Gigaset

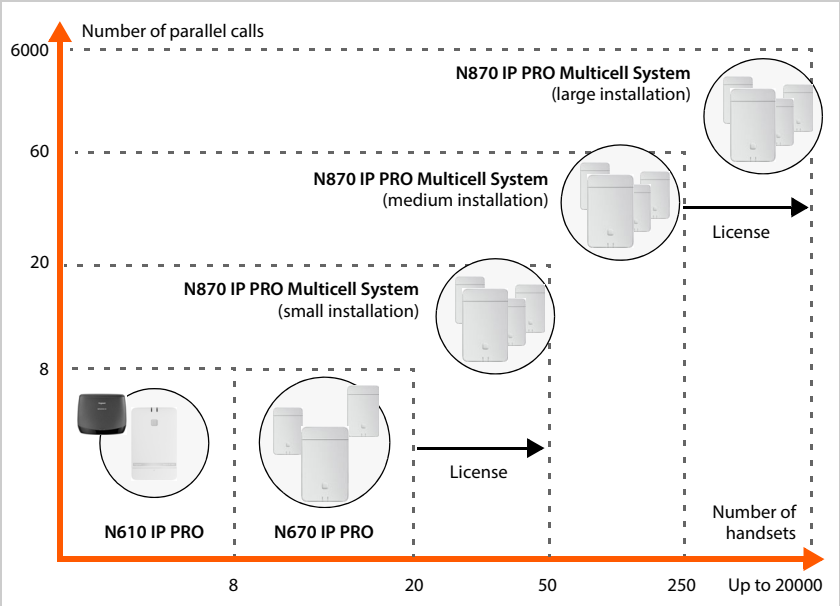
N670 IP PRO US

Installation, configuration and operation

Content

Gigaset DECT IP PRO devices – overview

Gigaset PRO DECT IP devices combine the possibilities of IP telephony with the use of DECT phones. They offer scalable telephone solutions for different company sizes and requirements.

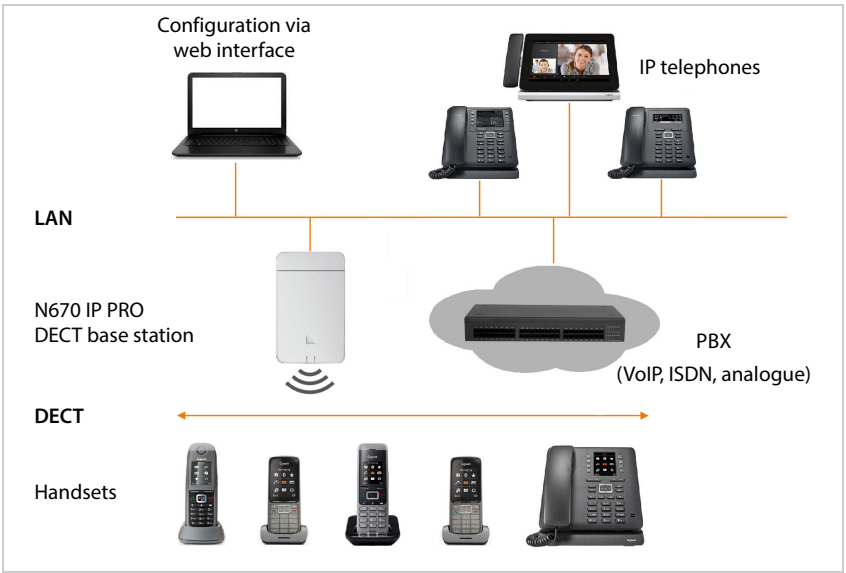


N610 IP PRO	Single cell, 8 handsets, 8 simultaneous calls Repeater support for range extension (up to 6)
N670 IP PRO	Single cell, 20 handsets, 8 simultaneous calls Mini multicell system operation with 3 base stations for range extension is possible. Upgrade to a device in an N870 IP PRO Multicell System is possible via license key.
N870 IP PRO	Multicell system Small: 10 base stations, 50 handsets, 20 simultaneous calls Medium: 60 base stations, 250 handsets, 60 simultaneous calls Possible upgrade to a large system with up to 6000 base stations, 20000 handsets, 6000 simultaneous calls. Licenses are required for this.

N670 IP PRO – Introduction

N670 IP PRO is a DECT base station for connecting to a VoIP PBX. It can be expanded with two additional N670 IP PRO devices in base only role to form a small multicell system.

The following illustration shows the way the N670 IP PRO is embedded in the IP telephone environment:



- **N670 IP PRO DECT base station**
  - Provides cell site DECT functions
  - Combines all necessary functions in one device – integrator for central management, DECT manager and base station
  - Provides media processing from handset directly towards PBX
  - Provides connection channels for the handsets, the number depends on various factors such as the approved bandwidth
  - Has an integrated DECT manager providing an application gateway between SIP signalling and DECT signalling as well as handset DECT registration
- **Handsets (mobile devices)**
  - N670 IP PRO can manage up to 20 handsets.
  - Up to eight DECT calls could be made simultaneously via VoIP, including network directory sessions and info centre sessions. For information on handset functions in relation to Gigaset base stations, visit wiki.gigaset.com.

  In operation as a small telephone system (→ p. 8):
  - Multiple lines (SIP accounts) can be assigned to one or multiple handsets. Every handset has an internal number.

- Users can perform internal free of charge calls to other participants and transfer external calls to internal participants.

> For the "multiple connections" and "internal telephony" functions, at least firmware version V2.51 must be installed.

Number of parallel calls depending on the selected codec: → p. 36

Configuring handsets → p. 42

Detailed information about approved Gigaset handsets can be found in the relevant user guide. These are provided on the Internet at wiki.gigaset.com.

- **PBX** (Private Branch Exchange)

  You need to connect your DECT telephone system to an IP PBX or Provider with VoIP (SIP) connections, e.g.,

  - On premise PBX
  - Hosted PBX
  - Cloud PBX
  - VoIP Provider

  The PBX

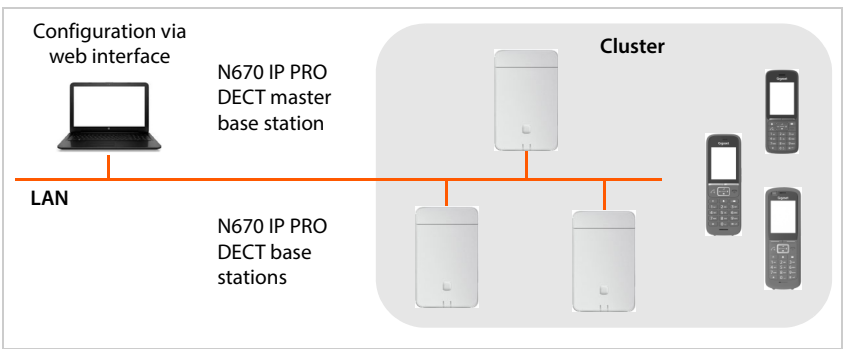
  - Establishes the connection to a public telephone network
  - Enables central management of telephone connections, directories, network mailboxes

N670 IP PRO is a smaller variant of the N870 IP PRO Multicell System. It is possible to upgrade the Gigaset N670 IP PRO US to the N870 IP PRO feature set by license key (→ p. 71).

Detailed information on the N870 IP PRO Multicell System can be found in the corresponding user documentation.

Creating a mini multicell system with N670 IP PRO devices

To expand the range of the DECT network an N670 IP PRO device can be installed in a network where another N670 IP PRO is already present. One of these devices acts as a master, the second device is switched to the **Base only** role. Two additional N670 IP PRO devices in **Base only** role are supported. The master device contains, in addition to the local base station, the components (Integrator/DECT manager) for managing the mini multicell system.



All N670 IP PRO 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.

Multi-line operation and internal telephony

By default, the N670 IP PRO is assigned the **All in one** role. This means that one SIP account is assigned to one handset. Internal calls between different handsets registered to the base station are not possible.

You can switch the device to multi-line operation. In this mode, you can assign multiple SIP accounts to a handset, e.g. different accounts for incoming and outgoing calls as well as multiple accounts for incoming calls. This makes it possible, for example, to assign a common phone number for incoming calls to different members of a team.

In addition, internal free phone calls between handsets are possible in this mode. Participants can transfer external calls to other participants.

To convert your N670 IP PRO to a multi-line device, do the following:

- Reset the device to the **All in one + internal telephony - dynamic IP** role. All your configuration data will be deleted.
- Set up your provider profiles (➜ p. 31).
- Set up all SIP accounts (➜ p. 39).
- Register the handsets with the base station and assign the SIP accounts for incoming and outgoing calls to the handsets (➜ p. 42).

When you start the Web configurator for the first time after set up, you can assign the role **All in one + internal telephony - dynamic IP** directly to the device on the start page (➜ p. 16).

Overview

Front

Device button

Reset the device → p. 14

LED displays

Operation status of the device → p. 14

Top

LAN and power cable slot

Connecting the device → p. 10

Rear

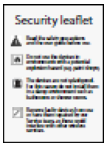
Wall mounting slots

Wall mounting → p. 13

First steps

Package content

- One N670 IP PRO
- Security leaflet
- Screws and wall plugs for wall mounting



The N670 IP PRO devices are powered by Power over Ethernet (PoE). If you do not use an Ethernet switch with PoE functionality and require a power adapter to connect to the mains power supply, you can order this as an accessory (→ p. 115).

Whenever there are new or improved functions for your Gigaset device, firmware updates are made available for you to download to your DECT base station. If this results in operational changes when using your phone, a new version of this user guide or the necessary amendments will be published on the Internet at

wiki.gigaset.com

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

To find out which version of the firmware is currently loaded, see → p. 76 and/ or p. 82.

Mounting the device

For useful information on DECT radio coverage and the resulting optimum installation please refer to the "DECT Site Planning Kit (SPK) PRO" Guide.

- The N670 IP PRO is intended for wall mounting (→ p. 13).

- The N670 IP PRO is designed for use in dry rooms with a temperature range of +5°C to +45°C.
- Never expose the N670 IP PRO to heat sources, direct sunlight or other electrical appliances.
- Protect your device from moisture, dust, corrosive liquids and fumes.

Connecting to the LAN

You can connect the N670 IP PRO to your local network via a router or switch. A VoIP PBX is required for Internet telephony. This must be accessible via the local network and must have network access.

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

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

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

Data protection notice

Once the device is connected to the Internet, it automatically contacts the Gigaset support server to make it easier for you to configure the devices and to enable communication with Internet services.

For this purpose, the system sends the following information when it is started and then once a day:

- MAC address
- Device name
- Number of registered handsets
- Number of connected base stations
- Number of connected DECT managers
- License information
- Software version

On the support server, this information is linked to the existing device-specific information:

- System-related/device-specific MAC address - MAC address password

Connecting the power supply

Your N670 IP PRO is supplied with sufficient power via PoE (Power over Ethernet) if the device is connected to an Ethernet switch with PoE functionality (PoE IEEE802.3af class 1). In this case, you do **not** need to connect the device to the mains power supply.

Defining the device role

On delivery a N670 IP PRO device is configured as **All in one** device. It is able to upgrade the device to a N870 IP PRO Multicell System component via license key. In this case the device role can be changed.

You can use the device button on the front side to change the role of the device. The following settings are possible:

- **Base station**
- **All in one** (integrator/DECT manager/base station) with dynamic IP settings
- **All in one** (integrator/DECT manager/base station) with fixed IP settings
- **DECT manager and base station**

All other roles must be set via the web configurator.

Selecting the role

▶ Press the device button for at least 10 seconds until all LED switch off . . . the device is now in programming mode.

Base station:

▶ Release the button . . . the right LED lights green.

This role is only to be used for a slave base station in a mini multicell system (→ p. 7). Licenses are required for integration into a large multicell system (→ p. 71).

All in one with dynamic IP settings:

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

All in one with fixed IP settings:

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

DECT manager and base station:

▶ Short press the device button until the left LED lights blue and the right LED lights green.

This role is only needed in combination with a virtual/embedded Integrator.

Saving the selected role

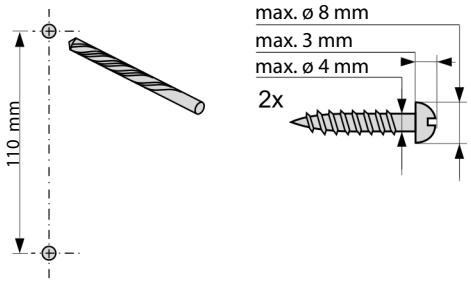
- The selected role is automatically assigned to the device, when the button is pressed for four seconds . . . both LED light red. The device is reset and rebooted (this can take up to 5 minutes).

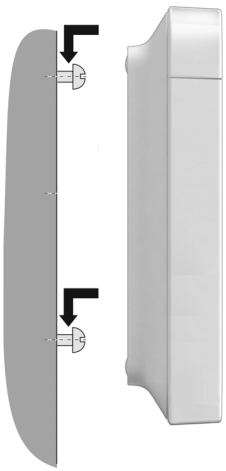
When changing the device role the system is reset to factory setting. This means, that existing configuration and user data will be lost.

If you change the role of a device that has been acting as Integrator, you should save the configuration previously .

Wall mounting

N670 IP PRO is intended for wall mounting. After connecting the LAN cable you can place it to the destined location.





Fix the device to the wall with two screws:

- Drill holes with the vertical spacing of 110 mm.
- Affix wall plugs and secure the screws. Let the screws protrude by approx. four mm.
- Hang the device on the screws.

Setting up a mini multicell system

You have installed a N670 IP PRO and want to expand the range of your DECT network (→ p. 7).

- Install one or two additional N670 IP PRO as slave base stations.
- Change the role of the slave base stations to **Base**.
  Via device button: → p. 12
  Via the web configurator: → p. 79
- On the master device add the slave base stations to the DECT network (→ p. 24).

Operation hints

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 or RTP traffic
		DECT or RTP overload

LED status display for base stations can be disabled (→ p. 26).

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 the device button at least three seconds but less than 10 seconds . . . 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 the device button for at least four seconds . . . the device is reset and rebooted.

Configuring the system

System settings are made via the web configurator of the N670 IP PRO and cannot be changed using the handsets.

This applies in particular for:

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

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

This applies, for example, for

- Display settings, such as language, colour, backlight etc.
- Settings relating to ringtones, volume, speaker profiles etc.

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

The web configurator

Use the web configurator to set up your N670 IP PRO 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 N670 IP PRO 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 N670 IP PRO to communicate with each other.

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 gigaset-config.com in the address field of the web browser

  If several Gigaset devices can be reached at this address, a list is displayed ▶ Select device . . . the N670 IP PRO web configurator is started

or

- Enter the current IP address of the base station (the master base station in a mini multicell system) 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 (→ p. 21).

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 (→ p. 69).

- 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 upper-case character
  - at least one number
  - at least one special character
  - from 8 to 74 characters

If you want to activate the functions "Mulit-line operation" and "internal telephony" (→ p. 8) for your device:

- Select the role **All in one + internal telephony - dynamic IP** from the **Reset to device** options menu.
- 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

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.

Licence terms

The login screen provides information on the open source software included in the product.

▶ In the lower right corner of the login screen click on **Licence terms**.

Showing/hiding the navigation menu

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

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 in the configuration.

> Changes that have not been saved are lost if you move to another web page or the connection to the web configurator is lost, e.g., due to exceeding the time limit (→ p. 16).

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

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

		Provisioning and configuration	→ p. 72
		Security	→ p. 73
		System log	→ p. 86
		Date and time	→ p. 75
		Firmware	→ p. 76
		Save and restore	→ p. 77
		Reboot and reset	→ p. 79
		DECT settings	→ p. 80
Status	**Overview**		→ p. 82
	Statistics	**Base stations**	→ p. 83
		Incidents	→ p. 85
		Diagnostics	→ p. 88
		DECT measurements	→ p. 89

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

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.

An error occurred: ▶ Reset the device to the factory settings.

→ p. 14

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 connected to the router/gateway.

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

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

Subnet mask

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

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

Standard gateway

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

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

Preferred DNS

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

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

Alternate DNS

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

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: 1–4094.

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; Default = 6)

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 (→ p. 14). This means that all settings are lost.

Base stations

This page is only to be used in the case that the device is used as master in a mini multi-cell system.

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**.

▶ **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.

Displaying detailed statistical data on the base stations

- Click on the ⧉ button next to the name of a base station ... statistical evaluations about the base station synchronisation as well as further system information are output.

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.

ⓘ This function can be used if the device is operated behind an external integrator (device role **DECT-Manager+Base**) and is to be replaced by another device.

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.

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. 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.

The page is only used when the device is used as a master in a small multi-cell system.

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 multicell DECT network. It consists of:

- PARI (Primary Access Rights Identity): unique system ID of a base station
- RPN (Radio Fixed Part Number): base station number within the DECT network
  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. 21). 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 transmitting power for external antenna operation

Only relevant if the unit has external antennas.

The transmitting power of the external antennas can be reduced. This may be necessary in order not to violate country-specific emission regulations if the unit is equipped with external antennas and an external patch antenna (with a gain of 8dB) is used instead of the normal external sleeve antenna (with a gain of 3dB).

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

Act as Sync Master redundancy

Only relevant in multi-cell systems.

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.

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 multicell 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 synchronisation planning, please refer to the "N870 IP PRO - Installation, configuration and operation" guide.

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

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.

- 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 multicell 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.

  This device should only be used as a base station. Devices on which the DECT Manager/Integrator is active in addition to the base station are not suitable as LAN masters due to the variety of tasks and traffic to be served.
- 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 20 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.

This page shows all available VoIP connections.

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

▶ **Settings** ▶ **Provider or PBX profiles**

Name The name that you have defined for the connection is displayed, or the default name (IP1 - IP20). It can be edited.

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

▶ Use the **Previous**/**Next** button to change between VoIP connection 1 to 10 and 11 to 20.

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.

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

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

General provider data

Domain

▶ Enter the domain IP address or FQDN (Fully Qualified Domain Name).

Mandatory field for SIP registration. It is used to form the host part of the URI (AoR) together with the assigned user names of the handsets.

Example: URI: <sip/sips>:<hsUsername>@<domain>

Proxy server address

It provides the proxy host, i.e. the network gateway for SIP traffic as a first preference.

- Enter the IP address or the FQDN (Fully Qualified Domain 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.

Deregister detached HS

The SIP account of handsets that are not reachable can be de-registered automatically.

▶ Click on **Yes**/**No** to enable/disable automatic de-registration.

Redundancy settings

Redundancy - DNS query

Defines the type of a DNS query. A DNS query is triggered if the **Domain** field contains an FQDN.

A	Query for IPv4 records based on the FQDN.
SRV + A	Query for SRV records based on the FQDN, transport protocol and SIP/SIPS scheme flag. SRV list provides list of A records with associated ports. Effectively, the provider obtains a redundancy list of host ports.
NAPTR (NAPTR + SRV + A)	Query for NAPTR records based on the FQDN. NAPTR returns a list of SRV records with the associated transport protocol and SIP/SIPS scheme. Choose only one SRV record with best priority. Query for SRV records. Effectively, the provider obtains a redundancy list of host ports.

Failover server

If **Redundancy - DNS query** = A

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

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

Registration server

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

SIP server port

▶ Enter the communication port used on the failover registrar.

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

Network data of the service provider

Outbound proxy mode

The N670 IP PRO 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.

Connection ringtones

Not available when the device is in **All in one + internal telephony - dynamic IP** mode.

Different ringtones are possible for internal, external, group, door, emergency and optional calls.

Prerequisite: The provider/platform sends the correct information via the Alert-Info field in the SIP header.

The user can select different ringtones for specific calls at the handset. You can here define which different ringtones are allowed to be set by the user.

- In the **Name** field enter the name for the menu entry that should be shown in the handset menu.

  Note: **Internal calls** cannot be changed.
- The **Alert-Info pattern** field contains the Info-Alert definition that must be contained in the SIP header to identify the appropriate call type.

  Field is empty: The entry is not shown in the handset menu.

Settings for codecs

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

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

Active codecs / Available codecs

The following voice codecs are supported:

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

To enable wideband connections via G.722 you have to activate the codec explicitly on the **Telephony** – **VoIP** page (➔ p. 53).

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 ? law): Used in USA.

G.729A 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.

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 codec

Codecs enabled	Number of calls
G729 and G711	8
G722 and G729 and G711	5

RTP and Hold options

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 option menu **Calling Party (User Part)** 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.

Parameters

FROM	Only the FROM information can be added. Caller identity in the form number@server, e.g.:12345678@192.168.15.1
PPI+FROM	P-Preferred-Identity (PPI) or FROM can be added The P-Preferred-Identity header field is used from a user agent to a trusted proxy to carry the identity the user sending the SIP message wishes to be used for the P-Asserted-Header field value that the trusted element will insert.
PAI (sip)+PPI+FROM, **PAI (tel)+PPI+FROM**, **PAI (tel)+FROM+PAI (sip)**	P-Asserted-Identity (PAI) or PPI or FROM can be added PAI (sip): The P-Asserted-Identity header field is used among trusted SIP entities (typically intermediaries) to carry the identity of the user sending a SIP message as it was verified by authentication. PAI (tel): Instead of the SIP URI, the TEL URI (telephone number) is transmitted.

Service Codes

Not available when the device is in **All in one + internal telephony - dynamic IP** mode.

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

Not available when the device is in **All in one + internal telephony - dynamic IP** mode.

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 (→ p. 49).

- 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**.

SIP accounts

You can set up SIP accounts and assign them to handsets that are registered to the base station. Multiple accounts can be assigned to one handset. One account can be assigned to multiple handsets.

For example, a handset can have different accounts for incoming and outgoing calls or multiple accounts for incoming calls. Teams can be assigned the same phone number for incoming calls. Users can make calls to each other or forward external calls to internal participants.

The function is only available when the device role is set to **All in one + internal telephony - dynamic IP** (→ p. 79).

SIP account administration

At least one provider or PBX profile must be available.

This page allows you to set up SIP accounts and assign them to handsets.

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

▶ **Settings** ▶ **SIP accounts** ▶ **Administration**

The currently configured SIP accounts are listed with the following information:

Account ID	Internal identifier for the SIP account, assigned automatically.
Account name	SIP account name, e.g. the name of a user or a team or a user group.
Username	Caller ID for the VoIP provider providing the SIP account. It is usually identical to the phone number for the account.
SIP	Indicates whether the connection works.
✔	The SIP account is registered and a connection to the provider has been established successfully.
✖	There is no SIP account configured or it is not possible to establish a connection to the configured VoIP provider.

Actions

Adding a SIP account to the list

▶ Click on **Add** . . . the SIP account data page is opened.

Deleting a SIP account from the list

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

Editing the data of a SIP account

▶ Click on ✎ next to the entry you want to edit . . . the SIP account data page is opened.

Registering SIP accounts

The page allows you to set up SIP accounts and assign them to handsets.

▶ Enter the data for the SIP account

SIP account name

▶ Enter a name for the SIP account that gives an indication of how it will be used, e.g. the name of a user, call group or organisational unit.

Personal provider data

Authentication name

▶ Specify the SIP authentication 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, no spaces allowed

Authentication password

▶ Enter the password for SIP authentication. 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, no spaces allowed

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.

Network mailbox configuration

▶ Enter the **Call number or SIP name (URI)** for the network mailbox.

▶ Activate the function via the **Activate network mailbox** check box.

Assigning handsets to SIP accounts

Lists of already assigned and available handsets are displayed for incoming and outgoing calls.

- Select the required handset from the **Assigned handsets** / **Available handsets** list and use the ← / → buttons to move the handset from one list to the other.

If you have not registered any handsets yet, you can do the assignment later.

SIP account assignment

On this page, you can assign SIP accounts to handsets that are not yet assigned or change assignments.

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

- **Settings** ▸ **SIP accounts** ▸ **Assignments**

All registered handsets are listed under **Internal Handset**.

All registered SIP accounts are listed both in the **Send** option menu and under **Receive**. For each handset you can select one SIP account for outgoing and multiple SIP accounts for incoming calls.

- From the **Send** option menu select the SIP account that should be used for outgoing calls.
- From the SIP accounts displayed under **Receive** select the one/ones you want to assign to the handset for incoming calls.

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 administration

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:

Parameters for all device roles:

IPUI International Portable User Identity used in order to uniquely identify a handset within the DECT network.

Location Name of the DECT manager the handset belongs to.

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

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
	The symbol indicates that the handset is currently not reachable (powered down, battery removed, out of range, broken, stolen, ...)

DND Indicates, if DND (Do not Disturb) 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.

Parameters for all device roles except **All in one + internal telephony - dynamic IP:**

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.

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.

Parameters only for the device roll **All in one + internal telephony - dynamic IP:**

Internal nr Internal call number under which the handset can be reached by other handsets registered on the same base station.

Internal name Internal name for the handset. It is shown in the handset idle display.

Actions

Adding a handset to the list

▶ Click on **Add** . . . the mobile devices data page is opened.

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. 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. 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.

Not available when the device is in **All in one + internal telephony - dynamic IP** mode.

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.

Setting the name to be displayed in the idle display

Not available when the device is in **All in one + internal telephony - dynamic IP** mode.

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

Registering/de-registering 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/de-registration 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.

▶ 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. Default: 3 min.

On the handset

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

Registering a set of handsets

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

▶ Enter the actual IPUI and maybe an individual PIN

or

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

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 de-register the handset.

Authentication Code (PIN)

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

- Enter a PIN in the text field. Value: 4 digits

or

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

Internal nr

Only when the device is in **All in one + internal telephony - dynamic IP** mode.

- Select the internal call number under which the handset can be reached by other handsets registered on the same base station.

Internal name

Only when the device is in **All in one + internal telephony - dynamic IP** mode.

- Enter an internal name for the handset. It is shown in the handset idle display.

De-registering handsets

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

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

Settings for the handset

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

Personal provider data

Provider data is not required if you operate the device in **All in one + internal telephony - dynamic IP** mode. In this case, the handsets receive the provider data via SIP account assignment.

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.

VoIP provider

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

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

Authentication name

- Specify the SIP authentication 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, no spaces allowed

Authentication password

- Enter the password for SIP authentication. 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, no spaces allowed

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.

Do not use spaces in **Authentication name** and **Username**. Spaces may cause problems with SIP registration of the device.

Assigning accounts

Only available when the device is in **All in one + internal telephony - dynamic IP** mode.

Lists of already assigned and available SIP accounts are displayed for incoming and outgoing calls.

- Select the required account from the **Assigned accounts** / **Available accounts** list and use the ← / → buttons to move the account from one list to the other.

Online directories

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

Directory for direct access

The user can open a directory via the handset directory key (bottom of the control key). By default, **short** pressing the directory key opens the list of online directories, **long** pressing opens the local directory of the handset.

- Choose which directory should be called up by short pressing the directory key.

Online directories	A list of online directories is opened by short pressing. Long pressing opens the local directory.
Local directory	The local directory is opened by short pressing. Long pressing opens the online directories.

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.

Not available when the device is in **All in one + internal telephony - dynamic IP** mode.

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.

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**).

The feature is not available when the device is in **All in one + internal telephony - dynamic IP** mode.

Network mailbox configuration

Not available when the device is in **All in one + internal telephony - dynamic IP** mode.

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 via the **Activate network mailbox** check box.

Group pick-up

Not available when the device is in **All in one + internal telephony - dynamic IP** mode.

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

▶ Enter the **Call number or SIP name (URI)** of the pick-up group.

▶ Activate the function via the check box.

Call manager

Not available when the device is in **All in one + internal telephony - dynamic IP** mode.

- From the option menu select, whether calls that are initialised by a PBX call manager are to be accepted directly:

via Headset	To accept the call the handset automatically activates the connected headset.
via Handsfree	To accept the call the handset automatically activates the speaker phone function.
No	The call is not accepted automatically at all.

Direct call acceptance requires a secured signalling to the PBX (TLS).

Accepting calls via a Call Manager has no impact on the DECT system performance, because it is handled on SIP level.

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

Not available when the device is in **All in one + internal telephony - dynamic IP** mode.

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.

CSTA must be provided by your PBX and must be activated in the provider/PBX profile (→ p. 38)

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.

XSI services must be activated (→ p. 57).

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

Not available when the device is in **All in one + internal telephony - dynamic IP** mode.

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.

Provisioning and configuration

With this function you initialise the handset settings manually without having to wait for the automatic provision. You can use it to check whether all settings are correctly adopted.

The handset provisioning must be enabled. A provisioning server must have been set up on the **Settings – System – Provisioning and configuration** page.

Provisioning server

Shows the URL of your provisioning server.

Last sync time

Shows the time at which the last synchronisation was carried out.

Start auto configuration

- Click on the button . . . the provisioning of the handset settings is started.

  The button is enabled, if the IPUI is set.

You receive a message, if the process was successful or not.

Use an AML license for the handset

You can activate/deactivate the alarm features **Location** and/or **Messaging** for the handset.

The online service AML must be is set up and there must be free licenses for the handset.

Show free licenses: ▶ Guide pointer over the check boxes . . . The number of available and used licenses is displayed.

Location

- ▶ Enable/disable cooperation with the location/alarm server. If enabled, the location of the handset is visible on the server.

Messaging

- ▶ Enable/disable cooperation with the alarm server. If enabled, messages from the alarm server can be sent to the handset and reactions from the user can be sent back to the server.

Mobile devices – Registration Centre

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

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 N670 IP PRO 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

Current time

Shows the current system time.

Registration start time

- ▶ 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

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.

- 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.

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.

To allow users to make wideband calls, the codec G.722 must have been activated for the provider profile that is used for the connection (→ p. 36).

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.

Ignore Access and Area Codes

Emergency numbers

You can enter numbers (e.g. emergency numbers) for which access or area codes must not be added (up to 5 numbers with a max. length of 9 digits, separate the numbers by comma).

Internal number length

You can also specify the length of internal numbers up to which no access and area codes will be added.

Exceptions to this rule can be added in the field "Ignore length for numbers".

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 configuration. These settings apply to all registered handsets.

Access Code

- Enter an access code in the text field. Value: max. 3 digits (0 – 9, *, R, #, P)

is added to numbers

- 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

Use area code

- Select from the option menu when the area code is to be prefixed to the call number: **For local calls**, **For local and national calls** or **No** (never)

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.

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 phone system 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.

Enable XSI call logs

Not available when the device is in **All in one + internal telephony - dynamic IP** mode.

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

Online directories

N670 IP PRO 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 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.
Server url	If the directory is configured, the server URL is displayed.
Activation status	Indicates if the directory is activated or not.
✔	The directory is activated.
✖	The directory is not activated.

Configuring LDAP directories

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

ⓘ Detailed information about LDAP configuration can be found at wiki.gigaset.com

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 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.
- Enter 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.

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.

- 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 ➔ p. 61

Name filter

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

Example:

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

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

Number filter

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

Example:

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

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

Additional filters

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

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

Example:

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

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

Display format

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

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

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

Example:

Data of an directory entry on the LDAP server:

displayName	Peter Black	**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

- 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

Field of a directory entry	Attribute name in the LDAP database
Street	street
City	l, postalAddress
Zip	postalCode
Country	friendlyCountryName, c
Additional attribute	user-defined

- Mark the check box, if an additional attribute is defined and it is a phone number.

A detailed configuration example can be found in section "LDAP directory – configuration example" ➔ p. 97

LDAP configuration with Windows Active Directory server

Active Directory Domain Services (AD DS) is the directory service for Windows server. In a multi-domain AD DS forest (container within an Active Directory configuration containing domains, users, hosts and group policy) the Global Catalog is a distributed data repository that contains a searchable, partial representation of every object in every domain. The global catalog is stored on domain controllers that have been designated as global catalog servers and is distributed through multi-master replication. Searches that are directed to the global catalog are faster, because they do not involve referrals to different domain controllers.

In addition to configuration and schema directory partition replicas, every domain controller in a forest stores a full writeable replica of a single domain directory partition. A domain controller can locate only the objects in its domain. Locating an object in a different domain would require the user or application to provide the domain of the requested object.

To use an LDAP directory provided via Active Directory service you can use the following ports:

Default ports: 389 (LDAP) / 636 (LDAPS)

These ports are used for requesting information from the local domain controller. LDAP requests sent to port 389/636 can be used to search for objects only within the global catalogues home domain. However, the requesting application can obtain all of the attributes for those objects.

Default ports: 3268 (LDAP) / 3269 (LDAPS)

These ports are used for queries specifically targeted for the Global Catalog. LDAP requests sent to port 3268/3269 can be used to search for objects in the entire forest. However, only the attributes marked for replication to the Global Catalogue can be returned.

Online directories in XML format

A public and/or a corporate online directory in XML format can be made available to the user.

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

▶ **Settings** ▶ **Online directories** ▶ **XML**

Name	The name that you have defined for the directory is displayed, or the default name (Public/Corporate). It can be edited.
Server url	If the directory is configured, the server URL is displayed.
Activation status	Indicates if a directory and what kind of directory is activated.
	✔ The directory is activated.
	✖ The directory is not activated.

Configuring XML directories

▶ Click on ✎ next to **Public** or **Corporate** ... the XML directory configuration page is opened.

Entering the data for an XML directory

Use this page to enter the provider's details and a name for the 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.

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.

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**.

The XSI directory service must be enabled on the **Telephony – XSI Services** page (→ p. 57).

▶ **Settings** ▶ **Online directories** ▶ **XSI**

Server address

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

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.

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.gigaset.com

▶ **Settings** ▶ **Online directories** ▶ **Central phonebook**

Directory name

- 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.
- Mark the **Enable directory** option, so that the directory is 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.

Max. number of search results

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

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 the phone book 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.

Save the phone book to PC

You can backup the central phone book to your computer.

- Click on **Save phonebook** ▶ Select the location where the phone book should be stored using the system file selection dialogue. Enter a name for the phone book backup file.

Delete the phone book

- Click on **Delete phonebook** to remove the phone book from the handsets.

A search in the central telephone book returns all entries that contain the characters entered by the user somewhere in the first or last name.

Alternatively, the following can be set via provisioning: Only those entries are returned that have the entered characters at the beginning.

Detailed information about provisioning parameters can be found at wiki.gigaset.com.

Online services

XHTML

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.gigaset.com.

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.
Display key	Name of the display key on the handset with which the function is triggered.
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.

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.

Name for display key

▶ Enter a name in the text field (max. 8 characters). This is the name under which the display key function 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**).

Alternatively, the following credentials can be used.

Username

▶ Enter a user name for access to the menu.

Password

▶ Enter a password for access to the menu.

Application Server

Not available when the device is in **All in one + internal telephony - dynamic IP** mode.

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.
DGUV support:	DGUV-compliant protection of employees working alone in dangerous situations with the aid of special DECT devices. For example, alarms that are triggered in certain cases: "man down" function triggered, emergency button pressed, explosion, detached cable.
Messaging:	Messages from an alarm server (or another server/platform) are sent to the DECT handsets. Reactions from users can be sent back to the server. Messages may contain an icon (coloured) if the DECT phone supports this, e.g. for fire alarm, nurse call, . . . Prioritised messages can be signalled with specific different ringtones.
Location:	The location of a handset is made visible on an alarm server. The alarm server can show visited and neighbouring base stations including signal strength.

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

Detailed information about working with application servers and AML can be found at wiki.gigaset.com.

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 an application server

▶ 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** (➜ p. 16). 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**.

If you have forgotten the password, you will have to reset the device to the factory settings (➜ p. 14).

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.

▶ Enter a new password for the user access to the web configurator and repeat it.

Enabling CLI access to the device configuration

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

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

Repeat password

- 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**.

Loading the 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 multicell system, you need to upload a 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 multicell 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 multicell 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/multicell DECT network is possible **DECT Manager - Multi cell** Used for single cell devices to be used as DECT manager in the multicell system. Licenses for AML (Alarming, Messaging, Location) **Messaging** Enables cooperation with an alarm server (or other servers/platforms). Messages from an alarm server can be sent to the DECT handsets. Reactions from users can be sent back to the server. **Location** Enables cooperation with location/alarm servers. The location of an handset can made visible on the server. Each handset that is required to send location data needs an own handset location license. The **Location** license includes a **Messaging** license.
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).

Showing detailed information on the license currently used

▶ Click on **Show licence status** ... the name of the license package, the license status and the activation time is shown.

Uploading the license file

Your distributor will send you the license activation file.

▶ 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.
- The Messaging and Location licences do not have a grace period. Instead, test licenses for Messaging and Location are granted for one handset.

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.

Detailed information on how to establish a provisioning server and create provisioning profiles for Gigaset phones: → wiki.gigaset.com

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

Provisioning server

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

Auto configuration file

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

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

Start auto configuration

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

The process will take some time.

For security reasons you should save the configuration before you start an auto-configuration process.

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

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

Last sync time

Time of the last synchronisation.

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. If you have a time server available, you should not activate this function.

▶ Click on **Yes**/**No** to determine the internal time server to act/not to act as local time server.

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

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.

DECT manager firmware update

On this page you enter the planning data for a firmware update of the DECT Manager.

DM Name and **Current version** are shown.

URL to firmware file

▶ In the text field specify the URL of the configuration server where the firmware is located .

Planned schedule

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.

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 de-registering handsets, you should save the latest settings in a file on the computer so that the current system can be restored quickly if problems occur.

If you change the settings accidentally or you need to reset the 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.
The default file name is
<MAC address of integrator><firmware version><date of export>_device-settings

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.

Automatic backup

You can automatically back up your configuration to an SFTP server at regular intervals (SFTP = Secure File Transfer Protocol).

Enable automatic backup

▶ Select the check box next to **Enabled** . . . the automatic backup of your configuration is activated according to the following settings when you click on the **Set** button.

Server

▶ Enter the address of the server to which the backup should be sent.

> The URL must end with a slash (/), otherwise the SFTP upload will not start.

Example: sftp://192.168.178.200/

The system creates a backup file with the following name:
<MAC address>_<software version>_YYYY_MM_DD_device-settings

You can also enter the name of the file directly:

Example: sftp://192.168.178.200/system_backup.cfg

Server port

▶ Enter the port number, where the SFTP server expects to receive requests (default: 22).

Authentication name

▶ Specify the authentication name for the access to the SFTP server.

Authentication password

▶ Enter the password for the access to the SFTP server.

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.

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.

Factory reset can also be performed by using the device key (➞ p. 14).

Defining the role

▶ From the option menu, select the role the device should have after the reset.

Base only

The device is used as base station.

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

All in one + internal telephony - dynamic IP

The roles Integrator + DECT manager + base station are active. Multiple lines (SIP accounts) can be assigned to the handsets. Internal calls between handsets registered to the base are possible. The network configuration is set to dynamic IP.

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 a Gigaset N670 IP PRO US. All three components are active in one device (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.

The **Base only** role can only be assigned to a device that should be used as slave in a mini multicell system. The device cannot be used as base with a DECT manager of a multicell system.

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.
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 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.

Diagnostics and troubleshooting

Status information

The status page offers important information on the system operation and the involved devices.

▶ **Status** ▶ **Overview**

The following information is provided.

Integrator status

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

Note: The integrator is the central management station of a DECT network. In single-cell systems, it is integrated as a software component in the base station.

- Licence information

Base stations

Only with a multicell system

- Number of active base stations
- Number of pending base stations
- Number of online base stations
- Number of offline base stations
- Call limit for base station only

Mobile devices

- Number of registered mobile devices (reachable/all)
- Number of mobile devices to register

Number of mobile devices with SIP registration (connected/all)

Accounts

Number of accounts with SIP registration (connected/all)

(Only shown when the device is in **All in one + internal telephony - dynamic IP** mode.)

▶ Click on See also... in the header line ... a list of all pages providing information or settings for diagnostic purposes is shown.

System backup

Besides **Last backup** date and time of the last backup is shown. As long as no backup has been created, **Never** is displayed instead.

Creating a new backup or restoring an existing backup file:

▶ Click on **System** ▶ **Save and restore** . . . the **Save and restore** page is opened.

Administration

For some entries you can directly jump to the associated Web configurator page.

▶ Click on the button next to the corresponding entry in the table.

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 (always **local**), time period in which the events have been collected, total number of missed and active callswithin the given time period.

Missed Calls: These are incoming calls that were successfully received by the DECT manager but did not reach the handset, e.g. due to insufficient coverage. This does not refer to missed calls by the user.

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

Cluster Cluster number, summary of the collected events

A cluster includes all base stations of a DECT network. A singlecell system or a mini multicell system always has only one cluster. Therefore the cluster number is always 1.

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

Base station Name of the base station

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

Sync Level Synchronisation level

Statistics

Conn	Number of established connections on DECT MAC layer. For example, through user actions: VoIP calls, accesses to an online phone book, Internet connections, etc. Or through system actions: Updating idle displays, date/time synchronisation, locating handsets for roaming, etc.
Ho setup	Number of incoming handovers
Ho release	Number of outgoing handovers
Call drops	Number of lost connections, i.e. interrupted calls
Async	How often the base station has lost on-air DECT synchronisation
Busy	How often the maximum number of possible connections of the module was achieved.
Conn. drops	How often the LAN connection to the base station was interrupted
Calls	Active calls
Calls-pk	Peak number of parallel calls
Sync swaps	Number of sync swaps, i.e. , how often the sync master has been changed due to a sync master crash.
q-idx-lt	LAN synchronisation quality > 90% LAN sync is functional. The remaining 10% evaluate the synchronisation quality. > 93% Good synchronisation quality.
o-thr-exc	PTP offset threshold exceeded counter If the PTP deviation > 500 ns, the counter is increased. The requirement for the network is that the PTP deviation is < 500 ns.
d-thr-exc	DLS offset threshold exceeded counter If the DLS deviation > 1000 ns, the counter is increased.

Synchronisation-specific (Sync) and handover-specific values (Ho) are not relevant for single cell systems.

Actions

Displaying detailed statistical data on the base stations

▶ Click on the button next to the name of a base station ... statistical evaluations about the base station synchronisation as well as further system information are output.

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:

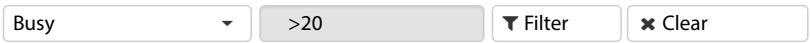
<	less than	>	more than	=	equal to
<=	less or equal	>=	more or equal		

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)

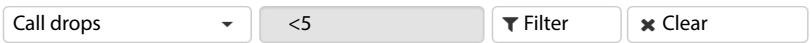
Deleting the filter: ▶ Click on **Clear**

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.



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



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 system 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
Incident Type	e.g. **Crash**, **Reboot**, **Reset**
Severity	Degree of severity: **Critical**, **High**, **Medium**, **Low**, **Info**
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.

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

Transport protocol

- Select the transport protocol used for communication with the Syslog server.

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 single and mini multicell systems.

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. SNMPv3 is supported, with authentication and privacy communication.

- 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 single and mini multicell systems.

Configuration

Default configuration

User name:	admin
Authentication protocol:	SHA
Password:	snmp-admin
Privacy protocol:	AES
Target for SNMP traps (SNMP manager IP address and port):	0.0.0.0:162

SNMP manager configuration example

Target host:	N670 IP PRO IP address
User name:	admin
Target port:	161
Security level:	Auth, Priv
Authentication protocol:	SHA
Authentication password:	snmp-admin
Privacy protocol:	AES128
Privacy password:	snmp-admin

SNMP commands (examples):

Obtaining MIB information starting from a specific MIB variable:

snmpwalk -v3 -l authPriv -u admin -a SHA -A snmp-admin -x AES -X snmp-admin “ipaddress” 1.3.6.1.4.1.32775.1.1.1

Obtaining next information in the MIB tree:

snmpgetnext -v3 -l authPriv -u admin -a SHA -A snmp-admin -x AES -X snmp-admin “ipaddress” 1.3.6.1.4.1.32775.1.1.1.1

Configuring SNMP-Traps:

trapsess -v 3 -u admin -l AuthPriv -a SHA -A snmp-admin -x AES -X snmp-admin "ipaddress"

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.

Diagnostics

For diagnostic purposes you can create a dump with different contents. A dump may help software developers and system administrators to diagnose, identify and resolve problems that led to system failures.

▶ **Status** ▶ **Incidents** ▶ **Diagnostics**

A standard set of diagnostic info will be downloaded. Additionally you can add following options:

Core dump	Includes, if available, a core dump of a crashed application.
Ram dump	Includes, if available, a RAM dump of a crashed CSS (co-processor for DECT and media real-time processing). Core dump and CSS RAM dump can be used by service personnel for post-mortem debugging. Because the file size is several MBytes, not all data can be collected due to limited overall sysdump file size. Therefore, these options should be used carefully.
Last incident sysdump	Dump of the last incident. Contains only the system memory part that represents the last incident.
Save settings	If the option is activated, the diagnostic file contains the complete backup (default). A full backup makes problem resolution faster because all settings are included. The option can be deactivated if the client does not want to include such a backup for confidentiality reasons. In this case, the check mark must be removed each time a diagnostic file is created.

▶ Mark the check mark next to the dump type you want to include.

▶ Click on **Download** ▶ Select the location where the dump file should be stored using the system file selection dialogue. Enter a name for the dump file. The file is stored as tar archive. The default file name is

<MAC address of integrator><firmware version><date of export>_diagnostics.tar

DECT measurements

For planning DECT sites or analysing specific network problems, you can collect DECT measurement data, save it in the N670 IP PRO and download it in CSV format for evaluation.

The measurement data of up to 20 sites can be stored.

You take DECT measurements with handsets that can be operated in measurement mode, for example, handsets included in the DECT Site Planning Kit (SPK) PRO. You could also use other handsets. However, the handsets in the measurement kit are calibrated. Only calibrated handsets provide calibrated measurement values.

Start measurement: ▶ Dial [*] [*] [*] [9] [2] [2] ▶ press the off-hook key [ ] ... the measurement starts immediately

Save measurement data: ▶ Press the **Log** display button ▶ enter the requested information about the location and position of the measuring devices ... the measurement data is saved in the system

On this page you can download measurement data stored on the system to your PC in CSV format.

▶ **Status** ▶ **Statistics** ▶ **DECT measurements**

DM Name

If you have carried out the measurement in a living system with several DECT managers:

▶ Select the DECT manager behind which you have carried out the measurement.

In case of an all-in-one system, you do not need to select the DECT manager.

Site

The names of the sites you entered when you started measuring processes on the handsets are listed. The number of the existing files for the site are shown below **Files**.

▶ Mark the check box next to the sites whose data you want to download.

Click on Download and select the desired file location in the file system.

For each measurement file of the selected sites a file is created in CSV format. The files of a site are taken into a tar file. All tar files are saved in another superordinate tar file.

▶ Click on **Delete** to remove the log files which are not longer needed from the system.

The oldest files are overwritten automatically when the maximum capacity of 20 sites is reached and no sites are deleted.

For detailed information on how to work with the DECT Site Planning Kit (SPK) PRO devices and how to evaluate the CSV files, refer to the corresponding user manual.

Using a handset connected to an N670 IP PRO base

The functions of your N670 IP PRO 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.

For information about which Gigaset handsets support the complete functionality of the N670 IP PRO multicell system please refer to wiki.gigaset.com.

Making calls

You can make calls using any handset registered to your N670 IP PRO.

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

Each handset is assigned a send and receive connection (➔ p. 46).

If your N670 IP PRO 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.

If internal telephony is permitted on the base station (device role **All in one + internal telephony - dynamic IP**), internal calls between the handsets are also possible.

The N670 IP PRO 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.

Depending on the specifications of your PBX, you may need to dial an access code for calls outside the area covered by your VoIP PBX (➔ p. 56).

Calling

▶ enter a number ▶ **briefly** press the Talk key

or

▶ Press and **hold** the Talk key ▶ enter a number

The connection is established using the SIP connection assigned to the handset (➔ p. 46).

If you make a call to the fixed line network, you may also have to dial the area code for local calls (depending on the PABX/provider). This is not necessary if the area code is entered in the telephony configuration (➔ p. 56).

Dialling from the redial list

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

▶ **Briefly** press the Talk key … the redial list is opened ▶ select an entry ▶ press the Talk key

Dialling from the call list

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

▶ ▶ ▶ **Call Lists** ▶ **OK** ▶ select a list ▶ **OK** ▶ select an entry ▶ press the Talk key

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

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 (→ p. 37).

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

Accepting calls

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

▶ Press the Talk key to accept the call.

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

Reject a call: ▶ Press the End call key

Information about the caller

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

Using a PBX call manager

In case a PBX call manager is used it is possible to define that incoming calls are accepted directly via headset or handsfree. This has to be configured for the handset via web configurator in the **Call manager** section (→ p. 49).

Group pickup

You can also accept incoming calls for the group.

Group pickup must be activated and the call number or SIP URI of the group must be entered. This has to be configured for the handset via web configurator in the **Group pick-up** section (→ p. 48).

Accepting/rejecting call waiting

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

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

Holding a call

You can place an ongoing call on hold:

▶ **Options** ▶ **Hold Call** . . . the call placed on hold receives music

You can initiate a consultation call by typing a number, accessing a directory or using a short dial.

End hold and return to the initial call: ▶ **Retrieve**

Accepting a third call while call is on hold:

- Reject a call: ▶ **Reject**
- Accept a call: ▶ **Accept** ▶ Speak to the new caller. The previous call is placed on hold.

Swapping calls between accepted call and call on hold:

▶ Press to switch back and forth between calls

Conversation with three participants

Consultation calls

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

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

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

Ending a consultation call

▶ **Options** ▶ **End Active Call** ▶ **OK** . . . the connection to the first caller is reactivated

or

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

Call swapping

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

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

Transferring a call in call swap mode

You can transfer the active call in call swap mode.

- **Options** ▶ **Call Transfer** ▶ **OK** ... the call is transferred

You can also transfer the call by R-key or On hook depending on your system settings (➜ p. 55).

Ending a currently active call

- **Options** ▶ **End Active Call** ▶ **OK** ... the connection to the other caller is reactivated

or

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

Conference

Speaking to both participants at the same time.

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

Initiate conference call:

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

Return to call swapping:

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

End call with both participants:

- Press the End call key

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

Call transfer

Connecting an external call with a second external participant.

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

Call transfer options must be set correctly for the PBX/provider (➜ p. 55).

Internal calls

Internal calls are only possible, if the device is in **All in one + internal telephony - dynamic IP** mode (→ p. 8) and at least two handsets are registered to the base station.

Calling

- Press INT key **briefly** ... the handset list is opened, the own handset is marked with <
- select a handset ▶ press the Talk key

or

- enter the internal number of the handset ... the call is initiated automatically

Incoming calls

An incoming internal call is shown in the display with the internal number and the internal name of the calling handset.

- Press the Talk key to accept the call.

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

Reject a call: ▶ Press the End call key

Consultation call / Call transfer

You are on a call with an external participant and want to consult with an internal participant or transfer the call.

Press the INT key ▶ select a handset ▶ press the Talk key ... the external call is put on hold, both calls are shown in the display

Toggle between the external and internal call: ▶

Transfer the call to the internal participant: ▶ Press the End call key

Message indication

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

Which messages are displayed on the handset is defined during handset configuration in the **Missed calls and alarms** section (→ p. 49).

Missed calls count

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

Message Waiting Indication (MWI)

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

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

Using directories

The options are:

- The (local) directory for your handset (see handset user guide)
- Corporate directories provided by an LDAP server (→ p. 58)
- Miscellaneous online directories

The directories available are defined by the web configurator of the telephone system (→ p. 58).

Opening directories

Opening the corporate directory using the INT key

The INT key (press left on control key) on the handsets opens a corporate directory, provided that this is set up via the web configurator using the **Corporate directory for INT key** option and can be accessed by the telephone system. The directory to be opened can be set for each handset (→ p. 47).

Opening directories using the directory key

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

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

This assignment can be changed for each handset via the web configurator using the **Directory for direct access** option (→ p. 47). Direct access can be assigned to a specific online directory. In this case, open the local directory by pressing and holding the directory key.

The description below assumes the default assignment.

Opening directories via the menu

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

Local directory

▸ ▸ **Contacts** ▸ **OK** ▸ **Directory** ▸ **OK**

List of all online directories set up on the telephone system

▸ ▸ **Contacts** ▸ **OK** ▸ **Online Directory** ▸ **OK**

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

Example for handling a corporate directory on the handset → p. 103

If handsets are connected to an N670 IP PRO, it is not possible to transfer entries from the local directory to another handset.

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 on 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 N670 IP PRO

- In the provider/PBX configuration activate the **SIP SUBSCRIBE for Net-AM MWI** option (→ p. 33). 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 (→ p. 48).
- Optional: In the mobile devices configuration enable the **Flashing LED (MWI) for network mailbox** option (→ p. 49). New messages on the network mailbox are indicated by the MWI light on the Message key.

Playing back messages on the handset

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

or

- Press the Message key ▸ select the network mailbox ▸ **OK**

or

- ▸ **Answer Machine** ▸ **OK** ▸ **Play Messages** ▸ **OK** ▸ **Network Mailbox** ▸ **OK**

Listen to announcement out loud: ▸ Press the handsfree 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:

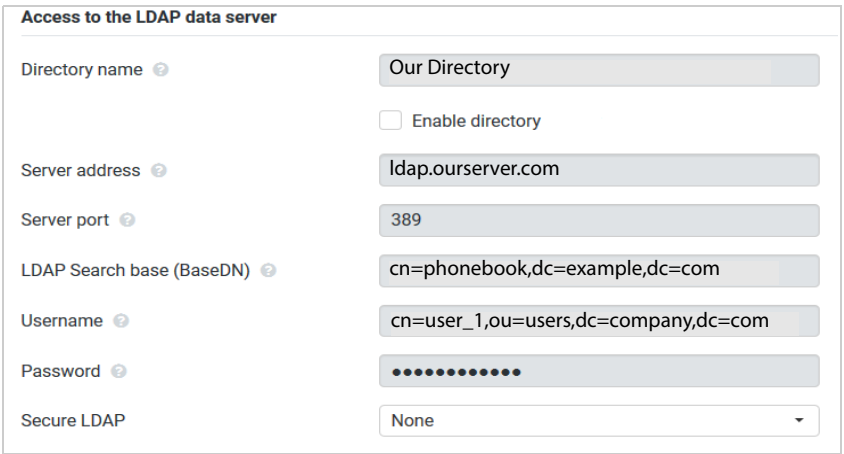
- Setting up access to the LDAP server and database
- Specifying the attributes to be displayed (➔ p. 102)
- Defining search criteria (filters) (➔ p. 99)

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.



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

This is the name under which the directory will appear in the list of network directories on the telephones (➔ p. 103).

▶ 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. 48).

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. 99

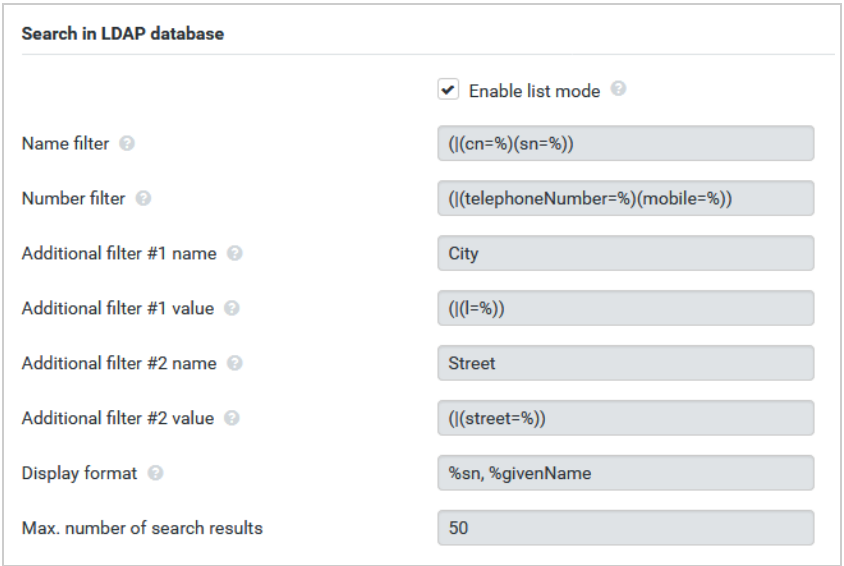
Examples:

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.



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
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.

Display on the handsets

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

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

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

To display the corporate directory on the telephone screen

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

Depending on the settings for the handset in the web configurator (➔ p. 47), you may also be able to access a corporate directory via the directory key .

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

Entries in the directory

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

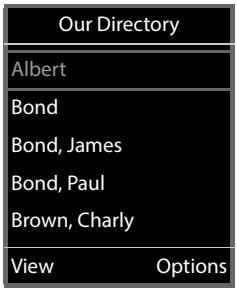
The menu shows all directories that have been set up and activated on the **Online directories** page in the web configurator. Each one appears with the name entered under **Directory name** in the web configurator (➔ p. 97). In the example on the right, the LDAP directory is shown as **Our Directory**.

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

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

The LDAP directory is displayed according to the following rules:

- The search begins in the directory/subdirectory which is defined as the search base on the LDAP server and specified with the **LDAP Search base (BaseDN)** parameter in the web configurator (→ p. 98).
- The entries are listed in alphabetical order.
- The entries are displayed with **Surname** and **First name** if both attributes are available in the LDAP database. Otherwise only the surname or first name is displayed.



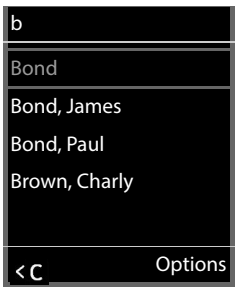
Searching the directory

▸ Use to scroll through the directory

or

▸ use to enter a name (or the first few letters).

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



▸ Use < C to delete the last character you entered.

The current search string is shown in the top line.

Displaying a directory entry

▸ Use to select the entry you want.

▸ Press the display key **View** or the navigation key .

or

▸ Press the display key **Options** ▸ **View**

The directory entry is displayed with its detailed information. Only attributes for which a value is stored are shown (→ p. 99).

▸ Use to scroll through the entry.

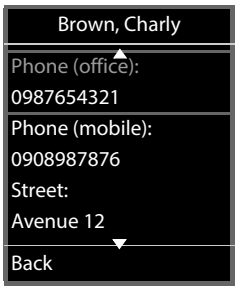
▸ Press the End call key or the **Back** display key to close the entry.

Dialling a number from the directory

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

or

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



Appendix

Innovation, Science and Economic Development Canada - Certification

This device complies with Industry Canada licence-exempt RSS standard(s).

Operation is subject to the following two conditions (1) this device may not cause interference, and (2) this device must accept any interference, including interference that may cause undesired operation of the device.

NOTICE: The ISED label identifies certified equipment. This certification means that the equipment meets certain telecommunications network, protective, operational and safety requirements as prescribed in the appropriate Terminal Equipment Technical Requirements document(s). The Department does not guarantee the equipment will operate to the user's satisfaction.

Before installing this equipment, users should ensure that it is permissible to be connected to the facilities of the local telecommunications company. The equipment must also be installed using an acceptable method of connection. The customer should be aware that compliance with the above conditions may not prevent degradation of service in some situations.

Repairs to certified equipment should be coordinated by a representative designated by the supplier. Any repairs or alterations made by the user to this equipment, or equipment malfunctions, may give the telecommunications company cause to request the user to disconnect the equipment.

This product meets the applicable Innovation, Science and Economic Development Canada technical specifications including licence-exempt RSS standard(s).

FCC / ACTA Information

Warning: Changes or modifications to this unit not expressly approved by Gigaset Technologies GmbH could void the FCC authority to operate the equipment. This includes the addition of any external antenna device.

This equipment complies with Part 68 of the FCC rules and the requirements adopted by the ACTA. On the bottom of the base station is a label that contains, among other information, a product identifier in the format US:AAAEQ##TXXXX. If requested, this number must be provided to the telephone company.

A plug and jack used to connect this equipment to the premises wiring and telephone network must comply with the applicable FCC Part 68 rules and requirements adopted by the ACTA. A compliant telephone cord and modular plug is provided with this product. It is designed to be connected to a compatible modular jack that is also compliant. See installation instructions for details.

This telephone system equipment has been tested and found to comply with the limits for Class B digital device, pursuant to Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) This device must accept any interference received, including interference that may cause undesired operation. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications.

However, there is no guarantee that interference will not occur in a particular installation. If this telephone system does cause harmful interference to radio or television reception, which can be determined by turning the system off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

1 Reorient or relocate the receiving antenna.

2 Increase the separation between the equipment and receiver.

3 Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.

4 Consult the dealer or an experienced radio TV technician for help.

Notice to Hearing Aid Wearers:

This phone system is compatible with inductively coupled hearing aids.

Power Outage:

In the event of a power outage, your cordless telephone will not operate. The cordless telephone requires electricity for operation. You should have a telephone that does not require electricity available for use during power outages.

Radio frequency radiation exposure Information:

The installation of the base unit should allow at least 8 inches between the base and persons to be in compliance with FCC RF exposure guidelines.

For body worn operation, the portable part (handset) has been tested touched to the phantom and meets FCC RF exposure guidelines. Nevertheless, the device should be used in such a manner that the potential for human contact during normal operation is minimized.

Safety precautions

Before using your telephone equipment, basic safety instructions should always be followed to reduce the risk of fire, electric shock and injury to persons.

1 This product should be installed by a qualified technician.

2 This product should only be connected to the host equipment and never directly to the network such as Public Switch Telephone Network (PSTN) or Plain Old Telephone Services (POTS).

3 Read and understand all instructions.

4 Follow all warnings and instructions marked on the product.

5 Unplug this product from your power source* before cleaning. Do not use liquid cleaners or aerosol cleaners. Use damp cloth for cleaning.

6 Do not use this product near water, for example, near a bathtub, wash bowl, kitchen sink, or laundry tub, in a wet basement or near a swimming pool.

7 Place this product securely on a stable surface. Serious damage and/or injury may result if the unit falls.

8 Slots or openings in the cabinet and the back and bottom are provided for ventilation, to protect it from overheating. These openings must not be blocked or covered. This product should never be placed near or over a radiator or heat register. This product should never be placed in any area, where proper ventilation is not provided.

9 This product should be operated only from the type of power source indicated on the marking label. If you are not sure of the type of power supplied at the premises, consult your dealer or local power company.

10 Do not place objects on the network cable or power cord. Install the unit where no one can step or trip on the cord.

11 Do not overload wall outlets and extension cords as this can result in the risk of fire or electric shock.

12 Never push objects of any kind into this product through cabinet slots as they may touch dangerous voltage points or short out parts that could result in the risk of fire or electric shock. Never spill liquid of any kind on this product.

13 To reduce the risk of electric shock or burns, do not disassemble this product. Take it to a qualified service center when service is required. Opening or removing covers other than specified access doors may expose you to dangerous voltages, dangerous electrical current or other risks. Incorrect reassembly can cause electric shock when the appliance is subsequently used. Disconnect TNV circuit connector before removing cover.

14 Unplug the product from your power source* and refer servicing to qualified service personnel under the following conditions:

a.) When the power cord is damaged or frayed.

b.) If liquid has been spilled onto the product.

c.) If the product has been exposed to rain or water.

d.) If the product does not operate normally by following the operating instructions. Adjust only those controls that are covered by the operating instructions. Improper adjustment of other controls may result in damage and may require extensive work by a qualified technician to restore the product to normal operation.

e.) If the product has been dropped or physically has been damaged.

f.) If the product exhibits a distinct change in performance.

15 Avoid using a telephone (other than a cordless type) during a thunderstorm. There may be a remote risk of electrical shock from lightning. Therefore we suggest a surge arrestor.

16 Do not use the telephone to report a gas leak in the vicinity of the leak. Under certain circumstances, a spark may be created when the adapter is plugged into the power outlet, or when the handset is replaced in its cradle. This is a common event associated with the closing of any electrical circuit. The user should not plug the phone into a power outlet, and should not put a charged handset into the cradle, if the phone is located in an environment containing concentrations of flammable or flame-supporting gases, unless there is adequate ventilation. A spark in such an environment could create a fire or explosion. Such environments might include: medical use of oxygen without adequate ventilation; industrial gases (cleaning solvents; gasoline vapors; etc.); a leak of natural gas; etc.

*Power source for the base station will be via the ethernet cable or a power injector; for the handset it will be the battery and the AC adapter to the charging cradle.

Battery safety precautions

To reduce the risk of fire, injury or electric shock, and to properly dispose of batteries, please read and understand the following instructions.

CONTAINS NICKEL METAL HYDRIDE BATTERY. BATTERY MUST BE RECYCLED OR DISPOSED OF PROPERLY. DO NOT DISPOSE OF IN MUNICIPAL WASTE.

1 Only use the batteries specified for use with this product.

2 DO NOT USE NICKEL CADMIUM OR LITHIUM BATTERIES, or mix batteries of different sizes or from different manufacturers in this product. DO NOT USE NONRECHARGEABLE BATTERIES.

3 Do not dispose of the batteries in a fire; the cells may explode. Do not expose batteries to water. Check with local waste management codes for special disposal instructions.

4 Do not open or mutilate the batteries. Released electrolyte is corrosive and may cause damage to the eyes or skin. The electrolyte may be toxic if swallowed.

5 To prevent fire or shock hazard, do not expose batteries to water or any type of moisture.

6 Exercise care in handling the batteries in order not to short the batteries with conducting materials such as rings, bracelets, and keys. The batteries or conducting material may overheat and cause burns or fire.

7 Charge the batteries provided with, or identified for use with, this product only in accordance with the instructions and limitations specified in the user's manual. Do not attempt to charge the batteries with any means other than that specified in the users manual.

8 Periodically clean the charge contacts on both the charger and handset.

9 The battery cannot be subjected to high or low extreme temperatures during use, storage or transportation.

10 Avoid leaving a battery in an extremely high temperature surrounding environment that can result in an explosion or the leakage of flammable liquid or gas.

11 The battery cannot be subjected to low air pressure at high altitude during use, storage or transportation.

12 A battery subjected to extremely low air pressure may result in an explosion or the leakage of flammable liquid or gas.

Service (Customer Care)

Customer Care Warranty for Cordless Products
To obtain Customer Care Warranty service, product operation information, or for problem resolution, please contact Support at:

www.gigaset.com/contact

End-user limited warranty

This product is covered by a one year limited warranty. Any repair replacement or warranty service, and all questions about this product should be directed to: www.gigaset.com/contact.

This limited, non-transferable warranty is provided to the original buyer/end-consumer ("you") for systems, handsets and accessories (collectively, "Product") provided by Gigaset Technologies GmbH, Frankenstraße 2, D-46395 Bocholt. Gigaset Technologies GmbH warrants to you that at the date of purchase, the Product is free of defects in workmanship and materials and the software included in the Product will perform in substantial compliance to its program specifications.

1. WARRANTY PERIOD

The Product warranty period is one (1) year from the original date of purchase by you. Proof of purchase (*e.g.*, sales slip or invoice) must be provided with any Product returned during the warranty period. Batteries supplied with the Products are warranted to be free from defects at the time of purchase only.

2. EXCLUSIVE REMEDY

Gigaset Technologies GmbH's entire liability and your exclusive remedy if the Product is defective in materials or workmanship during the warranty period and is returned shall be that the Product will be repaired or replaced as set forth in Section 4 below. Reconditioned replacement components, parts or materials may be used in the replacement or repair. Data in the memory of the Product may be lost during repair.

3. THIS LIMITED WARRANTY DOES NOT COVER AND IS VOID WITH RESPECT TO THE FOLLOWING:

- Cosmetic damage, physical damage to the surface of the Product, including, without limitation, breakage, cracks, dents, scratches or adhesive marks on the LCD screen or outside casing of the Product.
- Products which have been repaired, maintained or modified (including the antenna) by anyone other than Gigaset Technologies GmbH-approved repair facility, or that have been improperly installed.
- Cost of installation, removal or reinstallation.
- Damage due to any telephone, electronic, hardware or software program, network, Internet or computer malfunctions, failures, or difficulties of any kind, including without limitation, server failure or incomplete, incorrect, garbled or delayed computer transmissions.
- Equipment and components not manufactured, supplied or authorized by Gigaset Technologies GmbH.
- Modification of the Product's components, or operation of the Product in an unsuitable environment or in a manner for which it is not intended, including but not limited to failures or defects caused by misuse, abuse, accidents, physical damage, abnormal operation, improper handling or storage, neglect, alterations, unauthorized installation, removal or repairs, failure to follow instructions, problems caused by the carrier's network coverage, exposure to fire, water or excessive moisture or dampness, floods, or extreme changes in climate or temperature, acts of God, riots, acts of terrorism, spills of food or liquids, viruses or other software flaws introduced into the Product or other acts which are not the fault of Gigaset Technologies GmbH and which the Product is not specified to tolerate, including damage caused by mishandling or blown fuses.
- Products which have had warranty stickers, electronic serial number and/or serial number label removed, altered, rendered illegible or fraudulently applied to other equipment.
- Signal reception problems (unless caused by defect in material or workmanship in the Product).
- Products operated outside published maximum ratings.

- Performance of the Products when used in combination with other products or equipment not manufactured, supplied or authorized by Gigaset Technologies GmbH.
- Consumables (such as batteries and fuses).
- Payments for labor or service to representatives or service centers not authorized to perform product maintenance by Gigaset Technologies GmbH.
- Loss of data.
- Testing and examination discloses that the alleged defect or malfunction in the Product does not exist.

This warranty does not cover customer education, instruction, installation or removal, set up adjustments, problems related to service(s) provided by a carrier or other service provider, and/or signal reception problems. Gigaset Technologies GmbH shall not be responsible for software, firmware, information, or memory data contained in, stored on, or integrated with any Products returned for repair, whether under warranty or not. This warranty is valid only in the country in which it is purchased (*i.e.*, the United States of America or Canada respectively, but not both).

USE WITH ACCESSORIES NOT SUPPLIED BY Gigaset Technologies GmbH OR NOT OTHERWISE EXPRESSLY AUTHORIZED BY Gigaset Technologies GmbH MAY VOID WARRANTY.

4. WARRANTY CLAIM PROCEDURE

All warranty claims must be made by notifying Gigaset Technologies GmbH prior to the expiration of the warranty period. Gigaset Technologies GmbH's obligation to provide warranty support shall not extend past the end of the warranty period, except that any product repaired or replaced during the warranty period shall continue to be warranted for the balance of such warranty period or thirty (30) days, whichever is greater.

Support service will be provided for you at:

www.gigaset.com/contact.

5. LIMITATION OF WARRANTY

Gigaset Technologies GmbH makes no warranty or representation that the software in the Products will meet your requirements or will work in combination with any hardware or applications software products provided by third parties, that the operation of the software will be uninterrupted or error free, or that all defects in the software products will be corrected.

6. LIMITATION ON REMEDIES; NO CONSEQUENTIAL OR OTHER DAMAGES

Your exclusive remedy for any breach of this limited warranty is as set forth above. Except for any refund elected by Gigaset Technologies GmbH, **YOU ARE NOT ENTITLED TO ANY DAMAGES, INCLUDING BUT NOT LIMITED TO CONSEQUENTIAL DAMAGES**, if the Product does not meet the limited warranty, and, to the maximum extent allowed by applicable law, even if any remedy fails of its essential purpose. The terms below ("Exclusion of Incidental, Consequential and Certain Other Damages") are also incorporated into this limited warranty. Some states/jurisdictions/provinces do not allow the exclusion or limitation of incidental or consequential damages, so the above limitation or exclusion may not apply to you. This limited warranty gives you specific legal rights. You may have others which vary from state/jurisdiction/province to state/jurisdiction/province.

7. DISCLAIMER OF WARRANTIES

Gigaset Technologies GmbH AND ITS SUPPLIERS PROVIDE THE PRODUCT AND SUPPORT SERVICES (IF ANY) AS IS AND WITH ALL FAULTS. THE LIMITED WARRANTY IS IN LIEU OF ANY OTHER EXPRESS WARRANTIES (IF ANY) CREATED BY ANY DOCUMENTATION OR PACKAGING EXCEPT FOR THE LIMITED WARRANTY, AND TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW IS IN LIEU OF ANY IMPLIED OR STATUTORY WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, OF ACCURACY OR COMPLETENESS OR RESPONSES, OF RESULTS, OF WORKMANLIKE EFFORT, OF LACK OF VIRUSES AND OF LACK OF NEGLIGENCE, ALL WITH REGARD TO THE PRODUCT, AND THE PROVISION OF OR FAILURE TO PROVIDE SUPPORT SERVICES. ALSO, THERE IS NO WARRANTY OR CONDITION OF TITLE, QUIET ENJOYMENT, QUIET POSSESSION, OR CORRESPONDENCE TO DESCRIPTION OR NONINFRINGEMENT WITH REGARD TO THE PRODUCT. Some states/jurisdictions/provinces do not allow limitations on how long an implied warranty lasts or the exclusion or limitation of incidental or consequential damages, so the above exclusions or limitations may not apply to you. If an implied warranty or condition is created by your state/province and federal or state/provincial law prohibits disclaimer of it, you also have an implied warranty

or condition, BUT ONLY AS TO DEFECTS DISCOVERED DURING THE PERIOD OF THIS LIMITED WARRANTY (ONE YEAR). AS TO ANY DEFECTS DISCOVERED AFTER THE ONE YEAR PERIOD, THERE IS NO WARRANTY OR CONDITION OF ANY KIND. This limited warranty gives you specific legal rights, and you may also have other rights which vary from state to state/province to province. In no event shall Gigaset Technologies GmbH's liability exceed the cost of repairing or replacing defective Products as provided herein, and any such liabilities will terminate upon expiration of the warranty period.

Any supplements or updates to the Product or the software in the Product, including without limitation, any (if any) software fixes or upgrades or bug fixes provided to you after the expiration of the one year limited warranty period are not covered by any warranty or condition, express, implied or statutory.

8. EXCLUSION OF INCIDENTAL, CONSEQUENTIAL AND CERTAIN OTHER DAMAGES

TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, IN NO EVENT SHALL Gigaset Technologies GmbH, SELLER OR THEIR SUPPLIERS BE LIABLE FOR ANY SPECIAL, INCIDENTAL, INDIRECT, OR CONSEQUENTIAL DAMAGES WHATSOEVER (INCLUDING, BUT NOT LIMITED TO, DAMAGES FOR LOSS OF PROFITS OR CONFIDENTIAL OR OTHER INFORMATION, FOR BUSINESS INTERRUPTION, FOR PERSONAL INJURY, FOR LOSS OF PRIVACY, FOR FAILURE TO MEET ANY DUTY INCLUDING OF GOOD FAITH OR OF REASONABLE CARE, FOR NEGLIGENCE, AND FOR ANY OTHER PECUNIARY OR OTHER LOSS WHATSOEVER) ARISING OUT OF OR IN ANY WAY RELATED TO THE USE OF OR INABILITY TO USE THE PRODUCT, THE PROVISION OF OR FAILURE TO PROVIDE SUPPORT SERVICES, OR OTHERWISE UNDER OR IN CONNECTION WITH ANY PROVISION OF THIS LIMITED WARRANTY, EVEN IN THE EVENT OF THE FAULT, TORT (INCLUDING NEGLIGENCE), STRICT LIABILITY, BREACH OF CONTRACT OR BREACH OF WARRANTY OF Gigaset Technologies GmbH OR SELLER OR ANY SUPPLIER, AND EVEN IF Gigaset Technologies GmbH OR SELLER OR ANY SUPPLIER HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. REPAIR OR REPLACEMENT, AS PROVIDED UNDER THE WARRANTY, IS YOUR SOLE AND EXCLUSIVE REMEDY FOR BREACH OF THE LIMITED WARRANTY.

9. LIMITATION OF LIABILITY AND REMEDIES

NOTWITHSTANDING ANY DAMAGES THAT YOU MIGHT INCUR FOR ANY REASON WHATSOEVER (INCLUDING, WITHOUT LIMITATION, ALL DAMAGES REFERENCED ABOVE AND ALL DIRECT OR GENERAL DAMAGES), THE ENTIRE LIABILITY OF Gigaset Technologies GmbH, SELLER AND ANY OF THEIR SUPPLIERS UNDER ANY PROVISION OF THIS LIMITED WARRANTY AND YOUR EXCLUSIVE REMEDY FOR ALL OF THE FOREGOING (EXCEPT FOR ANY REMEDY OF REPAIR OR REPLACEMENT ELECTED BY Gigaset Technologies GmbH OR SELLER OR SUPPLIER WITH RESPECT TO ANY BREACH OF THE LIMITED WARRANTY) SHALL BE LIMITED TO THE GREATER OF THE AMOUNT ACTUALLY PAID BY YOU FOR THE PRODUCT OR FIVE DOLLARS ($5.00 USD/CAN). THE FOREGOING LIMITATIONS, EXCLUSIONS AND DISCLAIMERS SHALL APPLY TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, EVEN IF ANY REMEDY FAILS ITS ESSENTIAL PURPOSE.

10. GOVERNING LAW

If this Product was purchased in the United States of America this limited warranty will be governed by the laws of Texas, and exclude the United Nations Convention on Contracts for the International Sale of Goods. If this Product was purchased in Canada this limited warranty will be governed by the laws of the Province of Ontario and the federal laws of Canada applicable therein, and exclude the United Nations Convention on Contracts for the International Sale of Goods.

If you want to learn more about Gigaset Service or for Support on your Gigaset phone, visit our web site at **www.gigaset.com** or please contact Support at
www.gigaset.com/contact

Issued by

Gigaset Technologies GmbH

Frankenstraße 2, D-46395 Bocholt

Product attributes subject to change.
We reserve the right, to make changes without notice in equipment design and/or components.
Part Number: A31008-M2714-R311-1-3S19

Manufacturer's advice

Environment

Environmental management system

Further information on environmentally friendly products and processes is available on the Internet at www.gigaset.com.

Gigaset Technologies GmbH is certified pursuant to the international standards ISO 14001 and ISO 9001.

ISO 14001 (Environment): Certified since September 2007 by TÜV SÜD Management Service GmbH.

ISO 9001 (Quality): Certified since 17/02/1994 by TÜV SÜD Management Service GmbH.

Disposal

Batteries should not be disposed of in general household waste. Observe the local waste disposal regulations, details of which can be obtained from your local authority or the dealer you purchased the product from.

All electrical and electronic equipment must be disposed of separately from general household waste using the sites designated by local authorities.

The appropriate disposal and separate collection of used equipment serve to prevent potential harm to the environment and to health. They are a prerequisite for the re-use and recycling of used electrical and electronic equipment.

For further information on disposing of your used equipment, please contact your local authority, your refuse collection service or the dealer you purchased the product from.

Care

Wipe the device with a **slightly moistened** cloth or an antistatic cloth. Do not use solvents or microfibre cloths.

Never use a dry cloth; this can cause static.

In rare cases, contact with chemical substances can cause changes to the device's exterior. Due to the wide variety of chemical products available on the market, it was not possible to test all substances.

Impairments in high-gloss finishes can be carefully removed using display polishes for mobile phones.

Contact with liquid

If the device comes into contact with liquid:

1 **Unplug all cables from the device.**
2 **Remove the batteries and leave the battery compartment open.**
3 Allow the liquid to drain from the device.
4 Pat all parts dry,
5 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).
6 **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.

Open Source Software

General

Your Gigaset product includes Open Source software that is subject to various license conditions. With regard to Open Source software, the granting of usage rights that go beyond the operation of the product in the form supplied by Gigaset Technologies GmbH is governed by the relevant license conditions of the Open Source software.

The list of Open Source software used and the relevant licenses of this Open Source software can be found on the login page of the web configurator of the product.

As far as Gigaset is obligated by an OSS license to make available the source code of an OSS module (e.g. GPL V2, LGPL 2.1, MPL, etc.), source code, documentation and other supplementary information, can be found at www.gigaset.com/opensource

Technical data

Specifications

Power consumption

N670 IP PRO < 3.8 W

General specifications

Power over Ethernet	PoE IEEE 802.3af < 3.8 W (Class 1)
LAN interface	RJ45 Ethernet, 10/100 Mbps Protection class IP20
Ambient conditions for operation	41°F to 113°F (+5°C to +45°C) indoors; 20% to 75% relative humidity
Protocols	IPv4, SNTP, DHCP, DNS, TCP, UDP, VLAN, HTTP, TLS, SIP, RTP, MWI, SDP, SRTP
Radio technology	DECT6.0
Radio frequency range	1920–1930 MHz
Transmission power	5 mW average power per channel, 120 mW pulse power
No. of channels	60 channels
Number of connections	8 simultaneous connections per base station (G.711), 8 simultaneous connections (G.729), 5 connections in wideband operation (G.722)
Range	Up to 200 m outdoors, up to 30 m indoors
Codec	G.711, G.722, G.729ab
Quality of Service	TOS, DiffServ

Accessories

Power adapter (Gigaset power adapter N series US)

You only need a power adapter if your devices are not powered by PoE (Power over Ethernet).

Part Nr.: L36280-Z4-X749

Model type: C39280-Z4-C749

UPC: 845306003047

DECT Site Planning Kit (SPK) PRO (Site Planning Kit)

Equipment for planning and analysing your DECT multicell system. The case contains two calibrated Gigaset R700H SPK handsets and one Gigaset N870 SPK PRO base station, plus other useful accessories for measuring the signal quality and wireless coverage on your DECT network.

Item number: S30852-H2737-R301

Gigaset handsets

Upgrade your telephone system with extra handsets.

For information on handset functions in relation to Gigaset base stations, visit wiki.gigaset.com.

Index

Issued by
Gigaset Technologies GmbH
Frankenstraße 2, D-46395 Bocholt

wiki.gigaset.com