Gigaset

N530 IP PRO

Installation, configuration and operation

Content

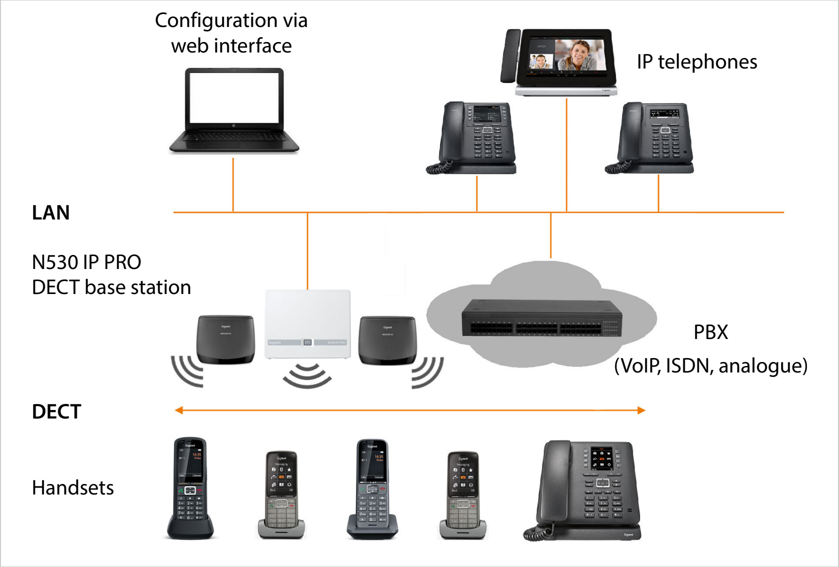
Template Module, Version 2.2, 15.11.2022 / Template Basiseinstellungen: Version 3.1 - 07.07.2020

Template Module, Version 2.2, 15.11.2022 / Template Basiseinstellungen: Version 3.1 - 07.07.2020

N530 IP PRO – Introduction

N530 IP PRO is a DECT base station for connecting to a VoIP PBX.

The following illustration shows the way the N530 IP PRO is embedded in the IP telephone environment:



- **N530 IP PRO**
  - Provides cell site DECT functions
  - 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
  - Up to six repeaters can extend the range of the base station‘s DECT network. The repeaters can only be arranged in a star configuration, not as a chain.

For the time being, repeaters without encryption can be registered (e.g., Gigaset Repeater V1.0). For information on registering repeaters to the base station, visit wiki.gigaset.com.

Template Module, Version 2.2, 15.11.2022 / Template Basiseinstellungen: Version 3.1 - 07.07.2020

- **Handsets (mobile devices)**
  - N530 IP PRO can manage up to six handsets.
  - Up to 4 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.
  - 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.

  Configuring handsets → p. 30

  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

Multi-line operation and internal telephony

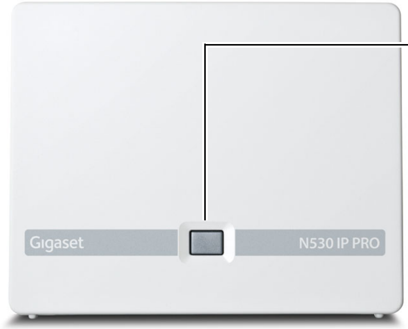
The device supports multi-line operation. You can assign multiple SIP accounts to a handset, e.g. different accounts for incoming and outgoing calls. This makes it possible, for example, to assign a common phone number for incoming calls to different members of a team.

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

Template Module, Version 2.2, 15.11.2022 / Template Basiseinstellungen: Version 3.1 - 07.07.2020

Overview

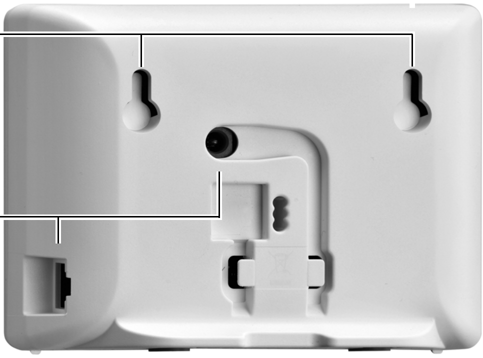
Front



Base station button and LED display

- Register Handset
- Paging
- Reset Handset → p. 10
- Operation status of the device → p. 10

Back



Wall mounting slots

Wall mounting → p. 9

LAN and power cable slot

Connecting the device → p. 8

First steps

Package content

- One N530 IP PRO
- Security leaflet

Security leaflet

ⓘ 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. 52 and/ or p. 57.

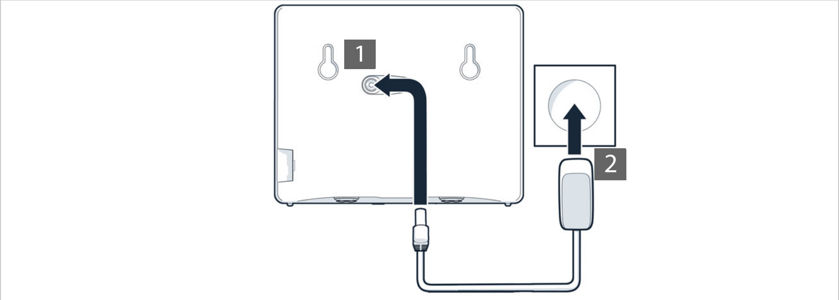
Mounting the device

- The N530 IP PRO has a desk stand and can also be mounted to a wall (→ p. 9).

!
- The N530 IP PRO is designed for use in dry rooms with a temperature range of +5°C to +45°C.
- Never expose the N530 IP PRO to heat sources, direct sunlight or other electrical appliances.
- Protect your device from moisture, dust, corrosive liquids and fumes.

Connecting the power supply

Your N530 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 class IEEE802.3af). In this case, you do **not** need to connect the device to the mains power supply.



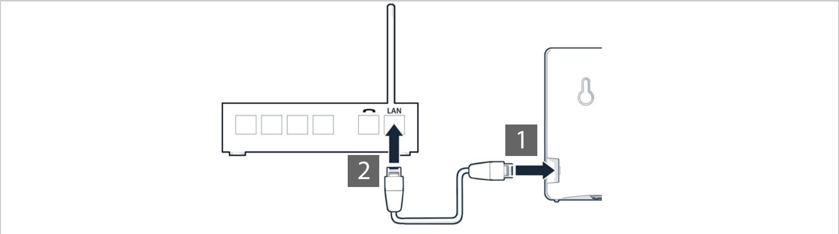
- Connect the power supply cable to the power connector on the base station 1.
- Plug in the power supply 2.

Connecting to the LAN

You can connect the N530 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.



- Insert a plug from an Ethernet cable into the LAN connection socket at the bottom of the device 1.
- Insert the other Ethernet cable plug into a LAN socket for your local network or on the PoE switch 2.

Template Module, Version 2.2, 15.11.2022 / Template Basiseinstellungen: Version 3.1 - 07.07.2020

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:

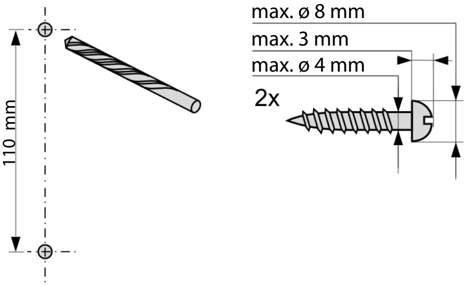
- MAC address
- Device name
- Number of registered handsets
- Number of connected base stations (for N530 IP PRO always 1)
- Number of connected DECT managers (for N530 IP PRO always 1)
- License information
- Software version

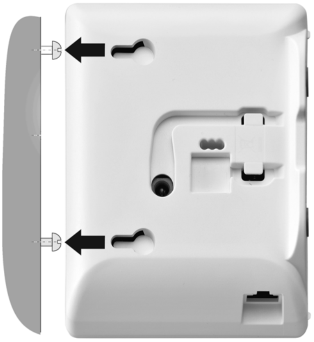
On the support server, this information is linked to the existing device-specific information:

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

Wall mounting

N530 IP PRO is suitable for wall mounting and has a desk stand. 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.

Operation hints

Light emitting diode (LED)

The LED on the front side show different operational states.

The LEDs can have three different colours (red, green, amber) or can be off.

LED				Description
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

ℹ LED status display for base stations can be disabled.

Resetting the base station

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

- Hold the base station button for 10 seconds.
- The RED LED will be switched off.
- Release the button
- Press the base station button for 5 seconds and release the button.
- Reset to factory will be initated.

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

Configuring the system

System settings are made via the web configurator of the N530 IP PRO.

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.

Following tasks can be performed without use of the web configurator:

- Registering a handset.
- Assigning lines to a handset.
- Paging and display the IP address on the handsets.
- Delete handsets.
- Reset base station.

Registering a handset with the base station button

To register a Handset without the web configurator you can do following steps:

▶ Press the base station button for approximately 5 seconds.

- If the handset is not registered to a base:

▶ Press the display key: **Register**

- If the handset is already registered to a base:

▶ **Settings** ▶ **Registration** ▶ **Register Handset** and press **OK**

Assigning lines to a handset with the handset menu

You can change the assignment of lines with the **Select Service** of your handset:

▶ Press down on the control key to scroll through the list.

▶ Press the display key **OK** if you wish to change the Send Connection setting.

▶ Press the display key **OK** if you wish to change the Receive Connections setting.

Deleting handsets with the handset menu

You can De-register a Handsets without accessing the N530 IP PRO:

▶ Open the handset menu on a registered DECT handset

▶ Go to: **Settings** ▶ **Registration** ▶ **De-register Handset** Select the internal party you wish to de-register and press **OK**.
The handset you are currently using is marked with <.

The web configurator

Use the web configurator to set up your N530 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 N530 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 N530 IP PRO to communicate with each other.

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

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

▶ Launch the web browser on your PC/tablet.

▶ Enter gigaset-config.com in the address field of the web browser
The first time you open the webinterface you will get a security message, please ignore this message. The reason is that IP devices are using self signed certificates that can not be validated by the PC's browser.

If several Gigaset devices can be reached at this address, a list is displayed ▶ Select device . . . the N530 IP PRO web configurator is started

or

▶ Press the paging key: In case your basestatison is connected to the LAN and a handset is already registered, the paging call display shows the IP address.

▶ Enter the current IP address of the base station in the address field of the web browser (for example: http://192.168.2.10).

IP address of the device via your DHCP server

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. 18).

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. 47).

- 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
- Select the radio frequency band used in your region from the list (→ p. 56).

ℹ 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. 13).

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

Settings	Network	IP/LAN	→ p. 18
	Provider or PBX profiles		→ p. 21
	SIP accounts	Administration	→ p. 27
		Assignments	→ p. 29
	Mobile devices	Administration	→ p. 30
		Registration Centre	→ p. 34
	Telephony	Audio	→ p. 37
		Call settings	→ p. 38
		VoIP	→ p. 36
		XSI Services	→ p. 40
	Online directories	XML	→ p. 41
		XSI	→ p. 42
		Central phonebook	→ p. 43
	Online services	XHTML	→ p. 45
	System	Web configurator	→ p. 47
		Provisioning and configuration	→ p. 48
		Security	→ p. 49
		System log	→ p. 58
		Date and time	→ p. 51
		Firmware	→ p. 52
		Save and restore	→ p. 53
		Reboot and reset	→ p. 54
		DECT settings	→ p. 55
Status	Overview		→ p. 57
	Statistics	Incidents	→ p. 57
		Diagnostics	→ p. 60

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. 10

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.

Template Module, Version 2.2, 15.11.2022 / Template Basiseinstellungen: Version 3.1 - 07.07.2020

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. 10). This means that all settings are lost.

Provider and PBX profiles

You can use up to 8 different VoIP PBX or VoIP provider profiles.

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 - IPn). It can be edited.

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

Configuring provider and/or PBX profiles

▶ Click on ✎ next to the name of the VoIP connection you want to edit . . . the provider/PBX configuration page is opened.

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.

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.

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 N530 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).

Template Module, Version 2.2, 15.11.2022 / Template Basiseinstellungen: Version 3.1 - 07.07.2020

Send settings of DTMF transmission

- Make the required settings for sending DTMF signals:

Audio or **RFC 2833**	DTMF signals are to be transmitted acoustically (in voice packets).
SIP Info	DTMF signals are to be transmitted as code.

Settings for codecs

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

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

Active codecs / Available codecs

The following voice codecs are supported:

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

To enable wideband connections via G.722 you have to activate the codec explicitly on the **Telephony** – **VoIP** page (→ p. 36).

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.

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.

Template Module, Version 2.2, 15.11.2022 / Template Basiseinstellungen: Version 3.1 - 07.07.2020

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.

SIP account administration

ℹ 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.

ℹ 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.

Broadsoft XSI services

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

ℹ XSI services must be activated (→ p. 40).

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).

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.

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.

Template Module, Version 2.2, 15.11.2022 / Template Basiseinstellungen: Version 3.1 - 07.07.2020

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.

Editing the data of a handset

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

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**.

> ℹ Registration/de-registration in this context refers to the handset’s relationship to the DECT network but not to SIP registration.

Registering handsets

Activate registration mode via the base station button:

- Press and hold the base station button for 2 to 8 seconds.

or

Activate registration mode via Web Configurator:

- 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.

ℹ 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

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

Internal name

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

De-registering handsets

Via the handset menu:

- Settings- In the handset list click on ✎ next to the handset you want to de-register. The status is **Registered**.

Via the Web Configurator:

- 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.

Assining accounts

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.

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).

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.

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 N530 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.

▶ **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.

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

ℹ To allow users to make wideband calls, the codec G.722 must have been activated for the provider profile that is used for the connection (→ p. 25).

Call settings

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

- **Settings** ▶ **Telephony** ▶ **Call settings**

Call transfer

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

Call transfer via R key

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

Transfer call by on-hook

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

Determine target address

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

  From transfer target's AOR (Address of Record)

  From transfer target's transport address (Contact URI)

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

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

Access Code

You may have to enter an access code for external calls (external prefixes e.g., "0"). You can save this access code in 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.

▶ **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.

Online directories

N530 IP PRO allows you to set up 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.

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**.

ℹ The XSI directory service must be enabled on the **Telephony – XSI Services** page (→ p. 40).

▶ **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.

ℹ 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.

Template Module, Version 2.2, 15.11.2022 / Template Basiseinstellungen: Version 3.1 - 07.07.2020

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.

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. 13). 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**.

ℹ If you have forgotten the password, you will have to reset the device to the factory settings (→ p. 10).

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.

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.

ℹ 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.

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

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

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

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

Current version

Shows the current firmware version.

Backup available for previous version

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

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

Selecting the firmware update file

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

or

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

Starting the firmware update

At a specific date:	▶ Deselect the check box **Immediately** ▶ Enter the exact start time in the format: YYYY-MM-DD HH:mm
Immediately:	▶ Select the check box next to **Immediately** (default) . . . the firmware update is started when you click on the **Set** button.

Confirmed schedule

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

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

Once the update process starts, the handsets lose their connection to the base. You can tell that the update has been successful when the handsets re-establish the connection to the base.

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

Save and restore

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

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

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

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

ℹ 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. 10).

Resetting the device via Web Configurator

- 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.

Resetting the device via key procedure

- Turn device off if needed.
- Hold the base station button for 10 seconds.
- The RED LED will be switched off.
- Release the button.
- Press the base station button for 5 seconds and release the button.
- reset to factory settings will be initiated.

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.

Template Module, Version 2.2, 15.11.2022 / Template Basiseinstellungen: Version 3.1 - 07.07.2020

DECT Encryption

▶ Activate/deactivate the option.

Activated: All calls are encrypted.

Deactivated: No calls are encrypted.

Enhanced Security - Early Encryption and Re-Keying

▶ Activate/deactivate the option.

Activated: The following messages are encrypted:

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

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

Deactivated: No CC messages or early data are encrypted.

Enhanced Security - Automatic release for non-encrypted calls

▶ Activate/deactivate the option.

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

Deactivated: Encryption is never released.

DECT radio settings

Due to different national regulations DECT units are required to use different frequency ranges to make them compatible with DECT systems in other areas. You can adapt the frequency range of the N530 IP PRO to the requirements of your region.

DECT Radio band

▶ Select the radio frequency band used in your region.

Radio frequency range	1880–1900 MHz (Europe) 1910-1930 MHz (Latin America) 1910-1920 MHz (Brazil) 1880 MHz - 1895 MHz (South East Asia/Taiwan)

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

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.
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)

▶ 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.

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.

Template Module, Version 2.2, 15.11.2022 / Template Basiseinstellungen: Version 3.1 - 07.07.2020

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:	N530 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:

Template Module, Version 2.2, 15.11.2022 / Template Basiseinstellungen: Version 3.1 - 07.07.2020

```
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

Template Module, Version 2.2, 15.11.2022 / Template Basiseinstellungen: Version 3.1 - 07.07.2020

Using a handset connected to an N530 IP PRO base

The functions of your N530 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.

ℹ For information about which Gigaset handsets support the complete functionality of the N530 IP PRO multicell system please refer to wiki.gigaset.com.

Making calls

You can make calls using any handset registered to your N530 IP PRO.

Each handset is assigned a send and receive connection (→ p. 33).

If your N530 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.

Internal calls between the handsets are also possible.

The N530 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.

ℹ Depending on the specifications of your PBX, you may need to dial an access code for calls outside the area covered by your VoIP PBX (→ p. 38).

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. 33).

ℹ 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. 39).

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 ☎

Template Module, Version 2.2, 15.11.2022 / Template Basiseinstellungen: Version 3.1 - 07.07.2020

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 ☎

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

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.

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 ☎.

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

Template Module, Version 2.2, 15.11.2022 / Template Basiseinstellungen: Version 3.1 - 07.07.2020

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. 38).

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

ℹ Call transfer options must be set correctly for the PBX/provider (→ p. 38).

Template Module, Version 2.2, 15.11.2022 / Template Basiseinstellungen: Version 3.1 - 07.07.2020

Internal calls

Internal calls are only possible, if 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 ☎

Template Module, Version 2.2, 15.11.2022 / Template Basiseinstellungen: Version 3.1 - 07.07.2020

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. 34).

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)
- Miscellaneous online directories

The directories available are defined by the web configurator of the telephone system (→ p. 41).

Opening directories

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. 33). 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.

ⓘ If handsets are connected to an N530 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 one a network mailbox the following settings are necessary:

On the VoIP PBX

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

On the N530 IP PRO

▶ In the provider/PBX configuration activate the **SIP SUBSCRIBE for Net-AM MWI** option (→ p. 23). A subscription is established for the purpose of receiving notifications about new messages on the network mailbox.

▶ Optional: In the mobile devices configuration enable the **Flashing LED (MWI) for network mailbox** option (→ p. 34). 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 [🔈]

Template Module, Version 2.2, 15.11.2022 / Template Basiseinstellungen: Version 3.1 - 07.07.2020

Appendix

Safety precautions

!i	Read the safety precautions and the user guide before use. **Comprehensive user guides for all telephones and telephone systems as well as for accessories can be found online at wiki.gigaset.com. We thereby help to save paper while providing fast access to the complete up-to-date documentation at any time.**

	Do not use the devices in environments with a potential explosion hazard (e.g. paint shops).
	The devices are not splashproof. For this reason do not install them in a damp environment such as bathrooms or shower rooms.
	Remove faulty devices from use or have them repaired by our Service team, as these could interfere with other wireless services.
	Using your telephone may affect nearby medical equipment. Be aware of the technical conditions in your particular environment, e.g. doctor's surgery. If you use a medical device (e.g. a pacemaker), please contact the device manufacturer. They will be able to advise you regarding the susceptibility of the device to external sources of high frequency energy (for the specifications of your Gigaset product see "Technical data").
⚠	For outdoor installations, please observe the Safety precautions of the installation environment, in particular with regard to lightning protection.

Customer Service & Help

Do you have any questions?

For quick help and information, please refer to this user guide or visit wiki.gigaset.com.

For online information and services concerning

- Products
- Documents
- Interop
- Firmware
- FAQ
- Support

please refer to wiki.gigaset.com.

For further information our Gigaset specialised reseller will be happy to help you related to your Gigaset product.

Template Module, Version 2.2, 15.11.2022 / Template Basiseinstellungen: Version 3.1 - 07.07.2020

Authorisation

Voice over IP telephony is possible via the LAN interface (IEEE 802.3).

Depending on your telecommunication network interface, an additional router/switch could be necessary.

For further information please contact your Internet provider.

Country-specific requirements have been taken into consideration.

Gigaset Technologies GmbH hereby declares that the following radio equipment types are in compliance with Directive 2014/53/EU:
Gigaset N530 IP PRO

The full text of the EU declaration of conformity is available at the following internet address:
www.gigaset.com/docs.

If this product will as well be imported into the UK:
Gigaset Technologies GmbH hereby declares that the following radio equipment types are in compliance with the Radio Equipment Regulations 2017:
Gigaset N530 IP PRO

The full text of the UK declaration of conformity is available at the following internet address:
www.gigaset.com/docs.

The importer’s postal address is: Gigaset Technologies UK Ltd., 2 White Friars Chester, CH1 NZ, United Kingdom

This declaration could also be available in the "International Declarations of Conformity" or "European Declarations of Conformity" files.

Therefore please check all of these files.

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.

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

This crossed-out wheeled bin symbol on the product means the product is covered by the European Directive 2012/19/EU.

UK: The Waste Electrical and Electronic Equipment Regulations 2013.

The correct disposal and separate collection of your old appliance will help prevent potential negative consequences for the environment and human health. It is a precondition for reuse and recycling of used electrical and electronic equipment.

For more detailed information about disposal of your old appliance, please contact your local council refuse centre or the original supplier of the product.

Care

Wipe the device with a **damp** 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.

Technical data

Specifications

Power consumption

N530 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	+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
DECT standard	DECT EN 300 175-x
Radio frequency range	1880–1900 MHz (Europe), 1910-1930 MHz (Latin America), 1910-1920 MHz (Brazil) 1880 MHz - 1895 MHz (South East Asia/Taiwan)
Transmission power	10 mW average power per channel, 250 mW pulse power
No. of channels	120 channels
Number of connections	4 simultaneous calls
Range	Up to 300 m outdoors, up to 50 m indoors
Codec	G.711, G.722, G.729ab
Quality of Service	TOS, DiffServ

Power adapter

Manufacturer	VTECH TELECOMMUNICATIONS LTD Commercial registration number: 0494425200010242 23/F., Tai Ping Industrial Centre, Block 1, 57 Ting Kok Road, Tai Po, Hong Kong
Model identifier	VT05EEU05100 (EU version) VT05EUK05100 (UK version)
Input voltage	100-240 V
Input AC frequency	50/60 Hz
Output voltage	5.0 V
Output current	1.0 A
Output power	5.0 W
Average active efficiency	> 73.62 %
Efficiency at low load (10%)	not relevant - only at output power > 10 W
No-load power consumption	< 0.10 W

Template Module, Version 2.2, 15.11.2022 / Template Basiseinstellungen: Version 3.1 - 07.07.2020

Index

All rights reserved. Rights of modification reserved.

Template Basiseinstellungen: Version 3.107.07.2020 / ModuleVersion 1.0

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

© Gigaset Technologies GmbH 2025
Subject to availability.
All rights reserved. Rights of modification reserved.

wiki.gigaset.com