	Synchronised but DECT overload

Reference

Sync reference:	Sync type, DECT manager or RFPI, cluster
Sync type:	
1	no Sync Slave function, running free
D	DECT slave within cluster: name of cluster in **Reference** column
D →	DECT slave running inter DM synchronisation rule **Best DECT base of DM**: name of DM in **Reference** column
L	LAN slave within cluster: name of internal DM in **Reference** column
L →	LAN slave running external/inter DM synchronisation rule **LAN Master of DM xy**: name of external DM in **Reference** column
R →	DECT slave running external RFPI synchronisation rule: RFPI in **Reference** column

Cluster configuration

The page allows you to synchronise the system manually.

Base station synchronisation

- Select the DECT manager you want to synchronise from the **DM Name** option menu . . . the cluster configuration of the selected DECT manager is displayed below

Synchronising all clusters of the DECT manager

- Click on **Synchronise all**

Synchronising a specific cluster of the DECT manager

- From the **Sync Slave** option menu select which kind of synchronisation you want to perform (**LAN** or **DECT**) ▶ Click on **Synchronise**

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 multi-cell system can manage up to nine clusters.

- Select the synchronisation level for the base station from the **DECT Level** option menu.

  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.

Provider and PBX profiles

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

- your company's VoIP PBX
- and/or public providers from which you have requested VoIP services.

This page allows you to create a list of systems providing VoIP connections and other services for your phones.

It is only available for the user role **admin**.

▶ **Settings ▶ Provider or PBX profiles**

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 (→ page 29).

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 (→ page 29).

Configuring provider or PBX profiles

On this page you can edit the data for the selected provider or PBX telephony server profile.
It is only available for the user role **admin**.

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.

Phone system

System

▶ Select the type of PBX you use for VoIP provisioning from the option menu.

ℹ For Auerswald PBX use the option **Automatic**.

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 dialled number.

Examples:

sip.domain.net	for	john.smith@sip.domain.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 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: **600** 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.

Use SIP Security (SIPS)

Only if TLS is selected. SIPS enhances SIP with TLS/SSL encryption. Using SIPS makes it more difficult to listen in on the connection. Data is transmitted encrypted over the internet.

- Mark/unmark the check box to enable/disable the use of SIPS.

SRTP options

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.

- Select which calls should be accepted:

Secure Real Time Protocol Security is activated for voice connections.

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

Redundancy settings

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 your service provider

Outbound proxy mode

The DECT IP multi-cell system allows you to configure an outbound proxy. Despite 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:

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

If 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.

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 the PT (Payload Type) for the 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

- No automatic attempts to set DTMF transmission type: select **No** (DTMF transmission type is **Audio** by default).

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.

Distinctive Ringing

Do not make any changes to the default setting here. The ringtone is assigned to the call type on the handset (→ Advanced Information of the handset).

The setting of the call type-specific ringtones offers the possibility of setting different ringtones for different call types. For each call of the call type, the ringtone specially assigned to this call type sounds. Specific ringtones can be assigned to the following call types:

- Internal calls
- External calls
- Group calls
- Door station
- Emergency
- Optional

The option **Optional** is currently not supported by the PBX.

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 (→ page 44)

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

Activate/deactivate a codec:

- Select the required codec from the **Available codecs**/**Active codecs** list and click on ← / →.

Define the sequence in which the codecs should be used:

- In the **Active codecs** list select the required codec and click on ↑ / ↓ to move it up/down.

ℹ 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

Codecs enabled	Number of calls
G729 and G711	8
G722 and G729 and G711	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 requests 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 sent 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

- 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.

Service Codes

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

- In the text fields **Call Completion on (CCBS, CCNR)**/**Call Completion off (CCBS, CCNR)** enter the key sequence for activating/deactivating CCBS and CCNR.

CSTA

Computer Supported Telecommunications Applications is a standard for the interaction between a computer and a PBX, independently from the manufacturer. If your PBX provides CSTA applications to be used by the registered handsets you have to activate the standard here. Account data for handset access can be configured for each handset (→ page 42).

- Define, whether CSTA should be activated (**Yes**) or not (**No**).

Deleting the profile

- Click on **Delete** to delete the profile ▶ Confirm the operation with **Yes**.

Mobile devices

You can use the web configurator to register all handsets at the DECT network and for a VoIP connection. Use the add function of the **Administration** page to register single handsets or use the **Registration Centre** 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.

Mobile devices

This page allows you to register single handsets to the phone system.

It is available for both the user role **admin** and **user**.

▶ **Settings** ▶ **Mobile devices** ▶ **Administration**

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. The setting can be changed.

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.Always **local** as for the COMfortel WS-500S the DECT manager is always located in the base station.

DECT DECT registration state of the handset:

Status	Meaning
To register	System ready to register a handset
Not registered	Registration not possible
Registering	Registration in progress
Registered	Handset is registered
To deregister	System ready to deregister a handset

SIP Indicates, if the handset has a working VoIP connection.

✓	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.

DND Indicates, if DND (Do not Disturb) is activated for the handset.

CSTA Indicates, if CSTA (Computer Supported Telecommunications Applications) is activated for the handset.

Type Model designation of the handset.

FW Current firmware version of the handset.

PIN Authentication code defined for handset registration.

Actions

Adding a handset to the list

- Click on **Add** . . . the mobile devices data page is opened (→ page 37).

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 (→ page 37). The settings of the selected mobile device except personal data are taken over for the new handset configuration.

Replace a mobile device for a user by another one

- Select the check box next to the handset of a user who should get another handset. ▶ Click on **Replace** . . . the mobile devices data page is opened (→ page 37). The old mobile device will be set to **To deregister**. Personal provider data will be removed. User-specific data remain preserved. You will be prompted register a new mobile device.

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.

Exporting/Importing the handset configuration

You can export the handset configuration and import it into another device.

Exporting:

- Select all handsets you want to be transferred via the check mark ✓ next to the IPUI.
- Click on **Export** ▶ Select the location where the export file should be stored using the system file selection dialogue.

Importing:

- Click on **Import** ▶ Select the previously exported handset configuration file from your computer's file system.

Editing the data of a handset

- Click on ✎ next to the handset you want to edit . . . the mobile devices data page is opened (→ page 37).

Setting the name to be displayed in the idle display

By default, the **Username** is displayed in the handset's idle display. You can determine that the **Display name** should be used instead.

Registering/deregistering handsets

The page allows you to register a handset with the DECT 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.

It is available for both the user role **admin** and **user**.

Registration/deregistration in this context refers to the handset's relationship to the DECT network but not to SIP registration.

Registering handsets

- Enter an IPUI, if you want to restrict the registration to a specific handset.

You can find out the handset's IPUI on the packaging label or scan it in. Alternatively, you can view the IPUI on the display. To do so, press the centre of the control key ■ to display the menu. In it, enter ***#06#**. The first entry you see is the IPUI.
Example: 1: 029E74A560.

- 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 Centre** page (→ page 43). Default: 3 min. The registration duration can be configured via provisioning.

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

- Leave the IPUI empty 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 Centre** (→ page 43).

Parameters

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 deregister the handset.
To deregister	The system is ready to deregister a handset. ▶ Select **Registered** to keep the handset registered.

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: 4 digits

or

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

Deregistering handsets

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

DECT deregistration successful:	The handset is deleted from the **Mobile devices** list.
DECT deregistration not successful:	The handset stays in the **Mobile devices** list with status **To deregister**.

Settings for the handset

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

Personal provider data

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 (→ page 29).

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

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.

VoIP provider

- Choose a configured VoIP PBX/provider from the option menu.

  The connection must be configured on the **Provider or PBX profiles** page (→ page 29).
- Enter the access data for the VoIP account in the relevant fields. These fields may vary depending on the PBX/provider profile.

Online directories

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

Directory for direct access

The user can press or 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. Depending on how long the key is pressed (short or long), the local directory or a list of online directories opens.

- Choose which directory is called up with short pressing of the directory key.

Online directories	By shortly pressing the directory key, a list of online directories is opened.
Local directory	By pressing and holding the directory key, the local directory is opened.

Directory for INT key

If any online 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 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.

Selected LDAP book

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

> At least one LDAP directory must have been set-up in the PBX (→ Instructions of the PBX).

Show other LDAP servers

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

LDAP authorisation 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

> At least one mailbox must have been set-up in the PBX (→ Instructions of the PBX).

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

- Enter the **Call number or SIP name (URI)** for the network mailbox.
- Activate the function **SIP SUBSCRIBE for Net-AM MWI** (→ page 31)
- Activate the function via the check box.

Group pick-up

> At least one group must have been set-up in the PBX (→ Instructions of the PBX).

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.

Settings must be made in the PBX and not in the base station.

Call manager

This function is currently not supported.

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.

- Select **Yes**/**No** next to **Missed calls count**/**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.

CSTA

CSTA (Computer Supported Telecommunications Applications) is a standard for the interaction between computer and PBX, independently from the manufacturer. If the provided CSTA applications require individual access control you can enter the access data for the handset here.

ℹ CSTA must be provided by your PBX and must be activated in the provider/PBX profile (→ page 35)

Username

- Enter the user name for the handset's access to CSTA applications.

Authentication name

- Specify the authentication name for the handset's access to CSTA applications.

Authentication password

- Enter the password for the handset's access to CSTA applications.

Broadsoft XSI services

If BroadSoft XSI services should be provided to the user on the handset, enter the credentials.

ℹ XSI services must be activated (→ page 47).

Use SIP credentials

If activated, the credentials for the user's SIP account (**Authentication name** and **Authentication password** are used.

Alternatively, define the following credentials.

Username

- Enter a user name for the user access to the menu (max. 22 characters).

Password

- Enter a password for the user access to the menu (max. 8 characters).

Feature key synchronisation

This option permits the users to use keys on their phones to handle Do Not Disturb and Call Forwarding. If activated, the phones synchronise with the BroadWorks Application server on the status of these features.

- Select **Yes**/**No**, to activate/deactivate key synchronisation with the BroadWorks Application server.

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 one after another during the registration duration.

It is available for both the user role **admin** and **user**.

- **Settings** ▶ **Mobile devices** ▶ **Registration Centre**

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**.

Additionally, the page shows the total amount of DECT managers (for this device always 1) and if the DECT manager is currently ready to register handsets. The DECT manager is set in registration status **Registering** when a registration process is started automatically according to the time settings on this page or when registering handsets manually.

Registering handsets time-controlled

Shows the current system time. Time settings: → page 64

- 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.

Telephony settings

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.

The page allows you to enable/disable the use of the wideband codec G.722 for the telephone system.
It is only available for the user role **admin**.

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

ℹ 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 (→ page 33).

Call settings

On this page you can make advanced settings for VoIP connections.
It is only available for the user role **admin**.

- **Settings ▶ Telephony ▶ Call settings**

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 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 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 worthwhile to test with transfer target address derived from transfer target’s transport address.

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.

- 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.

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).

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.

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** = 207

- Select if and if so what the code is used for.

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 scheme

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

General VoIP settings

This page allows you to make some general settings for the VoIP connections.
It is only available for the user role **admin**.

▶ **Settings ▶ Telephony ▶ VoIP**

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 registation retry timer

▶ Specify after how many seconds the phone should attempt to re-register 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.

SIP security certificate

- 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.

XSI services

BroadSoft XSI (Xtended Service Interface) allows remote applications to integrate with BroadSoft services to perform telephony-related actions and to be notified about telephony events. The device enables the use of XSI services to provide the user with XSI directories and call lists.

If you want to use XSI services, you need to enable the services and enter the XSI server address on this page.
It is only available for the user role **admin**.

- **Settings** ▶ **Telephony** ▶ **XSI Services**

Server address

- Enter the URL of the XSI server in the text field.

Enable XSI directories

- Mark the check box, if you want to use XSI directories. Specific XSI directories must be set up as online directory on the XSI page (→ page 54).

Enable XSI call logs

- Mark the check box, if you want to use XSI call logs.

Online directories

The device allows you to set up up to ten corporate directories in LDAP format, a public and a corporate directory in XML format, different XSI directories, as well as a central directory and make them available to the registered handsets.

Use the handset settings (→ page 39) to specify which keys are to call up the directories.

Corporate online directories (LDAP)

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

The page lists the available LDAP directories.

It is only available for the user role **admin**.

- **Settings ▶ Online directories ▶ Corporate**

Name The name that you have defined for the directory is displayed, or the default name (LDAP1 - LDAP10). It can be edited (→ page 48).

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 (→ page 48).

Detailed information about LDAP configuration can be found at wiki.auerswald.de

Configuring an LDAP directory

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

It is only available for the user role **admin**.

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.

- 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 (→ page 39).

Secure LDAP

By default, LDAP traffic between the phone system and the LDAP directory server is handled via an insecure connection. You can encrypt traffic by enabling secure LDAP. This is accomplished by installing a CA certificate signed by the secure LDAP server onto the system (→ page 61).

- Select the security protocol **SSL/TLS** or **STARTTLS** to be used for encryption or **None** to dispense with encryption.

Settings for searching the LDAP database and displaying the result

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.

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 → page 51

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** andthe **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	**telphoneNumber**	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

A maximum of 99 entries can be displayed.

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

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 LADP server. The majority of attribute designations are standardised, however specific attributes can also be defined.

- 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
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 dialled**, if an additional attribute is defined and it is a phone number.
- Click on **Set** to save the settings of this page.

A detailed configuration example can be found in section "LDAP directory – configuration example" (→ page 76)

Online directories in XML format

A public and/or a corporate online directory in XML format can be made available to the user. Use this page to enter the provider's details and a name for the directory.

It is only available for the user role **admin**.

- **Settings** ▸ **Online directories** ▸ **XML**
- Select **Public** or **Corporate**

Entering the data for an XML directory

Directory name

- Enter a name for the directory. This is the name that will be displayed on the handsets when the user opens the directory list by pressing the directory key.

Server address

- Enter the URL of the online directory provider in the **Server address** field.

Username / Password

- Enter the access data for the online directory in the **Username** and **Password** fields.

List update / refresh

Activated:	The result list at the handset will automatically request the next portion of results when browsing through it.
Not activated:	The number of entries defined in **Maximum number of entries** is downloaded during one reading operation.

Enabling online directories

You can enable/disable different kinds of public directories (White Pages, Yellow Pages or Public Private Pages) that are provided by the given provider.

- Mark/unmark the check box next to the public directory you want to enable/disable.
- Click on **Set** to save the settings of this page.

Online directories – XSI

If one or more online directories are provided via an BroadSoft XSI service, use this page to set up the server access, enable the directories and assign directory names that are to be displayed on the users‘ handsets.

It is only available for the user role **admin**.

ℹ The XSI directory service must be enabled on the **Telephony – XSI Services** page (→ page 47).

▸ **Settings ▸ Online directories ▸ XSI**

Server address

If XSI services are enabled the address of the XSI server is shown here.

Enable XSI directories

▸ Mark the check box, if you want any of the following XSI directories to be provided on the users' handsets.

Enable specific XSI directories

▸ Mark the check box next to the XSI directories that should be provided.

Directory name

▸ For the selected XSI directories enter a name in the **Directory name** field. This is the name under which the directory will be displayed on the handsets.

Central phone book

You can provide a central phone book for all users' handsets. The phone book can be provided via a server in the network or uploaded directly from a computer to the phone system.

It is only available for the user role **admin**.

The phone book must be available in well-defined XML format. For detailed information please refer to wiki.auerswald.de

▸ **Settings ▸ Online directories ▸ Central phonebook**

Directory name

▸ Mark the **Enable directory** option, so that the directory is displayed on the handsets.

▸ Enter a name for the phone book in the **Directory name** field. This is the name under which the phone book will be displayed on the handsets.

Server address

▸ Enter the URL of the server providing the phone book in the text field.

Daily refresh time

The phone book will be refreshed automatically once a day.

▸ Enter the time when the automatic refresh should take place.

Enable list mode

▸ Define what should be initially shown, when the user opens the phone book.

Activated:	A list of all entries of the phone book is shown.
Not activated:	An editor is opened first that allows the user to select a specific search area within the phone book and thereby to reduce the number of entries.

Load phonebook from PC

You can download an XML phone book from your computer directly to the phone system.

Phonebook file

- Click **Browse...** and select the XML phone book file from your computer's file system ▶ click on **Upload** . . . the selected file is loaded and can be made available for the users.
- Click on **Set** to save the settings of this page.

Online services

XHTML

The function Info Centre is currently not supported by the handsets.

Additional functions as Info services, PBX control, and customer specific RAP (XHTML) applications can be made available to the user via the handset menu **Info Centre**. For this purpose four additional menu entries can be defined that will be inserted into the handset user interface.

The additional functions must be available as well formatted XHTML pages. For information on the supported XHTML format, please visit wiki.auerswald.de.

The page is only available for the user role **admin**.

- **Settings ▶ Online services ▶ XHTML**

The page shows the following information for the defined menus:

Name The name that you have defined for the menu is displayed.

Server url If the XHTML access is configured, the server URL is displayed.

Add SIP-ID

If the option is enabled, the device will add the SIP ID in the GET request that are addressed to the server.

- Mark the check box **Add SIP-ID** in order to activate the option.
- Click on **Set** to save the settings of this page.

Adding / editing an entry

You can define up to four menu entries.

- Click on ✎ in an empty row or in a row with an already configured entry in order to edit it.

Activate

- Mark the option, so that the menu is displayed on the handsets.

Name for menu

- Enter a name in the text field (max. 22 characters). This is the name under which the menu will be displayed on the handsets.

Server address

- Enter the URL of the server providing the service.

The access to the service can be protected by user name and password.

Use SIP credentials

If activated, the credentials for the user's SIP account are used (**Authentication name** and **Authentication password**, → page 39).

Alternatively, the following credentials can be used.

Username

- Enter a user name for access to the menu (max. 22 characters).

Password

- Enter a password for access to the menu (max. 8 characters).

Application-Server

The phone system supports the AML feature (Alarming - Messaging - Location). AML includes the following functions:

Alarming: The user can start an alarm from the DECT handset. The alarm is forwarded to an alarm server.

Messaging: Messages from an alarm server (or another server/platform) are sent to the DECT handsets.

Location: The location of a handset is made visible on a location/alarm server.

A licence is required for each handset that is to receive messages from an alarm server or that is to send location data.

On this page you enter the servers to be used for AML.

This page is only available for the user role **admin**.

- **Settings** ▶ **Online services** ▶ **Application Servers**

The page shows the following information about the servers:

AS Id Automatically assigned ID for the application server.

AS Name Name you can set for the server.

Actions

Adding an application server

- Click on **Add** . . . the application server page is opened.

Deleting an application server from the list

- Select the check box next to the application server you want to delete. Multiple choice is possible. ▶ Click on **Delete** ▶ Conform with **Yes** . . . all selected application server are deleted.

Editing the data of a DECT manager

- Click on ✎ next to the application server you want to edit . . . the application server configuration page is opened.

Adding/editing an application server

AS Id

- ID that external clients need for access. The ID is automatically assigned as soon as you set up an entry for the application server.

Application server name

- Enter the user name for accessing the server in the text field.

Password

- Enter a password for accessing the server (min. 32 characters).

System settings

Web configurator access rights

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

It is available for both the user role **admin** and **user**. The user is only allowed to change the own password.

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

Changing the web configurator password

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

There are two user roles with different user IDs, **admin** and **user** (→ page 5). The **user** ID is disabled by default. You can activate it here.

The password is set depending on the user role. The administrator is allowed to change the password for both **admin** and **user**. Logged on as **user** you can only change the password for **user**.

New password

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

Repeat password

- Repeat the new password entered in the **Repeat password** field.

Show password

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

Activate user access

- Click on **Yes**/**No** to enable/disable the ID for the **user** role.

CLI access via ssh

Only available for user role **admin**.

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.

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

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

Repeat password

ℹ 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**.

Web security certificate

Only available for user role **admin**.

The web configurator is protected by SSL/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.

▶ 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.

▶ If the certificate requires a password, enter it in the **Web security password** field.

Licensing

In the case that you want to integrate a single cell device into a multi-cell system, you need to upload a license file containing the license key.

The page is only available for user role **admin**.

▶ **Settings** ▶ **System** ▶ **Licencing**

The table shows the licenses that are currently in use.

Item under Licencing

Features that are licensed.

Single cell to Multi cell upgrade

Used to upgrade a single cell device to a multi-cell device.

A factory reset sets back the device to a single cell device. Licenses would have to be applied anew.

One of the following licenses must be applied to the integrator in order to connect the single cell device to the DECT network.

DECT Manager - Single/Mini-Multi cell

Used for single cell devices that should be integrated as single cell into a multi-cell system (with virtual or embedded integrator).

- No handover and roaming between base stations
- Handsets are registered and bound to the single cell device
- Pure single cell or mixed single cell/multi-cell DECT network is possible

DECT Manager - Multi cell
Used for single cell devices to be used as DECT manager in the multi-cell system.

Available Licences Feature quantity of the ordered licenses. During the activation period the maximum quantity is available.

Used Licences How many licenses are needed by the current configuration.

Status Remaining days of the activation period (or expired).

Creating a request file

This function is not available.

Uploading the license file

▶ Acquire the voucher for your upgrade in the Auerswald/FONtevo shop ▶ Enter the voucher code from the voucher center and the serial number of your device. ▶ Click on **Exchange** . . . the license code is output. ▶ Save the output code.

▶ Click on **Browse...** ▶ Select the previously saved license file from the file system of your computer. ▶ Click on **Upload** . . . the license will be enabled.

Grace period

- After the first start-up and after each full factory reset an installation can be tested for 35 days without any limitation and any purchased license (grace period). In the **Status** column the remaining days of the grace period is shown.
- After 35 days the message **Check license status** will be shown on all registered handset for additional 35 days. The **Status** column shows **Grace period - expired**. The system will still stay fully functional.
- After a total number of 70 days after first startup/factory reset the number of parallel calls will be reduced to 1 call per connected DECT manager, unless a valid license file will be uploaded.

Master DECT manager

As the virtual integrator is not a physical device, a master DECT manager must be defined for licensing via DECT manager administration. The license is assigned to the MAC address of the master DECT manager.

If the master DECT manager is broken and replaced, the license is not valid anymore. You have one month to request a new license file.

Provisioning and configuration

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.
It is only available for the user role **admin**.

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.

ℹ Detailed information on how to establish a provisioning server and create provisioning profiles for Auerswald phones: → wiki.auerswald.de

- **Settings** ▶ **System** ▶ **Provisioning and configuration**

Provisioning server

- Enter the URL of your provisioning server in the text field. Value: max. 255 characters; Default: the Auerswald Redirection Server

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 (→ page 66).

Security

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

It is only available for the user role **admin**.

- **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.

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.

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 used for HTTP digest authentication of the provisioning client with the provisioning server.

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

System log and SNMP manager

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

It is only available for the user role **admin**.

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

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.

The **Use on all DECT Managers** button is not relevant to this device.

SNMP statistics

The Simple Network Management Protocol (SNMP) is a common protocol used for monitoring and controlling of network devices. To gather management and statistic information concerning base station events to be processed by an SNMP manager you have to enter the address and authentication information according to the SNMP server configuration.

- Enter the IP address of the SNMP manager server in the **SNMP manager address** field and the port number used by the SNMP manager in the **SNMP manager port** field. Default: 162

To access the SNMP database authentication is necessary.

- Enter the **SNMP username** and the **SNMP password**.

The **Use on all DECT Managers** button is not relevant to this device.

- If the access data defined here should be used for all DECT managers, click on **Use on all DECT Managers**.

Storing management information in MIB format

You can store management information for all base stations in MIB syntax.

- Click on **Download MIB** ▶ Select the location where the MIB file should be stored using the system file selection dialogue . . . the file with the MIB information is stored in TXT format.
- Click on **Set** to save the settings.

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.

It is only available for the user role **admin**.

▸ **Settings** ▸ **System** ▸ **Date and time**

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.

Date and time are synchronised system-wide on the base station and all 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 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.

Firmware

Use this page to make adjustments in order to keep the phone system up-to-date via firmware updates.

It is only available for the user role **admin**.

Regular updates to the firmware are provided by the operator or supplier on a configuration server. You can upload these updates onto the device as required. If a firmware update is provided in the form of an update file, you can store it on your computer and download it from there.

▶ **Settings** ▶ **System** ▶ **Firmware**

Current version

Shows the current firmware version.

Backup available for previous version

You can downgrade the firmware by installing any older version. When installing a new firmware the system automatically creates a data backup for the recent firmware. If you later downgrade to this version the data backup will be installed on the system. This way you have a downgrade to previous firmware version and data settings.

> ! Downgrade to any other version will reset the device to factory settings.

Selecting the firmware update file

▶ In the **URL to firmware file** text field specify the URL of the configuration server where the firmware is located

or

▶ 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 handsets lose their connection to the base. 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 device from the local network during this time.

Save and restore

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

It is available for both the user role **admin** and **user**. The user is only allowed to save the settings but not to restore them.

▶ **Settings** ▶ **System** ▶ **Save and restore**

Once you have configured the phone system and after making any changes to the configuration, particularly registering or deregistering 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 device 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.

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 secured 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.

Reboot and reset

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

It is available for both the user role **admin** and **user**.

▶ **Settings** ▶ **System** ▶ **Reboot and reset**

Manual reboot

▶ Click on **Reboot now** ▶ Confirm with **Yes** . . . the reboot starts immediately.

Reset to factory settings

All configuration settings can be reset to the factory default. This will delete all settings, disconnect all connections, and terminate all calls!

When resetting to factory defaults all settings are lost. You can save your current configuration previously (→ page 66).

Factory reset can also be performed by using the device key (→ page 82).

Defining the role

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

All in one - dynamic IP

The roles Integrator + DECT manager + base station are active. The network configuration is set to dynamic IP.

All in one - static IP

The roles Integrator + DECT manager + base station are active. The network configuration is set to the following static IP settings:

IP address:	192.168.143.1
Subnet mask:	255.255.0.0
Gateway:	192.168.1.1

DECT-Manager+Base - dynamic IP

The roles base station + DECT manager are active. The network configuration is set to dynamic IP.

DECT-Manager+Base - keep IP

The roles base station + DECT manager are active. The network configuration is set to static IP.

All in one is the default setting for COMfortel WS-500S - . All three components are active (Integrator + DECT manager + base station).

The roles **DECT manager + base station** are intended for the operation behind an external Integrator (available at a later time). The Integrator allows several base stations at different locations to be managed centrally.

Resetting the device

- ▶ Click on the **Reset to** button to reset the device 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 (→ page 66).

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

Cancel The reset procedure is interrupted.

DECT settings

This page allows you to make settings for the DECT radio network.

It is only available for the user role **admin**.

- ▶ **Settings** ▶ **System** ▶ **DECT settings**

Changing one of these settings requires a restart of the system. Ongoing calls will be cancelled.

ECO DECT

ECO DECT is an environment-friendly technology which reduces the power consumption and enables a variable reduction of transmission power.

DECT settings

DECT Radiation power

- Set the DECT radiation power to your needs:

Maximum range: The device range is set to maximum (default). This guarantees the best connection between the handset and the base stations. In idle status, the handset will not send radio signals. Only the base station will maintain contact with the handset via a low wireless signal. During a call, the transmission power automatically adapts to the distance between the base station and handset. The smaller the distance to the base, the lower the radiation.

Limited range: The radiation is reduced by up to 80 %. This will also reduce the range.

DECT security settings

DECT radio traffic between base stations and handsets is encrypted by default. The following options allow you to define the security settings in more detail.

DECT Encryption

- Activate/deactivate the option.

Activated: All calls are encrypted.

Deactivated: No calls are encrypted.

Enhanced Security - Early Encryption and Re-Keying

- Activate/deactivate the option.

Activated: The following messages are encrypted:

- CC (Call Control) messages in a call
- Data that may be sensitive at early stages of the signalling, e.g., dialling or CLIP information sending

The key used for encryption is changed during an ongoing call and thus improving the security of the call.

Deactivated: No CC messages or early data are encrypted.

Enhanced Security - Automatic release for non-encrypted calls

- Activate/deactivate the option.

Activated: If encryption is activated, it will be released in the case that a call is initiated by a device that is not supporting encryption.

Deactivated: Encryption is never released.

DECT radio settings

Due to different national regulations DECT units are required to use different frequency ranges to make them compatible with DECT systems in other areas. You can adapt the frequency range of the device to the requirements of your region.

DECT Radio band

- Select the radio frequency band used in your region.

❗	Please select the DECT frequency band your system should operate according to your region.This is a system wide setting. Changing the setting will reboot the DECT radio part. Wrong setting may cause violation of legal regulations. In case of doubt, contact your Telecommunications Authority.

▶ Click on **Set** to save the settings.

Diagnostics and troubleshooting

Status information

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

▶ **Status** ▶ **Overview**

The following information is provided:

Integrator status

- Device name
- Device role
- MAC address
- MAC-ID
- IP address
- DECT Frequency band
- DECT PARI
- Firmware version
- Date and time
- Last backup

DECT Managers

- Number of DECT Managers (for this device always 1)
- Number of DECT Managers with deviating Firmware Version

Base stations

- Number of active base stations (for this device always 1)
- Number of pending base stations (for this device always 0)
- Call limit for base station only

Mobile devices

- Number of registered mobile devices
- Number of mobile devices to register
- Number of mobile devices with SIP registration

Base station events

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

It is available for both the user role **admin** and **user**.

▶ **Status** ▶ **Statistics** ▶ **Base stations**

The following information is given:

DECT Manager Name of the DECT manager (for this device always **local**), period of time during which the events have been collected, total number of missed calls within the given time period.

▶ Click on ⊞ next to the **DECT Manager** entry to display the clusters of the DECT manager.

Note: The symbol ⚠ next to the DECT manager name indicates that there could be a situation which requires attention.

Cluster Cluster number (for this device always 1), summary of the collected events

▶ Click on ⊞ next to the **Cluster** entry to display the base station information.

Base station Name of the base station (for this device always **LocalBS**)

Some of the following information may be hidden. Use the **View** option menu to display the desired columns.

Properties

MAC address MAC address of the base station

RPN Radio Fixed Part Number, identifying the radio-entity

Sync RPN RPN of the other base station the base station is synchronising with (not relevant to this device)

Sync Level Synchronisation level (not relevant to this device)

Statistics

Conn Number of connections, i.e. calls made

Ho setup Number of incoming handovers (not relevant to this device)

Ho release Number of outgoing handovers (not relevant to this device)

Call drops Number of lost connections, i.e. interrupted calls

Async How often the base station has lost on-air DECT synchronisation (not relevant to this device)

Busy How often the maximum number of possible connections of the module was achieved.

Conn. drops How often the LAN connection to the base station was interrupted

Actions

Exporting the information into a CSV file

For further processing of the statistic data you can export the data into a file with CSV (Comma separated Value) format.

- Click on **Export** ▶ Select the location where the file should be stored using the system file selection dialogue.

Resetting the statistics

- Click on **Reset all** . . . the counters in the table are reset to 0.

Filtering the list

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

For filtering the list according to specific counter values the following operators are possible:

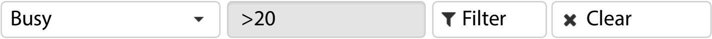
<	less than	>	more than	=	equal to
<=	less or equal	>=	more or equal		

For the **MAC address** column only the following condition is allowed: = MAC address
The MAC address must be in the following format: **aabbccddeeff** (without colons)

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

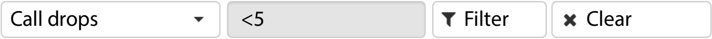
Examples:

Only base stations with more than 20 busy situations should be displayed in the table. This could be achieved by the following filter settings.



Busy ▾ | >20 | Filter | ✖ Clear

Only base stations with less than 5 call interruptions should be displayed in the table. This could be achieved by the following filter settings.



Call drops ▾ | <5 | Filter | ✖ 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.

Incidents

The page contains information on incidents concerning DECT manager operation.

It is available for both the user role **admin** and **user**. The user is not allowed to delete entries.

▶ **Status ▶ Statistics ▶ Incidents**

Timestamp	Date and time of the incident
DECT Manager	DECT manager affected (for this device always 1)
Incident Type	e.g. **Crash**, **Reboot**, **Reset**
Severity	Severity of the incident
Info	Detailed information, e.g., the component producing the incident

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.

Using a handset connected to a COMfortel WS-500S

The functions of your device 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.

ℹ The handsets COMfortel M-5x0 support the complete functionality of the COMfortel WS-500S please refer to wiki.auerswald.de.

Making calls

You can make calls using any handset registered to your device.

Prerequisite: You are located in the radio cell of the base station.

Each handset is assigned a send and receive connection (→ page 39).

If your device 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 device uses a VoIP PBX 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.

ℹ 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 (→ page 45).

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 with the provider settings (→ page 34).

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

Using the network mailbox

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

Prerequisites

In order to allow the user to listen voice messages stored one a network mailbox the following settings are necessary:

On the VoIP PBX

- Set up a network mailbox for the VoIP connection that is to be assigned to the handset.

On the device

- In the provider/PBX configuration activate the **SIP SUBSCRIBE for Net-AM MWI** option (→ page 31). A subscription is established for the purpose of receiving notifications about new messages on the network mailbox.
- In the mobile devices configuration enter the **Call number or SIP name (URI)** and activate the network mailbox in the **Network mailbox configuration** section (→ page 41).
- Optional: In the mobile devices configuration enable the **Flashing LED (MWI) for network mailbox** option (→ page 42). New messages on the network mailbox are indicated by the MWI light on the Message key.

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:

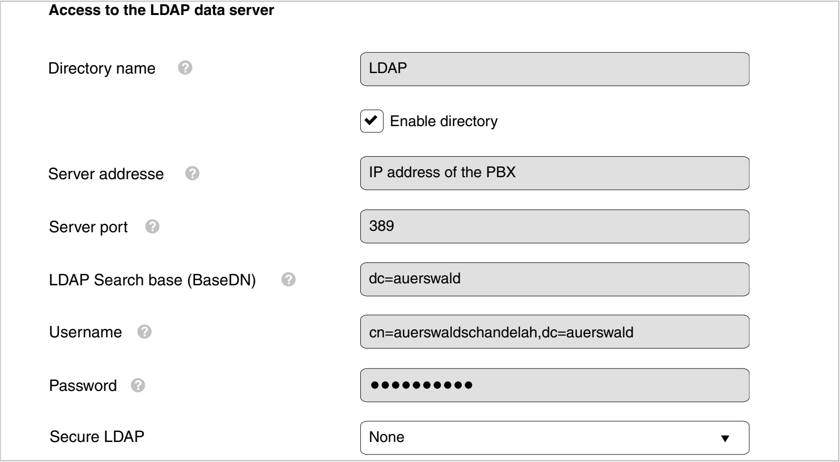
- Setting up access to the LDAP server and database
- Specifying the attributes to be displayed (→ p. 77)
- Defining search criteria (filters) (→ p. 77)

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	LDAP
	☑ Enable directory
Server addresse	IP address of the PBX
Server port	389
LDAP Search base (BaseDN)	dc=auerswald
Username	cn=auerswaldschandelah,dc=auerswald
Password	●●●●●●●●●●
Secure LDAP	None ▾

▶ 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.

▶ 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. 39).

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 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. 77

Examples:

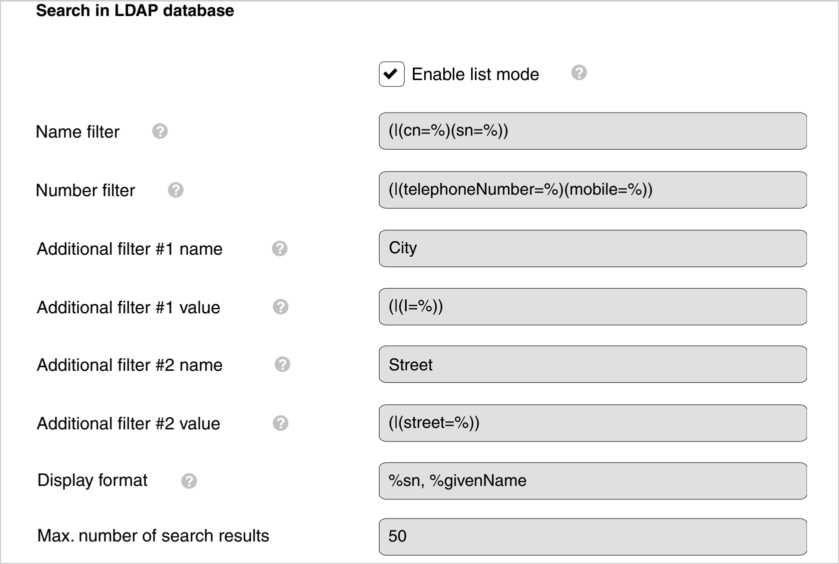
Starting point:	Object PhoneBook, in the domain example.com
Definition:	cn=PhoneBook,dc=example,dc=com
Starting point:	Object PhoneBook in the subdirectory sales/support, in the domain example.sales.com.
Definition:	cn=PhoneBook,o=support,ou=sales,dc=example,dc=sales,dc=com

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.

Filters



Search in LDAP database

☑ Enable list mode

Name filter: (|(cn=%)(sn=%))

Number filter: (|(telephoneNumber=%)(mobile=%))

Additional filter #1 name: City

Additional filter #1 value: (|(l=%))

Additional filter #2 name: Street

Additional filter #2 value: (|(street=%))

Display format: %sn, %givenName

Max. number of search results: 50

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.

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)
~	Proximity (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)"

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.

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".

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.

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

Attributes of a directory entry	Attribute name in the LDAP database
Fax	facsimileTelephoneNumber
Company	company, o, ou
Street	street
City	l, postalAddress
Zip	postalCode
Country	friendlyCountryName, c
Additional attribute	can be freely defined

Specifying attributes for display on the phone

In the web configurator 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 predefined 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.

Appendix

Contact with liquid ⚠

If the device comes into contact with liquid:

1. **Unplug all cables from the device.**
2. Allow the liquid to drain from the device.
3. Pat all parts dry.
4. Place the device in a dry, warm place **for at least 72 hours** (**not** in a microwave, oven etc. with the battery compartment open and the keypad facing down (if applicable).
5. **Do not switch on the device again until it is completely dry.**

When it has fully dried out, you will normally be able to use it again.

Light emitting diodes (LED)

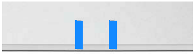
The LEDs on the front side show different operational states. The LEDs can have three different colours (red, blue, green) or can be off.

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	
⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	Power off
🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	Device is booting
🟦	🟦	⬜	⬜	⬜	⬜	🟦	🟦	Firmware update in progress
🟥	🟥	⬜	⬜	⬜	⬜	🟥	🟥	No connection to LAN or no IP address available/assigned
🟦	🟦	🟦	🟦	🟩	🟩	🟩	🟩	DECT ready
🟦	🟦	🟦	⬜	🟩	🟩	🟩	⬜	DECT traffic
🟦	🟦	🟦	⬜	🟩	⬜	⬜	⬜	DECT overload

Resetting the base station

You use the device button on the front side to reset the base station.

- ▶ Press the device button for at least 10 seconds until all LEDs switch off. ▶ Release the button . . . the device is now in programming mode.
- ▶ Short press the device button until both LED lights blue.
- ▶ Press and hold the device key until the LEDs go out again . . . the device is reset and rebooted.



❗ The system is reset to factory setting. This means, that existing configuration and user data will be lost.

Emergency reset to factory settings

When the device is booting

- Press the device button for at least 10 seconds until all LED switch off. ▶ Release the button . . . the device is now in programming mode.
- Press the device button until both LED lights blue.
- Press and hold the device key until the LEDs go out again . . . the device is reset and rebooted.

Index