Gigaset

T300 PRO - T500 PRO

Administration manual

Gigaset pro

INSPIRING CONVERSATION.

Contents

Contents

Introduction

The PBXs Gigaset T300 PRO/Gigaset T500 PRO offer extensive options for the operation and configuration of your phones.

This user guide describes the **administration** functions for both devices. Information about **operating** the PBX can be found in the user guide.

Information on ...	... is located here.

Initial configuration
Set up your Gigaset phones automatically, configure the lines and create a user account for the administrator.

User accounts and groups
Create user accounts and manage user groups.

Phone lists
Set up additional phones and softphones.

Modules
Use additional standard functions or create your own functions using the module designer.

Phone functions
Set up voicemail boxes, prepare conferences, set up a directory for all connected phones.

Phone numbers and lines
Re-assign phone numbers, configure VoIP, ISDN and analogue connections on your PBX and configure routing properties.

Server features
Update software, set up the server features for your PBX and create system backups.

Resetting the system
If your PBX is no longer functioning, you can reset your system with the aid of a USB stick.

Further information about your PBX can be found at: www.gigaset.com/pro

UI elements for Gigaset T300 PRO / Gigaset T500 PRO

UI elements and symbols

ⓘ	To call up help topics
✎	To edit
✕	To remove entries
▶ ▼	To open/close sub-menus
⊕	New element
✚	To add detail
☑	Property activated
⊟	Property partially activated
⚲	To select a user symbol/user entry
⚺	Group symbol
⚺⚺	Conference room
⬦	Module (configuration)
✿	User settings
⬚	To select addressbook entries
⊙	To display other actions
冝	To open or save fax in PDF format
«✆	To listen to calls/announcements on the phone
▥ ≡	Contact surfaces for positioning drag and drop
☎	To listen to voicemail messages
⊗	To close a window
◁⊟ **Page 2/7** ▷⟫	To scroll forward/back in lists
⊙	View options for list columns
	To sort list view

Last Name

Please note
Detailed information about operating your Gigaset T300 PRO / Gigaset T500 PRO PBX can be found in the user guide.

Your firewall settings
In the firewall of the network in which your PBX is used, ports for specific protocols must be opened for the IP address of the PBX. You will find an overview of protocols and logs in the appendix → **P. 103**.

Initial configuration

Your Gigaset T300 PRO / Gigaset T500 PRO PBX is supplied with a web user interface and can be configured using a browser on the computer of your choice. **Prerequisite:** You have connected your PBX to your local network, as described in the short user guide provided.

Please note
There are extension modules available to connect analogue and ISDN phones for Gigaset T300 PRO / Gigaset T500 PRO. If you wish to use these modules, install them in your PBX before starting the configuration.

Gigaset T300 PRO / Gigaset T500 PRO should already be assigned a fixed IP address or should have received an IP address automatically generated via DHCP. This IP address is shown on completion of the booting process on the PBX's start display, if a monitor is connected.

You can copy the IP address on to a USB stick:

▶ Insert a USB stick into the USB port on the server. The IP address is now stored automatically on the stick in a text file **pbxurl.txt**.

▶ Remove the USB stick and insert it into the workstation computer on which you wish to configure Gigaset T300 PRO / Gigaset T500 PRO.

▶ Open the text file **pbxurl.txt** using any text editor and copy the IP address to the clipboard.

To configure Gigaset T300 PRO / Gigaset T500 PRO, enter the IP address into the web browser's address bar as shown in the following example:

Example: **http://192.168.100.123/**

With 192.168.100.123 representing the IP address to be entered.

The configuration menu opens in the browser. Here you can start the initial configuration or restore the system using the security file. The PBX thus receives all the settings and user data stored in this file (➔ **P. 91**).

The initial configuration comprises three steps:

Locating and configuring the phones and adapters in the network that are to communicate via the Gigaset T300 PRO / Gigaset T500 PRO PBX.

Configuring the lines to be used by the PBX to establish connections in the phone network.

Creating the administrator account

Please note
With the exception of specifying internal phone numbers in **Step 2: Configuring the lines** and creating an administrator account in**Step 3: Setting up the administrator account**, the settings from the initial configuration can be carried out at a later stage.

▶ Click on **Next**, to start the initial configuration.

Step 1: Configuring the phone

During the first step, all phones and ATA adapters are set up in the network. There are three methods of set up available:

◆ Autoprovisioning

◆ Automatic scan and configuration of the phones

◆ Manual set up of the phones This is described in Chapter **General information about administration** in section **Manual configuration of phones** (➜ **P. 38**).

Preferences

Autoprovisioning new phones

───── **Caution** ─────────────────────────────────────
Autoprovisioning is activated by default. If you do not deactivate it, all the suitable IP phones located in the same subnet as the PBX, will be recorded by this process. This also relates to the advanced settings area. The selection of the devices to be included can be restricted in the restriction area for autoprovisioning/authorized MAC addresses.
──

Autoprovisioning can automatically provide Gigaset pro phones (e.g., Gigaset DE900 IP PRO, Gigaset DE700 IP PRO, Gigaset DE410 IP PRO, Gigaset DE310 IP PRO) with the following functions:

◆ SIP account (registering the phone on the system)

◆ Access data to protect the phone configuration

◆ Function keys

◆ Voice files

◆ User menu for the phone display

◆ Firmware updates

───── **Please note** ─────────────────────────────────
Autoprovisioning must be activated to be able to overwrite the phone settings and transfer the function key assignment to the devices.
──

Firmware update

The **Firmware auto update** option provides the phones with the latest firmware available. The devices use the new firmware once the machine is restarted. You can edit the devices to be updated in the **Limiting autoprovisioning/authorized MAC addresses** section.

If the firmware update is active, you can perform the update immediately via the **Update now** button.

───── **Please note** ─────

The firmware update is only available, if **Autoprovisioning new phones** is enabled.

Limiting autoprovisioning/authorized MAC addresses

If you do not wish autoprovisioning to be active for every newly connected phone, then you should enable the **MAC address constraint** checkbox. This setting means that only phones already registered to the PBX will be provisioned.

▸ Now enter the MAC addresses of the additional phones to be included in the list. The MAC address for Gigaset pro phones can be found on the devices' type plate or on the web user interface under **Status ➜ Device**.

▸ If you wish to deactivate the MAC address constraint temporarily, simply deactivate the **MAC address constraint** checkbox. MAC addresses already entered in the list are retained.

Detection and configuration of phones with network search

If you use SIP phones, which cannot or should not be automatically provisioned, these can be configured using a network scan. This process also works for various ATA and analogue cards.

Start the search by clicking on **Search now**, which will detect all the devices existing in the local network and automatically configure them, if they have not already been configured.

Configured phones				
These phones seem to be already configured. Do you want to overwrite the phone settings?				
Configured phones				
Overwrite	Type	Display Name	IP Address	MAC
☐	DE900 IP PRO	1029.DE900IP	192.168.150.14	00-21-04-F4-A8-64
☐	DE900 IP PRO	Gigaset Pro	192.168.150.9	00-0C-43-30-52-77

Overwrite selected phones   Cancel

The **Configured phones** section shows a list indicating all devices configured during the scan. If devices were found that have already been configured, the decision must be made in each case as to whether this configuration should be overwritten.

Devices that are used as fax machines must be configured manually despite the automatic configuration (**Fax functionality** ➔ **P. 39**).

Changing the search area

If you do not want to search for phones in the whole PBX subnet, it is possible to restrict the IP address range to be searched. Likewise, the IP range for the search in another IP subnet can be adapted.

Clicking on **Specify IP range to search** opens the **Subnet** dialog box.

Subnet			
Range:	192.168.250.* ⌄		
Start:	192 . 168 . 150 . 0		
End:	192 . 168 . 150 . 255		

Ok   Cancel

The address range to be searched can be changed here by changing the start and end IP. The network is therefore scanned for devices from the IP address in the start field (e.g., 192.168.150.0) to the IP address in the end field (e.g., 192.168.150.255).

If your server has several IP addresses and/or network cards, you can select the subnet you wish to scan via the areas dropdown menu.

Clicking on **Ok** accepts the restricted IP address range. The new search must now be started with **Search now**.

Please note
Not all phones that are to be connected to the Gigaset T300 PRO / Gigaset T500 PRO have to be configured during initial configuration. Additional phones can be added at a later stage in the configuration section.

Advanced settings

Depending on the manufacturer and model of a phone, it may have different access options for maintenance and configuration of the device. The access data stored at the factory is in general easy to memorise or to guess, which enables users or unauthorised persons to make undesired changes.

For devices from manufacturers officially supported by Gigaset, you can specify standard access data which is transferred to the phones during autoprovisioning.

Please note
If not stated otherwise, the access data stored at the factory corresponds to that of the applicable manufacturer or device. Please also read the tips and instructions from the phone manufacturer with respect to the importance and functions of access.

Gigaset PRO

◆ Desk phones: The **Admin password** field (default setting is admin) is needed for the network and VoIP configuration of Gigaset pro IP phones. In addition, it is used to log on to the devices' web interface.

◆ DECT devices: The **Admin PIN** field requires a four digit PIN (default setting is 0000). The PIN is used for the configuration of the DECT base and at the same time is the access PIN for logging mobile phones on to the DECT base.

Clicking on **Next** completes step 1 of the initial configuration.

Step 2: Configuring the lines

General settings

The general settings (area codes, prefix, country and deposit) apply across the whole PBX, as long as no deviating values have been set on individual lines. Individual lines to VoIP or ISDN providers, which are configured in the lines tab, can therefore each have deviating settings.

Prefix	In order to differentiate between internal and external numbers, a number can be inserted that must be entered when dialling. This is important because it is not possible to differentiate between assigned three-digit internal numbers and three digit external numbers (e.g., the emergency call number 110 is prefixed with 0 to change it to 0110 and thus clearly differentiate it from the internal number 110). If the previous PBX inserted a prefix, this can be retained for continuity purposes.
Deposit	Defines a number via which all unassigned connections are routed, e.g., calls for users without an active or registered phone. Specifying a deposit prevents incoming calls from "getting lost" in the system.
Internal Numbers	These are the connection numbers to be assigned locally, with which Gigaset T300 PRO / Gigaset T500 PRO network users communicate with each other.

After saving the general settings, you can continue with step 3 of the initial configuration, or set up lines with external phone numbers and emergency numbers at this point. In this case, please read Chapter 13.2 Lines and Chapter 13.2.7 Emergency call.

Step 3: Setting up the administrator account

The Gigaset T300 PRO / Gigaset T500 PRO user concept

A user is characterised by the following features in the Gigaset T300 PRO / Gigaset T500 PRO system:

◆ Login-ID
◆ Password
◆ First Name
◆ Last Name
◆ E-Mail
◆ Internal Number

A user logs in via the web user interface using a login ID and password.

The login ID is also used to log the user on to a phone via the keypad.

Setting up a user account

The **Login-ID** must be unique, i.e., two users cannot have the same login ID. The ID should be at least 4 characters long. Only the digits 0 to 9 may be used as characters to enable the user to log in using a phone's keypad!

--- **Please note** ---

You should always disable the feature available in most web browsers for automatically filling in boxes or saving passwords, otherwise the password fields for new users will be automatically filled in with a previous password.

The **Password** must be at least six characters long. All lower and uppercase letters of the alphabet can be used including umlauts as well as the digits 0 to 9, dash, underscore, full stop, hash and star. You should always choose a secure password. A secure password is made up of numbers and letters in both upper and lower case, and does not contain meaningful words (an example of a secure password is A_tz3-8pPj). Please ensure that you check each individual character when entering your password, i.e., the password is case-sensitive.

Login ID and password are sent to the user automatically via **eMail**. This is why the eMail address specified must be the user's current eMail address. Save the user profile to complete the initial configuration of your Gigaset T300 PRO / Gigaset T500 PRO PBX.

Completing initial configuration

After a successful initial configuration, the login dialog opens, where you can log in to the Gigaset T300 PRO / Gigaset T500 PRO user interface of one of the user accounts set up during initial configuration with the user ID and password.

Please note
Before you can operate your Gigaset T300 PRO / Gigaset T500 PRO via the web browser, it must be enabled to accept cookies and popups and JavaScript must be enabled.

General information about administration

You can edit all key system settings in the configuration tab.

▸ Click on **Configuration** in the main menu bar to open the configuration tab.

The configuration menu

On the left-hand side of the configuration tab, you can see a menu bar comprising buttons that open the individual setting tabs. The following chapter describes their function in order of appearance in the menu bar.

Users	For creating and editing user groups
Groups	For defining and editing groups
Phones	For autoprovisioning and integrating phones and ATA adapters
Modules	Gigaset PRO modules
Voicemail	For setting up voicemail boxes
Conference	Basic settings for managed conferences
Addressbook	For addressbook settings
Phone numbers	For assigning numbers to users
Lines	For VoIP, ISDN, analogue emergency call numbers
Routing	For routing priority and cost optimized routing
Server	For server settings, updates, backups and licenses
Statistic	For connection statistics
Interconnection	Interconnection
Security	Security settings for SIP/telephone access
Extended Settings	For on-hold loops, XMPP servers, macros

Users

Important

The number of user accounts is limited by the number of user licenses! If you have user licenses, register these beforehand under **Server** in the **Licenses** tab.

Creating user accounts

▶ Click on ⊕ or ⊕ **New User** to add a new user account to the user list. The procedure is identical to the one for initial configuration (→ **P. 13**).

▶ To edit a user entry, click on ✐ .

Please note

You should always disable the feature available in most web browsers for automatically filling in boxes or saving passwords, otherwise the password fields for new users will be automatically filled in with a previous password.

Importing user accounts

The import function enables you to create a large number of user accounts quickly. For this to work, the user data must be saved in a CSV file and saved on the server. There is a template available at www.gigaset.com/pro for you to download and create your own CSV file. The template already contains the correct field names.

Please observe the following when editing and saving the template with an editor:

◆ The individual values must be separated by commas and not by semi-colons!

◆ The file should be saved in UTF-8 format.

The fields in the import file

login	Is the login ID of the user as a text value
firstname	As a text value
lastname	As a text value
external	Optional external phone number as a text value (a phone number on the Gigaset T300 PRO / Gigaset T500 PRO server that already exists and is not assigned.)
internal	Requires an internal phone number (a phone number on the Gigaset T300 PRO / Gigaset T500 PRO server that already exists and is not assigned.)

mail	Requires an eMail address as a text value
password	As a text value
…_perm	(permission) indicates the individual user rights (➜ **P. 33**). To accept the standard permissions, leave all permission fields empty. To grant a right explicitly, insert **1**. To deny a right explicitly, insert **0** or leave the field empty.

A shortened example in the text editor is shown below:

login,firstname,lastname,external,internal,mail,password,(…)

0028,John,Sample,,57,user1@example.com,Pw1,(…)

0029,Test,User,,53,user2@example.com,Pw2,(…)

0008,Max,Muster,,24,user3@example.com,Pw3,(…)

Each line represents a user data record. The optional external phone numbers are not inserted; however, the empty "cells between two commas must be present.

Important

As soon as a value is inserted for a permission, all other permissions must be explicitly granted or denied! Empty fields represent permissions denied rather than standard permissions.

Examples:

(…),login_perm,callman_perm,redirect_perm,(…),voice_perm,(…),fax_perm

(…),1,1,0,1,1,0,1,1,0,0,0,1,1,0

The values deviate from the standard permissions in three places. This user has not been given permission to redirect calls, use a voicemail box or view faxes.

Please note

Invalid user accounts will not be imported and listed in an overview. You can either abort the complete import or click on **Import** to only import the valid data records.

Configuring user accounts

The main view for user administration gives an overview of the already existing user accounts and their properties:

◆ Name (settings in **User Data** tab, see below)

◆ Internal and external phone numbers (settings in **Phone Numbers** tab ➔ **P. 21**)

◆ Primary phone (settings in **Phones** tab ➔ **P. 20**)

◆ DND status (settings in **Phones** tab ➔ **P. 20**)

▸ Click on ✎ or double-click on the appropriate line to edit a user account.

The following sections describe the setting options in the individual tabs for user account administration.

User data

All core data for a user account including the login ID can be changed retrospectively here. The language settings are used both for the user interface and also for eMails from the system to the user. If the access data (login ID/password) is changed, the user receives an eMail message with the amended access data.

Fax Preferences.

These settings apply for the sending of Software Fax and Software Fax 2 Mail (see **Phone number properties** ➔ **P. 22**) using the Gigaset pro fax driver. If there is nothing specified for the user here, the system uses Gigaset pro FAX as the sender name and no sender number.

Important

The length of the sender name is restricted to 20 characters. Longer entries made in an earlier version of Gigaset pro will be shortened automatically and must be changed accordingly.

Two options are available to track sent faxes:

◆ Transmission report: A page with the applicable transmission report is inserted into the PDF file which is created from a sent fax.

◆ Transmission result by eMail: The report and the faxed document are sent to the eMail address of the user who sent the document.

If an option is active, it will still be carried out, even if a fax transmission fails.

Redirection rules

Redirection rules can be specified for the user's phone numbers using the corresponding tabs. These rules can always apply or apply only when the user is making a call or does not pick up a call after a certain amount of time.

▶ To activate a redirection for a number, activate the appropriate checkbox to the left. You can redirect a call to any number, including an external or mobile phone number.

───── **Important** ─────

If the line settings require a digit as a **Prefix**, then this must be included in the **Target Number** field for redirections to external phone numbers.

Alternatively, if the user has a voicemail box, you can specify this as the call destination. If a redirection is not activated in the **Timeout** tab, any unanswered calls are redirected to the "deposit" after 30 seconds. You can specify the number for this deposit in the general line configuration or alternatively during the configuration of each line you set up (see **Step 2: Configuring the lines** ➜ **P. 12** and **Advanced settings** ➜ **P. 61**).

───── **Please note** ─────

The user can make/edit these settings himself in his preferences.

Assigning phones to the user

User Data	Redirect	**Phones**	Phone Numbers	iFMC	Keys	Groups	Rights

Display Number: `no display` ▾   Primary Phone: `SIP/1001.DE410IP` ▾

Call Waiting Indication: ☐ activate   DND: ☐

Telephone	Ringing Number	Active	
▾ SIP/1001.DE410IP		⊟	✕
	10	☑	
	13	☐	
			⊞

Primary Phone for several assigned devices: The call manager (i.e., the phone interface on the Gigaset T300 PRO / Gigaset T500 PRO web user interface) and the clients use the primary phone to establish connections as standard.

Call Waiting Indication: If this option is active, the user will be notified of other incoming calls during a call. He can decide whether to take a call, hold it or call back later.

───── **Please note** ─────

By activating the **Call Waiting Indication** function, redirections will not occur when the line is busy!

DND: (DND) If this function is activated, the user cannot be reached on any phone number and at none of the phones assigned to him.

▶ Click on ⊕ **Add Phone** or ⊕ to open the selection of available phones. After making your selection, all the user's phone numbers will be active for this device.

Active: In the list of devices, you can activate or deactivate the individual phone numbers for each phone. This means that, for example, one phone is only available for internal calls and a second for external calls. This restricted activation is denoted by ⊟.

───── **Important** ─────

The device name **FMC/...** indicates an external mobile phone connected via iFMC. The configuration of such a connection is made in the tab of the same name and can also be deactivated there, even if the setting here is already active ☑. "Active" refers solely to the use of the selected phone numbers on this particular phone.

The first registered user "owns" the phone, i.e., his number is indicated on outgoing calls, the call will be assigned to him. If the user would like to listen to voicemails, he must be logged on to the corresponding phone.

────── **Please note** ──────

If a user logs off from the phone using ⟨7⟩⟨8⟩ + login ID, it is no longer assigned to him unless he logs back in again with ⟨7⟩⟨7⟩ + login ID or an administrator assigns him the phone.

When logging in directly on the phone, it must be noted that this phone will automatically become the user's primary phone as a result. If you log off on the same device with *78, the previous primary device is reassigned this property.

Assigning phone numbers

▶ Open the list of available internal and external phone numbers with ⊕ **Add Number** or ⊕ .

▶ To copy the number of your choice, highlight it and then **Select**. The new phone number is automatically activated for all of the user's phones.

If the user is assigned several external phone numbers, you can choose the number to be displayed to call participants from the **Display Number** selection menu. The default setting is the number display withheld, i.e., the call participant will see the call as "anonymous" or "unknown" on the display.

────── **Please note** ──────

The user can make or edit this setting himself in his preferences.

The **Primary internal number** is used for assigning the function keys in the web user interface.

The **Primary external number** is only of importance in an existing interconnection. It is used as an alternative number in the event of the user not being contactable via the internal phone number.

Default Rule: The default setting (**Standard Call**) for each phone number can be changed by selecting this option.

Phone number properties

Conference Room	Reserves the number permanently as a conference room. This option is independent of any planned conference (see **Conference → P. 50**). Conferences held on this number cannot be managed or followed in the web browser in contrast to the planned conferences.
Software Fax 2 Mail	Denotes this number as a fax number. Incoming faxes are forwarded to the user's eMail address and can be viewed in the fax lists on the web user interface.
Software Fax	Denotes this number as a fax number. The user can view incoming faxes in the fax lists on the web user interface.

iFMC

iFMC (Integrated Fixed Mobile Convergence) enables the user to be reached on his device phone numbers even on other phones (e.g., mobile phones), which are not part of the PBX. Outgoing calls are also possible via iFMC numbers or devices from the Gigaset T300 PRO / Gigaset T500 PRO user interface and using CTI clients and connectors. In the latter case (CTI), the iFMC must however be set as the primary phone (➜ **P. 20**).

Please note

By default, all PBX users are authorised to set up and use iFMC. You can change this in the authorisation settings.

To use iFMC, store the phone number where the user is to be reached. This number can only be assigned once system-wide, i.e., it cannot be used in two or more iFMC configurations or by more than one user!

The phone numbers on the PBX, for which iFMC is to be used, should be selected in the **Phones** tab in user settings. By default, all the user's phone numbers will be included in the iFMC.

Call delay: It is therefore possible for a call to be accepted on the system phone for a correspondingly high number of seconds, before the parallel call is started.

Include group calls: As a result of this option, additional calls are directed to the user groups via iFMC. This applies for all phone numbers in all groups, to which the user belongs.

Confirm answering calls by keypress: If this option is active, where there is an incoming call on the mobile phone, initially a voice message is played, whereupon the actual call can be accepted by pressing a digit. This procedure avoids calls being automatically directed via iFMC to the mobile phone's mailbox (if this setting has been activated on the mobile device).

Time-dependent use of iFMC

Users

To use iFMC only at certain times, use the **Period** tab for the applicable iFMC configuration. Here you can create any schedules for weekdays and times of day. Using the control box under **Active**, each iFMC can be switched off irrespective of time.

Function keys

Function keys offer the users of the telephone system simple operation of frequently-used standard actions:

◆ Call contacts

◆ Call pick-up (call grabbing)

◆ Activating and deactivating call redirection

◆ Logging in to and logging off call groups

◆ Automatic callback

◆ Parking calls

◆ DND

Many functions can be used not just in the user interface, but also on the phone's keys. The configuration and use of the keys in the interface exist irrespective of the user's phone model. The transfer of key assignment to the phone is carried out as an option when saving or accepting the configuration. However, this depends on the phone model, or if the user has been assigned a device which is suitable for the transfer and use of the Gigaset T300 PRO / Gigaset T500 PRO function keys.

Please note

To transfer key assignment to phones, autoprovisioning must be active.

You have two options to select a new function key:

▶ Drag and drop a key type from the selection on the right

▶ The **Add Keys** button in the window bottom left

Selecting opens the **Edit function key** window.

──────── **Please note** ────────

The selection of the function types depends on the user's rights, so, for example, only administrators can have keys to activate and deactivate modules.

Busy lamp field

The **Busy Lamp Field** function key is assigned an internal phone number (of a user or a user group) as a target and a status display.

Edit function key	
Key type:	Busy Lamp Field ▾
Key name:	Brown, Ben
User:	Brown, Ben [Choose user]
Target number:	11

The busy lamp field keys have several elements for status and presence display in the function key window, for:

◆ Telephony (available, incoming call, busy)

◆ Redirections

◆ DND

◆ Chat with presence message

If several entries are selected (press and hold Ctrl or shift key), a busy lamp field key is created for each selected user. The busy lamp field keys are also available in the call manager.

Signalling	Meaning	Action when pressed
Green	User is available	Call
Flashing	Incoming call for the user	Call pick-up
Red	User is making a call.	Call waiting indication, if active

Speed dial

The **Speed dial** function key is used for external phone number assignment. You can enter these manually or select them from the addressbook.

```
Edit function key

Key type:        Speed dial            ⌄
Key name:        Black, Susan

Target number:   0161111111      [ Select from Addressbook ]
```

This keypad does not have a status display. The direct dial keys are also available in the call manager.

Redirect

This allows you to activate or deactivate all or some of your general redirections.

◆ **Redirection (Single)**

```
Edit function key

Key type:        Redirection (Single)   ⌄
Key name:        General redirection[10,13]

Activate permanent redirections for call number
Activate         Incoming Line
  ☑                10
  ☑                13
  ☐                18
  ☐                19
```

Conditional redirections (when busy or for timeout) are not affected by this setting. This setting also contains redirections for group phone numbers. The destination for the redirections should already have been defined in the redirections function window. If no redirection destination has been defined for one or more phone numbers, calls will be directed to the voicemail box. If you do not have a voicemail box, the redirections will not be activated and an error message will be displayed.

Signalling	Meaning	Action when pressed
Off	Redirections inactive	Activating redirections
On	Redirections inactive	Deactivating redirections

◆ **Redirection (All)**

Edit function key	
Key type:	Redirection (All) ▼
Key name:	Redirection [Always]
Redirect on:	Always ▼
	Always
	Busy
	Timeout

If this key is assigned, it is possible to select between general call redirection (**Always**), redirection when **Busy** and redirection after **Timeout**.

The selected type of redirection applies for all phone numbers apart from group phone numbers. The destination of the redirections should already have been defined in the redirection settings. Of course it is possible to set different destinations for different phone numbers. If no redirection destination has been defined for one or more phone numbers, calls will be directed to the voicemail box. If you do not have a voicemail box, the redirections will not be activated and an error message will be displayed.

Signalling	Meaning	Action when pressed
Off	Redirections inactive	Activating redirections
On	Redirections inactive	Deactivating redirections

Logging on/off with groups

Using the **Group Log On/Off** key, you can log on to and off from groups to which you belong. The key can apply for one or more groups.

Edit function key	
Key type:	Group Log On/Off ▼
Key name:	Group[Sale]
Group Log On	
Activate	Group name
☑	Sale

Signalling	Meaning	Action when pressed
Off	You are not logged on to the group	Logging on to the group/ the groups
On	You are logged on to the group	Logging off from the group/ the groups

DND

With this key you can activate or deactivate the set DND (Do Not Disturb) for the whole PBX.

```
Edit function key

Key type:    DND                    ▼
Key name:    DND
```

If this key is active, all incoming calls will be rejected, unless a general redirection ("always redirection") or a redirection where the time limit is exceeded is active for the number called. In this case, the redirection is used.

The DND function can only be assigned once, i.e., to one function key. For this reason, the appropriate component in the list of key types is inactive ("greyed out") after assignment.

Signalling	Meaning	Action when pressed
Off	DND function inactive	DND is activated
On	DND function active	DND is deactivated

Call Completion on Busy (CCBS)

This key activates the automatic callback function.

```
Edit function key

Key type:    Call Completion on Busy    ▼
Key name:    Call Completion on Busy
```

The key flashes if the partner station for a call is busy. The user can now (even if he has already hung up) activate **Call Completion on Busy** by pressing the key. The key lights up and signals that **Call Completion on Busy** is active. The PBX now checks at 10 second intervals whether the call destination is available. If, after five attempts, the destination is still not available, an attempt is made every 20 seconds for up to an hour before the callback function is deactivated and the key goes out again. However, if the person called is available, the user's phone will ring. As soon as he picks up, the PBX creates the connection.

This function can only be assigned once, i.e., to one function key. For this reason, the appropriate component in the list of key types is inactive ("greyed out") after assignment.

Signalling	Meaning	Action when pressed
Off	**Call Completion on Busy** is inactive	No action
Flashing	Activation of **Call Completion on Busy** is possible	**Call Completion on Busy** is activated
On	**Call Completion on Busy** is active	**Call Completion on Busy** is deactivated

Parking calls in queues (Park & Orbit)

The system provides 100 holding spaces from 00 to 99, in each of which a call can be parked. A **Park & Orbit** key is created for each holding space selected during key assignment.

Different to standard call holding, other users have access to the holding spaces and can accept the calls parked there themselves. For this, the users must however also have keys with the appropriate orbit numbers.

Signalling	Meaning	Action when pressed
Off	Holding space is available	Call is parked (only possible via phone keypad)
On	Caller is waiting in orbit	Call is accepted

Please note

Only parked calls can be collected from orbit using the keys in the web interface. Call parking is only possible directly on the phone

---

Activate modules

Existing module configurations are activated and deactivated with the **Module** key. You can also assign a key to several module configurations.

Signalling	Meaning	Action when pressed
Off	Module inactive	Switching on module
On	Module active	Switching off module

Empty key

This key can be described in any way you want and you can therefore optically segregate groups or different key types.

Sorting and removing keys

▶ Highlight one or more keys by clicking with the mouse and pressing and holding the Ctrl key. Several keys can also be highlighted by dragging the mouse over the relevant keys while keeping the left mouse button pressed. The area is highlighted in orange when dragging.

The highlighted keys can then be pushed on the contact surfaces on the left using drag and drop ▥ ☰ and arranged. In the same way, complete columns can also be swapped with each other using their contact surfaces above the column headings.

▶ Remove the highlighted keys by clicking with the right mouse button in the highlighted area and then on the **Delete** option, or use the **Delete selection** button on the lower edge of the window.

Individual keys can alternatively be deleted using the ✎▼ editing menu.

Advanced options for Gigaset IP phones

If you have a Gigaset pro phone, you have access to additional convenience functions. You can access these via ⊙.

Transferring the keys to the phone

You can copy the user-defined assignment of the function keys for the PBX to the function keys on the phone. The first **n** numbers are copied to the phone keys, whereby **n** corresponds to the number of function keys on the set (e.g., 14 keys on a Gigaset DE700 IP PRO).

The dialogue with the question whether and to which device the keys should be transferred, can be switched off in the **Window** tab for user settings. In this case, the keys are not transferred to the device.

--- **Important** ---

For a successful transfer, the autoprovisioning of the PBX must be switched on and the relevant device must be set up using autoprovisioning.

Key labels for phones

Using the ⊙ option menu in the key window, you have the option of creating a PDF file for labelling the function keys in a suitable arrangement and size, and then to print it.

There are add-ons available for Gigaset DE410 IP PRO, Gigaset DE700 IP PRO and Gigaset DE900 IP PRO allowing additional keys to be programmed. You can also create the labelling for these.

Group assignment

In the list on the left, you can see all the groups that have been set up.

▸ Add or remove the user as a member of the highlighted group by using the arrow keys between the list fields.
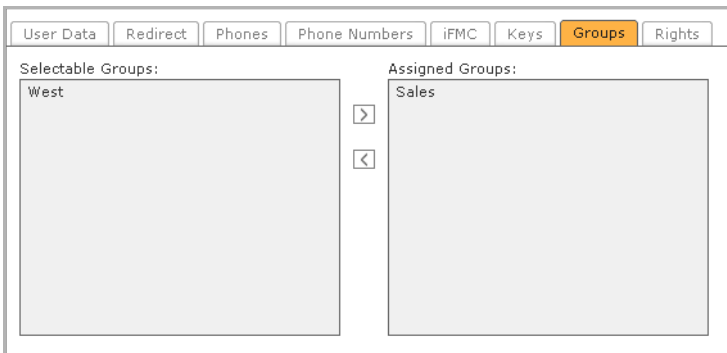
User rights

Activating/deactivating the check boxes assigns/revokes rights for the user. The buttons for changed areas are displayed in the menu bar of the web operating interface (in the case of authorisation) or are no longer displayed (after rights have been withdrawn). In the interface for a user who has just logged on, an appropriate message is displayed before the whole interface is automatically reloaded after a few seconds.

The withdrawal of rights for individual features in general only affects their availability in the user interface and on function keys. For example, access to addressbooks, call lists and voicemail boxes or in the phone menu is still provided, even though authorisation is missing. Likewise, the withdrawal of the call manager only affects its availability in the user interface (e.g., via the call menu button). The ability to make and receive calls is not restricted by this.

Automatic assignment of rights for new user accounts

Section	Subordinate	Active	Column name on import
Keys		Yes	fkey_perm
	Show redirection	Yes	fkey_shw_fwd_state_perm
	Show chat status	Yes	fkey_shw_im_call_perm
	Show incoming caller	Yes	fkey_shw_inc_call_perm
	Show "On the phone with"	No	fkey_shw_act_call_perm
Fax		Yes	fax_perm
Redirect		Yes	redirect_perm
Preferences		Yes	setting_perm
iFMC		Yes	ifmc_use_perm
	Changing	Yes	ifmc_edit_perm
Records		Yes	calllist_perm
Directory		Yes	address_perm
Voicemail		Yes	voice_perm
Login		Yes	login_perm
Conference		Yes	conference_perm
Administration		No	admin_perm
Call manager		Yes	callman_perm

Please note: The authorisations for Instant Messaging and Remote Connect are not implemented. All users are able to access the XMPP service.

Groups

Groups are used to define teams in which anyone is entitled to pick up a call. They are also used for mapping functions such as fax and broadcast.

▸ Click on the **New Group** button at the bottom of the **List of registered groups** window.

New Group			
Group Name:	Sales	Chat group: ☐ activate	
Ringing Strategy:	Ring All Group ⌄	Voicemail Box: ☑ activate	
Group ID:	0006	Password: 5716	Random Password

Assigned Phone Numbers

Internal Phone Number:
14
15
16

External Phone Number:
- none -

--- **Important** ---

In contrast to a user password, a group requires an identification number using the digits 0-9. Group members can then log in and out by entering the group ID and password on the keypad (see Appendix **Key combinations on the phone** ➔ **P. 101**).

Example: A group called Sales is created to improve customer orientation. This group is assigned the internal phone number 30 and the external connection number 20123746. A call to this number is indicated on the phones belonging to those members logged in to the group. Any of these users can accept the call.

Editing group preferences

There are only minor differences between group and user administration. Like users, groups have access to call redirection (), phone numbers (**Assigning phone numbers** → **P. 21**), voicemail boxes (**Voicemail** → **P. 47**) etc. The assignment of users to a group is made in the user assignment tab.

▸ Click on the editing icon in the **List of registered groups** window. You can configure or edit all group data here.

Group: Sale			
Group Data	Redirect	Phone Numbers	User Assignment

Group Name: `Sale`
Ringing Strategy: `Ring All Group` ▾
Group ID: `0004`   Password: `1549`   `Random Password`

Chat Settings

Chat group: ☐

The call properties for a group

Ringing Strategy: Apart from the standard call functions, simultaneous ringing of the phones for all logged-in group members (**Ring All Group**), the following options are available:

Broadcast Similar to an announcement (i.e., without having to actively accept the call), all members will receive the call via the phone loudspeaker (function only available on phone models supporting auto-answer).

Call Hunting The call is directed to only one group member. If the call is not accepted within 15 seconds, the next member's phone will ring, etc. The sequence for call hunting corresponds to the member list in the user assignment tab and can be changed there by dragging and dropping the list entries.

Software Fax This function turns the group into a collection point for faxes sent to the group's phone number. Each member has access to the fax messages received via the fax list in his user interface.

───── **Please note** ─────

Extended module configurations may create an additional option for the **Ringing Strategy**.

Chat settings

The **Chat group** option influences the presentation of the members in messaging clients (see **XMPP → P. 89**). As a result, the members are shown within the group and can all be contacted at the same time with a message to the superordinate group (similar to a group call/broadcast).

Whether a group is a chat group or not has no effect on its call properties ("ringing strategy") or on the XMPP access of individual members and their availability in chat.

User assignment

▶ Click on ⊕ or ⊕ **Add Person**. You can search for local users or users from other PBXs in an interconnection using the search/list view.

Group Data	Redirect	Phone Numbers	**User Assignment**	
List of Members				

	User Name	Logged On	
≡	1. Black, John	☑	✕
≡	2. Water, Jane	☑	✕
≡	3. Brown, Ben	☑	✕
			⊞

You can set the availability of the members via the group's phone number(s) by activating the checkbox in the **Logged On** column. This activation or deactivation corresponds with the setting that the user makes in his preferences. This means that if the member is logged in, the availability is activated in his user preferences and vice versa.

Phones

Preferences/Autoprovisioning

Phone autoprovisioning is described in chapter **Initial configuration** (see **Preferences** ➜ **P. 8**).

List of configured phones

All automatically and manually configured phones are displayed here. The list view can be restricted by selecting the first letter of the tab. The number of entries displayed can be changed to suit your individual needs under **Rows**. Depending on the number to be displayed, the list will be spread over several pages.

The list contains the following information and options for each phone:

◆ State (whether the device is registered on the PBX)

◆ Device Type

◆ Device Name: Name of the access (SIP account) to register a phone to the PBX

◆ IP address: A single mouse-click on an address marked in bold opens the web interface (if available) for the corresponding device in a separate browser window.

◆ Assigned users - users to whom the device is assigned.

◆ Double clicking on the row or a single click on ✐ opens the phone's detailed settings.

◆ Clicking on ✕ deletes the phone entry from the list and ultimately from the system.

Other phones can be added via the **Manually** and **Search** buttons.

Configuring phones

Instructions on automatically detecting and configuring phones via the network can be found in the **Initial configuration** chapter (see **Step 1: Configuring the phone ➔ P. 8**).

Manual configuration of phones

Softphones and phones that cannot be configured automatically can be set up manually.

▶ Using the **Manually** button, open the dialogue for configuring additional phones.

▶ Select the type of phone from the **Telephone Type** dropdown list.

This dropdown list contains all standard phones currently supported by Gigaset T300 PRO / Gigaset T500 PRO. If a device or softphone is not listed, you can either:

– Select "Standard SIP", which contains the basic function settings.

– Create your own configuration for this type of device (see **Defining new device types ➔ P. 40**).

▶ Enter a name and password in the **Telephone name** and **Password** fields for the end device. These two entries, in conjunction with the server (IP) address, from the **SIP account**.

Please note

The field corresponding to the **Telephone name** has different designations in the configuration interfaces for the individual phone types (clients), e.g., user ID, authorisation name/authentication name, user name

For some clients, the **Telephone name** must be entered in two or more separate fields, e.g., in **user name** and **authorisation name**.

▶ Click on **Save** to complete the manual configuration of a new phone.

▶ Assign the phone to a user. This will then show the phone's state as active.

Important

For softphones and manually configured end devices, it is also necessary to enter the SIP account (user name, password, server IP address) in the settings of the respective phone and to restart the device.

Overwriting phone settings

For several device types, there is an option to copy the settings of the Gigaset T300 PRO / Gigaset T500 PRO directly to the phone via the network without having to change the settings on the phone.

The prerequisites for this are:

◆ The phone has already been autoprovisioned.

◆ The phone's HTTP access must not be protected by a user name and/or password.

◆ The corresponding SIP account must be stored on the phone's primary line, as Gigaset T300 PRO / Gigaset T500 PRO only overwrites this line. If the SIP account is located on another line, Gigaset T300 PRO / Gigaset T500 PRO will create an additional account on Line 1.

Fax functionality

This must be specified via **Functionality** for ATA adapters used to connect fax machines.

Advanced settings

Important

When operating external phones, several ports in the firewall that protect the local network from Internet access (not the firewall for the Gigaset T300 PRO / Gigaset T500 PRO server) must be enabled. The following ports are affected: 5060 UDP and 10000-20000 UDP (for SIP and RTP), 4569 UDP (for the IAX protocol).

NAT   If the phone is not part of the local network, **NAT** must be changed to **yes** to allow the transfer of voice information via firewall/router.

Codecs   Codecs convert analogue (voice) information into digital data and vice versa (encoding and decoding). One or more codecs may be assigned to the phone. You must enter multiple codecs as comma-separated values, e.g., **alaw,ulaw,gsm**.

Although Gigaset T300 PRO / Gigaset T500 PRO supports many of the commonly used codecs, we recommend using the codecs G.711 alaw and ulaw. G.711 has the best voice quality (comparable to ISDN) and a minimal delay of 2 ms. However, it does require a (relatively) high bit rate of up to 84 kbit/s. In comparison, codes such as G.729 only require a bit rate of 8 kbit/s but have a delay of between 25 and 35 ms.

HD voice

The broadband codec G.722 (High Definition Voice), with its frequency range of 50 to 7000 Hz at a low transmission rate (64 kbit/s), offers a much higher voice quality than G.711. To preferentially use this codec, enter it as the first value in the codec field - followed by alternative codecs.

Example: **g722,alaw,ulaw**

Video telephony

To use a device for video telephony, you will also require the appropriate codec h263 or h263p.

If you wish the phone to transfer voice and video data, you must enter the voice codec first followed by the video codec.

Example: **alaw,ulaw,h263p**

restr. to IP   **restr. to IP** limits operation of the phone to the specified IP address.

Please note

Licences are required for the use of some codecs. G.729, for example, is integrated in Gigaset T300 PRO / Gigaset T500 PRO but must be registered first. A program is available for registration in**/usr/lib/asterisk/modules/g729/** which is started with the **./register-g729-32-bit** command.

Defining new device types

Please note

Licences are required for the use of some codecs. G.729, for example, is integrated in Gigaset T300 PRO / Gigaset T500 PRO but must be registered first. A program is available for registration in**/usr/lib/asterisk/modules/g729/** which is started with the **./register-g729-32-bit** command.

If you cannot find the device you wish to use listed in the default list, you can add several device types.

▸ Select **new...** from the **Telephone Type** dropdown menu.

Configure the new device type in the **New Phone** dialogue window.

▸ Give the device type a unique name.

In the entry screen, the fields **type**, **dtmfmode**, **canreinvite** and **qualify** are preset and can be applied in many cases. All other fields are not mandatory fields. Their importance is explained in the following section.

Options for phone configuration

type	The phone's connection type
peer	Can receive calls via the Gigaset T300 PRO / Gigaset T500 PRO server.
user	Can instigate calls via the Gigaset T300 PRO / Gigaset T500 PRO server.
friend	A device that can both receive and instigate calls. This is the most common setting and advisable in most instances.
host	Use the **dynamic** option (instead of specifying an IP address), as several device types can only log in with **dynamic**.
dtmfmode	Indicates the tone dialling standard that should be used. This is dependent on the phone type being configured (see manufacturer's specifications).
permit	IP address(es), via which the client can log on to the server. Either a pure IP (e.g., **192.168.0.1**) or IP/subnet mask (e.g., **192.168.0.2/ 255.255.255.0**). Multiple entries must be separated by commas.
deny	Is the opposite of **permit** and excludes the IP addresses specified here.
mask	If you have specified IP addresses without subnet masks under **permit** and **deny**, you can enter a single subnet mask (e.g., **255.255.255.0**) for both fields.
nat	**yes**: If the phone is located outside of the LAN firewall, or **no** (default value).
canreinvite	**yes** provides clients with the option to exchange data directly (without server involvement) after establishing a connection. As several hardware components malfunction with this setting, the default value **no** should not be changed.
disallow	It is advisable to prohibit all codecs by specifying **all** and explicitly allow the codecs of your choice by specifying these in the **allow** field. The codecs must be entered as comma-separated values, e.g., **alaw,ulaw**.
insecure	**very** - if the host is already registered, it can instigate calls without having to reauthenticate itself. **yes** - a peer can register himself easily with the IP address (without specifying a specific port).
trustrpid	**yes** or **no** (default value).
progressinband	**yes**, **no** or **never** (default value).
promiscredir	**yes** or **no** (default value).
port	The port number 5060 is the default value for the SIP protocol on the Gigaset T300 PRO / Gigaset T500 PRO server. This value can be replaced by a port number to be used exclusively for SIP.
qualify	Either **yes**, **no** or a specification in milliseconds. For **yes**, the server tests every 2000 ms whether the client is still available. If the client does not react within this timeframe, it is regarded as not available for Gigaset T300 PRO / Gigaset T500 PRO and no other calls are forwarded to the client.

defaultip	Standard IP address for a client; if the value **dynamic** is specified in the **host** field, the Gigaset T300 PRO / Gigaset T500 PRO will attempt to forward incoming calls for a client still to be registered to this IP address.
rtptimeout	Number of seconds after which a connection is automatically terminated after data traffic inactivity (RTP). This is advisable, e.g., when a subscriber forgets to replace the receiver.
rtpholdtimeout	If **rtptimeout** does not respond during a call, then specify the maximum number of seconds for which a call may be held here. The number must be greater than the **rtptimeout** value.
fromdomain and **fromuser**	Connections to some SIP networks require a user name and the domain name of the server.

▸ Click on **Save** to copy your configuration to the list of phone types.

In future, you can click on 🖉 in the dropdown list for device types to open it for editing purposes.

Modules

The Gigaset pro modules have additional features and functions that are not permanently integrated in Gigaset T300 PRO / Gigaset T500 PRO. Pre-defined modules are provided for the following functions:

Announcement before pick up	Playing back a sound file (music or an announcement) for incoming calls for specific numbers.
Call-Through	Connecting external calls via Gigaset T300 PRO / Gigaset T500 PRO to other external phone numbers. This will incur fewer costs for the caller, e.g., a field worker using a mobile phone, as he will only be charged for the connection to Gigaset T300 PRO / Gigaset T500 PRO.
Personal secretary	Redirecting various callers (groups) to two separate target numbers.
Single-stage IVR	Configuration of a voice menu with keypad input. A target number can be saved for each key, to which the caller can be forwarded at the press of a button.
Memo for me	Recording of voice files on the phone via selected phone numbers. Subsequently, the recording is sent via eMail to a user-defined address.
SIP password security check	Checking SIP passwords.
Voicemail playback	Listening to the messages on the voicemail box.
Time-controlled redirection	"Day and night service". Calls for phone numbers that correspond to the specified samples are redirected to a voicemail box or a voice message. Negative lists can be used to ensure callers and called numbers are not processed by this module.

The modules supplied with Gigaset T300 PRO / Gigaset T500 PRO can be modified to suit personal requirements. However, the module concept primarily offers the possibility of creating your own functions.

Detailed, up-to-date descriptions of the modules provided can be found in the Gigaset pro Wiki: http://wiki.gigaset.com

Module configuration allows you to apply the module quickly and easily. This configuration process is described below.

Module configuration

A **Module Configuration** is an executable instance of a module. The underlying module is modified for productive use in or by the **Configuration**.

Existing configurations are denoted by four indicators in the overview list.

State: If this is not highlighted in green, there is an error in the module. The error message is shown by moving the mouse over the status.

Module: Name of the underlying module

Name: The actual name of the configuration

Active: This option can temporarily deactivate each module configuration thus ensuring it will no longer be executed. Nonetheless, the settings within the configuration are retained.

Creating a new module configuration

▸ Open the selection of available modules via **New Configuration**.

▸ Select the module you wish to use from the list and click on **Create**.

This opens the configuration editing view. Depending on the module selected, this contains various tabs.

All module configurations contain the **General** tab.

▸ Specify a name for your configuration here, with the option of adding a short description or comment for internal documentation purposes.

Several module configurations contain the **Phonenumbers** tab. This is used to select phone numbers from your Gigaset T300 PRO / Gigaset T500 PRO PBX, for which the module should be used.

The following paragraphs illustrate the module configuration steps using the modules supplied with the Gigaset T300 PRO / Gigaset T500 PRO.

Log file

This section is used to display log entries for the respective module configuration. The scope and level of the log file is specified directly in the module on which the configuration is based. This log file cannot be changed here and varies considerably from module to module - some modules do not have any protocol features.

The log levels in the selection menu are sorted in ascending hierarchical order. This means that every level also contains information about the stages above it. For example, the **TRACE** level also can display the entries for the other levels.

If there are log entries in the selected view, a button for downloading a file containing these entries is shown below the list on the left. This file contains the number of entries or rows specified above.

─── **Please note** ───

The number of lines displayed relates to the last n rows in the log file; these are displayed in chronological descending order for improved readability!

Order of execution of several module configurations

Configurations of modules from **Call-Processing** may have the same rights and thus compete for access to calls. The **Execution order** domain is used to control this. Here, you can specify the sequence of the various call processing subtype modules, according to which the module configurations should process call connections. You can change the sequence using the arrow keys or drag & drop.

The execution lists only contain the relevant module configurations. This means that you do not have to add these yourself or put them in a sequence. If a sequence does not contain any entries, this means that there are no competing module configurations of this type.

Module library

The library contains the modules supplied with Gigaset T300 PRO / Gigaset T500 PRO and can be expanded by adding self-created and imported modules to suit your needs.

Modules are shown in the overview list with the following indicators:

State	If this is not highlighted in green, there is an error in the module. The error message is shown by moving the mouse over the status.
Name Version	Name the module
Vendor	The name of the module creator
🔒	The module is protected by its own password can not be edited, copied or downloaded. Click on this icon to enter the password.
🔓	The password protection is temporarily deactivated. This module can be edited, copied and downloaded during the current Gigaset T300 PRO / Gigaset T500 PRO session. One mouse-click on the icon closes the module again!
▤	For creating an identical copy (clone) of the module. The copy is inserted below the original version in the list and can be edited and modified independently of the original.
⤓	For downloading the module as a ZIP file. Downloading a module allows you to save it locally, e.g., to use on another Gigaset T300 PRO / Gigaset T500 PRO installation or to transfer it. Select the option "Save to hard disk/diskette" and save the file in the directory you wish to use.
✎	For editing this module in the module designer
✕	For deleting this module

Module import

▸ Click on **Import Module** to import a module.

▸ Then select a module file in ***.sfm, *.zip** or ***.jar** format in the file manager and upload it on to the server. The module is copied to the library list.

Caution ────────────────────────────────

When importing a module that is already available, this will be overwritten irrespective of the version number by the file being uploaded.

Creating new modules

The module designer is the development environment for creating modules.

You can edit existing modules and create new modules. Create functions and function components that you can adapt to suit your needs and integrate in various modules.

Open the module designer by clicking on ⊕ or **Create new Module**.

Voicemail

A list of the voicemail boxes already set up is displayed. Operation is standardised, i.e., with sorting, searching, alphabetical tabs etc. You can add, edit and delete voicemail boxes.

In the editing screen (accessed via ✐) for a voicemail box, you can add and remove users and user groups. It is possible to create, edit and play back announcements.

If the option for voicemail is checked when creating a user/group account, the names of the corresponding voicemail box are already assigned.

Configuring and editing voicemail boxes

```
Edit Voicemail Box

Mailbox Name:  mailbox 37      Mailbox Number:*9      Password:  3654
```

> **Please note**
> One a new voicemail box has been saved, its ID is automatically generated.
> This number is used to listen to any voicemails received via the key combination
> 9 + <ID for voicemail box> directly on the phone.

Voicemail Settings: If you activate the No recording option, callers are not able to leave voicemails on this box. Only the introductory announcement is played. If the voice recording is not deactivated, the recording length can be adapted. The default setting is 30 minutes. This is also the maximum recording time for each voicemail.

Send Message By E-Mail: Incoming messages on the voicemail box can be sent to the user as an eMail attachment as an option. Simply activate the checkbox below **Send Message By E-Mail**.

Recording a voicemail announcement

Announcements created here are saved as system-wide announcements meaning that they are visible to all users, can be selected and also be edited by users with administration rights. Personal, private announcements should thus always be configured in the user's own preferences.

▸ Select **Manage Announcements**. You will see the list of available announcements.

▸ You can open the dialogue window for recording new texts with the **New Announcement** button.

▸ First, select a name for the new text.

▸ Select the phone with which you wish to record the announcement and click on **Record**.

New Announcement	i
Name:	
⦿ Record Announcement:	
(SIP/1001.DE900I∨) [Record]	
○ Upload announcement:	
[_____] Browse [Upload]	
	[Save] [Cancel]

The telephone rings and you can hear a spoken instruction.

▸ Speak the new announcement text and then press [#] on the phone to end the recording.

▸ Then click on **Save** in the dialogue window to save the new announcement on Gigaset T300 PRO / Gigaset T500 PRO.

If you wish to change the announcement, click on ✐ and repeat the recording process.

Uploading a file with an announcement

▸ Select **Manage Announcements**.
▸ By pressing the **New Announcement** button, you will open the dialogue window with the same name.
▸ First, select a name for the new text.
▸ Activate the **Upload announcement** option.
▸ Click on **Browse** and select the file you need on the PC.
▸ Select **Upload**.

Please note

With respect to audio files for announcements, see also **Sound files for the Gigaset T300 PRO / Gigaset T500 PRO PBX**, **P. 100**.

If the file has been loaded successfully, the file name will be displayed.

▸ Then click on **Save** in the dialogue window to save the new announcement on the Gigaset T300 PRO / Gigaset T500 PRO.

If you wish to change the announcement, click on ✎ and repeat the recording process.

Conference

Several base settings must be made before you can use the managed conference function. First, phone numbers are defined, via which the participants can join the conference. When setting up an individual conference via the corresponding function window in the main menu, a PIN is automatically generated for each invited participant. This is required to be able to access the conference; otherwise participants will not be able to dial in to the conference.

The **Server Address for Web Link** specifies an internal or external IP address that is inserted into the eMail as a web link. By going to this address, participants can fully participate in the conference in the web browser.

The invitation text available is a general template and should be modified when planning and setting up individual conferences. There are **Template Variables** available for automatically creating texts of invitation. These are dynamically replaced with values such as conference PIN, phone number, time etc. when the eMail is sent.

▸ To insert a variable, mark the desired point in the text and click on the corresponding entry in the selection list.

Invitational eMails will always be sent to participants after creating a particular conference.

An eMail notification is also provided in the following cases:

◆ Where there are subsequent changes in conference details, e.g., if the start of the conference is changed,

◆ As a reminder, 15 minutes before the start of the conference,

◆ As an invitation to the next appointment in the case of a repeat conference, in each case at the end of a conference appointment.

Important

In the case of changes to conference administration – e.g., assigning new phone numbers – the participants of already planned conferences will not be notified by eMail. In these cases, the conference planning must be opened again and saved with the changes.

Directory

Selecting the addressbook

You have the option to either create new directories using the addressbook integrated in Gigaset T300 PRO / Gigaset T500 PRO or integrate existing directories via **LDAP**.

The directories required for the addressbook are created in the **Folder Configuration** - e.g., a directory for customer contacts and a second for business partners. You can create additional directories at any time. If users are supposed to be able to edit contact data and create new entries, activating the checkbox below **Write rights** will allow the directory to be edited.

The folders configured in this manner are accessible to the addressbook user in a selection list, which he can use to change between the individual directories.

The layout of the addressbook view and the view of the individual contact data records is configured in the **Layout** tab. The layout of the addressbook is already set up but can be modified here to suit the user's needs. However, the layout for LDAP folders must be set up first.

Connection to the LDAP server

To establish a connection to the LDAP server, you will require the IP address of the server, valid user name and password, and the base directory on the LDAP server that should be accessed. The format of this data should be in LDAP syntax. Once a connection to the server has been established, it is possible to select the directories that should be available in the addressbook in the folder configuration.

Folder configuration

Give the directories in the left-hand column a name that will then be used in the selection list for the addressbook folder.

Folder Configuration	
Name	Folder
Addresses	all
Users	users
Private Contacts	private
Partner	1

The "Private" folder has been renamed and folder "Partner" has been added.
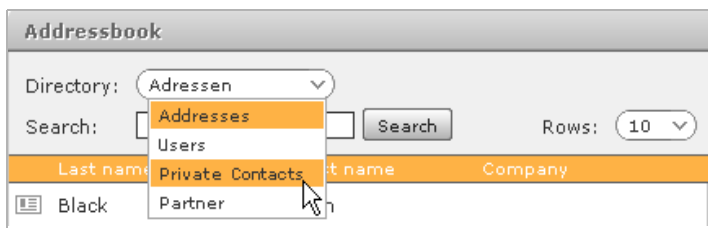
The modified directory list in the addressbook.

Please note

There is a layout already available for the addressbook. If it is intended for addressbooks to be accessed on the LDAP server, then the layout for these addressbooks must be configured first. More information about this can be found in the next section.

Layout

You can choose from several options:

◆ MS Active Directory 2003

◆ LDAP view

◆ Internal addressbook

◆ Extended internal addressbook

Individual modifications can be made here.

Configuring the list view

Here, you can specify entries that should be seen directly in the open addressbook. Column 4 is used for phone numbers. Gigaset T300 PRO / Gigaset T500 PRO uses name resolution, i.e., to assign names to phone numbers, with the phone numbers saved here. If one of these fields is removed from the view (e.g., "mobile"), the corresponding name cannot be shown in the call lists or the call manager.

Configuring the contact view

The blocks created here are used for the contact view, similar to an index card. All detail fields defined in the blocks are visible to the user in the index-card view and can be edited (if read/write permissions available).

The standard contact views

There are blocks ready for use for the addressbook from the Gigaset T300 PRO / Gigaset T500 PRO in the templates "Internal addressbook" and "Extended internal addressbook":

The contact view, as generated by the "Internal addressbook" template and displayed to the users.

The contact view, as generated by the "Extended internal addressbook" template and displayed to the users.

Extending existing blocks

▸ To add a new field or additional line to a block, simply click on ✛ in the block's right-hand column.

▸ In the **Displayname** column, select the column for the input field.

▸ By selecting the **Fieldname** column, you are assigning the value you require to the field.

Example: The entries in the **Contact** block should contain the position of the person within the company alongside the company's name. Add a row to the block as described above and select the entry **Job Title** below **Displayname**. For the field name, specify **job_title**.

Adding blocks to the contact view

▶ To add an additional block to the contact view, click on **New Block** or ⊕.

▶ Search for the title of the block section in the **Block name** selection.

▶ Then add the fields you require to the **Displayname and order** table, as described in the previous section.

Example: You want to expand the contact view to contain a field for the delivery address. Create a new block with the block name **Dispatch address** and insert the address fields you require for this into the table using ⊹.

Phone numbers

This list view provides an overview of the phone numbers already assigned and their mapping to users, groups and module configurations.

▶ To change a list entry, double click on it or click on ✎.

The **Phone Numbers** tab for the relevant user or group account or module configuration opens and the mapping can be modified.

Lines

General

The general settings affecting all lines in the first tab are described in Chapter **Initial configuration** in **Step 2: Configuring the lines** (➔ **P. 12**).

The following sections describe setting up individual lines in the same tab and their external call numbers.

Lines

Lines (or connections) denote the connections of the Gigaset T300 PRO / Gigaset T500 PRO PBX that are used for telephony.

These are:

◆ Direct Internet connections via a VoIP provider

◆ ISDN connections to an ISDN vendor or internal ISDN device

◆ Connections to analogue devices or to an analogue phone network

Hence, there are the following options available for connection in the selection list:

◆ Provider

◆ ISDN card, external/ISDN card, internal

◆ Analogue FXS/FXO

To add and set up a connection, click on ⊕ or ⊕ **New Line**.

> **Please note**
>
> Analogue and ISDN connections are only possible if you install an analogue and/or ISDN card in your Gigaset T300 PRO / Gigaset T500 PRO. You can obtain these cards from Gigaset Communications. Third-party cards may not be supported or only in part.
>
> If there are no cards installed in the PBX or these can not be recognised, then you can only select the lines for VoIP providers.

> **Please note**
>
> ISDN and VoIP connections can alternatively be set up using **Quickstart Wizards**.

Provider connection

Select the configuration of your VoIP provider from the **Provider** selection list. If this is not available in the list, then you can create a new configuration. See **Creating and editing the provider configuration ➜ P. 56**.

If your provider or the type of contract requires an authentication, you will find your user name and password in your provider's documents, with which the line will authenticate itself to the provider.

The phone numbers are input in the middle tab, Number range (see **Number range ➜ P. 60**). Successful authentication is indicated by a green **Provider Status** and the comment "Registered".

Creating and editing the provider configuration

If the VoIP provider is not in the selection list, you can create a new configuration for your provider by using the **new...** option.

In the **New Provider** dialogue window that opens, give the configuration a unique **Provider Name**. In the input mask at the bottom, the fields **type**, **dtmfmode**, **auth mode**, **auth**, **can reinvite** and **qualify** are preset and can be applied in many cases. Of course, the **host** field is important for the provider address.

The meaning of the individual fields:

type	The connection type

	peer	Can receive calls via the Gigaset T300 PRO / Gigaset T500 PRO PBX.
	user	Can instigate calls via the Gigaset T300 PRO / Gigaset T500 PRO PBX.
	friend	A partner station that can receive and instigate calls. This is the most common setting and advisable in most instances.

host	The IP address (or the DNS name) of the provider.
dtmfmode	Indicates the tone dialling standard that should be used. Possible values: rfc2833, inband, info
auth mode	Depending on the provider, the Gigaset T300 PRO / Gigaset T500 PRO authenticates itself via the IP address or by using a user name and password.
auth	When authenticating using user name and password, the login data is transferred as either **plaintext** or encoded (**md5**, **rsa**).

canreinvite	**yes** provides clients with the option to exchange data directly (without server involvement) after establishing a connection. As several hardware components malfunction with this setting, the default value **no** should not be changed.
qualify	Either **yes**, **no** or a specification in milliseconds. With **yes**, the server tests at regular intervals whether the client is still contactable with each query lasting 2000 ms. If the client does not react within this timeframe, it is regarded as not available for Gigaset T300 PRO / Gigaset T500 PRO and no other calls are forwarded to the client.

Additional options for the provider configuration

── **Please note** ──

The configuration parameters vary from provider to provider. Please contact your provider about the correct settings.

---

permit	IP address(es), via which the client can log on to the Gigaset T300 PRO / Gigaset T500 PRO server. Either a pure IP (e.g., 192.168.0.1) or IP/subnet mask (e.g., 192.168.0.2/255.255.255.0). Multiple entries must be separated by commas.
deny	Is the opposite of **permit** and excludes the IP addresses specified here.
nat	**no** is the default value. **yes** - if the provider's VoIP server (see address in **host**) is not directly contactable, but the address is affected by NAT.
disallow	It is advisable to prohibit all codecs by specifying **all** and explicitly allow the codecs of your choice by specifying these in the **allow** field. These must be entered as comma-separated values, e.g., **alaw,ulaw**.
insecure	**very** - if the host is already registered, it can establish connections without having to reauthenticate itself. **yes** - a peer can register himself easily with the IP address (i.e., without specifying a specific port).
progressinband	
	yes, **no** or **never** (default value).
port	The port number 5060 is the default value for the SIP protocol on the Gigaset T300 PRO / Gigaset T500 PRO server. This value can be replaced by a port number to be used exclusively for SIP.
defaultip	Default IP address for the host; if the **host** field is assigned a **dynamic** value, the Gigaset T300 PRO / Gigaset T500 PRO will attempt to establish connections via this IP address.
	Only effective for type=peer
rtptimeout	Number of seconds after which a connection is automatically terminated after data traffic inactivity (RTP). This is advisable, e.g., when a subscriber forgets to replace the receiver.
	Only effective for type=peer

rtpholdtimeout

If **rtptimeout** does not respond during a call, then specify the maximum number of seconds for which a call may be held here. The number must be greater than the **rtptimeout** value.

Only effective for type=peer

fromdomain / **fromuser** Connections to some SIP networks require you to reenter a user name and the domain name of the server.

Calling line display

Here, you can specify which format is used to show phone numbers in displays, phone lists etc. Please check with your provider which formats it supports!

Using cards/adapters

Cards already installed are usually recognised by the Gigaset T300 PRO / Gigaset T500 PRO and can be selected in the **Card Type** menu. The line can have whatever name you wish; however, it should be self-explanatory (e.g., the name of the respective ISDN vendor).

────── **Please note** ──────────────────────────

If you wish to assign the connections of a card to different lines/connections, then each line must be added using **New Line** or ⊕.

──
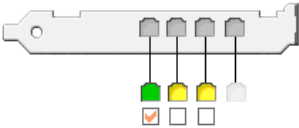
Activating the checkbox below the relevant line will assign it. The status of each connection is indicated by a colour:

◆ Lines already connected, i.e., physically linked to an outside line, are highlighted in green.

◆ Not connected but already configured connections are highlighted in yellow. This can occur, e.g., if a cable is disconnected.

◆ Connections that are still not configured or physically connected are indicated by dark grey.

◆ If a connection has already been assigned to a line, it is greyed out and does not have a checkbox.
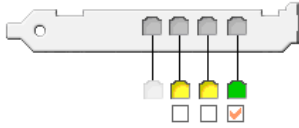
────── **Please note** ──────────────────────────

◆ If you wish to assign several ISDN cards to the same connection/number range, add each additional card using ⊹.

◆ The colour coding only pertains to ISDN cards. The individual connections on analogue cards are always shown in the same colour.

──

| TeleMaxxISDN | | Nr.: 2 | ISDN external |

Card Type	Manufacturer	Line Allocation	
PCI4S0 ISDN ∨	Sirrix PCI-Slot: 1		

ISDN-Card | Number area | Extended

| arcor | | Nr.: 3 | ISDN external |

Card Type	Manufacturer	Line Allocation	
PCI4S0 ISDN ∨	Sirrix PCI-Slot: 1		

ISDN-Card | Number area | Extended

Two connections on an ISDN card can be assigned different lines.

ISDN connection (external/internal)

The first step for configuring ISDN lines is specifying external or internal.

◆ Select **ISDN external**, if the line is to assume the connection to the telephone network. For external mode, the output of the ISDN card must be connected to the terminal with a standard patch or ISDN cable.

◆ Select **ISDN internal** to use the line for ISDN fax machines, phones or as a connection to an existing PBX. For this mode, the output of the ISDN card must be connected to the phone with a crossover ISDN cable.

Important

After any change to the ISDN configuration, the telephony subsystem must be restarted. This will end all running connections!

Analogue cards

Depending on the type of card used and its design, either one of the following options is available or both.

◆ **Analog External** (FXO interface) is for a connection to the telephone network.

◆ **Analog Internal** (FXS Interface) is intended for connecting analogue devices such as fax machines or phones.

Please note

Each analogue line can only be assigned one connection on the analogue card.

Number range

Enter the phone number(s) of your VoIP or ISDN provider here. If the **Country Code** or the **Area Code** deviate from the general settings in the **Preferences** tab, enter these here.

The **Number Type** selection aids the input of several phone numbers or number ranges. The method of input does not affect the functionality of the line.

Examples:

◆ **Single Number**: You have individual phone numbers: 2345-11, 2345-13, 2345-15. As these are not consecutive, select **Single Number** and add each number by clicking on ⊕.

◆ **Number Block**: Your provider has issued you with the numbers 2345-1 to 2345-99. Enter **2345** as the phone number and **1** to **99** as the number range.

Advanced settings

Here you can make changes to each line that deviate from the general settings.

The options and input elements differ depending on the type of line, i.e., whether it is a provider connection, an ISDN or analogue card.

The following settings are possible for all types of lines:

Line Prefix	If several lines have been configured, a dialling code can be created using the line prefix to establish connections via a specific line. Please note that only digits, i.e., single-digit numbers, may be entered as a prefix. The displayed ** * must be input during the dialling process at a later stage.
Deposit	An internal number can be entered for each line as an alternative deposit for incoming calls that are not answered. If **Default** is retained as a setting, this is assumed as a setting in the general settings.
No Screening	The feature **CLIP – No Screening** enables an alternative number to be sent and displayed to the call recipient on outgoing calls. The availability of these features is service provider dependent.
Phone Number Prefix	If **No Screening** is activated, the Gigaset T300 PRO / Gigaset T500 PRO PBX may have to be changed to match the service provider's specification regarding the phone number format of the dialling code. Please clarify this with your provider.

Extended settings for lines to VoIP providers

Max Connection	With provider lines, the maximum number of simultaneous connection per line can be specified manually. This depends on the respective provider/contract. With the preset value 0, the number is unlimited!

Extended settings for ISDN cards

Connection	The type of connection depends on your ISDN contract and the ISDN card used.

A basic connection (also known as BRI, BA) or the ISDN card intended for this connection can be either a **Device Connection** or **Multi-device Connection**.

Primary multiplex connections (also known as PRI, PMxA, S$_2$m, E1, T1, J1) and the cards used for these require the **Device Connection** option.

Important

Setting the line type is crucial for establishing connections and for the ISDN line to function. If you select the incorrect line type, the line will not work despite the line's status display showing green! Please check the documents from your ISDN provider to verify what type of connection you have!

Echo-Cancellation (EC): This feature is only currently available for specific ISDN cards. If you wish to activate Echo-Cancellation for these cards, the setting depends on the respective card, e.g.:

◆ Sirrix **PCI2E1**, Sirrix **PCI4S0** and **PCI4S0 EC** with EC hardware require the **Hardware** option.

Extended settings for analogue cards

The **Signaling** is the method by which connected devices are alerted that the other part has hung up. **Kewlstart** is usually the correct choice for internal lines to devices. For external lines to the telephone network, you may have to choose **loopstart** in the event of your provider not supporting **kewlstart**.

Important

The type of signalling depends on the respective device and/or phone service provider. Check with the manufacturer and your provider about the correct signalling!

Emergency number

Caution

So that direct dialling to emergency numbers works, each number must be assigned at least one external line. The line (or the provider) must support the dialling of emergency numbers. This is not the case with every provider, contract or line type!

The official emergency numbers 110 and 112 are set by default. However, these must still be named and assigned to at least one line. Open the details view via ▶ and add the line(s) using ✚. Where there are several lines, the top one in the list is given priority. You can changes the sequence by using arrow symbols in the **Position** column.

Using ⊕ or **New Emergency Telephone Code**, you can define any number of additional phone or special numbers.

Caution

As soon as a number is saved as an emergency number, it is no longer available as an internal phone number. This also applies for numbers already assigned to users. If emergency numbers are deleted, they can be assigned as internal phone numbers again. This must be considered when deleting the official emergency numbers 110 and 112.

Routing

Settings: Routing priority

The **Routing Priority** is required if
◆ more than one line is configured and
◆ at least one COR rule is defined in the **Cost Optimized Routing** tab,
◆ or the PBX is part of an interconnection with location routing (see **Interconnection** ➜ **P. 82** and **Location routing** ➜ **P. 84**).

The priority setting is particularly important for user phone calls that are configured to have a specific phone number display for outgoing connections.
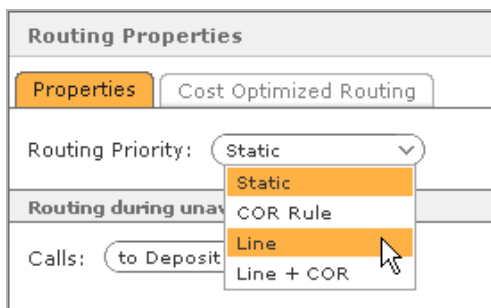
Options for routing priority

Static	A line is automatically selected. CID is withheld. Unless ◆ the routed line belongs to the phone number to be displayed, or ◆ **No Screening** is activated for the line currently being used and your provider supports this service. **Please note:** This setting is not the best option for several configured lines. Use the **COR Rule** option instead!
COR Rule	The routing rules specified in the **Cost Optimized Routing** tab are applied. CID is withheld. This is not the case if the routed line belongs to the phone number to be displayed or **No Screening** is activated for the line currently in use, the provider supports this service and the user has not suppressed CID.
Line	Select this option if the number specified in the user preferences should always be displayed for outgoing calls. This selects the line to this number. **Caution**: If this does not work, e.g., if the line is currently not available or overloaded, an alternative line will not be used. No connections will be established!
Line + COR	If the line requested for the number display is currently not available, then the routing is applied. **Please note**: If the user suppresses the number display, the COR rule is applied and the number is withheld.

Settings: Routing during unavailability

It must be defined how the PBX processes calls where the user receives a call but does not have an active phone (i.e., he is not logged in to a device) and has not set up redirection.
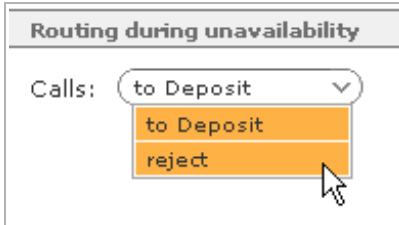
to Deposit	The caller is forwarded to the deposit, the number for which is entered during line configuration. If a deposit is not specified, the call is rejected.
reject	This is indicated to the caller by a special unavailability tone. The call is not redirected!

Cost optimized routing

> ── **Please note** ──
>
> If a call is established using a line prefix with ** *, the routing rules for the call are overridden.

▶ Click on ⊕ or **New Rule** to create a COR rule.
▶ Then enter the **Phone Number**, to which the rule should apply. This means that every routing rule created has a unique number range. For outgoing calls, the COR rule applied is the one whose number range best corresponds to the number dialled.

Example: Two COR rules have been defined - the first for the number range 0123, the second for the range 01234. The number 0123456 has just been dialled for an outgoing call. This activates the second COR rule (number range 01234) as 01234 has a longer matching sequence of digits with 0123456 than the 0123 of the first COR rule.

Each COR rule applies within a specific timeframe. You can specify the weekdays (via checkboxes) and the time for this.

In **Specify Line Sequence**, one or more lines are assigned to the timeframe using ⊹.
The sequence of lines determines their priority. This means that the top line is tried first
to establish a connection, then the next one etc. until all assigned lines have been tried. If
this fails for all specified lines, the next available line in the system is used to ensure the
connection is established.

A **Pre-Preselection** (call-by-call) can be specified for each line. These then prefix the
actual phone number when a connection is being established.

Example: The number 01234567 is dialled. Call-by-call 01019 has been entered for the
corresponding line, the Gigaset T300 PRO / Gigaset T500 PRO thus dials 0101901234567.

___
Important
Call-by-call numbers establish the connections via the respective provider by using
these prefixes. The phone tariffs for call-by-call numbers apply and not those from the
provider of the line used.
___

To use the COR rule in another timeframe, simply click on ⊕ or **New Time Frame**.

___
Important
The timeframes may not overlap. When creating a COR rule with overlapping
timeframes, an error message will appear and the row in question is highlighted.
___

Server

The server screen enables the administration of all key server features and functions of the Gigaset T300 PRO / Gigaset T500 PRO.

These include:

◆ Software updates
◆ Language settings
◆ Configuration of date and time (NTP)
◆ Network settings, DNS, proxy connection
◆ Mail server
◆ Web server
◆ Data backup and system recovery
◆ Log files for system diagnostics
◆ License administration

Status

Software updates

▶ Via **Updates**: **Search now**, you can open the list of available Gigaset T300 PRO / Gigaset T500 PRO updates.

Only versions that are more recent than the existing installation and also compatible with it will be executed. The newest available version is already selected on the right. This contains all features and properties of older versions. This allows you to update to the latest version without possibly have to install several updates one after another.

During the update process, the system's data is backed up. If an error should occur during the update, you can restore the current system status without losing any data.

Depending on the scope of the update, the process can last several minutes. On completion, your Gigaset T300 PRO / Gigaset T500 PRO PBX is restarted, and the update view contains the **To Login** button.

--- **Important** ---

During the updating process, all ongoing server connections and processes are aborted!

Update notification

If this setting is active, the system checks weekly to see if a new software version is available. If it is, the administrator automatically receives an eMail with the details of the available new Gigaset T300 PRO / Gigaset T500 PRO version.

Language

The server's language setting applies to administrative eMails, the login field and the web user interface for all users who have not specified a language in their settings. This language is also used on the phones, if no user can be identified (e.g., in the case of an unsuccessful login).

Server status

The key services (telephony, database, web server, instant messaging) or the complete PBX can be restarted, if it should be necessary.Please also see **Deactivating and restarting the PBX** (**P. 100**) in the appendix about this

After clicking on one of the buttons, you will see an overview of the current PBX usage, before the required action is carried out. If you carry out a restart or shutdown due to a malfunction or a technical problem, there is an option of sending log files to Gigaset Support.

───── **Caution** ─────
A restart disconnects all live connections.

Time and date – NTP server

───── **Important** ─────
After modifying the time settings, the web server must be restarted!

NTP (Network Time Protocol) is used for synchronising the system time of a computer with an NTP server. Depending on whether the server is inside or outside the actual network, it can set the computer time with an accuracy of between 10 ms and 20 s. The dropdown menu contains a list of NTP servers on the Internet. However, a different server address can be entered too. Alternatively, the time can be defined manually. The server's system clock imports the specified time and date information.

───── **Important** ─────
The Gigaset T300 PRO / Gigaset T500 PRO must enable Port 123 to be available for outgoing connections to external NTP servers.

Server

By being enabled for the network segment, the Gigaset T300 PRO / Gigaset T500 PRO becomes an NTP server too, from which the phones and client computers connected in this segment take their system time. This option must, however, be activated on the end devices.

> **Caution**
> After modifying the time settings, the web server must be restarted!

Network

> **Please note**
> After making changes in this tab, it is necessary to restart the PBX.

This tab provides an overview of the configurations entered during initial installation, which can be modified here.

SIP settings

SIP (Session Initiation Protocol) is an open network protocol standard for establishing connections between two or more SIP-capable VoIP end devices. A key SIP property is the usage of RTP (Realtime Transport Protocol). RTP "packets" the connection's audio and video data and sends it via UDP (User Datagram Protocol). As port assignment with UDP is dynamic, routers using NAT will not be able to assign the data packets to the corresponding ports. If the server is in a network that uses NAT, e.g., via a router, you must activate the NAT checkbox.

> **Important**
> The following ports in the firewall must be enabled for using external end devices:
> ◆ 5060 UDP and 10000-20000 UDP for SIP clients
> ◆ 4569 UDP for IAX-Clients

NAT (Network Address Translation) "masks" the individual internal IP addresses "to the outside" (to the Internet) using one or more public IP addresses. Port masquerading, as this is known, is also frequently used to replace the port numbers during data transfer. The NAT settings must be considered when the Gigaset T300 PRO / Gigaset T500 PRO server is linked via a provider connection and/or external phones are connected (see also **Advanced settings** ➜ **P. 39**).

The interaction of Gigaset T300 PRO / Gigaset T500 PRO and NAT is very dependent on the network architecture, and the settings should not be changed on a functioning system (telephony to be precise). Conversely, the cause of non-functioning connections may be found in the interaction of firewalls, routers and server.

A more in-depth explanation about NAT and its interaction with VoIP can be found at: www.voip-info.org

External address

The **External address** field is particularly important: both the server for instant messaging and the clients and connectors access this entry. With the help of the corresponding button on the right, the server's automatically detected address can be copied into this field. Nevertheless, you can also use the public domain name for your Gigaset T300 PRO / Gigaset T500 PRO server. In the event of Gigaset T300 PRO / Gigaset T500 PRO being masked by NAT, resulting in problems with the external address, the following **STUN** field can help.

STUN

STUN (**S**imple **T**raversal of **U**DP over **N**ATs) is a network protocol used to determine the external IP address of the server. You must enter the address of a freely accessible STUN server. Frequently, your VoIP provider will specify a STUN server.

A list of public servers and additional information on the topic of STUN can be found at http://www.voip-info.org/wiki-STUN.

Network settings

The server addresses determined or configured during installation are entered here. To manually change the addresses for the gateway and DNS server, you must ensure the DHCP setting is **static** for the **Network Adapter**.

```
Network Settings

Gateway IP:  192.168.178.1      DNS Server 1:  192.168.178.1
Hostname:    .                  DNS Server 2:
                                DNS Server 3:
```

The **Gateway IP** is the IP address for the interface between your network and the Internet.

The **Hostname** is the computer name of the server that should be unique within the network.

The function of **DNS servers** (**D**omain **N**ame **S**ervice) is to determine IP addresses from web addresses, e.g., www.gigaset.de is 85.214.20.166. Expressed in layman's terms, it is the same relationship as that between telephone numbers and names in the directory.

Proxy settings

If the Gigaset T300 PRO / Gigaset T500 PRO connects to the Internet via a proxy, enter the connection data for the proxy here. This is necessary so that the PBX can send queries for updates and the license management. The availability of the web user interface is ensured without the proxy settings.

Activate **Use for** option: **HTTP** to use the connection via the proxy. If the proxy for your network can manage HTTPS traffic, you can also activate the option **HTTPS** to encode and send the server queries mentioned above.

Address expects the network/IP address of the proxy.

Port: is **80** by default (if the proxy is not configured differently).

If the proxy expects an authentication, activate the corresponding option and enter the access data for the proxy. Your network administrator will supply you with this data.

Network adapter

This is an overview of the server network card(s) and their DHCP settings.

If the **Protocol** setting is set as **static**, you can enter the IP address and subnet mask manually.

Mail server

Gigaset T300 PRO / Gigaset T500 PRO sends voicemails, faxes, backup files, backup reports and other system messages (e.g., changes to user data by administrators) via eMail to users using an integrated SMTP server.

You can specify an alternative **Sender Email Address**. This is shown as sender (as "From" and "Return path" in the mail header) once the message is sent. The recipient of system eMails can thus reply to an existing address.

Configuration – external mail server

SMTP Server: The address of the SMTP server is available from your eMail provider or from your network administrator if you are using a company-owned mail server. To use a different port, rather than standard port number 25, enter a colon after the address and then the desired port number.

User: The user name is in general the eMail address or the part before the @. You can obtain the user name from the respective provider or your network provider.

Encryption: Many SMTP servers/providers provide the option of an encrypted connection. TLS (Transport Layer Security) has now become the most common form of encryption. If you use this option, a specific port must generally be used (standard for TLS is 993). Find out the correct port number from your provider or network administrator. Enter this in the SMTP server field after the server address and separated by a colon (e.g., smtp.example.com:993).

Important

The TLS encryption requires a valid server certificate. Self-signed certificates will not be accepted

---

Type of SMTP dispatch

Most SMTP servers await the sender to "log in" before sending eMails. This can occur via **SMTP with AUTH** with user name and password or with the, now seldom used **SMTP after POP3**, whereby it is checked whether there are new messages on the incoming post server (POP3) first. The log in data used here also applies for the subsequent eMail dispatch. To use this option, set **SMTP with AUTH** to **no**, then activate **SMTP after POP3** and input the address of the POP3 server.

Before saving the configuration, the correctness of the data can be checked by clicking on **Test**, where you can also make any necessary changes.

Web server

As a default, **HTTPS Service** is already activated alongside HTTP for the Gigaset T300 PRO / Gigaset T500 PRO web server. Both services are available on the standard port numbers, which you can freely change.

The **Force redirect to HTTPS** option enables access to the Gigaset T300 PRO / Gigaset T500 PRO web user interface via HTTPS only.

Please note

If HTTP is deactivated or the port number is not **80**, problems with several connections may arise, e.g., the addressbook for Gigaset SIP phones.

HTTPS and server certificate

HTTPS (Hypertext Transfer Protocol Secure) is a network protocol for encoding data being transferred using SSL/TLS and provides:

◆ Data confidentiality, i.e., the data can not be viewed by third parties.

◆ Data integrity, as the data can not be manipulated.

◆ Authenticity through the certainty of being connected only to the requested web server.

A certificate for the web server is required to use HTTPS. In the Gigaset T300 PRO / Gigaset T500 PRO, there is only a provisional certificate available.

Click on **New Certificate** to open an entry screen. Two entries are absolutely necessary in this screen:

◆ The server name indicates the domain for which the certificate should apply.

◆ The number of days for which the certificate should be valid.

The domain name must be complete and correct, e.g., **yourcompany.net** (without **https://**). A certificate usually is not valid for any possible sub-domains - however, exceptions are found in the form of the wildcard certificates.

The certificate should be signed by a certificate authority to satisfy the server certificate requirements. A selection of certificate authorities can be found in the settings of your browser (for Internet Explorer: **Internet options** ➔ **Content**; in Firefox: **Options** ➔ **Advanced** ➔ **Encryption**). Obtain the information for the certificate authority as to what details your certificate should contain and the requirements to be fulfilled by the applicant.

The **Certificate Request** button creates an encoded file from the certificate. You can copy the content of the window and send it via eMail to a certificate authority. The authority checks the request and returns the signed certificate via eMail.

Importing a certificate

Import Certificate Response opens a new window with two text fields. Copy and paste the signed CA certificate into the upper field and copy and paste the root CA certificate into the lower text field.

Backup

Standard data backup

Gigaset T300 PRO / Gigaset T500 PRO automatically creates a data backup of user, group and system configurations and the call lists, voicemails and voicemail announcements every 24 hours. The backup is stored on the server itself and USB storage media connected to the server. These must be formatted with the file systems FAT32, VFAT or ext2. The file will have the extension **.sar** and be saved on the server at **/root/starface/backup/Default/**.

The last seven backup files are stored, i.e., the data from seven days will be kept available. If the data volume exceeds the memory available, this is noted in the **Protocol** tab.

▶ In **List of backup schedules**, you can modify the standard backup settings.

▶ To create your own backup routines in addition to this, click on **Create** or **New Schedule** in backup options.

Creating a new backup

Step 1: Set name and schedule

The **Name** allows you to identify the backup file at a later stage. In the backup process summary, the protocol will also use this name. In addition, the subdirectory will be created on the server, in the folder **/root/starface/backup/**, where the file will be saved.

 In the **Report to** field, you can specify an eMail address, e.g., of a Gigaset T300 PRO / Gigaset T500 PRO administrator as recipient. The error report is also saved in the **Protocol** tab, if the back up routine is saved as a new configuration (see **Step 4: Finish backup**).

With **Start**, you must specify the time for the first execution. The time specified will be used for all subsequent backups.

```
Create Backup 1/4

Set name and schedule

Name:   OneClick              Report to:   admin@example.net

Define execution time:

Backup schedule:  ( Manual      v )

Start:            ( 10 v )  ( Septembe v )  ( 2010 v )    Time (hh:mm): ( 15 v )  ( 0   v )
```

Step 2: Choose backup details

A basic data backup comprises core data such as users, groups and configuration settings. In addition, voicemails, personally-created announcements and the so-called Call Detail Record (CDR) can be saved. The CDR is a connection data record that can be used for invoicing purposes. It contains information about the calls made, such as participants, time, duration etc.

Please note

Both the CDR and voicemails can contain considerable data volumes thus making the backup file correspondingly large. You should consider this when selecting the storage location for the backup.
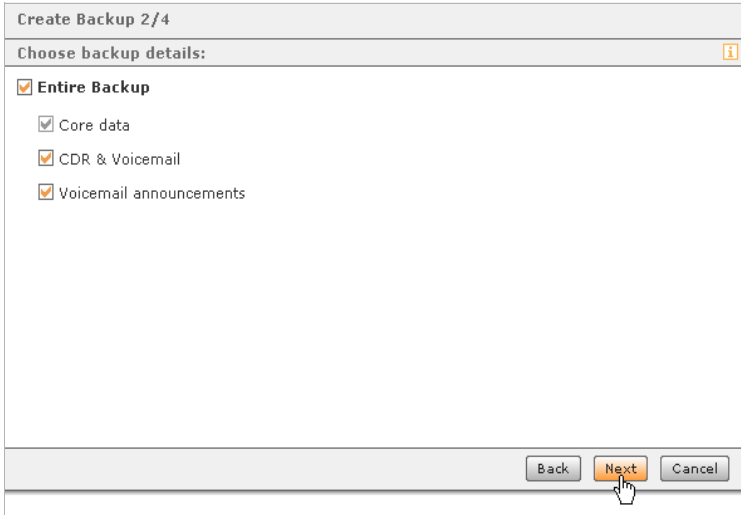
Step 3: Define location and data

When creating a new backup routine, you can only select one storage location. In Step 4, the new backup configuration can be copied for saving, whereupon you can add additional medium types.

The options **USB** and **SD-Card** relate to storage locations connected to the server!
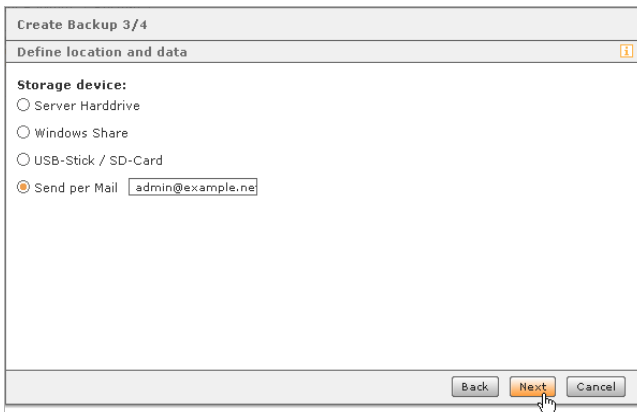
The **Send via E-Mail** option has the backup file sent as an eMail attachment to the address specified. After saving the backup configuration (in Step 4), the maximum file size of the attachment can be specified. If the specified size is exceeded, an eMail will not be sent. If you select **Windows Share**:

▶ Click on ✐ to enter the access data.

Depending on the configuration of the file server, it may be necessary to enter the domain together with the user name.

▶ For **Server**, enter the IP address of the file server without specifying the protocol.

▶ Enter the complete directory path in **Share** without the server address!

Step 4: Finish backup

───── **Please note** ─────

If the preferences have been adopted, it does not mean they have been saved permanently. To do so, you must click on **Apply** or **Save** in the **List of backup schedules**.

This starts the data backup and a progress bar for the process is opened. If the process reaches 100%, then the data backup has been completed successfully.
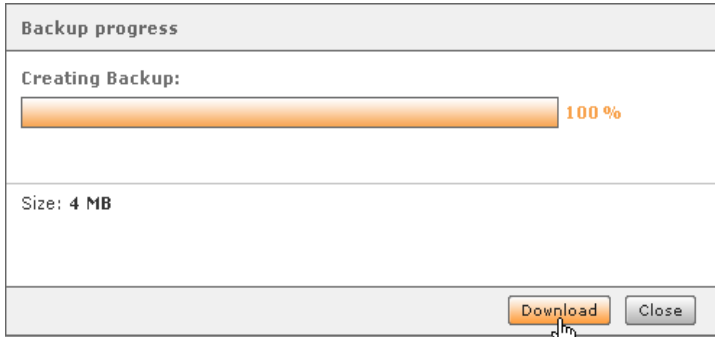
In addition to the storage location specified in Step 3, the backup file can be downloaded to be saved on the local computer.

Importing a backup

---- **Important** ----

When importing the data records, there is no comparison between existing and more recent data. This means that, for example, voicemail announcements rerecorded after the data backup will not be available alongside old announcements. The new ones will be deleted.
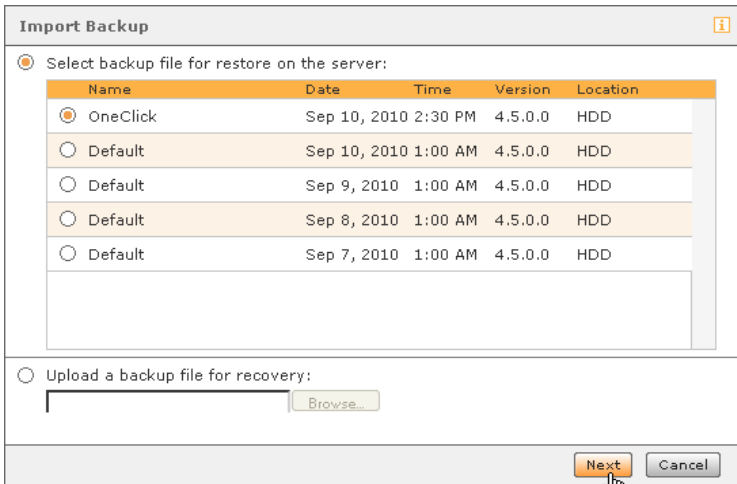
The list shows all of the backup files available on the server in descending chronological order. The most recent file is already highlighted. The name indicates whether the backup has been created as part of the daily routine ("Default") or a self-created backup.

To use a backup on the local computer, select **Upload a backup file for recovery**.

After selecting the backup file, all important related details are listed in the next step.

Backup content

If the backup file contains voicemail announcements, voicemails and the CRD, as well as core data, you can activate the adjacent checkbox to specify whether these data records should also be restored. The CDR (call detail record) is a communication data record that can be used for invoicing purposes. It contains the call records.

The **Ignore IP address** option is important if a backup is being imported from a different Gigaset T300 PRO / Gigaset T500 PRO server. In this case, it is imperative that this function is activated, or left activated.

After confirming with **Next**, you will receive a list of all logged in users and active calls. As the restoring process would end all these processes, you now have the final opportunity to decide whether this process should actually be executed.

List of backup schedules

The daily backup routine and all the saved self-created backup configurations can be edited retrospectively here. In addition, each routine can be started via **Execute**.

The setting options for the individual backups can be found in the detailed view by clicking on ▶. The options in the first three tabs correspond to the steps for creating backups (see **Creating a new backup** ➜ **P. 73**).

You can make extended settings in the **Location** tab:

In the **Limited to** column, you can specify the maximum number of backup files to be saved on data carriers. If the maximum number is exceeded, the oldest backup file is overwritten. The number is preset to seven files. The daily back-up can therefore save one week's worth of files before overwriting the first file.

For the eMail saving option, it is possible to restrict the files size of a backup. This enables you to prevent the sending of eMail attachments that are too large.

If problems arise due to the memory, error messages can be viewed in the **Protocol** tab.

The meaning of the error messages

◆ **No space left on this device** - This error message is displayed if there is only 512 MB memory available. This minimum capacity is required by the Gigaset T300 PRO / Gigaset T500 PRO during the update process!

◆ **Warning: No space for another backup on device** - The data backup was saved but the next backup will fail if no additional memory capacity is made available or if the storage medium is not changed.

Log files

With the **Send error report** option, the pop-ups that appear in the event of error messages have an additional button, with which the relevant error report can be sent directly to Gigaset Support. If you do not wish users (i.e., "non-administrators") to have this option, deactivate the function!

As administrator, you can use the **Send log files to Gigaset support** function at any time.

▸ Click on **Send**, to send the error reports via eMail: mailto:support.pro@gigaset.com

Selecting the log file

Here, you can view various log files and configure the scope of storage. By selecting **Level**, you can specify the level of errors/messages that should be stored in each respective file.

The log levels in the selection menu are sorted in descending hierarchical order. This means that each higher level also contains the information from the lower levels. For example: In the **WARN** level, all entries from the **ERROR** and **FATAL** categories are also saved and displayed. Any change to the log level must be saved or copied, before the view will update itself.

───── **Please note** ─────

Saving will not affect the existing entries, i.e., these remain in the file and view.

Licenses

Licence information

Licensed Users   shows the maximum number of user accounts available for your license.

Still available   shows the number of user accounts not yet used.

Please note

The number of licensed users always relates to user accounts and not to phones or phone numbers/connections. Each licensed user can be assigned any number of phones and phone numbers.

Update option

If you have an update agreement, you will see the corresponding option model and the end date of the agreement.

Licenses

To start the registration process for your server, click on **Add License** or ⊕. Now enter the licence key for the server licence in the **License Data** form, fill in the (mandatory) fields and click on **Register**.

If you have a additional user licences, repeat the above process to register the license key for the user license.

Important

Registering the service licence must occur before registering a user licence.

Statistical evaluation

Exporting call records

To aid statistical evaluation, you have the option to save the call detail records of individual users and groups as a CSV file locally. Select the corresponding person or group, the range for the calls and the timeframe and then click on **Export**. These can then be processed using an external application such as MS Office Excel and used for billing purposes.

Statistics

The visual display of the call detail record can be influenced by various parameters. This enables you to create views for each user and every group during timeframes of your choice.

Apart from the number and duration of calls, the type selection can provide a visual display of the capacity utilisation of the ISDN lines for the specified timeframes.
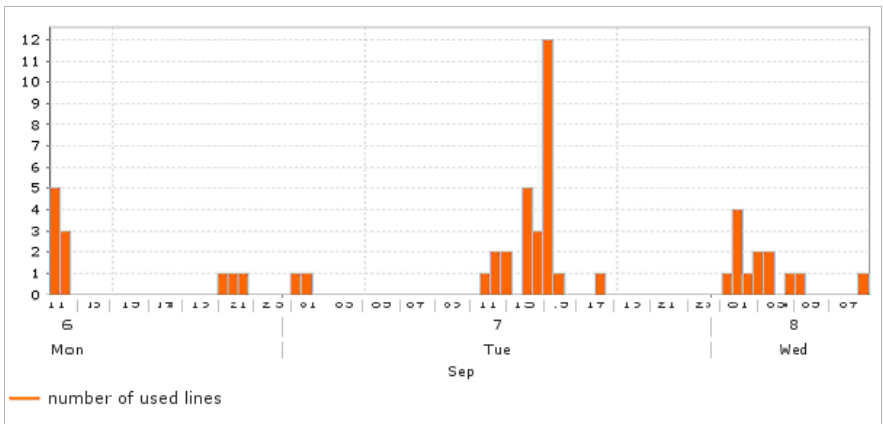
▶ Click on **Update** to generate a graphic table containing the data selected above.

Fax journal

To export the fax journal, the send information of all fax messages sent via the system is gathered. This also applies for faxes that have already been deleted from the fax list in the user interface.

The following information is exported for each fax:

▸ Date
▸ Time
▸ Length of transfer
▸ Users
▸ Sender name (if available)
▸ Sender number
▸ Recipient's number
▸ Number of pages (sent/total)
▸ Send result

Interconnection

A Gigaset T300 PRO / Gigaset T500 PRO interconnection is the linking up of several Gigaset T300 PRO / Gigaset T500 PRO PBXs at various locations. A prerequisite for the interconnection is that the locations are connected via virtual private networks (Site-to-Site VPN recommended) or static IP addresses with the appropriate firewall configurations. This is necessary as the interconnection depends on unfiltered IP communication between the various locations.

Important

Port 3090 must be enabled for TCP via the integrated firewalls for the interconnection.

Location details

Give the location an appropriate and unique name within the group. The name can contain letters, numbers and underscores (umlauts and ß are excluded).

The **Prefix** field requires a number that prefixes the internal phone numbers of the PBX within the group. The purpose of this is to avoid overlaps in internal phone number ranges.

Important

Only leave this field blank, when it is assured that all PBXs in the group have separate phone number ranges. In the case of overlaps or conflicts in number ranges, each PBX in the group gives priority to its own internal phone numbers.

Example: Two PBXs (A and B) both have internal numbers from 10 to 99. PBX A is given the prefix 3 and PBX B 4. If a user from PBX A calls the user with the phone number 10 on PBX B using a function key, the system automatically predials the prefix 4, meaning that 410 is dialled.

Caution

If a PBX has 1 as its prefix, this will overlap with the internal numbers 10 and 11 and with the emergency numbers 110 and 112! Emergency numbers are always given priority. This means: If you dial 110 or 112, you will always be connected to the emergency services.

Creating an interconnection

> **Important**
>
> The PBXs in an interconnection are equal. It doesn't matter at which location (on which PBX) the interconnection is created. The PBX on which the interconnection is set up does not act in the sense of a host, server or network node.

Once the **Location details** have been specified, click on **Create group**. In the dialogue window that opens, enter the collective name of the interconnection. The same restrictions apply to this name as stated for the location names. In the next step, you will create the group certificate and save it locally on your computer. Other PBXs will require this certificate to join the group. Clicking on **Save** creates the group and the PBX is online within the group.

Now otherGigaset T300 PRO / Gigaset T500 PRO PBXs can join the group.

Adding other Gigaset T300 PRO / Gigaset T500 PRO PBXs

Once the interconnection has been created (see section **Creating an interconnection**), other PBXs can be added to the group. Here, it is necessary to login to each respective PBX.

After logging in to the web user interface of the other Gigaset T300 PRO / Gigaset T500 PRO PBX, open the administration pane and select **Interconnection** from the menu. Enter the **Name** and **Prefix** of the location. Then click on the **Connect now** button in the **Group details** pane and upload the group certificate from the hard drive to the server. Save it to connect the PBX to the group.

The PBX is immediately shown as being online in the group. The **Number of connected locations** will not yet include the other PBX(s) in the group at this point. Just wait a few seconds and then click on the current tab **Settings** to update the status or change to the **Connected locations** tab.

If a location name or prefix should be changed retrospectively, a PBX can be disconnected from the group at any time via the corresponding button. To reconnect the PBX, you must upload the certificate once more by simply clicking on **Connect device**.

Connected locations

This overview shows the status and details of the other PBXs in the group. Each location is displayed with the following properties:

◆ Status of the location within the group (online/offline)

◆ Name

◆ Phone number prefix

◆ External and internal phone numbers

Unconnected locations can be removed from the list by clicking on the corresponding ✕.

> **Important**
>
> If a location is deleted from the list, the routing and assignment of rights (i.e., user, group and status information) for the location concerned are deleted from the PBX's configuration. If the location should rejoin the group, these settings must be edited in the corresponding tabs once more.

Location routing

Location routing controls which location(s) is/are used to establish outgoing connections on the telephone network. The routing is automatically assumed from all locations with the preset routing priority **COR Rule**. It is possible as a "minimum scenario" that all PBXs make phone calls in the network using only one phone line.

Multiple routing rules can be set for various timeframes and differing number ranges. For outgoing calls, it will then be checked, which number range (which rule) corresponds best to the phone number dialled.

Example: Routing rules have been defined for the number ranges 01 and 012 respectively. An outgoing call is instigated for the number 012 5656. The call will be set up via the routing for the number range 012, as this has a longer matching digit sequence than the rule for the 01 number range.

It is important to remember that routing rules on the individual PBXs (see **Cost optimized routing** ➜ **P. 64**) will be included too. This means that if a local COR is a better match for the phone number dialled, then this is given precedence over the location routing.

If a routing rule can not be executed (e.g., due to maximum capacity or over-capacity on a line), the closest corresponding rule is used.

> **Important**
>
> Routing only applies to locations with preset routing priority **COR Rule**.

Rights

The settings in the **Rights** tab are for releasing user and group information from the current location. Released information is available to other locations in the group in the addressbook, as a presence display for function keys and the call manager. Local users can also be members of remote groups, just as remote users can be assigned to local groups.

It is necessary to differentiate between user data, group data, user state and group state (the state is required for presence displays). The information can be released individually for each user and group account.

▷ To change the standard release settings for all locations, click on ✐ .

Using the **Default setting for new users** (**Groups**), you can specify whether future information from users and groups newly created at this location is automatically accessible. After the standard settings have been saved, all settings for each individual location in the interconnection can be modified separately.

Interconnection

| Settings | Connected locations | Location routing | **Rights** |

Location: For all (default)

Released informations from: Sales -> default

▼ Users ☑

Default setting for new users
Transmit user information: ◉ yes   ○ no

Rights for transmitted user information

Name	
Black, Susan	☑
Brown, Ben	☑
Water, Jane	☑
White, William	☑

▼ User state ☑

Default setting for new users
Transmit user status information: ◉ yes   ○ no

Rights for transmitted user status information

Name	
Black, Susan	☑
Brown, Ben	☑
Water, Jane	☑
White, William	☑

The West branch location receives neither information nor status from the local administrator.

▷ To edit the information release for a specific location, click on ⊕ and select the location you wish to edit from the list above.

A view containing the individual information groups for the selected location appears. The standard settings have been automatically copied and can now be changed.

Security

In the security area there are setting options to protect the PBX against hacking attempts by accessing the phone accounts (SIP accounts). These include guidelines for the complexity of access passwords, automatic checking and changing of passwords and a filter system for IP addresses, from which registration requests are sent to the telephone system. Using the filtering, the behaviour in the case of requests is analysed, so that a classification is possible into unsuspicious and attacking clients. Resulting from this, the system can automatically place the affected IP addresses in a whitelist or block them in a blacklist (→ **P. 87**).

Preferences

Guidelines for SIP passwords

To prevent unauthorised access via phone accounts (SIP accounts), there are two complexity guidelines for their passwords. The selected guideline is used in the autoprovisioning of phones and when generating random passwords in the manual configuration of phone access.

The requirements of both guidelines for minimum password strength are (in each case as a minimum):

Minimum number of specific characters for passwords

Guideline	Length	a-z	A-Z	0-9
Secure	16	3	2	2
Paranoid	30	5	5	5

Permit manual assignment of weak passwords: This option allows the configuration of SIP accounts with insecure passwords, whereby no warning is given before saving.

Password checking

Regularly check passwords: If active, all SIP passwords are checked immediately after saving the setting, and then at the interval set below. If the check results in one or more passwords not corresponding to the security guidelines, the first Administrator20 receives an eMail with a list of the affected phone accounts.

Automatic password update

Change insecure passwords automatically: This affects phones with existing access data, which contact the PBX with an autoprovisioning request. If this option is activated and the phone or SIP account password does not correspond to the security guideline, the PBX automatically assigns a new and secure password when the phone makes the next autoprovisioning request.

Please note
This setting works independently from the manual assignment of weaker passwords (if permitted) and regular password checking
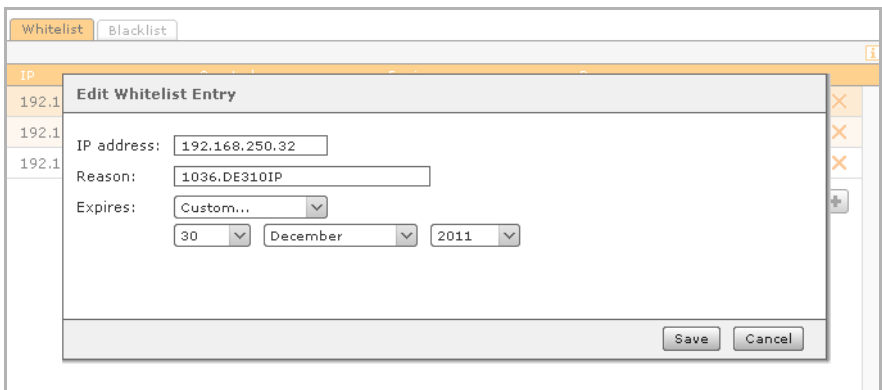---

Call screening

The PBX operates an automatic background service to detect network attacks using SIP requests. Attackers may try to gain access to a PBX phone account using a large number of requests (brute force attacks). The filter service detects these attack attempts and prevents them.

Automatic addition to blacklist and whitelist

With this, requests from attacking IP addresses are blocked and ignored for 24 hours. SIP registrations via these IPs are no longer possible in this case. At the same time, the IP addresses of the registered phones are included in the whitelist, whereby they are excluded from the checks for 24 hours. The validity period for list entries of 24 hours is renewed each time there is a registration request. However, it can also be amended for every IP address.

▶ To do this, click on the editing symbol ✏ for the required entry.

The optional eMail with the notification of automatically created blacklist entries is received by the first Administrator20.

--- **Please note** ---

The security of the system is greatly increased by using secure SIP passwords with at least 16 characters, consisting of numbers, upper and lower case letters.

Advanced settings

Music on hold

In this view, you can edit the existing music on hold and create additional music on hold tracks.

The "default" on-hold loop supplied with the Gigaset T300 PRO / Gigaset T500 PRO can be extended by additional sound files or the existing music file can be replaced. To listen to the music on hold, select the phone with which you would like to listen to the file.

▶ Now click on **Listen**. While the music on hold is being played back, you can adjust the volume of the sound files: click on 🔊 to reduce the volume and on 🔊 to increase it.

--- **Caution** ---

"Excessive" use of this function can damage the sound file! Every mouse-click edits and saves the file. This function does not correspond to simply changing the output volume on the computer or phone.

▶ To create an additional music on hold track, click on ⊕ or on **Add Music On Hold**.

▶ In **Settings**, specify the name of the music on hold and click on **Apply**.

▶ Go to the **Music** tab to upload the sound file(s) of your choice for music on hold on to the server.

The system regards music on hold with several music files as a single entity. Thus, when you click **Listen** to listen to one of the files, all files in the loop are played one after the other, just as the caller would hear them.

An on-hold loop is a "group", to which any phone numbers, users and/or user groups can be assigned via the corresponding tabs. However, this does not apply to the "default" on-hold loop. This is used across the system for all phone numbers not assigned to any newly created on-hold loops.

Macros

> **Caution**
>
> To extend the functionality scope of the Gigaset T300 PRO / Gigaset T500 PRO PBX, we recommend the use of Gigaset T300 PRO / Gigaset T500 PRO modules. Any intervention to the phone system using macros should always be a last resort and executed by experienced administrators!

This editor is used for creating your own extensions or macros for the dial plan. The dial plan essentially consists of all rules and routines for processing all VoIP connections.

In the **Global Includes** text field, global variables are defined, which the **Macros Definition** can use in the lower text field. The syntax has deliberately been kept simple: For every row, enter a variable in the form of **variablename=value**. A macro definition does not necessarily require pre-defined variables: the upper field can also remain blank.

Macros written here can be found in user administration in the editing view of a using account, 🖉 in the **Phone Numbers** tab or as an additional option under **Default Rule**.

The prerequisite for this is that the name of the macro (deviating from the official writing convention) is in the following format:

[[macro-...]]; ${...}

XMPP

XMPP (Extensible Messaging and Presence Protocol) is an XML-based standard protocol for instant messaging, voice services and intra-platform exchange of data. It stems from XMPP from the messaging protocol Jabber, whose core it represents. Both terms are used frequently synonymously.

Every Gigaset T300 PRO / Gigaset T500 PRO installation also contains an independent XMPP server. This establishes the connections for the following applications:

◆ Gigaset T300 PRO / Gigaset T500 PRO Client with
  – Gigaset T300 PRO / Gigaset T500 PRO Software Fax
  – Gigaset T300 PRO / Gigaset T500 PRO TAPI
◆ Different Gigaset T300 PRO / Gigaset T500 PRO integrations (CTI)
◆ Instant messaging via Jabber/XMPP chat applications, e.g., Psi, Miranda, Gajim, etc.

Status

The upper **Connected to XMPP server** display relates to the connection of Gigaset T300 PRO / Gigaset T500 PRO to the XMPP server. It is not an indicator of the state of the XMPP server!

The second **Connected WinClients** status display shows the number of currently connected Gigaset T300 PRO / Gigaset T500 PRO clients for Windows and their users. Moreover, clients connected for instant messaging are not listed here.

***

Important

All connections are interrupted when the XMPP server is restarted. This also applies to instant messaging as its connection status is not shown here!

***

Preferences

The **Domain** is the server address via which XMPP clients (instant messaging programmes, the Gigaset T300 PRO / Gigaset T500 PRO clients and several Gigaset T300 PRO / Gigaset T500 PRO integrations) are connected. The field is automatically filled in by the system:

◆ Either with the external IP address, if an external IP address has been identified

◆ Or with the internal IP address

However, the **Domain** can be entered manually:

◆ If, for example, only clients in the local network should establish connections, insert the internal IP address.

◆ For external clients, you can also specify the DNS name instead of the external IP address.

***

Important

When the domain is changed, the XMPP server is restarted! All existing connections are interrupted.

***

Resetting the system

Your Gigaset T300 PRO / Gigaset T500 PRO PBX comes supplied with a fully installed, functioning system. Should you experience serious problems during operation that make the system unusable, you can restore functionality using a recovery version. You can obtain a recovery version ready for installation on a USB stick from Gigaset PRO support.

Prior to installation

◆ Ensure data is available on the computer where necessary. A reset of the Gigaset T300 PRO / Gigaset T500 PRO is generally performed on a "non-customized" system, i.e., all partitions to be used for Gigaset T300 PRO / Gigaset T500 PRO are automatically deleted in full during the reset. It is not possible to install to available systems at the same time.

◆ The computer should already be connected with the local network and/or Internet via a network card.

◆ If you would like to use ISDN, the computer must be connected with the ISDN network terminator (NTBA/NTPM) via an ISDN adapter and ISDN cable.

◆ To ensure installation starts from the USB stick, USB must be entered as the primary boot medium in BIOS. Following successful installation, the setting can be changed specifying the hard disk as the primary boot medium. For security reasons, access to BIOS should be protected by a password.

Installation steps

▶ Insert the USB stick into a USB slot and restart the system.
The start screen appears.

▶ Press the enter or return key to start the installation process.

First, the process for detecting essential hardware components is performed.

After successfully detecting the graphic input and output components, the graphic installation wizard is launched.

Selecting the language

▶ Select the language setting for the operating system at this point.

This language is then used as you progress through the installation process and in future system messages and server console outputs. The language setting for the Gigaset T300 PRO / Gigaset T500 PRO is made at a later stage and is not affected by this setting.

Selecting the keyboard layout
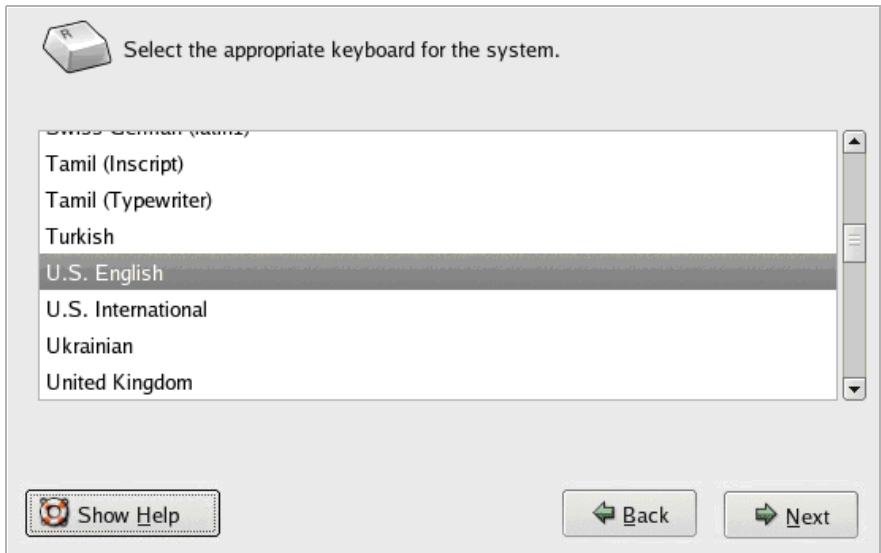
Selecting the keyboard layout is particularly important for defining the root password. Keys can be located in different positions on different keyboards. You must therefore select your country, and, if necessary, the keyboard layout for your computer.

Partitioning the hard disk

The next stage involves partitioning the hard disk. You can choose to manually or automatically partition the hard disk.

Automatic Partitioning sets partitions based on the selected
installation type. You also can customize the partitions once
they have been created.

The manual disk partitioning tool, Disk Druid, allows you to
create partitions in an interactive environment. You can set the
file system types, mount points, partition sizes, and more.

- ◉ Automatically partition
- ○ Manually partition with Disk Druid

Show Help   ⬅ Back   ➡ Next

Settings for automatic partitioning:

You have three options for automatic partitioning:
- ◆ **Remove all Linux partitions on this system**
- ◆ **Remove all partitions on this system**
- ◆ **Keep all partitions and use existing free space**

The hard disk to be used for automatic partitioning is also selected at this point.

Before automatic partitioning can be set up by the installation
program, you must choose how to use the space on your hard
drives.

I want to have automatic partitioning:
- ○ Remove all Linux partitions on this system
- ◉ Remove all partitions on this system
- ○ Keep all partitions and use existing free space

Select the drive(s) to use for this installation:

☑ sda   4095 MB VMware, VMware Virtual S

☑ Review (and modify if needed) the partitions created

Show Help   ⬅ Back   ➡ Next

The **Review (and modify if needed) the partitions created** option is already activated. The next step opens the overview of the partitions. You are still able to make manual changes to the partitioning at this stage. If you deactivate this option, the assistant will switch to **Network settings** (→ **P. 96**).

Caution

During the partitioning process, all data found in each partition is permanently deleted! If a pre-used hard disk is selected, any data on the hard disk must be saved onto a separate storage medium prior to partitioning! There is not a warranty covering any loss of data.

Manual partitioning

Here you can manually create logical volumes or software RAIDs for example, or enlarge or reduce partitions.

Caution

During the partitioning process, all data found in each partition is permanently deleted! If a pre-used hard disk is selected, any data on the hard disk must be saved onto a separate storage medium prior to partitioning! There is not a warranty covering any loss of data.

Deviations from the suggested partitioning process should only occur where specifically specified in your configuration. For all 'normal' Gigaset T300 PRO / Gigaset T500 PRO installations, we recommend following the recommended partitioning process.

Selecting the boot loader

The boot loader is responsible for selecting and starting the specified operating system. When installing Gigaset T300 PRO / Gigaset T500 PRO, GRUB is already selected as the boot loader. GRUB is able to boot various operating systems, e.g., Linux, Windows XP, Windows 7 etc. If Gigaset T300 PRO / Gigaset T500 PRO is the only system operated on the computer, or if Gigaset T300 PRO / Gigaset T500 PRO is booted as the standard operating system, no modifications need to be made at this stage. In this case, continue to **Network settings** (➔ **P. 96**).

Important

We recommend using Gigaset T300 PRO / Gigaset T500 PRO as the sole operating system on a computer by selecting the default settings during the installation process. If you make any changes to the boot loader settings, there should be a specific reasons for making this change with regard to the hardware or similar and you should have the relevant knowledge for this particular step!

Select **Change boot loader** and the option **Do not install a boot loader** if the machine you wish to use already has a boot loader.

If there is another partition present in addition to the partition suggested for Gigaset T300 PRO / Gigaset T500 PRO, and you would like to start an operating system using this partition, select the option **Standard** from the list for this partition.

If the operating system is not listed, select **Add** and specify the location of the system.

Extended boot loader options

The boot loader is installed in the master boot record by default, i.e., in the first block on the hard disk. If you are configuring multiple parallel operating systems, this setting must be modified where necessary, e.g., for operating Gigaset T300 PRO / Gigaset T500 PRO and an NTFS-based operating system.

Network settings

Instructions for configuring the network are as follows: Here, you can assign an IP address and subnet mask to the individual network cards if the computer is not connected to a DHCP server or if automatic assignment of a network address is not required. When manually entering the computer name, the gateway and various DNS server settings must also be configured. The gateway specifies the IP address of the computer or router, which in principle acts as an interface between the network and the Internet.

Selecting the time zone

The time zone of the computer is entered on the following screen. One of the yellow points on the world map can be selected using the mouse. Alternatively, you can select the time zone from a list. By activating the UTC option, the coordinated world time is used to calculate time shifts in your specified time zone.

Entering the root password

The administrator of a Linux system is always automatically given the user name "root". The password must contain at least six characters. As you enter the password, it will not appear on the screen. You must enter the password twice. If the two entries do not correspond, the installation program will request that you re-enter the password.

You should always choose a secure password. A secure password is made up of numbers and letters in both upper and lower case, and does not contain meaningful words (an example of a secure password is **Atz38pPj**). Please ensure that you check each individual character when entering your password, i.e., the password is case-sensitive.

The general configuration for the installation is completed on entering the root password.

Starting the installation process

Click next to begin installation of Starface.

A complete log of the installation can be found in the file '/root/install.log' after rebooting your system.

A kickstart file containing the installation options selected can be found in the file '/root/anaconda-ks.cfg' after rebooting the system.

Show Help   Back   Next

▸ Click on **Next** to confirm the start process and install the system on the hard disk.

After restarting the system, a full installation protocol can be viewed in the file: **./root/install.log**.

───── **Please note** ─────

The console command for opening the installation protocol and/or the "kickstart" file is: **less /root/install.log** or **less /root/anaconda-ks.cfg**

Completing the installation

Congratulations, the installation is complete.

Remove any installation media used during the installation process and press the "Reboot" button to reboot your system.

Show Help   ⇐ Back   Reboot

▸ Remove the USB stick from the drive and restart the computer.

Gigaset T300 PRO / Gigaset T500 PRO can now be configured and operated in the Internet browser from any computer within the local network. For this, enter **http://** and the IP address of the Gigaset T300 PRO / Gigaset T500 PRO server into the web browser's address bar. The IP address is shown on the start display.

The start display

After restarting the server, the start display appears showing the IP address of your Gigaset T300 PRO / Gigaset T500 PRO device.

▸ To log into the system, press Alt+F2.

▸ Click on **OK** to open the diagnostic and admin menus.

In the diagnostic menu, you are supplied with general information about the system, e.g., available memory, operating time, version of operating system etc.

In the admin menu, you can restart or switch off the system, for example, or amend the IP address if no DHCP server is available.

Appendix

Deactivating and restarting the PBX

The Gigaset T300 PRO / Gigaset T500 PRO PBX is designed for permanent operation and must not in general be restarted or deactivated. However, if this should be necessary or desired, use the appropriate buttons in the administrator interface (➜ **P. 67**, **Server status**) or - if a monitor is connected to the device - the admin menu.

If access to the interface is not possible, deactivate the PBX as follows:

◆ Press the start button on the front side of the device three times within 30 seconds. This method prevents an unintentional deactivation of the PBX.

───── **Caution** ─────
Restarting the PBX disconnects all live connections.

HD monitoring

HD monitoring is an independent application that runs in the background to check the space available on the hard disk. If the space available should fall below the minimum of 512 MB, the Administrator20 will automatically receive an eMail with an appropriate warning.

Sound files for the Gigaset T300 PRO / Gigaset T500 PRO PBX

All audio files uploaded onto the PBX for use as announcements, music on hold, etc., must already be available in the suitable WAV format. Use a suitable multimedia programme, such as VLC, Windows Mediaplayer or WinAmp to convert from other file formats.

Key combinations on the phone

Keys	+	Description
`* 2`	+ Phone number	Highlights the call as private. It will be identified accordingly in the CDR.
`* 3 2`	+ Group ID	Logging the user in to the group
`* 3 3`	+ Group ID	Logging the user out of the group
`* 6`	+ Speed dial	Calling a phone number using speed dial
`* 7 7`	+ Login ID	Logging the user on to the phone
`* 7 8`	+ Login ID	Logging the user out of the phone
`* 7 9`		Logging all users out of the phone
`* 8`	+ Internal phone number	Picking up a call for the user with this phone number (call grabbing)
`* 8`		Randomly picking up a call (call grabbing)
`* 9`	+ ID for a voicemail box	Checking a voicemail box
`* * *`	+ digit +	Establishing a call via a line with corresponding line prefix

During the call

Keys	Description
`* *`	Call2Go: Placing the call on the user's other phones
`* 1`	Recording the call and sending as a voicemail
`* 2`	Transfer with consultation: After entering the combination, a voice menu is heard to specify the required target call number. The current call is put on hold during this. After the consultation with the participant at the target call number, the caller on hold is transferred by hanging up.

Additional service features

`*` `0` `1` `1` + target call number	Activate general redirection for all calls to the target call number (always redirection)
`*` `0` `1` `0`	Deactivating redirect
`*` `0` `2` `1` + target call number	Activating redirection of all calls on busy to the target call number
`*` `0` `2` `0`	Deactivating redirection of all calls on busy
`*` `0` `3` `1` + target call number	Activating redirection of all calls when time limit exceeded (no reply) to the target call number
`*` `0` `3` `0`	Deactivating redirection of all calls when time limit exceeded (no reply)
`*` `0` `7` `1`	Activating callback on busy
`*` `0` `7` `0`	Deactivating callback on busy
`*` `0` `8` +00 to 99 (Holding space ID)	Parking a call on hold in a holding space or collecting it from the holding space
`*` `0` `9` `1`	Activating DND for all phones
`*` `0` `9` `0`	Deactivating DND for all phones

Moderating a conference

`*`	Calling up voice menu for control options
`*` `1`	Activating and deactivating mute (microphone)
`*` `2`	Asking to speak, if muted by the moderator
`*` `3`	Moderator: Blocking and unblocking conference
`*` `4` … `4` `8`	Reducing earpiece volume; pressing 4 several times reduces the volume. 8 must be pressed to confirm the command.
`*` `6` … `6` `8`	Increasing earpiece volume; pressing 6 several times increases the volume. 8 must be pressed to confirm the command.
`*` `7` … `7` `8`	Reducing microphone volume; pressing 7 several times reduces the volume. 8 must be pressed to confirm the command.
`*` `9` … `9` `8`	Increasing microphone volume; pressing 9 several times increases the volume. 8 must be pressed to confirm the command.

Port sharing in network and firewall configurations

Port number	For protocol	Is used for
80	TCP	HTTP
443	TCP	HTTPS
5060	UDP	SIP
10000–20000	UDP	RTP
123	UDP or if necessary TCP	NTP, if this is to be used to control the system time
5222	TCP	XMPP with TLS
5223	TCP	XMPP with SSL
3090	TCP und UDP	JMS, for setting up and using an interconnection

Index