Gigaset

T640 PRO - T440 PRO

Administration

Gigaset pro

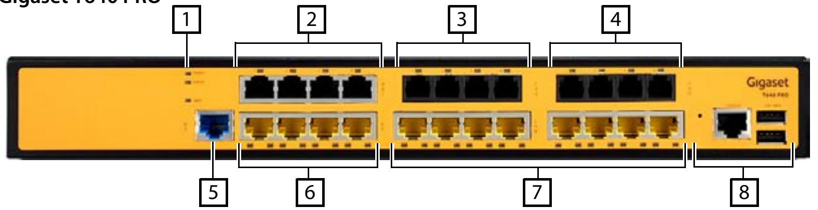
INSPIRING CONVERSATION.

Contents

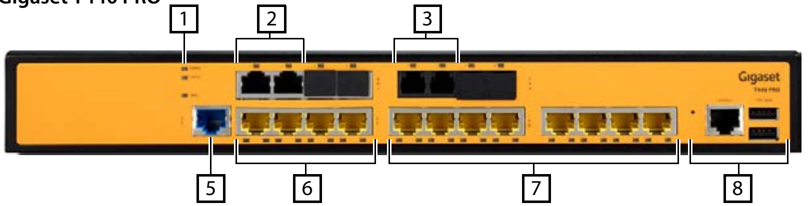
Overview

Connections

Gigaset T640 PRO



Gigaset T440 PRO



1	POWER STATUS	LEDs for displaying the status
2	BRI	BRI ports for ISDN telephony (➜ p. 8); Gigaset T640 PRO: 4 x; Gigaset T440 PRO: 2 x
3	FXS	Ports for connecting analogue devices (phone/fax) (➜ p. 7); Gigaset T640 PRO: 4 x; Gigaset T440 PRO: 2 x
4	FXO	Connection to the analogue phone network (➜ p. 7); Gigaset T640 PRO: 4 x
5	GE	Ethernet RJ-45 port (10/100/1000Base-T), currently not used
6	GE	4 x Gigabit Ethernet LAN ports (10/100/1000Base-T) for connecting IP phones, computers and IP switches (➜ p. 7).
7	LAN	8 x Fast Ethernet LAN ports (10/100Base-TX) for connecting IP phones, computers and IP switches (➜ p. 7).
8		Currently not used

Information on the current status of ports and interfaces ➜ p. 76.

All LAN ports support PoE (Power over Ethernet) as per the IEEE 802.3af-2003 standard

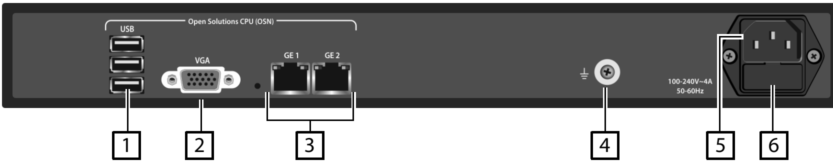
LEDs

LEDs on the front:

LED	Colour	State	Description
STATUS	Green	On	Device being used
		Flashing	Device being restarted
	Red	On	Fault on restart
POWER	Green	On	Power supply available
	–	Off	No power supply

LED on port	Colour	State	Description
LAN on right (Ethernet)	Green	On	Ethernet connection established
		Flashing	Port sending data
	–	Off	No Ethernet connection
LAN on left (PoE)	Yellow	On	The LAN port is powering the device connected (e.g. an IP phone)
		Flashing Fast	Line overload or short-circuit detected – PoE not enabled
		Flashing Slow	PoE loading on port, but the device has insufficient current to provide the power required – PoE not enabled
	–	Off	No current on the output line – PoE not enabled
FXS	Green	On	The phone connected is busy
		Flashing	Extension being called
	Red	On	Fault – not operational due to connection fault or SPI fault (SPI=Serial Peripheral Interface)
	–	Off	Phone receiver down or device without power
FXO	Green	On	FXO line is busy to the PABX
		Flashing	PABX signalling
	Red	On	Fault – not operational due to connection fault or SPI fault
	–	Off	Phone receiver down or device without power
BRI	Green	On	Physical Layer (Layer 1) synchronised (normal mode)
	Red	On	Physical Layer (Layer 1) not synchronised
	–	Off	Trunk group not active

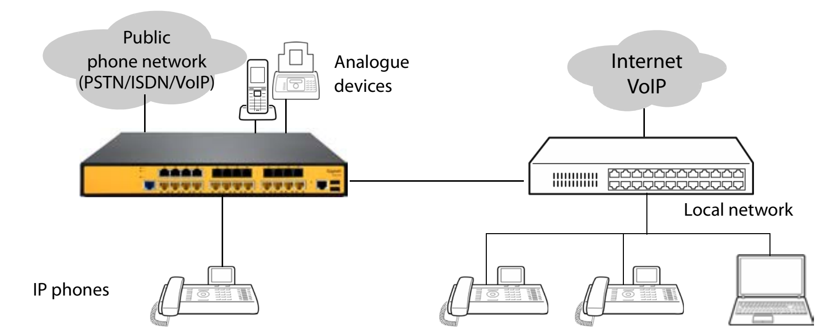
Back



1	USB	USB ports for connecting peripherals for the server (e.g. mouse and keyboard)
2	VGA	VGA port for connecting a screen for the server
3	GE1/GE 2	Currently not used
4	⏚	Earthing screw (→ p. 8)
5	100-240V~1.5A 50-60Hz	Power connector (→ p. 8)
6		250V fuse

Possible scenarios

VoIP PABX / VoIP TDM gateway



Setting up and connecting a device

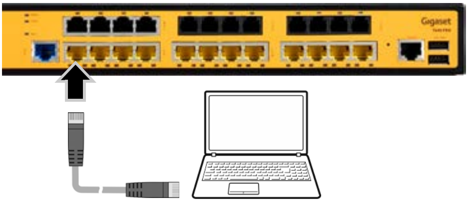
Observe the safety instructions and the information on the place of installation in the manufacturer documents provided.

The **installation instructions** supplied provide information on initial use of the PABX. Keep to the sequence described for initial use.

Connecting

Connect a computer

For the initial configuration, a computer needs to be connected directly to a LAN port on the device.



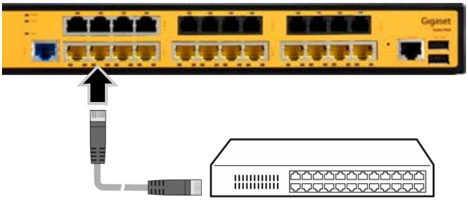
Straight-through Ethernet cable (not supplied)

- Connect the network connector of the computer directly to the LAN port

Establish a LAN connection

Use a LAN port to connect the PABX to the local network.

Remember that beforehand you must align the network configuration of the PABX to the settings of your network ➜ p. 72.



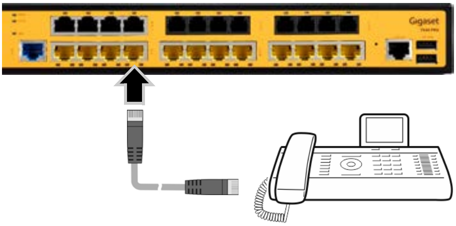
CAT 5e or CAT 6 Ethernet cable (not supplied)

- Connect the LAN port (GE or FE) to a Gigabit Ethernet or Fast Ethernet network, e.g. using a port on a switch

Connecting PoE clients to LAN ports

The device makes available 4 Gigabit Ethernet LAN ports (10/100/1000Base-T) and 8 Fast Ethernet LAN ports (10/100Base-TX) to connect Ethernet devices (such as IP phones).

The LAN ports support IEEE PoE standard 802.3af-2003. In addition to transmitting the other data, the connectors can power PoE-capable devices connected over the Ethernet cable. The LAN connectors automatically detect devices supporting the IEEE 802.3 standard, the device classification and the maximum power permitted.



CAT 5e or CAT 6 Ethernet cable (not supplied)

- Connect the GE or FE LAN port to the network connection of an IP phone

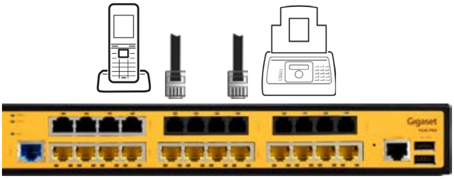
or

- Connect the IP phone directly to the Ethernet network

Connecting analogue devices

Analogue phones, dial-up modems and fax devices can be connected to the FXS ports. These analogue devices can then be used for Internet telephony.

An FXS port supplies the line voltage and ringing current for the phones.



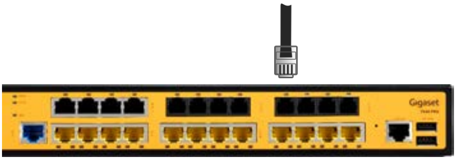
RJ11 phone cable (not supplied)

- Connect the FXS port to an analogue device (e.g. phone, dial-up modem or fax device)

Connecting to the phone network or PABX

FXO ports are only available for the Gigaset T640 PRO.

An FXO port establishes the connection to the public phone network (PSTN) or an analogue PABX. An FXO port receives the line voltage and ringing current for the phones from the phone network or PABX (as with analogue phones). An FXO port is the interface between the analogue phone network or system and the Internet.

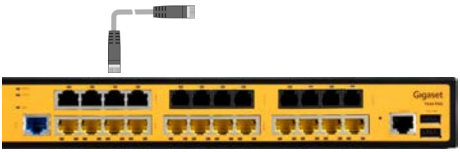


RJ11 phone cable (not supplied)

- Connect an FXO port to an analogue phone port (e.g. the phone network connector or PBX)

Connecting ISDN lines

The BRI ports (Basic Rate Interface) are used to connect ISDN PABXs. Every BRI port can be configured as an end device connector (TE) (➜ p. 48).



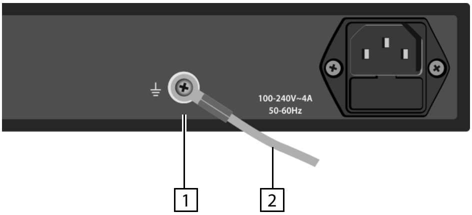
RJ11 phone cable (not supplied)

- Connect the BRI RJ-45 port to an ISDN device

> ⚠ A cable with a minimum rating of 0.14 A/mm is required for BRI port connections to the phone network to provide protection against electric shock and fire.

Affixing the earthing cable

The device must be earthed using a standard earthing cable (1.5 A/mm as a minimum).



Earthing cable: 1.5 A/mm minimum (not supplied)

- Undo the earthing screw 1 on the rear of the housing
- Attach the earthing cable 2 to the earthing screw. Connect the other end of the earthing cable to a protective earth conductor.

> ⚠ The devices are classified as Class I EN60950 and UL60950 and must be permanently earthed.

Connecting the power

Only use the power cable supplied.

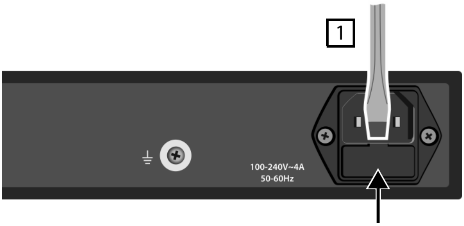
- Connect the device to the mains power

As soon as power is connected up, start the system. The **POWER** LED on the front lights up.

Replacing the fuse

The device has a fuse for overvoltage protection. It is located below the power connector on the rear.

> ⚠ Only use replacement fuses of the same type and having the same rating.

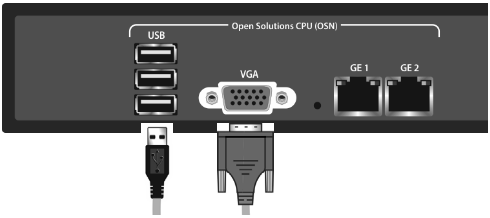


- Remove the mains connector from the device
- Use a small flat screwdriver to carefully open the fuse housing 1. ▶ Remove the fuse.
- Insert a new fuse into the housing and click it into place
- Connect to the power again and check the Power LED lights green

Connecting peripherals to the server ports

(only for experts)

The Gigaset PABX software runs on a server integrated in the device. Normally no direct access to the server is necessary. All configuration and administration functions can be performed from the web interface. The connectors required are available on the back of the device should direct access be required (such as for a reinstallation or fault analysis). Computer peripherals (such as mouse, keyboard and monitor) can be connected here.



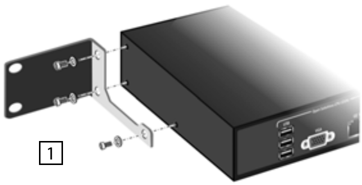
- **Connect a computer peripheral**: ▶ Plug a USB cable into one of the USB ports (type Standard-A) and connect it to the peripheral device.
- **Connect a monitor**: ▶ Use a VGA cable with a male connector (15-pin D-type) to connect the monitor to the VGA port.

Installation

Installation in a server cabinet

The device is intended for installation in a server cabinet. Use the installation adapters supplied.

Installation width: 19", height: 1 HE



- Attach the installation adapters to both sides of the housing 1. Use the screws supplied.
- Position the device on a pre-installed shelf in the server cabinet

- Secure the ends of the installation adapters 2 to the vertical carriers of the server cabinet frame. Use the standard screws for server cabinets (not supplied).

Installation without server cabinet

If you are not installing the PABX in a server cabinet:

- To install the device so as to be non-slip, affix the rubber knobs to the underside of the housing

Base configuration

Gigaset T440 PRO / Gigaset T640 PRO PABXs feature comprehensive options for the use, administration and configuration of your phones.

This manual describes the **administration** for both devices.

> The user instructions provide information on the phone functions and an introduction to the user interface.

For administration, the PABX features a web interface from which, using a browser on any computer, you can access your network.

Prerequisite: You have integrated the PABX into your local network as described in the installation instructions.

> The PABX must be integrated into the local network infrastructure of the company. If, on delivery, the network configuration does not match your network environment, carry out a base configuration from a computer connected directly to the PABX (➜ p. 6).

Logging in

To log into the user interface, you need the IP address of the PABX and a user name with PIN.

> IP address on delivery: 192.168.0.50
>
> Predefined user name for the Administrator:
> User name = **admin**, PIN = **0000**

- Open a standard browser on a computer
- In the address field, enter the IP address of the device . . . the login screen is displayed (**Login**)
- Enter the user name (**User name**) and associated PIN

Installation Wizard

An Installation Wizard starts automatically on initial login to the user interface. This guides you step-by-step through important settings.

- Set language for Wizard ▶ **Next**
- A screen follows enabling you to load a backup

  On initial use: ▶ Skip screen with **Next**

  To restore the configuration from a backup file: ▶ Click **Yes** ▶ Select backup file ▶ **Next**

  > The configuration of the PABX must be stored in a backup file: ▶ **Administration** ▶ **System** ▶ **Backup** ➜ p. 72

- Select country ▶ **Next** . . . Country-specific settings are loaded, such as dial tone and ISDN & FXS/FXO parameters
- Change the PIN for Administrator ID **admin** ▶ **Next**

You can now exit the Wizard and configure the other settings later from the Administrator menu of the interface.

> Running the Wizard through to the end is recommended however to connect the PABX to the local network and to get an exchange line to work successfully.
>
> Configure other settings with the Wizard: ▶ **Next**

Now end the Wizard: ▶ **Finish installation and reboot** . . . The PABX is restarted. You can now log in with user name **admin** with the new PIN, and configure other settings.

Other settings

Changing the network configuration → p. 68

- Enter the IP address of the PABX in the local network. The PABX requires a fixed IP address. This may have to be included in the configuration of the DHCP server in the network.
- Align to the network the settings for the subnetwork mask, the standard gateway (DHCP server) and the DNS servers

Disabling the DHCP server → p. 69

The PABX features an integrated DHCP server (this is enabled on delivery). If another DHCP server is active in the network, the PABX's DHCP server must be disabled.

- Disable the DHCP server using switch **Enable DHCP Server**

Configuring the email server → p. 70

An external email server must be set up to be able to send emails.

- Enable the sending of emails with switch **Email delivery** and enter the details for the SMTP server
- Or skip the step with **Next** to configure email later

Configuring an outside line → p. 46

Configure an outside line. The PABX supports SIP, ISDN and analogue connections. Access details are available from your telephone provider.

- Select the type of outside line (SIP, ISDN or FXO) from the list next to **Outside line**, and enter the connection details

The connection configured is entered into the configuration as a SIP or TDM gateway. A gateway group for the connection is set up automatically. All incoming and outgoing connections are routed via this gateway group.

Later, you can set up other gateways and gateway groups from the Administrator menu, and align routing to the needs of the company.

Entering users → p. 20

- Enter three users with **First name**, **Last name** and **Extension** for the users . . . The users are created with user names **demo101**, **demo102**, **demo103** and PIN **0000**

Ending the installation Wizard

You can re-check the settings on the last screen of the Wizard.

Change settings: ▶ Select tab ▶ Change settings as required ▶ Run Wizard again to end

Confirm settings: ▶ **Submit settings** . . . The PABX is restarted

> The network settings configured may mean you now have no access to the interface from the computer. ▶ Restore the connection with a new IP address as required

Licensing

To use the PABX, the license made available on purchasing the system must be activated.

▶ **Administration** ▶ **System** ▶ **License**

▶ Click and select the license file from your file system ▶ **Upload**

The system is now enabled.

> Information on installing other licences is available from http://wiki.gigasetpro.com or contact your Gigaset partner.

User interface

Once the basic configuration is complete and login is successful, the **Home** screen of the interface is opened.

> Change PIN: → Personal profile, p. 15.
>
> Detailed information on **Home** screen and **Menu**:
> → User instructions

Logging out

Logging out of the user interface: ▶ **Profile** ▶ **Logout**

Controls

Switch:	ON / OFF		Enable/disable function	
In lists:	✎	Edit entry	🗑	Delete entry
Backup:	+	Add and save entry		

Screen navigation

Switch screen: ▶ Select required function from menu

Save changes: ▶ Click button **Save** (button is only active when changes need to be saved)

Exit screen without changes: ▶ Click button **Cancel**

Filtering and sorting lists

A lot of information is shown in list form. You can sort or filter lists by column content to reduce the number of entries shown and to search for specific entries.

Sorting lists

Some lists (such as the lists of contacts and users) can be sorted in ascending or descending order by different column content.

- ▶ In the title of the column whose content you want to sort, tap ˅ . . . the list is sorted in descending order alphabetically or numerically.
- ▶ Click ˄ to sort the list in ascending order again.

Setting the number of displayed entries

For lists with many entries, it is possible to set the number of entries displayed on one screen.

- ▶ Select from the list the number of entries to display. The number of screens and the current position are displayed.
- ▶ Use **Next** and **Back** to scroll through the screens.

10

Back 2 / 3 Next

Alphabetic filter

A bar with the alphabet is shown above lists which can be filtered by alphabetic values.

▶ Click the letters in the ABC bar.

Only entries starting with the letter selected are displayed. Which field/fields is/are used for the filter is dependent on the list.

The user list for example is only filtered by name, and the contact list by name and first name. Clicking **A** in the user list shows the list of all users whose name starts with A. Clicking A in the contact list shows all contacts whose first or last name starts with A.

Name/number filter

Different search fields are available depending on the list type to search for single or multiple entries, such as by **Name** or **Number** in a contact list, or by **MAC address** or **IP address** in the phone list.

▶ Enter one or more letters/digits in a search field ▶ Click . . . Only entries starting with what is entered in the search field are displayed

Delete filter

▶ Click . . . The filter is deleted ▶ Click . . . The list is updated

Personal profile

A personal profile containing the following information is set up for every user:

- **First name**, **Last name** and **E-mail address** as per user entry
- The **Extension** assigned to the user
- User interface language
- Any personal phone numbers

Checking/adding personal details

▶ **Profile** ▶ **Personal data**

Adding personal phone numbers

▶ Enter the phone numbers in fields **Mobile** and **Home** ▶ **Save** . . . The numbers are transferred to your entry in the internal directory (➔ p. 22)

Add an image to be displayed as the caller image (CLIP image)

Formats: PNG, GIF, TIFF and JPG

▶ Click ▶ Select the image from the file system on the computer or network . . . The file name is entered in the text field ▶ **Save** . . . The image is loaded and displayed

Delete image: ▶ Click ▶ Confirm with **OK**

Changing the PIN

▶ **Profile** ▶ **Change PIN** ▶ Enter current PIN ▶ Enter new PIN ▶ Repeat new PIN ▶ **Save**

Changing the language

▶ **Profile** ▶ **Change language** ▶ Select the language required ▶ **Save**

> The change of language also applies for the language settings on the phone.

Pretending to be another user

Here you can change settings for users and check them when faults occur.

▶ **Profile** ▶ **Impersonate** ▶ Enter a user name or select the user name you want to use as an alternative ▶ **Save**

Administration menu overview

Users & extensions	Users & groups	Users	→ p. 20
		Pickup groups	→ p. 24
		Hunt groups	→ p. 25
		User import	→ p. 22
		Name / number	→ p. 23
	Permissions	Permission groups	→ p. 27
		GUI	→ p. 30
	Global contacts	Contact list	→ p. 32
		CSV import/export	→ p. 33
	Queues		→ p. 35
	IVR		→ p. 37
	Audio files		→ p. 39
	Hold music		→ p. 40
System	License		→ p. 66
	Update		→ p. 66
	CDRs		→ p. 67
	Network	IP configuration	→ p. 68
		DHCP server	→ p. 69
		Email delivery	→ p. 70
	Fax		→ p. 71
	Date & time		→ p. 71
	System settings		→ p. 72
	Backup	Automatic backup	→ p. 72
		Manual backup	→ p. 73
		Restore	→ p. 73
	SIP Transports		→ p. 71
	Certificates		→ p. 71

Provisioning	Phones		→ p. 41
	Provisioning groups		→ p. 41
	Key profiles		→ p. 41
	Provisioning parameters		→ p. 41
Routes	Gateway groups		→ p. 54
	SIP gateways		→ p. 54
	TDM Gateways	FXS ports	→ p. 54
		FXO ports	→ p. 54
		BRI ports	→ p. 54
	Inbound routes	Inbound routes	→ p. 58
		Night answer service	→ p. 54
	Outbound routes		→ p. 61
	Call forward	Queues	→ p. 63
		Hunt groups	→ p. 65
System status	General information		→ p. 76
	Interfaces		→ p. 76
	SIP-Status		→ p. 77
	Diagnostics	System log	→ p. 77
		Telephony	→ p. 77
		Operating system	→ p. 77
		Intrusion detection	→ p. 77
	Reboot & shutdown		→ p. 78

Users, groups and extensions

From the viewpoint of the PABX, a user name is assigned to an extension. A user is able to phone using the PABX when the user name is assigned an extension and the phone (with this extension) is registered with the PABX. If a user has multiple phones (e.g. a desktop phone and a DECT handset), an ID must be set up for every extension.

The PABX Gigaset T440 PRO / Gigaset T640 PRO is delivered with a predefined user name for the Administrator. User name = **admin**, PIN = **0000**.

During set-up with the installation Wizard, three more user names (demo101 - demo103) are set up (➜ p. 11) - which you can change or delete for internal purposes.

You set up additional user names for PABX users:

- Gigaset T440 PRO: up to 40 users
- Gigaset T640 PRO: up to 80 users

User names can also be imported from a CSV file (➜ p. 22).

Users can be assigned to different groups in line with their functions:

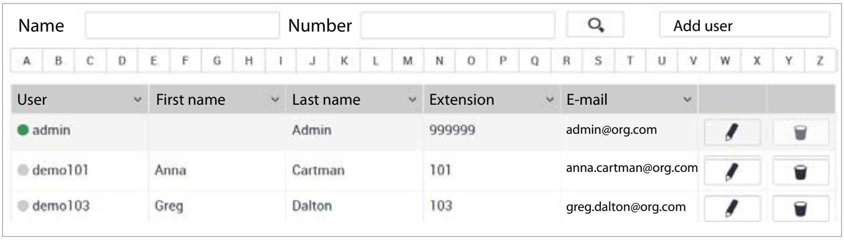
- Pickup groups: Members can accept the calls of other group members (➜ p. 24)
- Hunt groups: All members are reachable on the same extension number (➜ p. 25)
- Queue: Callers are kept in a queue and transferred to group members in line with definable rules (➜ p. 35)
- Authorisation group: Members have access to a certain definable subset of user interface functions (➜ p. 27) or to call groups in the outgoing routing (➜ p. 62).
- Provisioning group: The phones are assigned certain key profiles or special provisioning parameters (➜ p. 45)

User names can only be changed or added once the license is activated successfully (➜ p. 13)

Managing users

▶ Administration ▶ Users & extensions ▶ Users & groups ▶ Users

Existing users are listed with their login name, correct name, extension and email address. Users registered with the PABX with their extension are denoted by a green dot.



Filtering lists

- ▶ In fields **Name** and/or **Number**, enter a value ▶ Click . . . Only entries starting with what is entered are displayed

  Value: one or more letters and/or digits

You can filter the list by **Name** and **Number** at the same time.

Example: **Name** = Ab, **Number** = 1; the filter returns all entries whose name starts with "Ab" and extension number with "1".

> Parameters **First name** and **Last name** of the user entry are used for the filter name, i.e. filter "A" returns all entries whose first or last name starts with "A".

Delete filter: ▶ Click in the field . . . The value is cleared ▶ Click . . . The list is updated

Sort list

- ▶ In the title of the column whose content you want to sort by, tap . . . the list is sorted in descending order alphabetically or numerically.
- ▶ Click to sort the list in ascending order again.

Delete list

- ▶ Click . . . The entry is deleted

> The preconfigured **admin** user name cannot be deleted.

Setting up new users / changing settings

- ▶ Set up new user: Click **Add user** (top right on screen)
- ▶ Change entry: Click next to the entry

Parameter

User	User name for logging into the user interface. It must be unique. Value: 2 - 50 alphanumeric chars. (lowercase letter and digits).
Extension	Extension number. Value: 2 - 10 digits An extension has a fixed assignment to a user. The value must therefore be unique. To use the extension on a phone, the user must enable the extension on this phone.
First name / Last name	First and last names of the user.
PIN	PIN for logging into the user interface. Value: 3 - 10 digits The user can change the PIN from the profile settings.
SIP password	Password for the VoIP account assigned to the user. It is generated automatically.
Voicemail box	Extension of the answering machine assigned to the user. The default value for this number is as displayed in field **Extension**. If the user wants to hear multiple answering machines: Enter the answering machines numbers separated by commas.
E-mail	Email address of user. The email address is used to provide notifications of arriving answering machine messages and for Fax2Mail. Fax2Mail is always enabled; notifications of answering machine messages can be set by the user (**Menu** ▶ **Call Forwarding** ▶ **Call Forwarding** ▶ **Email notification on new voice messages**).
Language	The setting determines the language for the phone, system announcements and the PABX user interface for the user. This setting can be changed by the user.
CLIP internal / CLIP external	
	Call numbers of the user for the caller display (CLIP). The call numbers entered here are available to the user as a selection in menu **Service attributes**. Any number of call numbers can be entered for internal and external. It must be possible to call the numbers entered. **CLIP internal:** Extension of the user or another extension to be displayed for internal calls. **CLIP external:** Numbers for outgoing external calls. ℹ The numbers can only be entered on changing of the user settings, not for a new entry.
Hide from phonebook	
	Activated: The user is not entered into the internal directory of the PABX.

Drop to operator	Activated: Incoming calls for the user extension are diverted to a central number when not answered. ▶ Enter number in field **Operator extension**.
Provisioning group	Assignment of the extension to a provisioning group (➜ p. 45). All provisioning groups set up are made available. ▶ Select required group from the list
Pickup groups	Assignment of the extension to pickup groups (➜ p. 24). All pickup groups set up are made available. ▶ Select the group(s) required
User groups	Assignment of the user to authorisation groups (➜ p. 27). All authorisation groups of type **User** are made available. Assign user: ▶ Click + Remove user from group: ▶ Click Assignments to **All Users** and **All visible** users cannot be deleted.
Image	Image shown as a CLIP image. ▶ Click ▶ Select the image from the file system on the computer or network . . . The file name is entered in the text field ▶ **Save** . . . The image is loaded and displayed **Formats:** PNG, GIF, TIFF and JPG

Only **User**, **Extension** and **PIN** are mandatory parameters. All other settings are optional and can be added later.

The user is included in the internal contact list (**Menu** ▶ **Contacts** ▶ **Internal**) provided this is not explicitly inhibited with parameter **Hide from phonebook**.

Users must register their phones with the PABX (together with the extension assigned) as follows:

▶ On the phone, press buttons * 0 <Extension> ▶ Press the hands-free key ▶ Enter the PIN ▶ Confirm with #

Authorisations

The authorisations of the user groups to which the user is assigned are listed in the parameter list.

Importing user names

You can import user names from a CSV file.

An import file must be stored locally on your computer or in the network.

File format:	User,Extension,First name,Last name,PIN,Voicemail box, E-mail,Language,CLIP internal,CLIP external,Hide from phonebook,Drop to operator,Operator extension,Call pick up group,Collective line
Separator:	Comma, semicolon or tab

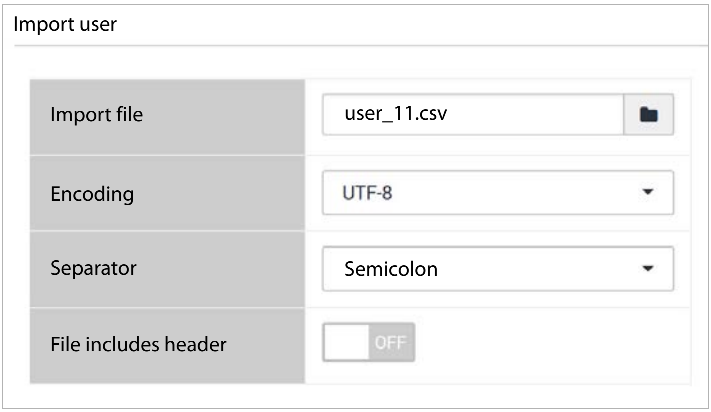
Example with semicolons and header:

1st line: User;Extension;First name;Last name;PIN;Voicemail box;E-mail; Language;CLIP internal;CLIP external;Hide from phonebook;Drop to operator;Operator extension;Call pick up group;Collective line

2nd line: susi;14;Susan;Brown;12345;14;susan.brown@company.org;English;;111;no;no;1;444

3rd line: ben;15;Ben;Smith;54321;15;ben.smith@company.org;English;;222;no;no;none;none

- **Administration** ▶ **Users & extensions** ▶ **Users & groups** ▶ **User import**



- Click ▶ Select the file from the file system of the computer or network
- Select character encoding (UTF8 or ISO) ▶ Select separator used
- **File includes header**

  Enabled: the first line in the file is not entered as a contact

  Disabled: The first line is taken as a contact entry
- Click **Upload** . . . The entries are displayed as a table for checking
- Click **Upload** . . . The entries are added to the personal directory. This also happens when a contact with identical details is already in the directory.

> Even identical entries are added to the user list.

Name / Number

- **Administration** ▶ **Users & extensions** ▶ **Users & groups** ▶ **Name / number**

This screen gives an overview of the user names. The first name and last name of the user and their telephone extension is shown for each user name. You are also given information about the affiliation to wait queues and collective lines and about settings for Calling Line Identification (CLIP) and incoming routing.

Group management

Your Gigaset PABX features pickup groups and hunt groups to handle calls which can be accepted by more than one person.

Pickup groups

Call pickup enables a user to accept a call for another subscriber. For this, the user presses a button on the phone which is specially reserved for this purpose and assigned the "Group pickup" function. Users belonging to the same call pickup group can accept calls for every group member.

▶ **Administration** ▶ **Users & extensions** ▶ **Users & groups** ▶ **Pickup groups**

Pickup groups already set up are listed with name and the number of its members.

Pickup Groups

ID	Group	Members		
1	demogroup	3		
2	Accounting	2		
3	Sales	2		
			+	

Setting up a new pickup group

▶ Enter the name for the group in field **Group** ▶ Click + . . . The group is entered without members

Adding/removing group members

▶ Click next to the group entry . . . The users assigned to the group are listed

Adding a user: ▶ Open the **User** list ▶ Click on the users to be included in the group (they are marked with a tick) ▶ Click +

Removing a user: ▶ Click next to the user entry

> You can also assign a user to a call pickup group by editing the relevant user entry and enabling the checkbox next to the group in area **Pickup groups** (→ p. 20).
>
> Users must belong to a user group with authorisation **Group pickup** (→ p. 27). Group **All Users** has this authorisation as standard.
>
> For call pickup, a button profile must be used to assign a button on the phone with parameter **Group pickup** (→ p. 42). Enter the group ID of the pickup group in field **Number/Data**.

Hunt groups

A hunt group bundles multiple numbers (extensions), which can then be called using one number. Incoming calls for the number of a hunt group are connected through directly to all the extensions.

▸ **Administration ▸ Users & extensions ▸ Users & groups ▸ Hunt groups**

Hunt groups already set up are displayed with group number (extension), name and other settings.

Edit Hunt Groups

Extension	Title	Display prefix	Call scheme	Group busy	Door Station	Members		
100	Hotline	14646	linear	no		2		
101	Reception	12345	parallel	yes		2		
			linear	OFF	OFF		+	

Setting up a hunt group

Parameter:

Extension	Hunt group extension. Incoming calls to this extension are put through to all extensions of group members.
Title	Group name
Display prefix	Is displayed on the phone to indicate the call is arriving over the hunt group.
Call scheme	**linear** The extensions of group members ring in succession. Calls are forwarded to the first extension. If this line is busy or the phone is not picked up within a specified time, the other extensions are called in succession. **parallel** All extensions ring at the same time. As soon as one extension user picks up, the parallel ringing stops.
Group busy	**Activated:** If one extension in the group is busy, the call is not forwarded to the next. This makes sense for example when the hunt group comprises a phone and a mobile device used by the same user. If the user is talking on one of the phones, this call is not interrupted. **Not activated:** If one extension in the group is busy, the call is forwarded to the next free one.
Door Station	**Enabled:** The "door interphone" ringtone type is signalled on telephones (such as Maxwell 3 and basic) which have a dedicated ringtone for the door interphone.
Members	Number of group members

▸ Enter the parameters for the group ▸ Click + . . . The group is set up

Adding/removing group members

- Click next to the group entry . . . The users assigned to the group are listed

Adding a user

- Open the **User** list ▶ Click on the users to be included in the group (they are marked with a tick) ▶ Enter a value for **Timeout** ▶ Click . . . The user is assigned to the group, the user's extension belongs to the collective line

Timeout: Time (in seconds) after which for call sequence **linear** the call is forwarded to the next extension (default = 5 seconds).

Removing a user

- Click next to the user entry.

Changing the order of users in the group

In the **linear** call sequence, the extensions of the group members are called in the order in which they are entered in the group.

- Use and to move the entry upwards or downwards.

> Screen **Administration** ▶ **Routes** ▶ **Call forward** ▶ **Hunt groups** enables you to define rules for diverting calls to a hunt group (➔ p. 65).

Authorisations

Menu **Permissions** enables two kinds of authorisations to be specified, and users and user groups to be assigned.

- **Permission groups** (➔ p. 27) provides different ways to structure how the phone, the directories and the queues are used for different users. It is possible for example to set up authorisation groups for international calls, call forwarding and editing the company directory. Complex user structures such as the executive-secretary function, and different strategies for actioning queues, can also be implemented with authorisation groups.
- **GUI groups** (➔ p. 30) provide the ability to differentiate access to different functions of the user interface for user groups. For example, a user without Administrator rights could be assigned the permission to manage users.

Permission groups

An authorisation group comprises a defined number of authorisations. An authorisation group is assigned to user names (➜ p. 22) or queues (➜ p. 35).

Predefined authorisation groups:

Admins	Group for the Administrator. This group is assigned to user name **admin**. This assignment cannot be deleted.
All Hosts	This group contains the entry for the in-house PABX. This entry is used for configuring Auto Answer, for example.
All invisible users	This group contains all users not shown in the internal directory. This group is assigned to user name **admin**. This assignment cannot be deleted.
All users	Default group for users. This group is assigned to all users, including **admin**. This assignment cannot be deleted.
All visible users	This group contains all users shown in the internal directory. This group is assigned by default to all users, except **admin**. This assignment cannot be deleted.
All queues	Default group for queues

Authorisation groups can be changed and redefined.

- First define an authorisation model for your company.

  Examples:

  - Dialling control for local, national and international calls:
    Set up authorisation groups Local, National and International, and select these groups accordingly for outgoing routing (➜ p. 61)
  - Users who may use the "Intercom" feature (executive-secretary combination)
  - Users who may edit the global directory

- Assign the user more sub-authorisations depending on the authorisation model

Setting up a new authorisation group

- **Administration** ▸ **Users & extensions** ▸ **Permissions** ▸ **Permission groups**

Existing groups are listed with **Name**, **Type** and **Members** (number).

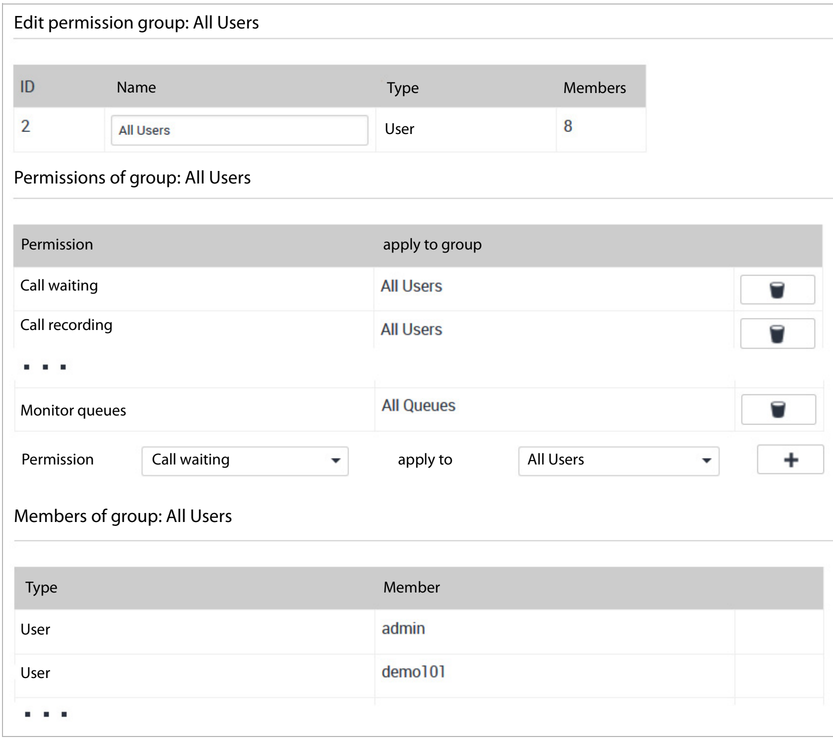
> ⚠ Do not delete the predefined groups as you may prevent users from accessing the functions of the PABX.

- Enter a name for the group in field **Name** ▸ Select the group type from list **Type**:

  User: For an authorisation group to be assigned to a user name

  Queue: For an authorisation group to be assigned to a queue

- Click . . . The group is entered in the list
- Click next to the group entry



Adding authorisations

- Select the authorisation from list **Permission**

  The list makes available these predefined authorisations:
  - **Call waiting**
  - **Call recording**
  - **Call forwarding, Override call forward**
  - **Manage automatic recordings**
  - **Busy Lamp Field**
  - **Allow CLIP, Allow CLIR, Allow DND**
  - **Direct Pickup**
  - **Manage own user recordings**
  - **Monitor own queues**
  - **Manage own queue recordings**
  - **Fax server**
  - **Show GUI** (assign authorisations to a GUI group → p. 30)

- **Edit global contacts**
- **Group pickup**
- **Hot desking**
- **Impersonate**
- **Ringtone configuration**
- **Manage manual user recordings**
- **Member of internal phonebook**
- **Set night answer service**
- **Receive push messages**
- **Allow intercom**
- **Night profile status**
- **Allow reminder**
- **Allow voicemail configuration**
- **Queue logon/logoff**
- **Call forward queues**
- **Monitor queues**

▶ In list **apply to**, select the group to which the authorisation is to apply ▶ Click + . . . The authorisation is shown in the list

You need not assign authorisations to an authorisation group for outgoing routing (e.g. restriction to local calls, and time or number restrictions). You only create the group itself and assign the required members. This group is then assigned to a routing rule (→ p. 62).

Adding members

▶ Open the **Member** list ▶ Click on the users to be included as members (they are marked with a tick) ▶ Click + . . . The user is assigned to the group

Example: Call pickup rules for executive's office and secretariat

The acceptance of calls can be regulated specifically using authorisations and pickup groups.

▶ Create authorisation group "Secretariat" with authorisations **Call forwarding** and **Direct Pickup**, and apply them both to the group "Secretariat".

▶ Create authorisation group "Executive's office" with authorisation **Direct Pickup**, and apply it to the group "Executive's office" and **Override call forward**, apply it to the group "Secretariat".

▶ Assign "Executive's office" and "Secretariat" to a shared call accept group (→ p. 24).

▶ Create key profiles for the two phone types (→ p. 42), with key assignments **Intercom** and **Group pickup**, and assign these key profiles to the provisioning groups for the executive's office and secretariat (→ p. 45).

▶ **Call waiting** must be enabled for "Secretariat" (from menu **User Settings**)

A caller dials the number of the queue (→ p. 35). If the executive's office phone is registered in the queue, the call is routed to this phone. If the executive's office phone is not registered in the queue, the call is routed to the secretariat's phone. If the secretariat's phone is busy, enabled call divert can be ignored from the executive's office and the call is taken on the secretariat's phone. The shared pickup group now means the call can be accepted by the executive's office.

> Call recording is another example where authorisations and authorisation groups are used (**Call recording**).
>
> There is a detailed description in the Gigaset portal at
>
> → https://teamwork.gigaset.com/gigawiki/display/GPPPO/FAQ+T640+T440+Call+recording

GUI groups

Which functions (modules) of the user interface are available to a user is specified by the affiliation to GUI groups.

There are two predefined GUI groups:

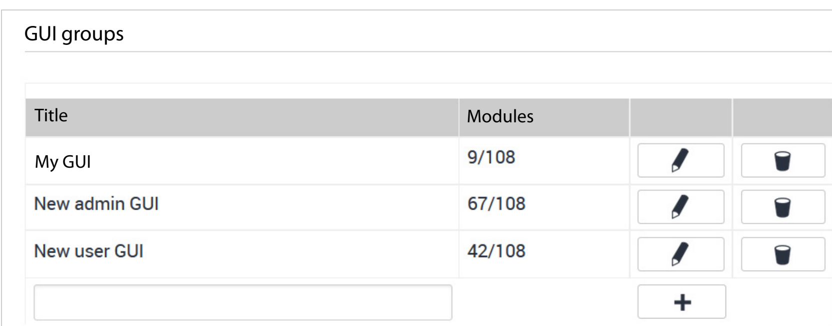
New admin GUI	For the Administrator, assigned by default to authorisation group **Admins**
New user GUI	For users without Administrator authorisation, assigned by default to authorisation group **All Users**

You can set up more GUI groups. They are made available for selection when authorisation groups are set up.

▸ **Administration ▸ Users & extensions ▸ Permissions ▸ GUI**

Existing GUI groups are displayed with the name and number of modules permitted for the group.

New admin GUI 63/108 means for example, for authorisation group **New admin GUI** 63 of 108 possible GUI modules are enabled.



GUI groups

Title	Modules		
My GUI	9/108		
New admin GUI	67/108		
New user GUI	42/108		

Setting up a new GUI group

▸ Enter the name for the group in the text field ▸ Click + . . . The group is entered without authorisation.

Deleting a GUI group

▸ Click in the line for the group . . . The group is deleted

Adding/deleting modules

- Click next to an entry . . . All GUI modules are listed

The positioning of the modules corresponds to the layout of the user interface. Lower-level modules are denoted by the relevant number of dashes (-, - -, - - -), and indented.

To enable a module, the associated higher-level modules must also be enabled. When a higher-level module is disabled, all the lower-level modules are also disabled.

- Enable/disable a module using the **ON/OFF** switch.
- Click **Save** to save the settings

Example

- **User Settings**		ON
- - **Service attributes**	Service attributes	OFF
- - **Device configuration**		ON
- - - **Keys**	Keys	ON
- - - **Ringtones**	Ringtones	ON
- - - **Display**	Display	OFF
- - - **Miscellaneous**	Miscellaneous	OFF
- - **Contacts import/export**		OFF

The **Login** and **Logout** functions should be allowed for a GUI group as a minimum because otherwise no activities at all are then possible.

Assigning a GUI group to users

- Create the authorisation group, applying authorisation **Show GUI** to the GUI group and adding it to the authorisation group
- Enable the authorisation group for the user(s) to be assigned this GUI authorisation (→ p. 22)

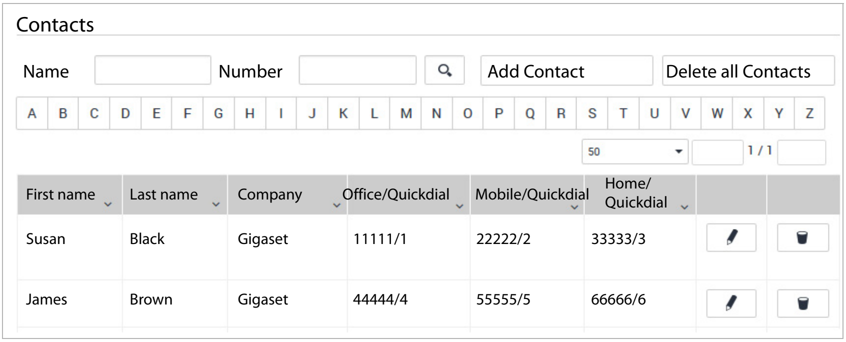
Global contacts

In **Menu** → **Contacts**, the interface makes available three directories to the user: **Internal**, **Global** and **Private**. The entries for the **global** directory can be entered manually or imported from a CSV file.

Manually creating a contact list

▶ **Administration** ▶ **Users & extensions** ▶ **Global contacts** ▶ **Contact list**

All existing directory entries are displayed.



Parameters **First name** and **Last name** are used for the name filter. The number filter uses the **Office**, **Mobile** and **Home** parameters.

Filtering and sorting lists → p. 14.

Use the **Delete all Contacts** button to remove all entries from the global contact list. This makes sense for example when you want to re-import contacts from a file (→ p. 34). It prevents the creation of duplicate entries.

Creating a new contact

▶ Click **Add Contact** in the top right of the screen

Parameter:

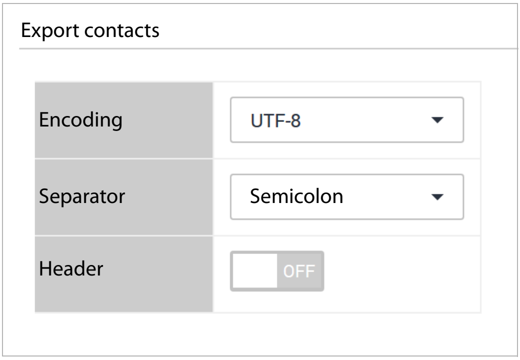
First name	First name of contact
Last name	Last name of contact
E-mail	Email address of the contact
Company	Company or organisation
Office	Work phone number
Mobile	Mobile number
Home	Private number

Quickdial	You can enter a quick dial for **Office**, **Mobile** and **Home**. Dial the quick dial on your phone like this: [*] [1] <Quick dial>
Image	Image shown when this contact rings. ▶ Click ▶ Select the image from the file system on the computer or network . . . The file name is entered in the text field ▶ **Save** . . . The image is loaded and displayed **Formats:** PNG, GIF, TIFF and JPG

Exporting contacts

You can export contacts from the global directory and import them again as required, or use them on another system. CSV (Comma Separated Value) files are used for this.

▶ **Administration** ▶ **Users & extensions** ▶ **Global contacts** ▶ **CSV import/export** ▶ **CSV export**



- **Encoding** (UTF8 or ISO) and **Separator** (comma or semicolon) must be selected for the export file
- **Header** must be enabled if the first line in the file is to have a header
  Enabled: the first line in the export contains
  First name,**Last name**,**Company**,**Work**,**Mobile**,**Home**
  Disabled: Only the contacts are exported
- Start export: ▶ Click **Download CSV** ▶ Select the destination for the file in the file system and enter a file name
  The default is prv_pb_<ID>.csv

> The file name and the destination for the file can only be selected and entered when the settings in the browser permit the downloading of files.

Importing contacts

You can import contacts saved with an export, or import into the global directory from other directories.

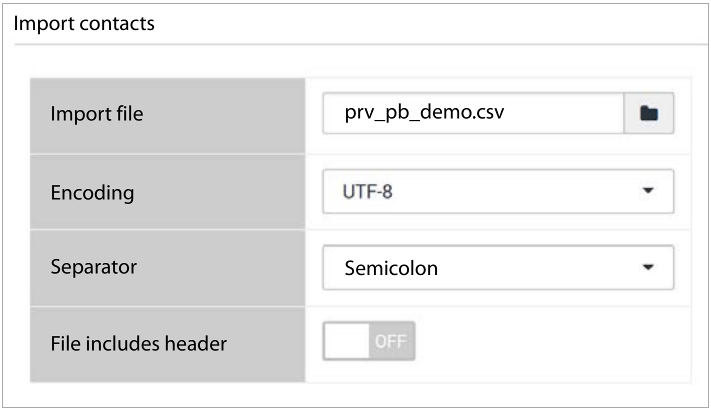
An import file with the contacts must be stored locally on your computer or in the network.

File format:	First name,Last name,Company,Office,Office-Quickdial,Mobile,Mobile-Quickdial,Home,Home-Quickdial,E-mail
Separator:	Comma, semicolon or tab

Example with semicolons and header:

First name;Last name;Company;Office;Office quick dial;Mobile;Mobile quick dial;Personal;Personal quick dial;Email
Peter;Brown;Company;123456789;1;01784567;2;083416786;3;peter.brown@org.com
Susan;Black;Org;987654321;;015679787878;;;;susan.black@org.com

- **Administration** ▸ **Users & extensions** ▸ **Global contacts** ▸ **CSV import/export** ▸ **CSV import**



- Click ▸ Select the file from the file system of the computer or network
- Select character encoding (UTF8 or ISO) ▸ Select separator used
- **File includes header**

  Enabled: the first line in the file is not entered as a contact

  Disabled: The first line is taken as a contact entry
- Click **Upload** . . . The entries are displayed as a table for checking
- Click . . . The entries are added to the personal directory. This also happens when a contact with identical details is already in the directory.

> Even identical entries are added to the directory. Delete the contact list if necessary (→ p. 32) before you import contacts from a file.

Queues

The **Queues** module makes available an additional group type. It enables a user group to be assigned a queue function for incoming calls. Once a caller is in the queue, checks are performed at specified intervals whether and to which member of the queue group the call can be put through. Members of queue groups are called agents.

▶ **Administration** ▶ **Users & extensions** ▶ **Queues**

Queues

Queue	Title	Max. callers		
5000	Service	5		
5001	Hotline	10		
			+	

Screen **Administration** ▶ **Routes** ▶ **Call forward** ▶ **Queues** enables you to specify rules for diverting calls to a queue (→ p. 63).

Setting up a new queue

▶ In field **Title**, enter the name for the queue ▶ Click +

Parameter:

Title	Queue name
Extension	Queue extension
Hold music	Callers hear whilst waiting the PABX's hold music or custom hold music. ▶ Select the hold music class from the options list. Hold music class → p. 40 **Default:** A caller hears the default hold music. **Ring instead of hold music**: The caller hears the dialling tone.
Greeting	Select an audio file for the introductory greeting - which is played once before the call is passed to the queue. ▶ Choose an audio file from the options list. All available audio files are shown.
Announce hold time	Interim announcement interrupting the hold music and announcing the anticipated wait time . This announcement is internal to the system and cannot be changed. **Yes**: The wait time is announced at regular intervals **Once**: The wait time is announced only once **No**: The wait time is not announced

High load announcement	Interim announcement interrupting the hold music and informing the caller of a high number of calls. ▶ Choose an audio file from the options list. All available voice files are shown. **None**: The caller is not informed **if more than xxx callers waiting:** A caller is only notified when more callers than the number specified are waiting.
Wrap-up time	Pause (in seconds) for agents before the next call is put through. The **Wrap-up time** starts when call pickup is ended.
Weight	Queue priority. Value range: 0 – 255. **Weight** specifies which queue is prioritised and when free agents are available. The higher the value, the higher the prioritisation over others.
Ring time per agent	Time after which a call attempt to an agent is cancelled. Entering 0 means the maximum duration of 3,600 seconds is used. For the **Least recent** call strategy, **Ring time per agent** determines when the next agent is called.
Max. callers	Maximum number of callers kept in a queue. Once the maximum number is reached, subsequent callers hear the engaged signal. For certain queue statuses (such as full and no agent answering), call divert to another number, an announcement or an answering machine can be set up (→ p. 63).
Strategy	Specifies the method used to put incoming calls through to agent extensions: **Round robin**: Every agent is assigned a time slot in which he/her is reachable. When the time is over, the agent is placed at the back of the agent list and next agent moves forward. **Least recent**: The caller is put through to the agent who has been waiting the longest to take a call **Random**: The agent is chosen randomly **Fewest calls**: The agent with the lowest number of calls receives the call **Ring all**: All free agents are called. The first one to pick up receives the call.
Enter	Specifies when a queue is enabled: - **Do not enter if no agent is logged on or no agent is available** - **Do not enter if no agent is logged on** - **Always**
Leave	Specifies when a queue is disabled: - **When all agents log off** - **When all agents log off or when no agent is available** - **Never**

- Save the settings with **Save** . . . The queue is entered in the list

i	You can record yourself, or upload, the audio files for the welcome message and announcements: **Administration** ▸ **Users & extensions** ▸ **Audio files** (→ p. 37)

Assigning users

Users register as agents for a queue with key sequence [*] [5] <Queue extension> [◄], and use [*] [5] [*] to remove themselves from.

Agents can also be assigned to a queue statically. Users are then added automatically and they cannot remove themselves.

Adding a user: ▸ Open the **User** list ▸ Click on the users to be included in the group (they are marked with a tick) ▸ Click +.

Removing a user: ▸ Click 🗑 next to the user entry

i	The function is only available when editing a queue, not when setting it up.

IVR

An IVR makes it possible to navigate a caller through the phone system before the caller is connected to a particular person.

Example: A caller calls the service extension of your company - which is configured as an IVR. The caller hears an announcement prompting: "For question about your product, please press "1", for technical problems, please press "2", ... One key press by the caller connects the caller to the correct person.

Prerequisite: You have at least one voice file you can use as an announcement. You must record this voice file, or load it onto the PABX, beforehand (→ p. 37).

Setting up an IVR

- **Administration** ▸ **Users & extensions** ▸ **IVR**
- In field **Title**, enter the name for the IVR ▸ Click +

Parameter:

Title	Name of IVR
Extension	Extension of IVR. A call to this extension activates the IVR.
Announcement file	Audio file played as an announcement when the extension is called. This announcement includes for example instructions on how to use key codes for menu control. ▸ Select the required audio file from the options menu

Time to wait for input	Time the system waits for a response from the caller (pressing of a button). The announcement is repeated if no response is received within this time. Specify the maximum number of repetitions with parameter **Repetitions**. What happens when afterwards there is still no response is defined in an interaction rule (➜ p. 38).
Repetitions	Maximum number of times the announcement text is repeated.
Allow direct dial	**Enabled**: The caller can enter several digits in succession to dial a subscriber directly. Only internal numbers can be dialled. There is a short pause after the last digit before dialling starts. **Disabled:** Callers must select their way through the voice menu digit by digit.

Key assignments

Specify the subsequent action when the caller presses 0 – 9, * or #.

None	No action. The connection is not ended. The caller can press another button.
Hang up	The call is ended
Go to extension	The caller is diverted to another number or extension ▶ Enter the number/extension
Play audio file	Another message is played and the call ended. ▶ Select the audio file from the options menu
Repeat announcement	The initial announcement is repeated once more

Interaction rules

You specify with interaction rules the subsequent action when a caller does not respond at all or performs an invalid action.

Parameter:

Hang up	The call is ended
Go to extension	The caller is diverted to another number or extension ▶ Enter the number/extension
Play audio file	Another message is played. ▶ Select the audio file from the options menu
Repeat announcement	The initial announcement is repeated once more

Audio files

You require audio files for greeting text, wait time announcements and announcement text for IVRs. You can load audio files onto your PABX or record them yourself using a phone connected to the PABX.

Formats allowed:	aif, aiff, wav, au, al, alaw, la, ul, ulaw, lu, gsm, cdr, mp3 and ogg
Maximum size:	20 MB

▶ **Administration** ▶ **Users & extensions** ▶ **Audio files**

Existing audio files are displayed with description and duration. The file name is used as the description. You can change the description at any time (this applies for files you record on the phone and audio files uploaded).

Play file:	▶ Click . . . The audio file is played over the computer speaker Repeat/pause playback: ▶ Click
Delete file:	▶ Click

Recording an audio file

- In field **Extension**, enter the extension number of the phone for the recording ▶ Click **Record** . . . The phone rings
- Pick up the receiver, or enable the hands-free function, and follow the instructions
- Refresh the display of screen **Audio files** (by clicking menu **Audio files** again for example) . . . The new announcement is displayed
- In field **Description**, enter a name for the audio file

Loading audio files

- Click ▶ Select the audio file from the file system on the computer or in the network . . . The file name is entered in the text field
- In field **Comment**, enter a description for the audio file ▶ Click **Upload** . . . The file is loaded

Hold music

Hold music is played for callers who are put on hold during a call or who are waiting in a queue for an agent to become free (→ p. 35). Hold music is divided into certain classes. Every class can be assigned multiple audio files (played in sequence).

▶ **Administration** ▶ **Users & extensions** ▶ **Hold music**

Existing classes are displayed with name and number of files assigned.

▶ You can select hold music as the default music in the **default** column. This is used for a queue if **Default** is selected as the hold music.

Class **default** contains predefined music for the PABX. This music is used for queues provided no other music is available and selected. It cannot be changed or deleted.

Defining new classes

▶ Enter the name for the hold music and click +

Assigning/editing audio files

▶ Next to the entry for the class, click ... Audio files already assigned are listed

Listening to an audio file:

▶ Click **Call** in column **Call assigned ext.**

or when the extension is not registered to the phone:

▶ Enter a phone extension in field **Call custom ext.** ▶ Click **Call** ... The phone with the extension specified rings ▶ Pick up the receiver or press the hands-free button

Adding audio files:

▶ Click ▶ Select the audio file from the file system on the computer or in the network ... The file name is entered in the text field

▶ Enter the description for the audio file ▶ Click + ... The file is loaded and entered in the list of audio files

> After the file has been uploaded, the volume can be adjusted to the system.
>
> A warning is issued if it is too loud. It is not possible to increase the volume further than that.

Provisioning

Provisioning means providing registered devices with configuration data. All devices are set up with Autoprovisioning when the PABX is started.

> If broadcasts are permitted in the network, the PABX recognises devices in the same sub-network and sends provisioning data to them (SIP multicast).
>
> If an SIP multicast is not possible, you must use option 114 to assign the IP address of the PABX for the telephones on the DHCP server of the network (→ p. 69).

In Autoprovisioning, the parameters stored in the PABX are used as defaults for device configuration. The default settings cannot be changed.

You can overwrite or add to one or more of these provisioning parameters, and the preconfigured key assignments for individual devices or device groups.

Changing default provisioning:

- Create a special key profile (→ p. 42) and/or provisioning profile (→ p. 44)
- Assign one or more profiles to a provisioning group (→ p. 45)
- Assign the provisioning group to users (→ p. 20)

On every restart of the phones registered for the users, the profile is sent and the relevant default values are overwritten.

Phones

- **Administration** ▶ **Provisioning** ▶ **Phones**

This screen shows all phones known to the PABX. The PABX automatically detects all phones of the following device types when in the local network:

- Gigaset DE310 IP PRO
- Gigaset DE410 IP PRO
- Gigaset DE700 IP PRO
- Gigaset DE900 IP PRO
- Gigaset N510 IP PRO with a maximum of 6 handsets
- Gigaset N720 DM/IP PRO with a maximum of 100 handsets
- Maxwell 10
- Maxwell 3
- Maxwell basic

> For the Gigaset N720 DM/IP PRO only one unassigned account is displayed by default.
>
> Display all the Gigaset N720 DM/IP PRO accounts: ▶ From the **Phone Type** list, select the entry **Gigaset N720 DM/IP PRO (all)**.

Because an analogue device can be connected to every FXS interface, these interfaces are also maintained and displayed as phones.

Phones

MAC address	IP address	Phone type
		(all)

MAC address	IP address	Phone type	User	Extension	Firmware version	
00:90:8F:59:01:EB:-0:...	169.254.231.252	T440/T640 PRO FXS	-	950001	6.60A.304.001	
. . .						
7C:2F:80:20:4A:3E	192.168.250.66	Gigaset DE700 IP PRO	Martin B...	13	02.00.08	unassign user
7C:2F:80:20:AB:3B	192.168.250.69	Gigaset DE310 IP PRO	Admin	999999	02.00.05	unassign user
7C:2F:80:21:08:90	192.168.250.68	Gigaset DE900 IP PRO	Susan Br...	11	02.00.08	unassign user
7C:2F:80:A0:F7:39	192.168.250.249	Gigaset Maxwell Bas...	Beatrice...	102	201512071119	unassign user
7C:2F:80:A1:00:38	192.168.250.120	Gigaset Maxwell 3	John Sm...	12	2016-03-04_19:07:00	unassign user

The following information is displayed for every phone:

- MAC address
- IP address as a link to the configuration interface of the end device
- Phone type
- User and Extension if the phone is registered. Phones not registered are given a default number on which they can be called.
- Current firmware version

> The list also includes devices no longer in the network.

Key profiles

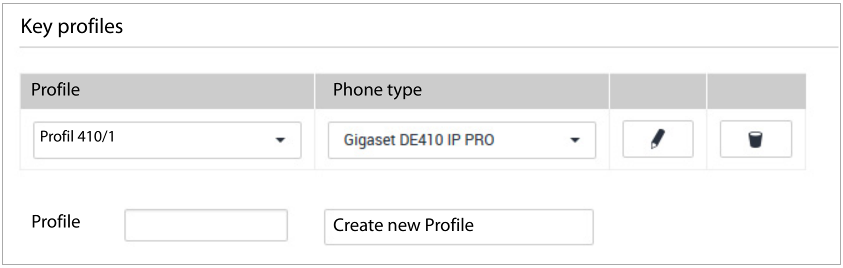
A key profile can be defined for every device with function keys. If key assignments are already in the default settings for the PABX, they can be added to or overwritten.

Function keys are available on the following phones:

DE 410 IP PRO:	7 function keys, can be upgraded to 21 with expansion module
DE 700 IP PRO/ DE 900 IP PRO:	14 function keys, can be upgraded to 56 with a maximum of 3 expansion modules
Maxwell 10	100 programmable keys
Maxwell 3	8 programmable keys

> When expansion modules are used, the PABX is not able to provide enough power to the phones over PoE. Use separate power adapters to power the phones.

▶ Administration ▶ Provisioning ▶ Key profiles



▶ Enter the name for a new profile in field **Profile** ▶ Click **Create new Profile** . . . The profile is entered into the options lists (in alphabetical order)

▶ Select the required profile ▶ **Phone Type** ▶ Click

You can allocate a key assignment for every possible function key (PK1 - PKn) on the phone type selected.

> Several key assignments, one per telephone type, can be created under one profile.
>
> Users themselves are able to assign functions to the function keys of a phone (not the expansion modules). You can prevent this by locking the keys assigned a function.

▶ Enable function assignment for a key (PK1 - PKn) with the **ON**/**OFF** switch ▶ Select the function from the list:

- inherit -	The key keeps the default PABX assignment (if available)
External destination	Dial external number ▶ Enter the number in field **Number/Data**
Extension	Select the extension ▶ Enter the extension number in field **Number/Data**
Group pickup	Call pickup for those belonging to the same pickup group (→ p. 24) ▶ Enter the number in field **Number/Data**
Intercom	Dial a connection to an intercom extension ▶ Enter the extension number in field **Number/Data** **Prerequisite:** The extensions involved require authorisation **Allow intercom** (→ p. 27)
DTMF	Send a DTMF code during an active call for example to query and manage a network mailbox using digit codes. ▶ Enter the DTMF code in the **Number/Data** field

- In field **Label**, enter a description for the key assignment. It is used to create the keypad inserts.
- Lock the key to prevent changes by other users: ▶ Enable/disable the lock with the **ON**/**OFF** button in column **Locked?**
- Save the settings with **Save**

> **Assigning a key profile:**
> - Create a provisioning group containing this key profile → p. 45
> - Assign the provisioning group to those users receiving this key assignment → p. 22

Provisioning parameters

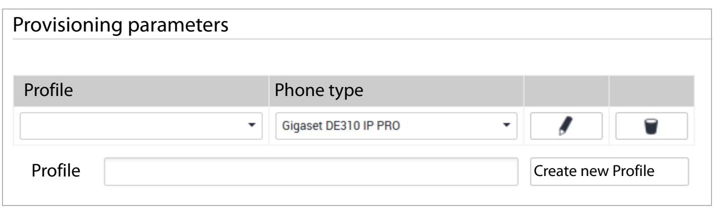
Provisioning profiles are only required in exceptional circumstances. They are used to store functions differing from the standard on certain devices.

There is detailed information on the parameters for each end device in the Gigaset portal at

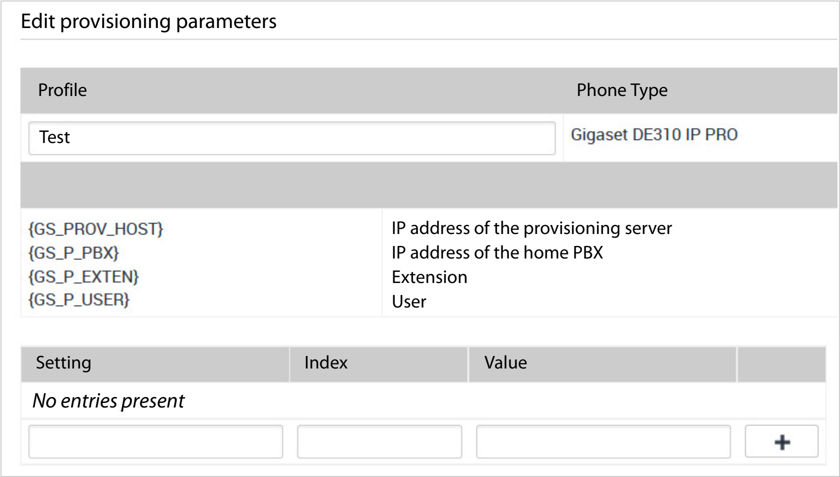
→ https://teamwork.gigaset.com/gigawiki/display/GPPPO/Provisioning+step+by+step

Creating a provisioning profile

- **Administration** ▶ **Provisioning** ▶ **Provisioning parameters**



- Enter the name for a new profile in field **Profile** ▶ Click **Create new Profile** . . . The profile is entered into the options lists (in alphabetical order)
- Select the required profile ▶ Select **Phone Type** ▶ Click



- Enter a parameter in field **Setting** ▶ Enter the index as required (the index is at the end of the parameter name in brackets) ▶ Enter the required value in field **Value** ▶ Click ✚ . . . The parameter is entered in the list
- Once you have entered all the parameters you wish to change: ▶ **Save**

Provisioning groups

You can now create provisioning groups with the key and (as required) provisioning profiles you have created. Groups can have a hierarchical structure (i.e. a group can contain sub-groups). This makes it possible to differentiate further the allocation of key assignments within a group of users.

Example: You create key profile T1 - which is assigned to provisioning group P1 and only assigns the first 4 keys. Key profile T2 assigns keys 5 and 6 and is created as sub-group P2 under P1. You can now assign to users provisioning group P1 with key assignment T1, and other users P2 - comprising key assignments T1 and T2.

- **Administration** ▶ **Provisioning** ▶ **Provisioning groups**

- In field **Group**, enter a name for the group ▶ In field **Title**, specify an optional name for the group. This is then shown instead of the group name in the group configuration.
- From list **child of**, select a group under which the new group is a sub-group. All groups already created are made available. Groups on the topmost level are assigned to the **Root node**.
- **Key profile** and/or **Provisioning profile** must be selected from the lists
- Where applicable, select the number of available expansion modules for the phone type
- Click ✚ . . . The group is entered in the list and is now available for user configuration (➜ p. 20)

Routing

Your PABX features different ways to connect to a public phone network - over the Internet (SIP), using an analogue exchange line (FXO) and digital (ISDN). These connections must be configured in line with information provided by the phone provider responsible.

You have already set up a phone connection during the start-up phase (→ p. 11). The connection configured is entered into the configuration as a SIP or TDM gateway (FXO or ISDN). A gateway group for the connection is set up automatically. All incoming and outgoing connections are first routed via this gateway group.

You can set up other gateways and gateway groups from the Administrator menu, and align routing to the needs of the company.

Configuration process

You require provider access details and any other information about the connection provided.

> Help on setting up SIP accounts / trunks is available from:
>
> https://teamwork.gigaset.com/gigawiki/display/GPPPO/ITSP+SIP+Trunking

SIP:
- Set up at least one gateway group
- Set up a SIP gateway for every provider account, and assign it to one gateway group

Analogue or ISDN:
- Set up at least one gateway group.
- Configure a TDM gateway for every available trunk line (FXO, ISDN).

  All calls are routed internally over SIP. This is why SIP gateways are created automatically for configured FXO and ISDN gateways.
- Assign SIP gateways to the gateway group.

- Specify rules for incoming and outgoing calls

> Different rules can be defined for incoming and outgoing calls, and for how call numbers are handled. For this, call number groups must be specified in the form of patterns, or regular expressions. An introduction to working with regular expressions is in the appendix (→ p. 79).

TDM gateways

TDM (Time Division Multiplex) means digital phone technology for analogue and ISDN connections. You can deploy your PABX as a gateway between SIP (Internet telephony) and TDM, i.e. analogue or ISDN outside lines. If you want to use a TDM connection or connect up analogue devices, you must configure the connections.

An SIP gateway with internal registrar is automatically entered for every TDM gateway configured (→ p. 49).

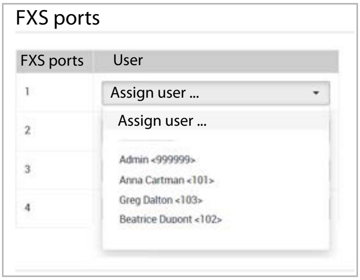
> Connections for analogue trunk lines (FXO) are only available on the Gigaset T640 PRO.

FXS ports – analogue devices

On a Gigaset T640 PRO, you can only connect up to four (on a Gigaset T440 PRO up to two) analogue devices to the FXS ports (→ p. 7). You can assign devices to users on this screen.

- **Administration** ▸ **Routes** ▸ **TDM Gateways** ▸ **FXS ports**
- Select one user from the list for every FXS port to which a device is connected ▸ **Save**

The analogue devices automatically receive the extension of the respective users (→ p. 21). If a user has already registered a phone having this extension with the PABX, it is deregistered.



> Information on the status of FXS ports is available on screen
> **Administration** ▸ **System status** ▸ **Interfaces** (→ p. 77)

FXO ports – analogue trunk lines

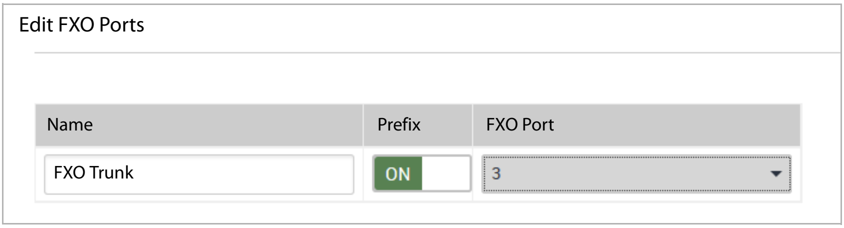
> FXO ports are only available on the Gigaset T640 PRO.

An FXO port establishes the connection to the public phone network (PSTN) or an analogue PABX (→ p. 7). You can combine FXO ports into one or more trunks, or connect a single line (outside line) to every port. Ports must be assigned continuously starting at 1.

- **Administration** ▸ **Routes** ▸ **TDM Gateways** ▸ **FXO ports**

Setting up an FXO trunk

- Enter the trunk name ▶



- Use the switch to specify whether a prefix is added at the front
- Select the number of ports to form the trunk. Only the number of ports still available is shown.
- **Save** . . . The trunk is displayed with **ID**, the associated ports and the Name; a SIP gateway for the trunk is created

Assigning call numbers

- Enter the associated call number for every FXO port assigned ▶

> Information on the status of FXO ports is available on screen
> **Administration** ▶ **System status** ▶ **Interfaces** (→ p. 77)

BRI Ports

ISDN ports (BRI) are used to connect ISDN devices (→ p. 8). Every ISDN port can be configured as a Point-to-Multipoint or Point-to-Point connection

- **Administration** ▶ **Routes** ▶ **TDM Gateways** ▶ **BRI ports**
- Enter the trunk name ▶

Parameter:

Country Code	Country code, e.g. 49 for Germany
Area code	Local area code, e.g. 30 for Berlin
PTP Pilot number	Main number of a Point-to-Point connection How connection number and extension numbers are handled for incoming calls is configured in the gateway group with parameter **Inbound DIDs** (→ p. 56).
National prefix	Digit which must be prefixed for national calls, e.g. 0 (depends on country)
International prefix	Digits which must be prefixed for international calls, e.g. 00 (depends on country)

Number substitution	Enabled: Suitable replacement rules are generated based upon the values in fields **Country Code**, **Area code**, **PTP Pilot number (PTP)**, **National prefix** and **International prefix** to guarantee correct signalling of the call number type in the ISDN protocol (type National, International, etc.). This guarantees that numbers are displayed correctly at the called end. This is important most of all for connections with the **CLIP no screening** feature - because invalid numbers are quickly shown at the called end if signalling is incorrect. If the option is enabled, the details entered in the different call number fields may no longer be entered in the fields for the associated gateway group (above all Outbound caller ID), because this information is appended in addition to that from the TDM gateway. Once all fields are entered, only the extension may be signalled by the gateway group. If only the country code is specified, a combination of local area code, trunk number and extension must be signalled.
Layer 2 mode	**PTP Pilot number (PTP)**: For a Point-to-Point connection **Point-to-Multipoint (PTMP/MSN)**: For a Point-to-Multipoint con-nection
Layer 3 mode	Protocol used for ISDN communication (country-specific)
Port	Number of ports belonging to this trunk. Ports must be assigned continuously starting at 1.

- Not all number fields need to be completed. If a local area code is entered, a country code and the right national/international prefixes must be specified. In conjunction with the settings in **Routes ▶ Gateway groups**, they have a bearing on the flexibility of numbers which can be signalled.
- Diverted calls are signalled correctly when (inter)national prefixes and country code are entered correctly. The other fields have no bearing on diverted calls.
- Information on the status of ISDN ports is available on screen **Administration ▶ System status ▶ Interfaces** (→ p. 76)

SIP gateways

At least one SIP gateway must be set up. If the Installation Wizard is used for start-up, a SIP gateway is already available for the trunk line configured.

If you use an Internet phone connection, you require the access details from your provider (ITSP).

Help on setting up SIP accounts/trunks is available from:

https://teamwork.gigaset.com/gigawiki/display/GPPPO/ITSP+SIP+Trunking

If you use an analogue or ISDN trunk line, configure the TDM gateways (→ p. 47). For every configured TDM gateway (FXO or ISDN trunk), a SIP gateway is automatically set up with the default rules, and displayed on screen SIP gateways. It is normally not necessary to make further changes to the configuration. It may be necessary to change the **Dial command** parameter.

- **Administration ▸ Routes ▸ SIP gateways**

The SIP gateways already set up are displayed.

- Enter the name for a new gateway ▸ **Create new gateway**

Parameter:

Registrar	Registration server of the provider; **internal** is entered automatically for TDM gateways
Proxy	Proxy server (if used)
User	Use name as per provider specifications, e.g. call number
Password	Password as per provider specifications
Allow outbound calls	Enabled: calls may also be made over the gateway
Register	Enabled: the PABX makes contact with the provider to register the SIP account (mandatory for ITSP)
Language	Announcement language
Dial command	Format in which numbers are sent PJSIP/{prefix}{number:1}@{gateway} {prefix} – is replaced by parameter **Add prefix** if defined (→ Outbound routes, p. 61) {number:1} – **number** is replaced by the number dialled **:1** removes the first digit of the number selected, e.g. when 0 must be dialled first to get an outside line {gateway} – is replaced by the name of the SIP gateway Examples: PJSIP/{number}@{gateway} = dial without dialling for an outside line 0 Extension dials 05251 123456; "Calling SIP/05251123456@gw_1_siptrunk (SIP Trunk)" is sent PJSIP/{number:1}@{gateway} = dial with dialling for an outside line 0 Extension dials 0-05251 123456; "Calling SIP/05251123456@gw_1_siptrunk (SIP Trunk)" is sent PJSIP/{number}@{gateway} = dial in local network without local area code 05251 and dialling for an outside line 0 Extension dials 0-123456 "Calling SIP/123456@gw_1_siptrunk (SIP Trunk)" = invalid number is sent PJSIP/{prefix}{number}@{gateway} = dial in local network without local area code 05251 and dialling for an outside line 0 Prefix 05251 must be entered in outgoing routing. Extension dials 0-123456 "Calling SIP/05251123456@gw_1_siptrunk (SIP Trunk)" is sent

Transport name	A transport must be set up for each external connection to an SIP provider which determines the bind address and the bind port. For the popular VoIP providers, you can use the pre-defined SIP transports default-udp or default-tcp. For a secure provider connection, set up another SIP transport (→ p. 74) and assign to it the certificate required for the connection (→ p. 75).
Source of destination number	
	INVITE request line The destination number is taken from the **Invite** request made to the SIP server by the connection request. **To: header** The destination number is taken from field **To:** in the SIP header.
Group	Gateway group to which the SIP gateway is assigned (→ p. 54). A gateway can only be used once it belongs to a gateway group.
Port	Port number for SIP communication; Default 5060 (default SIP port)
NAT	
	Default setting: **Yes** Connection problems may arise if you connect the PABX to a router with NAT firewall. Try the following settings: **Force rport** Causes the SIP server to return a response to the source (IP address/port) of the connection request. **comedia only** Symmetric NAT traversal. Enables the PABX to determine address information (IP address/port) from received data packets of the destination subscriber. If the settings do not result in improvement, you may need to change the NAT settings of the router.
Reroute RTP stream	The PABX normally tries to take the direct path from Subscriber A to Subscriber B for the data flow (RTP). If the system needs to respond to input during a call (such as control from the key codes) or the devices are in a network behind a NAT firewall, the server must act as a proxy. This parameter is used to change the RTP data flow. Not enabled (default): Only divert the RTP media flow when the subscribers are not behind a NAT and this can be detected by the server. This means the PABX always acts as a proxy. The setting should not be changed. Enabled: The server tries to establish direct RTP data flow between the two partners.

Check availability	Enabled: The PABX checks whether a call is possible with SIP, i.e. whether there is Internet access and the SIP server is available. If yes, the connection is established over SIP, if not, the PABX tries to establish the connection via another gateway in the same gateway group (such as an ISDN connection).
Simultaneous calls	Number of calls which can be made over the gateway at the same time. Default: 0 = unlimited. Normally limited in the provider contract.
DTMF mode	DTMF signalling (Dual Tone Multi Frequency) is required for example to poll and control some network mailboxes and to control automatic information systems using digit codes. To send DTMF signals over VoIP, you must define how the key codes are converted to signals and sent. **inband - RTP audio** The DTMF tone is digitalised as a tone sequence and transmitted in the same way as speech. That means that it is not known which button was pressed. **info - SIP INFO application/dtmf-relay** The value (= key pressed) is sent as an SIP data packet. **rfc2833 - RTP meta data** The DTMF tone is analysed and its value packed and dispatched in a RTP packet. Ask your provider which type of transmission it supports.
From user	User name assigned by the provider. Often the same as the call number (parameter **User**), but can be different.
From Domain	Domain name of the provider, almost always identical to **Registrar**. This information is available from your provider.
T38 support	T.38 is a protocol for sending faxes over data networks. It has to be enabled for ISDN connections in order to transmit faxes via the gateway. This protocol must be supported by the provider.
Update P-Asserted-Identity (CLIP) (provider-dependent)	
	no - Deactivated (default) **Use P-Asserted-Identity header** The caller's number is set to PAI. This is advisable particularly for calls which are forwarded or diverted externally. The user's outgoing number can also be defined in the gateway group as PAI. However, the two options should not be used simultaneously.
Update remote party ID (CLIP) (provider-dependent)	
	no - Deactivated (default) When the provider expects the remote party ID in the header: **Use Remote-Party-ID header**

Trust remote party ID (provider-dependent)

no - Deactivated (default)
Do not trust the remote party ID for incoming calls

Trust Remote-Party-ID
Trust the remote party ID for incoming calls

The PABX copies the number from the **RPI** header (instead of from the **From** header).

Codecs (provider-dependent) The voice quality of VoIP connections is dependent on the voice codec used for data transmission, and so the bandwidth of your DSL connection (the better the codec the more data needs to be sent).

- Enable the voice codecs to be used by the gateway

Observe the specifications from your provider.

Priority when using codecs: from left to right, and top to bottom.

Allowed IP subnet

Specify the subnets to which calls are allowed.
Default: 0.0.0.0/0 all subnets are allowed

Format: IP address / subnet mask

The subnet mask determines how many bits of the IP address specified are included:

32 All bits are included
Example: 192.168.1.1/32, only IP address 192.168.1.1 may be called

24 The first 24 bits are included
Example: 192.0.2.0/24, all IP addresses in network 192.0.2.* may be called

16 The first 16 bits are included
Example: 192.168.0.0/16, all IP addresses in network 192.168.*.* may be called

8 The first 8 bits are included
Example: 192.0.0.0/8, all IP addresses in network 192.*.*.* may be called

> Information on the status of Ethernet ports is available on screen
> **Administration** ▶ **System status** ▶ **Interfaces** (→ p. 77)

Enhanced parameters:

Some SIP providers require a special configuration. If not all the parameters are available in the SIP gateway, you can enter more parameters here.

- In the **Value** field, enter a parameter such as inband_progress=yes ▶ +

Gateway groups

In a gateway group, you combine multiple gateways and define common rules for incoming and outgoing calls. At least one gateway group must be set up so the system can be used for making calls. A gateway (SIP, FXO or ISDN) must be assigned to a gateway group.

If the Installation Wizard is used for start-up, a gateway group is already set up with the default settings for the trunk line configured.

- **Administration** ▸ **Routes** ▸ **Gateway groups**

Gateway group

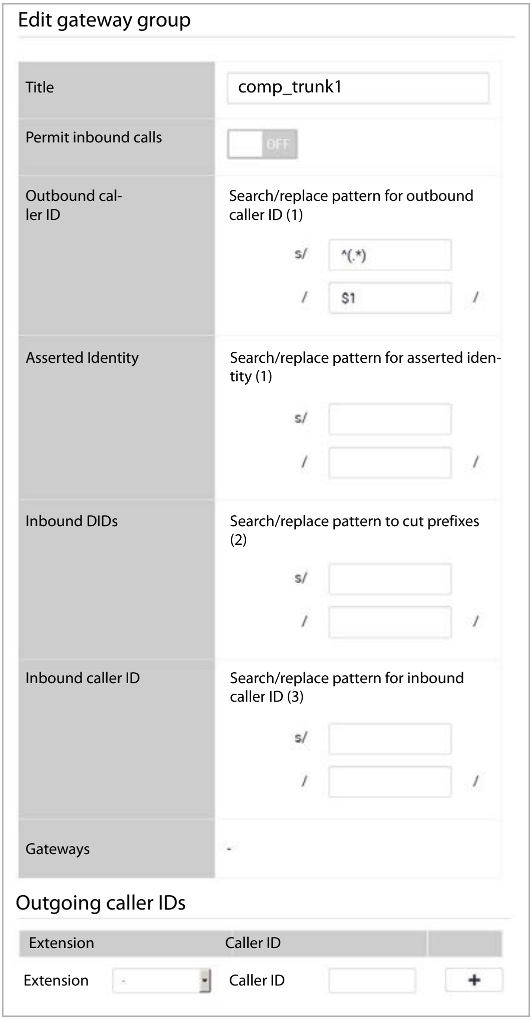
Gateway group	Gateways	Caller IDs		
comp_sip1 (comp-sip1)	2	0		
comp_sip2 (comp-sip2)	1	1		
			Create new group	

- Enter the name for the group ▸ **Create new group**

For the transfer of numbers to work correctly in the incoming and outgoing directions, the search/replace patterns for numbers must be changed in line with your location or the call number block provided.

The Installation Wizard defines default rules (depending on the specifications on setting up the trunk line). These can be changed as required.

Check the automatically created entries for the gateway group.



Help on testing the interoperability of your SIP trunk is available from:
https://teamwork.gigaset.com/gigawiki/display/GPPPO/ITSP+SIP+Trunking

Parameter:

Permit inbound calls	Enabled: calls may also be accepted over the gateway group
Outbound caller ID	Pattern for handling numbers for outgoing calls. The number replaced is sent to the called party. The caller can be called back on this number.
Search/replace pattern for asserted identity (1)	With some providers, the SIP header contains the caller's extension for identification (Asserted Identity). You use this parameter to specify what to do with this information for outgoing calls.
Inbound DIDs	Pattern for handling the prefix for incoming calls. Determines how an extension is forwarded internally, i.e. how the correct extension is reached.
Inbound caller ID	Pattern for handling the number for incoming calls. Determines the number on which the called party can call back the caller.
Gateways	Gateways belonging to the group. The gateways are only displayed here. They are assigned on screen **Administration ▶ Routes ▶ SIP gateways (→ p. 49)**

Outgoing caller IDs

In this area you can define more CLIP numbers with which outgoing calls from users are signalled.

▶ Select **Extension** ▶ Enter **Caller ID** ▶ ➕

Example: The user has extension 101, the trunk uses the last three digits in the range 750-759. The administrator can specify that user 101 uses 751 to make an external call. The incoming routing must be adjusted accordingly (→ p. 58).

Search/replace pattern

Numbers matching the pattern entered in the top field (s/) are replaced by numbers defined in the lower field. Regular expressions are used for the definition.

Examples of outgoing numbers:

The international format must be used to send all calls from all extensions.	
^(.*)	All numbers
00498912345678	are replaced by number 00498912345678 0049 or +49 can be used to specify the international format.
The company number is sent with local area code and extension	
^\d\d\d\d(\d)	Calls in format 12345, where 5 is used as variable $1
05251208$1	are replaced by number 05251208$1, $1 is replaced by the bracketed value of the search result

Examples of outgoing connection numbers (extension):

The connection number should not be sent.	
^(.*)	All connection numbers
	are replaced by nothing.
Connection number 10 (switchboard) should always be sent	
^(.*)	All connection numbers
10	are replaced by 10.
The number of the connection is sent.	
^(.*)	All connection numbers
$1	are sent

Example of prefix substitution for incoming numbers:

The last digit of the internal 3-digit number is replaced by a 1-digit extension.	
498912345678(\d)	Numbers in format 4989123456781, where 1 stands for a 1-digit extension and is used as variable $1
10$1	are replaced by 498912345678101.

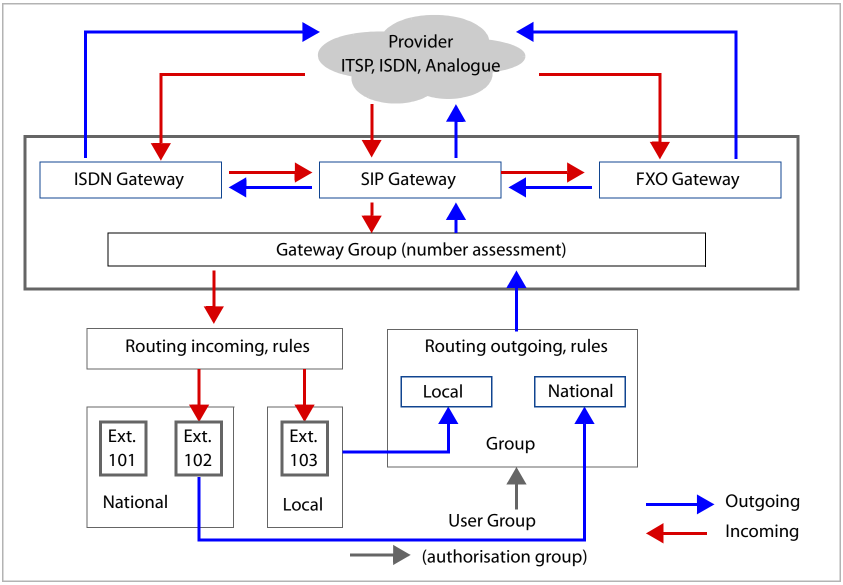
Examples of incoming numbers:

0 for dialling an outside line should be placed in front of incoming calls.	
^(\d*)	All incoming numbers, with the whole number used as variable $1,
0$1	are replaced by 0 + the number

An introduction to working with regular expressions is in the appendix (→ p. 79).

Routing

Routing specifies whether and how incoming and outgoing calls are forwarded to receiving parties through the system.



The routing for incoming and outgoing calls is already preconfigured by the Installation Wizard. For incoming calls, all recognised extension numbers from the gateway group are forwarded 1:1 by default as destination numbers.

Outgoing calls are passed 1:1 to the gateway group, and to the SIP gateway as per the gateway group configuration. For a TDM gateway with "dial for outside line" set for example, the SIP gateway sends the number to the exchange or TDM gateway in line with the variables in parameter **Dial command**. The leading "0" is removed there because it is no longer required (➜ p. 50).

Using the routing settings, you define rules according to which the forwarding of incoming and outgoing calls is to take place for certain times or people.

Inbound routes

For incoming routing, you specify for a gateway group what the process is for incoming calls under different conditions, such as calls having certain numbers and calls during normal business hours, on public holidays, at night, etc.

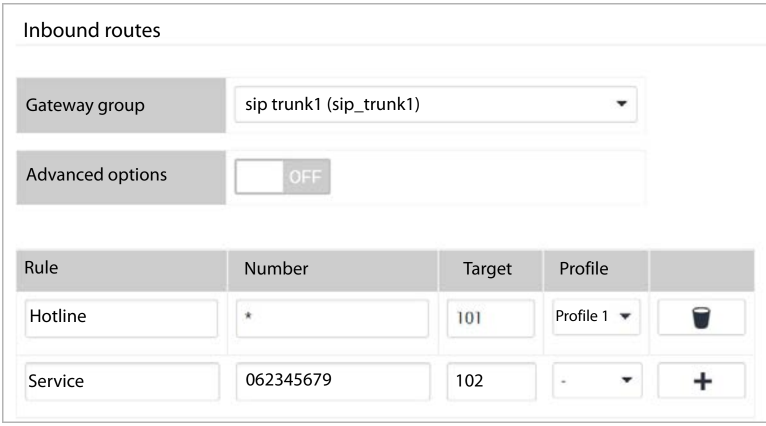
You can create up to 9 different profiles for every gateway group configured.

▶ **Administration ▶ Routes ▶ Inbound routes**

Diverting certain calls

The simplest form for incoming routing is diverting certain calls to a defined extension, e.g. an answering machine or secretariat.

▸ **Advanced options** = OFF



▸ Select required gateway group from the list

▸ Enter the name for the profile in the **Rule** field

▸ Enter the numbers of incoming calls to be actioned with this profile

▸ Enter as the **Target** the extension to which calls to this number are diverted

If you want to use the time-control: ▸ Select profile number (1-9)
If you do not select a profile for the time-control, all calls will be put through irrespective of the time (24/7).

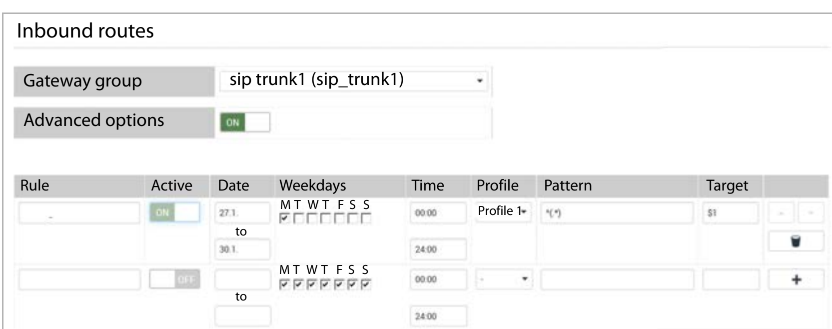
▸ **Save**

Time-controlled diverting of calls

With this you are able to specify different routes by business hours or public holidays.

▸ Select the required gateway group from the list

▸ **Advanced options** must be selected with the switch



- In field **Rule**, enter a name for the profile ▸ Select the profile number (1-9)
- **Date**, **Weekdays**, and **Time** must be specified for when the rule is to apply

  Example: Profile for weekday nights

Date	Leave fields free: the setting applies the whole year
Weekdays	Select all fields apart from **S** and **S**: the setting applies from Monday to Friday
Time	Enter 20:00 to 06:00

- **Pattern** and **Target**

  Incoming numbers can be routed to different destinations for local, national and international numbers depending on the search/replace pattern in the gateway group.

  Enter here the required pattern for analysing incoming numbers and forward it as the selected extension number to the destination.

  The transfer of the number to **Pattern** is dependent on the analysis of parameter **Inbound DIDs** in the gateway group (→ p. 56). A fixed internal number (extension) can be assigned as a destination.

  Example: Number 004989123456702 is selected. 00498912345670 is the number of the company, 2 the extension

  Configuration for **Inbound DIDs** in gateway group:

Search pattern	s/00498912345670(\d)	(\d) = $1
Replace pattern	/10$1/	10$1 = 102

  Incoming routing:

Profile	Pattern	Destination	Result
Day activation	^(.*)	$1	The call is put through to extension 102
Night activation	^(.*)	101	The call is put through to extension 101

- Enable/disable the rule with the **Active** switch. Enabled: The rule can be enabled in the **Night answer service** tab for users.
- **Save**

Night answer service

Enable/disable on this screen the profiles for incoming routing you have defined.

- **Administration** ▸ **Routes** ▸ **Inbound routes** ▸ **Night answer service**

Enable a profile for all users:

- Select the profile from list **Active Profile** ▸ **Save** . . . The rules of the profile are applied for all users

Users can choose another profile if this is allowed:

- Enable profiles 1 – 9 using the buttons

Enabled profiles are made available for selection by users.

- From the interface

  On the **Home** screen in the **Night answer service** area

- From the phone

  Activate: [*] [3] [8] [1] . . . [9] (for profiles 1-9)

  Deactivate: [*] [3] [8] [*]

> Users wanting to use it from the phone must belong to a user group with **Set night answer service** authorisation.

Outbound routes

For external routing, you specify which users (or user groups) may dial which external numbers, and how numbers are put through for outgoing calls.

After start-up with the Installation Wizard, outgoing routing is set such that every user can make unrestricted calls to anyone 24 hours a day every workday, regardless of their user / user group.

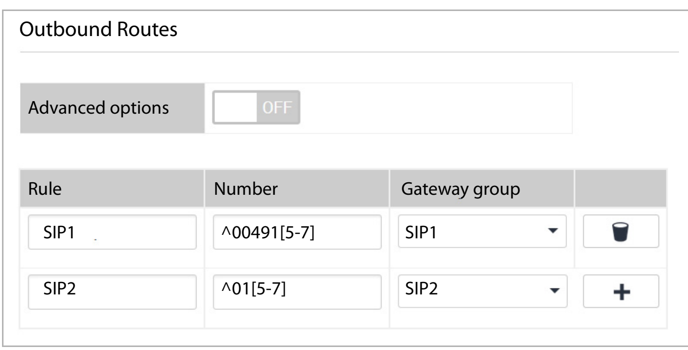
Additional rules must be defined if you want to limit this. You may want to specify for example that certain parties may only make calls, or call at certain times, in their own local area network, nationally or internationally. You can also ensure for example that emergency calls can be made from all phones, regardless of whether the parties are registered or not.

▶ **Administration** ▶ **Routes** ▶ **Outbound routes**

Simple outgoing routing to certain number

The simplest form of outgoing routing is diverting certain outgoing calls, such as calls to mobile numbers, through another gateway.

▶ **Advanced options** = OFF



▶ In field **Rule**, enter a name for the rule

▶ Enter the number

▶ Select the gateway from the list under **Gateway group** to be used for routing these calls. All SIP gateways configured are shown.

▶ **Save**

User group-dependent settings for outgoing calls

Outgoing calls can, depending on the authorisation group to which a user belongs, be restricted to certain times and numbers.

- **Advanced options** must be selected with the switch

- Enter the rule name in field **Rule**
- Specify **Weekdays** and **Time** for when the rule is to apply

  Example: Profile for weekday nights

Weekdays	Select all fields apart from **S** and **S**: the setting applies from Monday to Friday
Time	Enter 20:00 to 06:00

- In the **Pattern** field, specify the number which can be dialled

  Examples:

  ^[1-9] = only numbers within the same local area network, no area code

  ^0[1-9] = only national numbers
- Select the authorisation group for which this rule is to apply. Users must be assigned this authorisation group → p. 27).
- Select the gateway(s) from the lists under **Gateway group** to be used for routing these calls. All SIP gateways configured are shown.
- The number specified in field **Add prefix** is placed before the number dialled if the dial command defined for the SIP gateway contains variable {prefix} **(**→ p. 50).
- Enable/disable the rule with the **Active** switch.
- **Save**

Example:

User **Greg Dalton** may make calls to his own local area network (089 for Munich in the example), but not national or international calls.

The following settings are necessary:

- **Greg Dalton** is assigned to user group **Local (**→ p. 22)
- User group **Local** is identical to authorisation group **Local** (→ p. 27)

- On screen **Outbound Routes**, set up two rules with name **Local**
  Rule 1: the user dials with area code
  Pattern ^089 = numbers to the local area network with code 089 are allowed
  Rule 2: the user dials without area code
  Pattern ^[1-9] = Numbers with no dialling code are allowed
  All other numbers dialled are rejected (engaged tone).
  For both rules, assign group **Local** to the SIP gateway over which calls are to be routed. The associated gateway group determines the format of the number send.

> The rules defined are evaluated from top to bottom.
> Changing the order: ▶ Use the ▲ ▼ buttons on the right of a rule to move it up or down. The buttons are displayed as soon as more than one rule is defined.

Call diverts

Calls to extensions from a queue or hunt group are forwarded by default according to the rules specified for the queue or hunt groups.

This menu allows call diverts to be set up for certain cases or times.

> Currently, queues, collective lines and connections with voice menus can only set internal destination numbers for call divert. A user name, which has to be set up specifically for this purpose if necessary, must be used to divert a call to an external number,

Call divert for queues

Prerequisite: Queues must be set up (→ p. 35).

▶ **Administration** ▶ **Routes** ▶ **Call forward** ▶ **Queues**

The screen shows all queues set up with extensions and names.

▶ Click next to the queue for which you want to set up a divert

Destination numbers for call forwards

▶ Specify the destination numbers (internal) for the call divert. These numbers can then be used in the rule.

Default number
Number to be used mainly for call divert, e.g. always for external calls

Temporary number
Number to be used for call divert in special cases, e.g. for internal calls when nobody is in the queue

VM number (internal user)
A user's extension with an answer machine.

Specify rules for call divert

Forward ...

	always	full	timeout	empty
internal	-	Temporary number	Announcement 3	Temporary number
external	-	Announcement 2	AM with announcement 1	Default no.
			after (s) 15	

- Setting up rules separately for internal and external calls:

  When is call divert to apply?: ▶ Configure the settings in the required column. You can define call diverts in one, multiple or all columns.

always	All calls are diverted
full	Call divert when all extensions in the queue are busy
timeout	Call divert when no agent picks up within the time specified ▶ In the field next to **after (s)**, specify the time (in seconds) after which call divert is to apply
empty	Call divert when no agent is registered with the queue

  To where is the call diverted?: ▶ Select in each case the required destination from the selection menu

Default number	Divert to **Default number**
Temporary number	Divert to **Temporary number**
AM with announcement	Divert to the answering machine of the extension specified under **VM number (internal user)**. The caller hears the selected announcement and is able to then leave a message.
Announcement	The caller only hears the announcement selected and cannot leave a message

Uploading/recording announcements for the answering machine

You can upload/record multiple announcements, which are then available for selection for the destinations **AM with announcement** and **Announcement**.

- In the **Comment** field, enter a name for the announcement ▶ Click ... The announcement is entered in the list
- Click ▶ Select an audio file from the computer file system or the network . . . The file name is entered in the text field ▶ Click **Upload** . . . the file is uploaded

or

- Click **record** . . . The phone with the extensions of user name **Admin** rings ▶ Pick it up ▶ Say the announcement ▶ Press

Saving settings / enabling call divert

- Click **Save** . . . The call divert set for the queue is enabled

Call divert for hunt groups

Prerequisite: Hunt groups must be set up (→ p. 25)

- **Administration ▶ Routes ▶ Call forward ▶ Hunt groups**

The screen shows all hunt groups set up with extensions and names.

- Click next to the hunt group for which you want to set up a divert

Destination numbers for call forwards

- Enter the number ▶ +

  Specify as many destination numbers (internal) as you require. These numbers can then be used in the rule.

Specify rules for call divert

Forward ...

	always	busy	no answer
internal		Number 2	Number 3
external	Number 1		

- Setting up rules separately for internal and external calls:

  When is call divert to apply?: ▶ Configure the settings in the required column. You can define call diverts in one, multiple or all columns.

always	All calls are diverted
busy	Call divert when all the hunt group extensions are busy
no answer	Call divert when no hunt group party can be reached

  To where is the call diverted?: ▶ Select in each case the required destination number from the selection menu

- Click **Save** . . . The call divert for the hunt group is enabled

System

You will receive a message if changes made to the system settings require the PABX to be restarted.

Licensing

▶ **Administration ▶ System ▶ License**

Once you have successfully performed the licensing process for the PABX (→ p. 13), you can see the license code on this screen.

Firmware updates

Gigaset makes available new firmware versions as required on http://wiki.gigasetpro.com. They can be loaded and installed from this screen. You receive email notifications as required about new firmware versions.

The configuration of your PABX is not affected by firmware updates. To be on the safe side however, perform a backup before loading new firmware (→ p. 72) and store it on an external device.

Check before an update from version 1.x.x. to version 2.x.x. that the used provider has been re-certified. Go to https://teamwork.gigaset.com/gigawiki/display/GPPPO/ITSP+SIP+Trunking to find tested providers.

Always read the release notes for new firmware.

▶ Download the latest firmware from the Gigaset server and save it to the PC

▶ **Administration ▶ System ▶ Update**

Installed version shows the version number of the current firmware

▶ Click next to **Choose update file** ▶ Select the file from the file system of the computer . . . The file name is entered in the text field ▶ Click **Upload & install** . . . The firmware file is loaded and installed

Upload progress shows the progress of the installation.

The Login screen is shown once the installation is complete. All the configuration settings are kept as they were.

Do not close the browser window during the firmware update (it takes approximately 3 to 4 minutes).

Updating from a version older than V1.0.9. to a current version takes considerably longer (approximately 15 minutes). The switch on the front of the device restarts several times. For more information see the Release Notes for the software in question.

CDRs

All outgoing calls are listed on the **CDRs** (Call Data Records) screen.

▶ **Administration** ▶ **System** ▶ **CDRs**

Information on all calls currently being displayed:

Calls:	Number of calls displayed
Total call duration:	Total duration of calls displayed
Average call duration:	Average duration of calls displayed
Duration:	Total duration of calls, including ring time

The following information is displayed for every call:

Time	Date and time of call
Caller	Caller's extension
Target	Number called
Duration (s)	Call duration
Type	Shows whether a call took place, and if not why not: ● **answered**, ● **no answer**, ● **busy**, ● **failed**

Filtering lists

To evaluate CDRs by certain criteria, you can filter the list by **Time**, **Caller**, **Target**, **Duration (s)** and **Type**. It is possible to specify multiple filters. For call numbers, subsets can also be selected using * (e.g. 043*, i.e. all numbers starting with 043).

▶ Select filter criterion from the options lists / enter it in the fields ▶ Click 🔍 . . . Only the entries appropriate for the filter are displayed

Exporting the list

To process further CDRs, you can export the list displayed to your PC or storage medium as a CSV file. The specifications are as those for the contact list export (→ p. 33).

▶ Select the type of list formatting: **Encoding** (UTF or ISO) and **Separator** (**Semicolon** or **Comma**) must be selected, and enable/disable **Header**

▶ Click **Download CSV** ▶ Specify the destination and save

Network

If you ran the Installation Wizard all the way through when setting up your PABX, network configuration is already complete. You can make changes here if you wish.

The following values are taken as defaults if you have not yet performed a network configuration:

IP address	192.168.0.50
Network mask	255.255.255.0
Default gateway	None
DHCP server	Enabled
DHCP address range	192.168.0.100 - 192.168.0.150

Your PABX must be integrated into your local network for it to work properly.

> Changes to the network configuration can trigger a restart.
>
> Changing the network configuration may result in the link between your computer and the PABX going down. You will then not be able to access the user interface. In this case, you must restore access using the new IP address.
>
> If you make a mistake and the PABX can no longer be accessed from the network, connect your computer directly to the PABX (→ p. 6).

IP configuration

▶ **Administration ▶ System ▶ Network ▶ IP configuration**

Parameter:

IP address	IP address for your PABX. It must be assigned a fixed (static) value. The following must be observed: ◆ The IP address must be from the address range used on the router/gateway for the local network. The valid address range is determined by the IP address of the router/gateway and the network mask (see example). ◆ An IP address must be unique across the network, meaning it may not be used by another device connected to the router/gateway. ◆ The fixed IP address may not belong to the address range reserved for the DHCP server of the router/gateway. Check the settings on the router or ask your network administrator. Example: Router IP address: 192.168.2.1 Network mask in network: 255.255.255.0 DHCP server address range: 192.168.2.101 – 192.168.2.255 Possible IP addresses for the phone: 192.168.2.2 – 192.168.2.100
Netmask	The subnet mask specifies how many parts of an IP address the network prefix is made up of. 255.255.255.0 for example means that the first three parts of an IP address must be the same for all devices in the network, whilst the last part is specific to each device. For subnet mask 255.255.0.0, only the first two parts are reserved for the network prefix. Enter the subnet mask used by your network.
Default gateway	The IP address for the standard gateway through which the local network is connected to the Internet. Generally speaking, that is the local IP address of the router/gateway.

DNS Server (optional)	IP address of the DNS server The DNS (Domain Name System) allows you to assign IP addresses to symbolic names. The DNS server is required to convert the DNS name into the IP address when a connection is being established to a server. By default, the router/gateway's IP address is used here. This forwards PABX address queries to its DNS server. You can enter the IP address of an alternative DNS server in the second field **DNS Server (optional)**. This is used when the first DNS server cannot be reached.
NTP Server (optional) IP	IP address of the time server (NTP = Network Time Protocol). NTP ensures reliable time information across a network. You can enter the IP address of an alternative time server in the second field **NTP Server (optional) IP**. This is used when the first time server cannot be reached.
Host name	Host name for the PABX
Domain name	Name of the domain in which the PABX is located.

The last two options are only used for Window/Linux network identification and have no effect on the parameters used in the PABX.

DHCP server

The PABX has an integrated DHCP server, which is enabled on delivery and has an address range appropriate for the network mask set. If you want to use another DHCP server in your network, you must disable the one in the PABX. Running two DHCP servers in parallel in a network is not permitted.

▶ **Administration** ▶ **System** ▶ **Network** ▶ **DHCP server**

When you do not use the integrated DHCP server:

- Disable the DHCP server from the **ON**/**OFF** switch
- Enter the IP address of the PABX on which the DHCP server is running on the **IP configuration** screen. Define this IP address on the DHCP server as a static address for the PABX.

When you use the integrated DHCP server:

- Disable other DHCP servers in your network
- Enable the DHCP server from the **ON**/**OFF** switch
- Specify the address range such that it fits in with the other network settings, i.e. with the subnet mask and any IP addresses with a fixed assignment

Usually, a broadcast call-up is used for SIP multicast provisioning in the network. The telephones then receive the provisioning URL of the PABX via a broadcast response. If this is not possible in your network, you can use DHCP option 114.

- On the DHCP server, set option 114 (URL) as follows:

  http://<IP address of the PABX>/gigaset-prov/

  This option ensures that the PABX is set as a provisioning server on all phones. How this option is set depends on the system on which the DHCP server runs.

  Example for a Linux DHCP server:

  File dhcpd.conf: option dhcp_114_FW_URL "http://192.168.0.50/gigaset-prov/"

If there are any devices in your network with a fixed IP address, you must ensure these addresses are outside the address range of the DHCP server.

SMTP server

Using an integrated SMTP server, your Gigaset PABX emails to users voice mails, faxes, backup files, backup reports and other system messages (such as changes to user data by Administrators). You must configure the SMTP server of the system for this.

- **Administration ▸ System ▸ Network ▸ Email delivery**

Parameter:

Email delivery	Enable/disable SMTP server
Sender email address	Email address of sender. Default is noreply@localhost
Sender name	Name of sender. Default is Galilei PBX
SMTP server	IP address of SMTP server.
SMTP port	Port over which the SMTP server communicates. Default setting: 25
SMTP authentication	Enable/disable SMTP authentication. Enabled: The SMTP server expects "login" of the sender before emails are sent. Entering of a user name and password is used for this.
SMTP user name	User name for SMTP authentication
SMTP password	Password for SMTP authentication

SMTP authentication type	The following methods are possible for authentication on the server: **PLAIN**: Standard RFC 4616. User name (for authorisation), user name (for authentication) and password are sent unencrypted. The three strings are merged into one and Base64-encoded. **LOGIN**: As PLAIN, but authorisation and authentication are in two steps. **CRAM-MD5**: Standard RFC 2195 **SCRAM-SHA-1**: Standard RFC 5802 **NTLM**: Secure authentication method with encryption using random number.
SMTP transport type	Determines the security standard for sending **plaintext**: no security **SSL/TSL**: Security standards with data encryption. TSL is based on SSL and is the standard with higher security.

Fax

You can enable a Fax Service (Hylafax) for the PABX, and enter the relevant numbers. The PABX supports SIP protocol T.38, enabling the sending of faxes over (data) networks. The T.38 protocol must be enabled for the SIP gateway over which faxes are to be sent/received (➔ p. 52).

- **Administration** ▶ **System** ▶ **Fax**
- Enable/disable the fax service from the **ON**/**OFF** button
- **Fax prefix (incoming)** and **TSI prefix (outgoing)** must be entered
- **Additional TSIs:** Enter any other numbers, clicking + every time
- Save the settings with **Save**

> Enabling the fax service automatically causes a system restart.
>
> Users can use one of the TSIs specified here to send faxes. The TSI (Transmitting Subscriber Identification) identifies a fax device as a sender of a fax and is normally displayed at the top of a fax received.
>
> Consult the provider certifications at https://teamwork.gigaset.com/gigawiki/display/GPPPO/ITSP+SIP+Trunking for more information about fax compatibility.

Date & time

The current system date and time are displayed and can be changed manually as required. They cannot be changed manually if you are using an NTP server (➔ p. 69).

- **Administration** ▶ **System** ▶ **Date & Time**
- Enter date (**Day**, **Month** and **Year (4 digits e.g. 2014)**) and time (**Hour**, **Minute**) in the relevant fields ▶ **Save**

System settings

The **System settings** screen gives you many ways to change the basic system settings. The parameters are grouped in different tabs depending on function.

▶ **Administration** ▶ **System** ▶ **System settings**

Every parameter is displayed with name, set value and description.

Changing a parameter:

▶ Open the tab for the function whose parameter you want to change

▶ Change the parameter. ▶ Click .

The symbol is displayed for all parameters you change.

Resetting a change

▶ Click

Saving changes:

A bar is shown above the list provided there are changed parameters on a screen:

There are uncommitted values. Click to view

▶ Click **Click to view**. The changed parameters are listed with old and new values.

▶ **Confirming a change:** ▶ Click **Commit**

▶ **Rejecting a change:** ▶ Click **Revert**

Backing up and restoring the system

Perform regular backups of the data and system settings of your PABX. You can backup the data manually at any time or create a schedule for regular, automatic backups. Backup files are kept in the file system of the PABX. They can also be backed up to external storage manually. The backup files contain all the data and system settings of the PABX.

> If you wish to restore the system from a back up file after having reset the factory settings (→ p. 78) the back up file must be available on external storage.

Automatic backup

▶ **Administration** ▶ **System** ▶ **Backup** ▶ **Automatic backup**

The **Automatic backup** screen enables you to plan automatic system backups. You can have backups made every week on certain weekdays, or every month on certain days.

▶ Enable/disable automatic backup with the **Automatic backup enabled** switch ▶ Select **Weekly Schedule** or **Monthly Schedule**

When Monthly Schedule is selected:

- Specify time: ▶ In field **Days (comma separated)**, specify the days for the backup
  Example: Time = 00:30, **Days (comma separated)** = 1,10,20
  A backup is made on the 1st, 10th and 20th of every month at 0.30.

When Weekly Schedule is selected:

- Specify time. ▶ Use the switches to activate the days on which a backup is performed

Manual backup

- **Administration** ▶ **System** ▶ **Backup** ▶ **Manual backup**
- Click **Trigger backup**

The backup file is created as an archive file and stored in the file system of the PABX. The file name contains the time and date of the backup
(example: galilei-backup-20141118-144301.tar.gz).

Saving a file to an external location

- Click **Download backup file** ▶ Select the destination and save

> All backup files are available to download, including those created automatically.

Restore

Backup files created manually or with regular backups can be loaded back onto the system if required.

- **Administration** ▶ **System** ▶ **Backup** ▶ **Restore**

All backup files on the phone system are made available. The most recent file is at the bottom.

- Click **Upload** next to the file name

Restoring the system from a backup file stored externally:

- Click next to **Choose backup file** ▶ Select the file from the file system of the computer or network . . . The file name is entered in the text field ▶ **Upload**

> The process can take a while.
> Settings and information changed since this backup are lost.
> The Login screen is shown after the system is restored successfully.

SIP Transports

Every external connection to a SIP provider requires a transport which defines the bind address and the bind port.

▶ **Administration ▶ System ▶ SIP Transports**

A UDP and a TCP transport are pre-configured. The default value for the address is 0.0.0.0 for port 5070. These values can be used as default for the certified providers (➔ p. 49). Do not use port 5060 as this could conflict with the device registration.

If you use TLS encryption for connecting to the provider, you can select and verify the uploaded certificate here.

Setting up transport

▶ Enter the transport name ▶ Click + ▶ Enter parameter ▶ **Save**

Parameter:

Transport name	Name of the transport
Transport bind ip	IP address for the binding. 0.0.0.0 can create a binding with any IP address.
Transport bind port	Port, on which the PABX expects SIP queries from the provider (listen port).
Transport type	Used transport protocol: UDP, TCP or TLS (encrypted transmission via TCP)
External media address	External IP address for RTP handling.
External signaling address	External IP address for SIP handling.
External signaling port	External port for SIP signalling.

If TLS is used as a transport type:

Verify certificate	Enabled: When a connection is established, the certificate selected under **CA certificate** is verified.
CA certificate	Certificate for the connection to the provider. The certificate must be downloaded in advance (➔ p. 75).

Modifying parameters for a SIP transport

▶ Click next to the transport entry.

Removing SIP transport

▶ Click next to the transport entry.

SSL certificates

An SSL certificate uses encryption to create a secure connection. Each SSL certificate contains a key pair made up of a public and a private key. The private key contains the code for encryption and is only known to the owner, the public key contains the information for decryption and is made available to the communication partners on the network.

If you use TLS-encrypted connections to the provider, you must upload the SSL certificates this requires into the PABX. You can assign imported certificates on the **SIP Transports** screen (→ p. 74).

▶ ⚙ **Administration** ▶ **System** ▶ **Certificates**

Certificates that have already been imported are listed here.

Importing new certificate

- ▶ In field **Description**, enter a description for the certificate.
- ▶ Click 📁 next to **Private key** / **Public key** ▶ Select private/public key file from the file system of the computer or the network ... The file name is entered in the text field
- ▶ Click **Import** ... The certificate is imported

Status and diagnostic information

The **System status** menu has detailed information on the status of the PABX, the connections and interfaces, and diagnostic information. You can restart or shut down the system if required.

General information

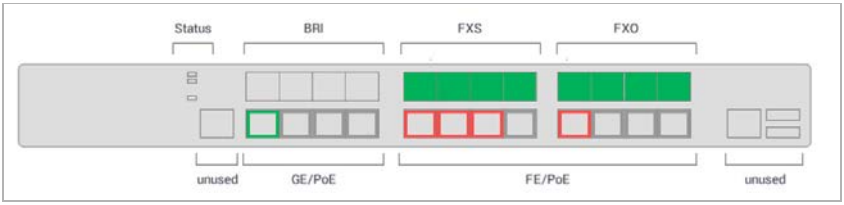
▶ **Administration ▶ System status ▶ General information**

General information: **Software version**, **Licence state**, **System date and time**, **System uptime**, **CPU load**, **Memory state**, **Disk state**, **Number of users**, **Number of phones**

Interfaces

▶ **Administration ▶ System status ▶ Interfaces**

The screen shows on a diagram the status of the PABX interfaces (connections).



Information on ISDN connections: BRI (digital modules)

Disabled	Not connected.
Active - OK	Connected and ready.
RAI alarm	Remote Alarm Indicator: is sent by a terminal when the input signal is lost.
LOS/LOF alarm	LOS (loss of signal): Fault message when a network component ascertains the loss of the input signal. LOF (loss of framing): Fault message when an ATM receiver station loses the frame description. It is used to monitor the performance of the bit transmission layer in frame-oriented networks.
AIS alarm	AIS (Alarm Indication Signal): Fault message when a transmission error is detected in the transmission channel, or a fault message is received by another unit on the transmission path.
D-channel alarm	Fault on the D-channel (used to transmit control information).
NFAS alarm	NFAS (Non-Facility Associated Signalling): Signalling protocols sent over a link completely independent of the carrier channel.

Information on the analogue connections: FXS/FXO (analog modules)

	Not connected	Not connected
	Idle	Connected, currently no connection
	Handset offhook	Receiver picked up
	Call connected	Connection established

FXO ports are only available for the Gigaset T640 PRO.

Information on Ethernet connections: Power over Ethernet (PoE)

	Not connected	Not connected
	Ethernet connected	Connection to Ethernet
	Power connected	Interface powering connected PoE device
	Ethernet and power delivered	Connection to Ethernet and power over PoE

SIP-Status

The screen provides information on the registered SIP connections.

The following are displayed for every registered connection:

SIP connection:	User name, refresh status, registration time and whether the DNS manager is enabled.
PJSIP connection:	Gateway name, server URL, status

Diagnostics

The diagnostic screens show the protocols created by the system. They may prove useful in the event service is required.

▶ **Administration ▶ System status ▶ Diagnostics**

The following protocols are available:

System log	Messages of the media server processes
Telephony	Messages on PABX activities
Operating system	Messages from the Linux operating system, e.g. boot information
Intrusion detection	The screen shows detected intrusion attempts into your system with the following information (where possible): **Date**, **Time**, **Jail**, **IP address**, **Description**

Blocked IP addresses are automatically removed from the list after 24 hours.

Reboot & shutdown

- **Administration** ▸ **System status** ▸ **Reboot & shutdown**

Restarting the PABX:

- Click **Reboot** . . . The system is restarted. It takes about 2 minutes and phoning is not possible during this time. All the configuration settings are kept as they were.

Shutting down the PABX:

- Click **Shutdown** . . . The system is shut down. Phoning is no longer possible.

> The PoE switch and fan remain ON.

Resetting the PABX to the default settings:

- Click **Factory reset** . . . The system is shut down and restarted with the default settings. All your configuration settings are lost, but can be restored from a backup file (→ p. 73).

> The back-up file must be on external storage.

Appendix

Regular expressions

Regular expressions are used in the PABX configuration to:

- formulate search and replace patterns for call numbers. For incoming or outgoing calls, searches are performed on equivalents of the search pattern - places found are replaced by others. They define how numbers are sent, how sent numbers are displayed and how they are used for return calls.
- define patterns for call numbers for which certain rules are to apply, e.g. for which special authorisations are assigned or which are diverted at particular times.

There are different "languages" for regular expressions, for which comprehensive syntax rules are defined. The PABX uses Perl Compatible Syntax Expression (PCRE).

> The syntax of regular expressions is very extensive and complex. Only a few elements are required for the PABX configuration. Only the main syntax elements used in the search and replace patterns for numbers are described here.
>
> Please refer to the relevant Internet sites for more information.

<table>
<tr><td>.</td><td>Any character</td></tr>
<tr><td>\d</td><td>Any digit</td></tr>
<tr><td>\D</td><td>Any character (not digit)</td></tr>
<tr><td>*</td><td>The preceding element may occur any number of times</td></tr>
<tr><td>?</td><td>The preceding element may occur but need not</td></tr>
<tr><td>+</td><td>The preceding element must occur at least once</td></tr>
<tr><td>^(pattern)</td><td>Searches for the expression defined in the pattern from the start of the string
Example: ^(.*) = Finds any call number
^ = Start of the string, . = Any character,
* = Any number of times</td></tr>
<tr><td>|</td><td>Sequence of alternatives
Example: 0049|0 = Either 0049 or 0</td></tr>
</table>

<table>
<tr><td>( ) Round brackets</td><td>Grouping of search patterns when multiple expressions are in a sequence or nested. Resolution is from the inside outwards.

Example: (((0049|0)89)3450) stands for 0049893450 or 0893450

Matches of groupings found are stored and can be reused for substitution (backward reference). A grouping is referenced with $n, where n is the position of the grouping within the whole expression.

Example for outgoing calls: Search pattern ^(.*), replace pattern 0$1

= "0" is placed in front of any number</td></tr>
<tr><td>?:(pattern)</td><td>Groupings not generating a backward reference

Example: (?:(?:0049|0)89)?3450 Pattern identical to the last pattern but no referencing possible</td></tr>
<tr><td>[ ] Square brackets</td><td>Alternatives; one of the characters in the brackets must be in the string

Example: [0-9][a-z] stands for exactly 1 digit from 0 to 9, and one character from a-z, e.g. 3a, 5c, 9z...

A difference is made between upper and lowercase.

Note: [0-9] is identical to \d</td></tr>
<tr><td>{ } Curly brackets</td><td>{Minimum, maximum} number of characters/digits

Example: [1-9][0-9]{1,4} stands for at least 1, and a maximum of 4 digits; the first digit may not be 0.</td></tr>
<tr><td>\ Special designation</td><td>If a string contains a regular expression also used as a meta character, it must be denoted specially using a preceding backslash \. This designation is required for:

^ $ ( ) < > | { [. * + ? \</td></tr>
</table>

Index

K

L

M

N

O

P

Issued by
Gigaset Communications GmbH
Frankenstr. 2a, D-46395 Bocholt

gigasetpro.com

A31008-N2003-R103-2-7620