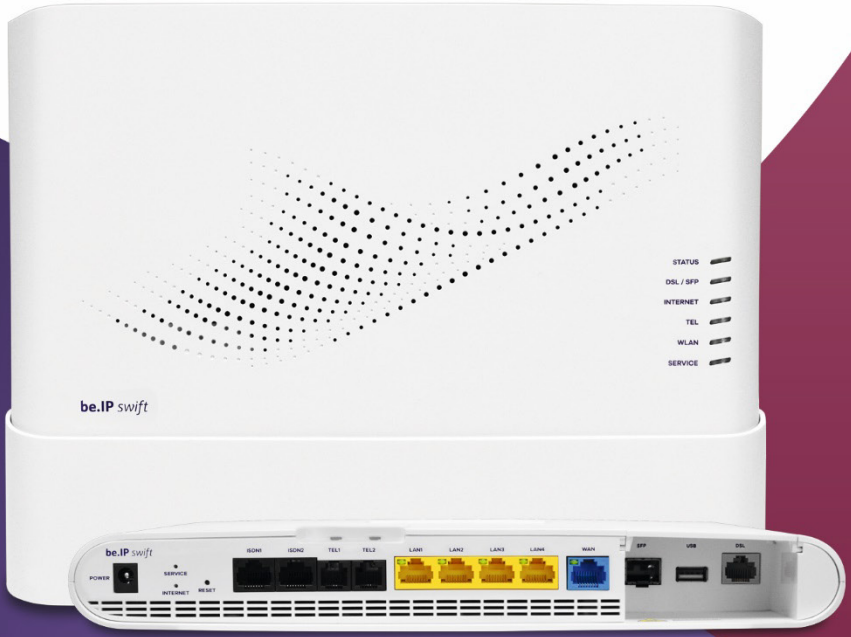
USER MANUAL
be.IP *swift*



Contents

User manual

be.IP *swift*

1 Welcome!

These instructions describe **with examples** the installation and initial setup of the **be.IP swift** for operation on a Telecom DSL port with the help of configuration wizards.

Additionally the following documents are available at *archive.bintec-elmeg.com*:

- *Advanced configuration:* This manual describes the configuration options for the menus that you can access via the **Show more** link in the main menu.
- *Operation via the telephone*: This document explains how, when operating as a telephone system, you can also control many functions using shortcuts on a connected telephone.

Video instructions for special setup tasks can be found at *helpcenter.bintec-elmeg.com.*

Important
Read these instructions carefully before using the router and keep them for future reference. If necessary, pass these instructions on to a new owner of the device.
Observe the safety instructions at the end of this document!

1.1 Scope of delivery

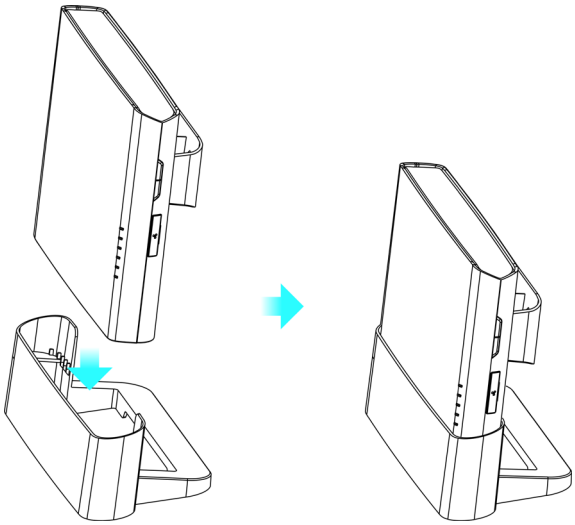
Unpack your **be.IP swift** and check the package contents for any missing parts:

- **be.IP swift**
- Stand
- Plug-in power supply unit
- DSL cable RJ45-TAE
- Network cable RJ45-RJ45
- Wall mounting bracket

Check whether the components have been damaged during shipping. If this is the case, do not put the router into operation and contact your supplier.

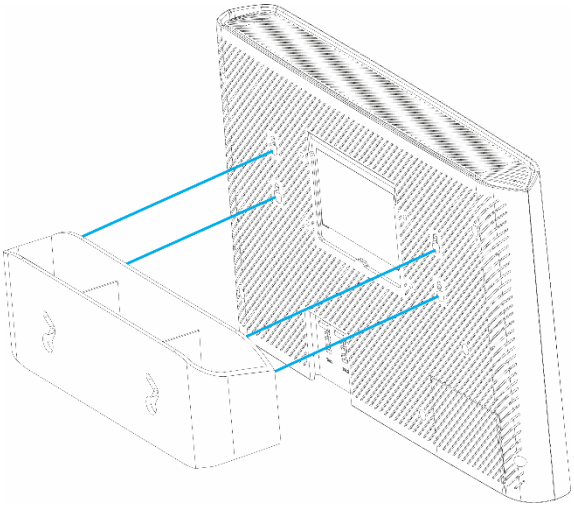
2 Router installation

2.1 Standing (table)

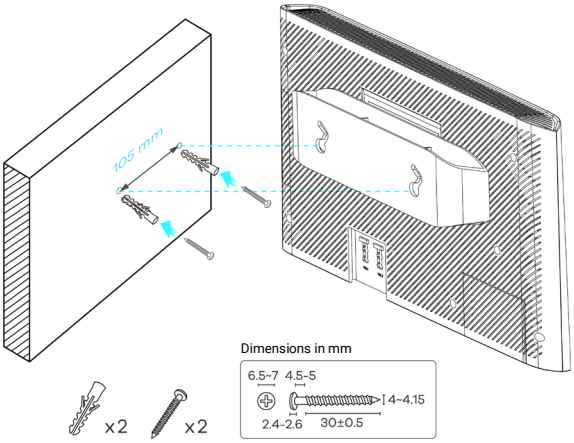


2.2 Wall mounting

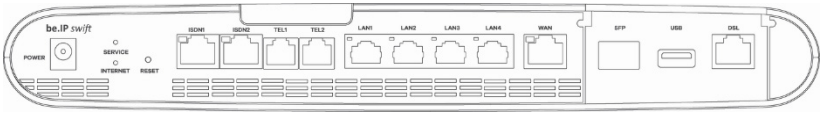
1. Attach the wall mounting bracket.



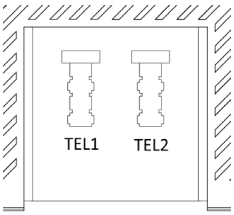
2. Attach the dowels and mount the router.



3 Putting be.IP swift into operation



Ports on the bottom



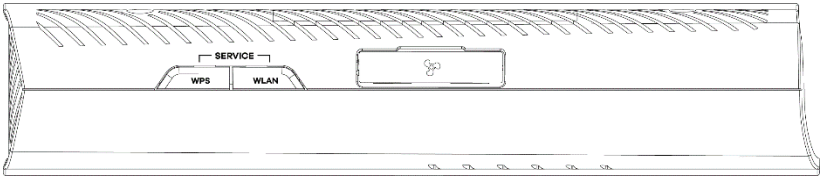
Ports at the rear

1. Connecting DSL
   Take the gray DSL cable (RJ45-TAE) and plug the RJ45 connector into the gray socket labeled **DSL** on your **be.IP swift**. Insert the TAE plug of the cable into the middle socket labeled **F** or ☎ on the telephone home connection (telephone socket).
2. Connecting analog telephones
   Take the telephone plug (TAE plug) of your DECT base station (or analog telephones) and plug it into the socket labeled **TEL1** or **TEL2** on the back of the router. Alternatively, you can also connect telephones via the black RJ11 sockets labeled **TEL1** or **TEL2**.
3. Connecting ISDN terminals
   You connect your ISDN telephones or your existing ISDN telephone system via the black RJ45 sockets labeled **ISDN**. To connect up to eight ISDN terminals (including a maximum of four telephones), please use an additional ISDN distributor.
4. Connecting IP telephones
   Wired IP telephones are connected via the yellow **LAN** sockets.
5. Connecting computers via LAN sockets

6. Take the network cable included in the scope of delivery and use it to connect your terminal device, such as notebook, media receiver or NAS, with the **be.IP swift**.
7. Connecting the power supply
   Insert the plug of the supplied power supply unit into the socket labeled **Power** on the **be.IP swift** and the power supply unit into a 230 V mains socket. The **STATUS** LED initially lights up red for 25 seconds and then starts flashing green. A steady green indicates completion of the startup process.

3.1 Connecting devices to the WLAN

The WLAN function of the **be.IP swift** must be switched on. Check the **WLAN** LED on the front panel. It must light up green continuously. If it is not lit, briefly press the **WLAN** button on the **be.IP swift**. The **WLAN** LED starts to flash green and lights up permanently after approx. 15 seconds.



Position of the WLAN and WPS buttons on the side of the router

Activating the WPS button

For security reasons, the **WPS** button, which facilitates quick connection of WLAN devices, is disabled when the device is delivered. To enable it, go to the **WLAN > Show more > Advanced WLAN settings > WLAN > 2.4 GHZ / 5 GHz** menu in the configuration interface and confirm the **Enable WPS Push Button** option. You have to make a setting for each frequency band.

Connecting devices under Windows 10/OS X

1. Click on the WLAN icon in the start bar.
2. Select the WLAN name of your router and click **Connect**.
3. Enter the WLAN password in the **Enter network key** input field or press the **WPS** button.

Connecting devices running Android or iOS

For smart phones and tablets running Android 5.x or iOS 11.x and above operating systems, you can simply scan the QR code on the enclosed router pass and the router will automatically connect to the WLAN.

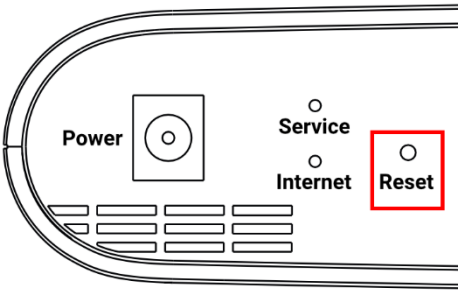
Router pass

3.2 Meaning of the LEDs

STATUS	green	on	Router in operation
	green	rapid flashing	WAN auto detection
	green	slow flashing	System software starting
	red	on	The router is booting (approx. 25 s) or a router error has been detected (>60 s)
	red	flashing	New system software is being loaded or reset
	off		No power supply available
DSL/SFP	green	on	DSL connection successfully established
	green	rapid flashing	Executing DSL synchronization
	green	slow flashing	DSL connection established
	yellow	on	SFP link detected
	off		DSL interface not activated, no SFP link
INTERNET	green	on	Internet connection successfully established
	red	on	Error while establishing the Internet connection
	off		No Internet connection
TEL	green	on	All telephone numbers registered
	red	on	At least one telephone number not registered
	off		Internet telephony not activated
WLAN	green	on	WLAN activated
	green	flashing	WLAN activating or deactivating
	yellow	flashing	WPS button pressed, waiting for client connection
	off		WLAN deactivated
SERVICE	off		Remote maintenance service off / Automatic configuration (TR-069) inactive

3.3 Reset button

The **Reset** button can be used to trigger various actions. Which action is initiated is determined by how long the button is pressed. You will find the button on the connection side of the **be.IP swift**:



You can initiate the following actions with the button:

1. 0 sec. to 2 sec. actuation: no action
2. >10 sec. to 15 sec. actuation: Router restarts; the **Service** LED lights up first and goes out as soon as 10 seconds have passed.
3. >15 sec. actuation: Restores factory settings; the **Status** LED starts flashing green as soon as 15 seconds have passed.

4 Areas of application for your be.IP swift

The **be.IP swift** is an outstanding all-in-one communications solution. Ideal for new connections or bandwidth upgrades. The **be.IP swift** is the next generation of routers and offers improved performance combined with greater ease of use.

Advantages at a glance

- Business routing functions with DSL, FTTH and Ethernet, dual stack (IPv4/6) Internet access
- VPN with 10 active IPSec tunnels, e.g. for home office or connecting mobile employees
- Individual adaptation to security requirements for voice and data networks
- Quality of Service (QoS) and bandwidth management
- Magenta TV compatibility: Supports multiple high-resolution streams, use of media receivers
- Flexible mounting: Wall, desktop or optional 19" rack mounting
- Continued use of existing PBX

Technology at a glance

- VDSL2 SuperVectoring up to 250 Mbit/s, G.fast support up to 1 Gbit/s
- WiFi 6 (802.11ax) dual-band WLAN with 4 x 4 2.4 GHz and 4 x 4 5 GHz with a total of up to 5.9 Gbit/s, WPA3 and WPA2 encryption
- Integrated telephone system for max. 30 users
- SFP module slot for GPON applications (module optional).

4.1 be.IP swift IP router with integrated telephone system

You will not need any other access device apart from the **be.IP swift**: Internet access and telephony functions are both provided by **be.IP**

swift, so you can connect your computer network as well as your telephones directly to **be.IP swift**.

4.2 be.IP swift as IP router with separate ISDN telephone system

You already operate an ISDN telephone system, but want to switch to an All-IP connection and therefore need a device that connects your ALL-IP connection to your existing infrastructure.

In this case, the **be.IP swift** works as a so-called media gateway that translates telephone calls transmitted from a separate system to the All-IP infrastructure. For this purpose, you may have to switch the operation mode of your **be.IP swift** to operation as a media gateway. Please refer to the instructions in the section *Changing the Operation Mode*.

4.3 Changing the operation mode

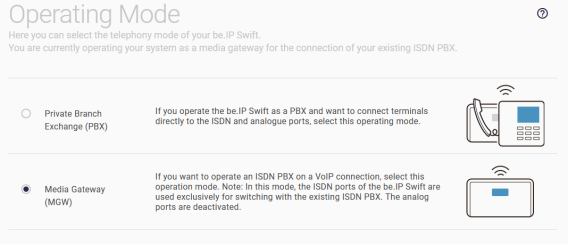
You can use the **be.IP swift** in one of two different operation modes:

As a PBX, **be.IP swift** provides a wide range of different telephony functions itself, while a so-called media gateway serves primarily as a switching point for switching between different target Interfaces (ISDN, analog, or IP) and a purely IP-based connection. Extensive telephony functions can then be provided by the telephone system that already exists in your network. So if you are already operating a telephone system with your own customized configuration, using **be.IP swift** as a media gateway can greatly simplify the transition to a purely IP-based connection.

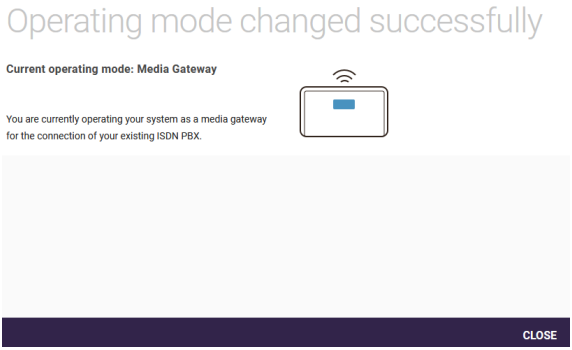
Note

Your settings are retained when you switch between operation modes, so you do not have to reconfigure them when you switch again. Likewise, when you first change the operation mode, all relevant settings are transferred to the new operation mode.

You can change the operation mode in the **Home** menu ➔**System settings**:

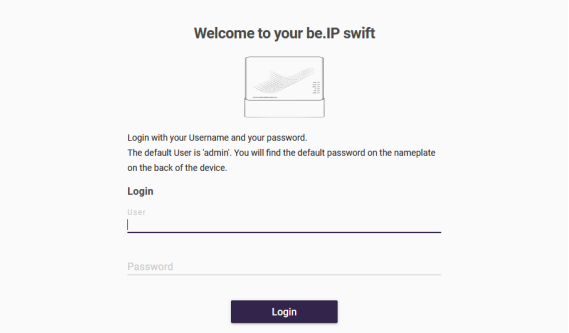


Select the desired operation mode and click on the **OK** button, the current configuration is prepared for the new operation mode and this is then switched over. You will receive a corresponding message:



5 be.IP swift login

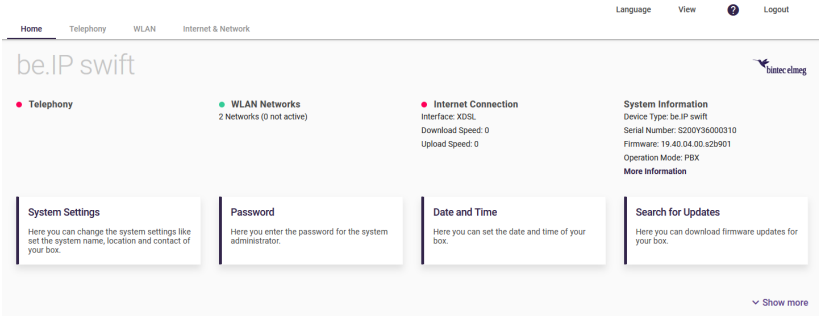
You will find access data for your **be.IP swift** on the enclosed router passport or on the nameplate of your router. Open a browser and log in to the **be.IP swift** with the default IP address **192.168.0.251**:



1. Enter the user name "*admin*".
2. Enter the password (you can find it on the router passport).
3. Click the **Login** button.

6 Home menu

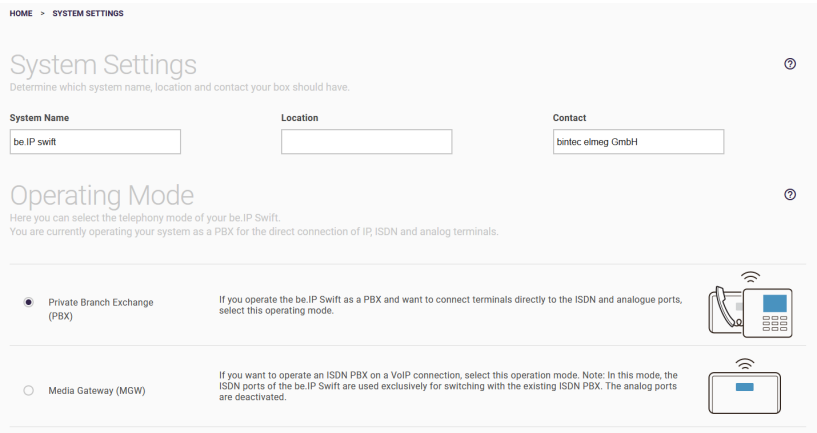
An overview shows you the most important system information.



For example, you can see if there is a working Internet connection and if the wireless network (WLAN) is active.

6.1 Home menu / System settings

Here you can enter or change the basic system data of your **be.IP swift** .



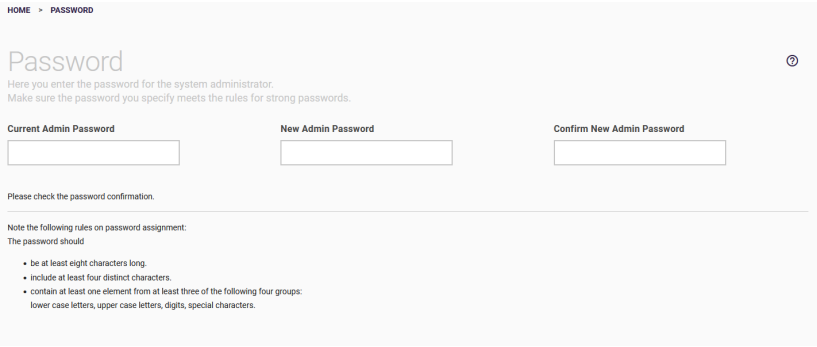
1. Under **System name**, enter a unique name for your router.
2. Under **Location**, enter where your router is located.
3. For **Contact**, enter the responsible contact person (e.g. the email address of the system administrator).
4. You can operate your router as a telephone system or as a media gateway. The current **Operation mode** is displayed. To change it, activate the required option.

In the **Show more** section, you can use the **Expert navigation tree** option to display a menu tree on the left side, which you can use to quickly navigate through the menus for advanced configuration.

6.2 Home / Password menu

All routers are shipped with the same user name, but with an individual password printed on the nameplate or router passport.

You can change the password to prevent unauthorized access to the router.

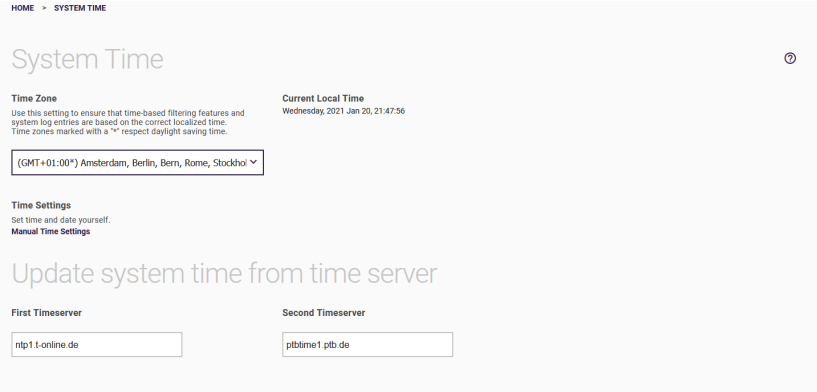


1. Enter your self-selected **Password** for the user "*admin*".
2. **Confirm** your **Password** by entering it again.

Click on **OK**.

6.3 Home / Date and time menu

You need the system time, for example, for the correct time information on system messages or charge entry.

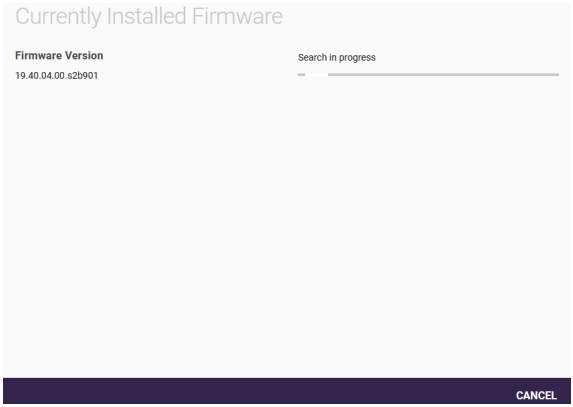


1. Select the **Time zone** in which your router is installed.
2. You do not normally need the **Manual time setting** option, as the system time is usually updated via a time server.
   If you want to use the **Manual time setting** option: Clicking on the input field for **New date** opens a standard calendar in month view. Clicking on the required date transfers it to the configuration interface.
3. Normally you can retain the default time servers. If you want to use other time servers, enter the name or IP address of the server(s) in **First time server** and **Second time server**.

Click on **OK**.

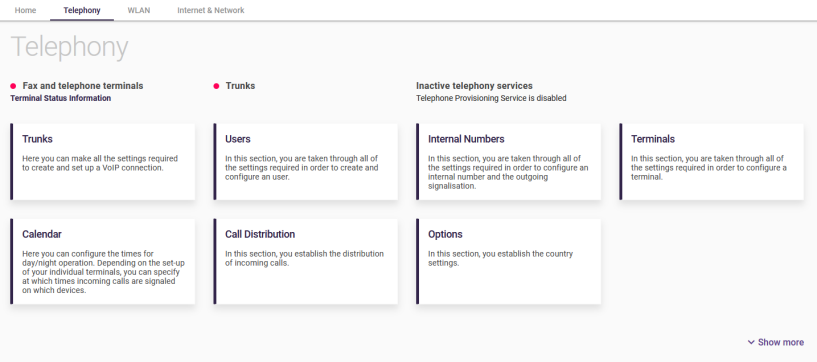
6.4 Home / Check for updates menu

Your router has the system software version that was available at the time of manufacture, newer versions may exist. You should perform a software update if necessary.



7 Menu for telephony in operation as a telephone system

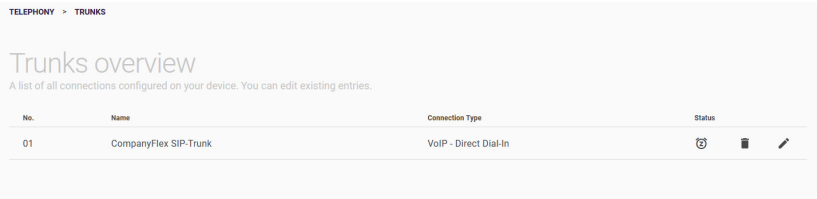
In this menu you make all the settings for **Telephony**: Connections, users, internal call numbers, terminals, basic calendar functions and general basic settings such as country and area codes. In addition, you have access to a call distribution list that shows you the currently active assignments of external and internal call numbers as well as the assignment to day or night mode.



Click the **Connections** button.

7.1 Telephony / Connections menu

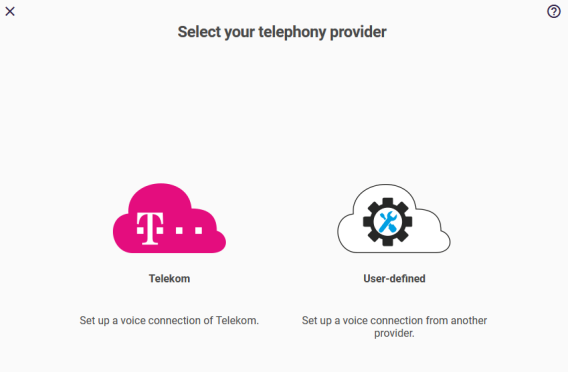
In the **Connections** menu, make the settings required to create and set up a VoIP connection.



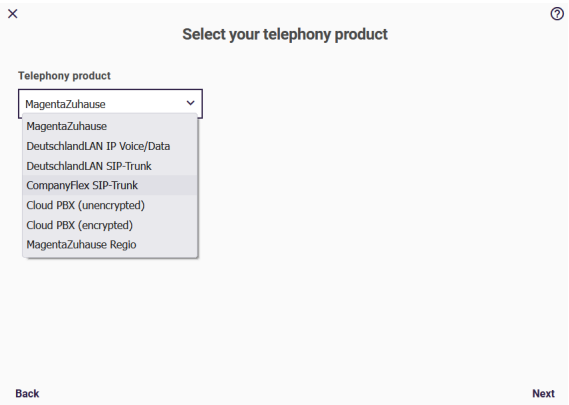
In the overview, all ports that have already been configured are displayed.

You can delete or edit existing entries. Use the **New** button to add a new connection.

Selecting your telephony provider



Selecting your telephony product

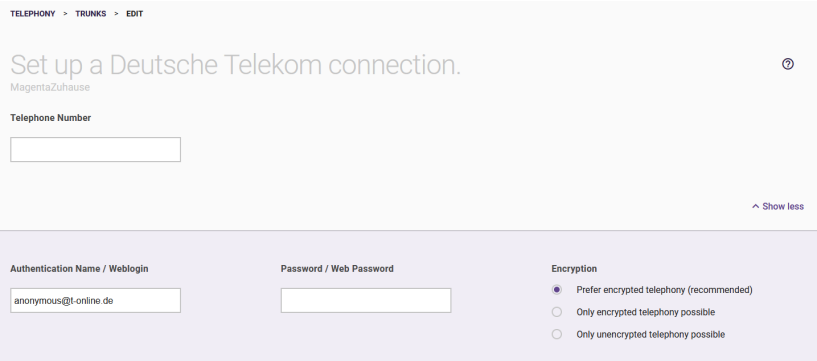


When you create a Telekom connection, you can choose between different variants:

- MagentaZuhause
- DeutschlandLAN IP Voice/Data
- DeutschlandLAN SIP Trunk

- Company Flex SIP Trunk
- Cloud PBX (unencrypted)
- Cloud PBX (encrypted)
- MagentaZuhause Regio

7.1.1 Configuration of MagentaZuhause DeutschlandLAN IP Voice/Data



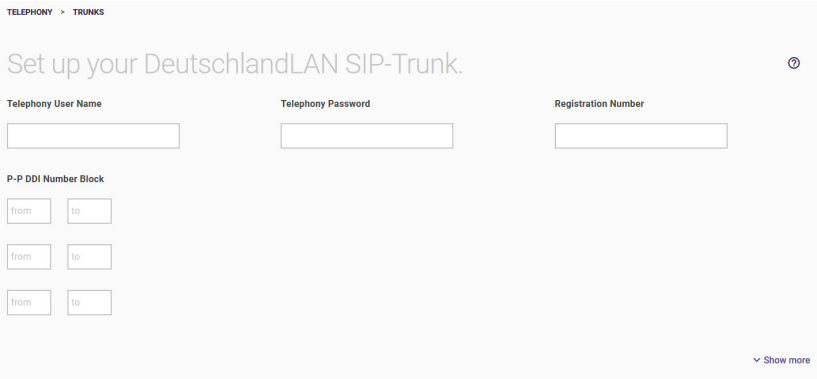
Enter the **phone number** given in your contract documents. Enter the *area code* and the *phone number*. The country code is automatically added.

Click on **Show more**.

1. Under **Authentication Name / Weblogin**, leave the default setting of Telekom *anonymous@t-online.de* if you want to make calls from your land line at home.
2. Assign a **Password / Web Password**.
3. In the **Encryption** section, you can specify whether telephone connections are to be established preferentially (this is the default setting), unconditionally or not encrypted.
4. If you have set up multiple Internet connections, you can select one of them for the **SIP interface binding** option; VoIP data traffic is then transmitted through this interface. By default, the primary Internet interface is selected here.

Click on **OK**.

7.1.2 Configuration of DeutschlandLAN SIP Trunk



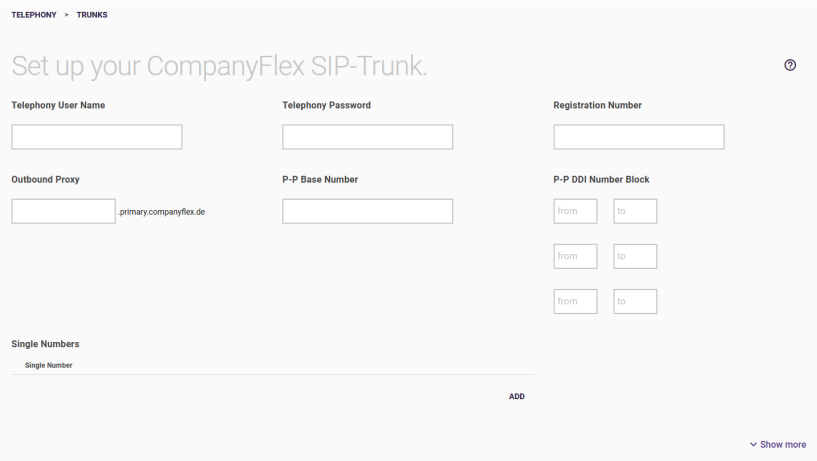
1. For **Telephony user name**, enter the user name you received from your provider.
2. For **Telephony password**, enter the telephony password you received from your provider.
3. Enter the international **Registration number** you received from your provider.
4. A **PABX extension** refers to the last few digits assigned to extensions through the PBX (e.g. *00–29*). A call number consists of area code, direct dial-in number (basic call number) and PABX extension, e.g. *089 – 12345 – (00–29)*.

Click on **Show more**.

1. In the **Encryption** section, you can specify whether telephone connections are to be established preferentially (this is the default setting), unconditionally or not encrypted.
2. If you edit an existing entry, you will also see the created **Direct dial-in exceptions** here. You can customize them to your requirements.
3. If you have set up multiple Internet connections, you can select one of them for the SIP interface binding option; VoIP data traffic is then transmitted through this interface. By default, the primary Internet interface is selected here.

Click on **OK.**

7.1.3 Configuration of CompanyFlex SIP Trunk



1. For **Telephony user name**, enter the telephony user name for authentication from the configuration portal in this format *+49199296xxxxxxxxxxx@tel.t-online.de* .
2. Enter the default **Telephony password** from the configuration portal.
3. Enter the CompanyFlex SIP Trunk **Registration phone number** from the configuration portal in this format *+49199296xxxxxxxxxxx*.
4. The outbound proxy must contain the 12-digit CompanyFlex-ID from the configuration portal. be.IP swift creates the necessary outbound proxy *<companyflex-id>.primary.companyflex.de* automatically.
5. If the CompanyFlex SIP Trunk is assigned a **Point to Point number**, enter the number in E.164 phone number format without extension in this field. If there is no assigned Point to Point number, the field remains empty.

For example: The number *0228 / 12345678* - with the extension *00–29* requires input of *+4922812345678* in the Point to Point number field. The PABX extension can be entered in the field next to/below it.

6. If a Point to Point number is stored, you must enter the **PABX extension** in the fields from and to.
   For example: The number *0228 / 12345678 – 0* with extension *00–29* requires input of *00* in the first **from** and *29* in the first **to** field.
7. If one or more **single call numbers** are assigned to the CompanyFlex SIP Trunk in the configuration portal, you can store them in the E.164 call number format. You can enter more single numbers via **Add**. If no single phone numbers are assigned, this field remains empty.
   For example: The phone number *0228 / 111111111* requires input of *+4922811111111*.

Click on **Show more** to display more Settings.

1. The **Activate additional access** option allows you to set up another CompanyFlex SIP Trunk that is used whenever the primary port is not available. The access data required for this second port can be found in your contract documents: There you may find a distinction between **Credentials Primary** and **Credentials Secondary**. To set up the backup port, you only need to enter the **Telephony user name**, **Telephony password**, and **Registration phone number**. The outgoing proxy is created automatically, and the phone numbers remain the same as for the primary port.
   If a second Internet connection is available for the backup telephony connection, it will be used. Which Internet connection is actually used is displayed under **SIP interface link**. In the **Telephony > Options** menu, you can specify which interface is used, if necessary.
2. In the **Encryption** section, you can specify whether telephone connections are to be established preferentially (this is the default setting), unconditionally or not encrypted.

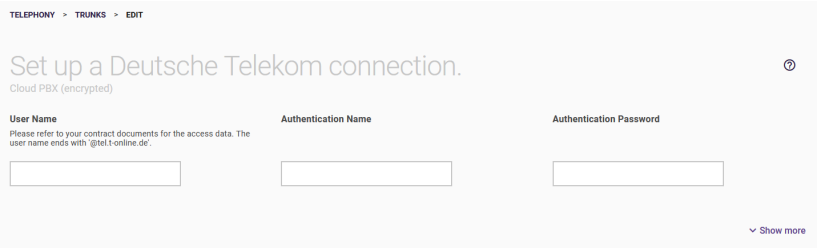
If you edit an existing entry, you will also see the created **Direct dial-in exceptions** here. You can customize them to your requirements.

Click on **OK**.

7.1.4 Setting up a Cloud PBX port

A cloud PBX port makes it possible to make calls at different locations and with different terminals using a single telephone number.

Note
If you operate the port on a Telekom Internet connection, you can choose the unencrypted variant. On a port from a different provider, you must select the encrypted variant (Cloud PBX (encrypted)).



1. Enter your **User name**. It is made up of connection phone number in the format *+49<connection phone number><001...008>@tel.t-online.de*, e.g. *+49255111111111001@tel.t-online.de*. The *001...008* suffix allows the same account to be used on more than one terminal or location and to be reachable on the same phone number on all of them.
2. Enter your **Authentication ID**. You will find it in your contract documents.
3. Enter your **password**. You will find it in your contract documents.

Click **Show More** to access more settings.

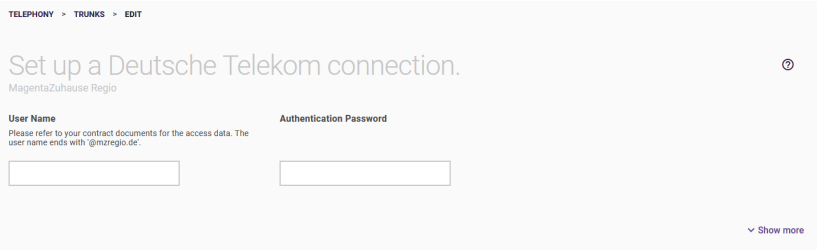
If you have set up multiple Internet connections, you can select one of them for the **SIP interface binding** option; VoIP data traffic is then

transmitted through this interface. By default, the primary Internet interface is selected here.

Save your settings by clicking **OK**.

7.1.5 Setting up a MagentaZuhause-Regio port

A MagentaZuhause-Regio port provides you with a single phone number like a MagentaZuhause port:



Enter the **SIP user name** and the **password** from your contract documents. The user name corresponds to the telephone number of the connection with *@mzregio.de* appended, e.g. *+49911123456@mzregio.de*.

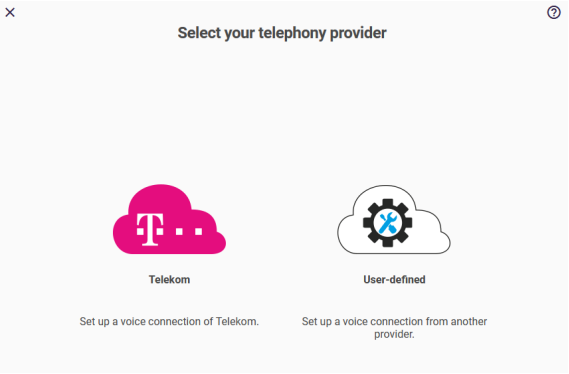
Click **Show More** to access more settings.

If you have set up multiple Internet connections, you can select one of them for the **SIP interface binding** option; VoIP data traffic is then transmitted through this interface. By default, the primary Internet interface is selected here.

7.1.6 Configuration of a user-defined VoIP provider (single number)

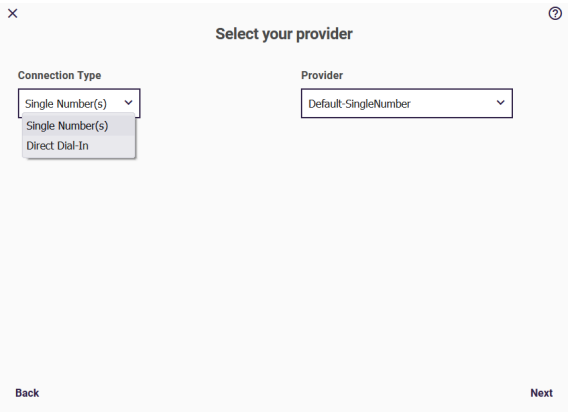
Here, you can configure a Point to Multipoint for any VoIP provider.

Select the **User-defined** telephony provider.



When you select a user-defined connection, you go to the select **Connection type** *Single number* or *Direct dial-in* and your **Provider**.

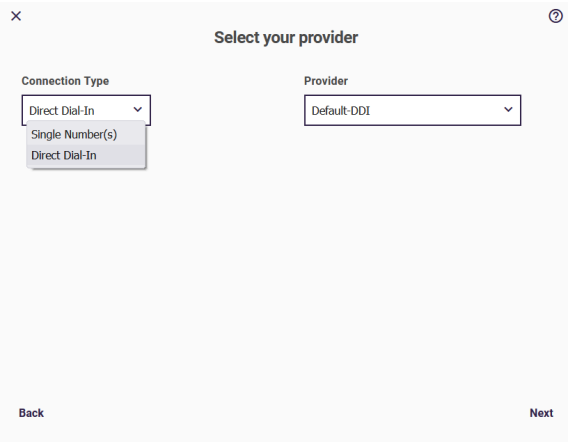
You can choose from a number of preset providers or create a provider by selecting the “Default” profile.



You will find more information about the **VoIP provider settings** and other settings in the Online Help.

7.1.7 Configuration of a user-defined VoIP provider (direct dial-in)

The **Direct dial-in** option corresponds with a Point to Point. Select **Connection Type** *Direct dial-in* and your **Provider**.



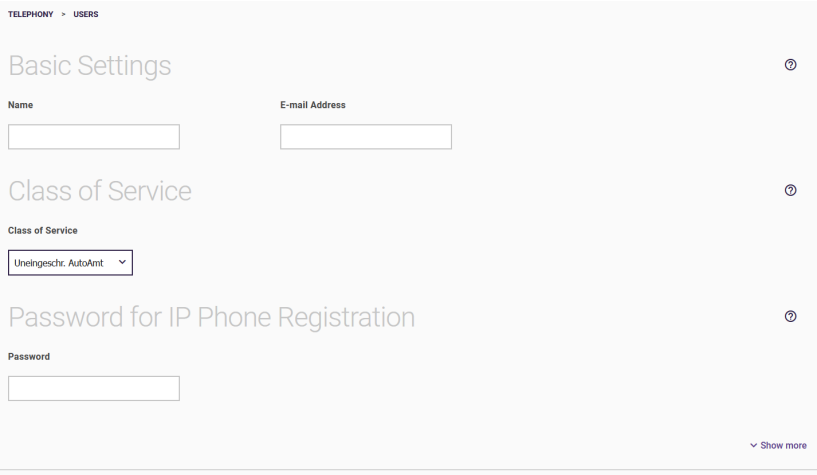
You can choose from a number of preset providers or create a provider by selecting the “Default” profile.

You will find more information about the **VoIP provider settings** and other settings in the Online Help.

7.2 Telephony / User menu

In this section you will be guided through all the settings required to create and set up a **user**. In the overview, all users that have already been configured are displayed.

You can edit existing entries. Use **New** to add a new user.



1. Enter the user's **Name**.
2. Here you can enter the user's **Email address**.
3. **Class of Service** is used to define which connections can be established, e.g. national or international connections. By default, you can select *Unrestricted*, *Unrestr.* Select *AutoAmt or Not permitted*.
4. You can enter a **password** that a user's IP phone must use to log on to the system.

Click on **Show more**.

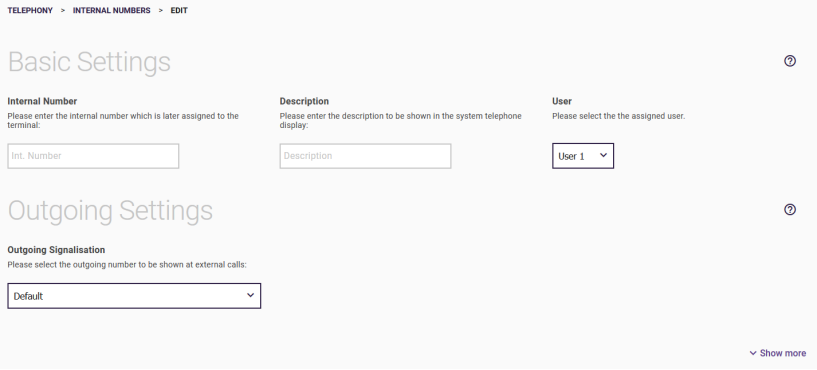
Individual user access can be set up under **User HTML Configuration**. This requires input of a **user name** and **password** and personal access must be enabled.

Click on **OK**.

7.3 Telephony / Internal Numbers menu

In this menu you set up an internal number and outgoing signaling. In the overview, all internal phone numbers that have already been configured are displayed.

You can edit existing entries. Use **New** to configure internal numbers.



1. Enter the user's **Internal Number**.
2. Enter a **Description** to be shown in the system telephone display.
3. Select one of the set up **users**.
4. For **Outgoing number** you can select from the numbers you configured in the **Telephony ➔ Connections ➔ New** menu.
   Select the *Default* option if your own direct dial-in is to be used as the outgoing number.
   This option is available with a SIP provider with direct dial-in.

Click on **Show more**.

1. The **Default destination** option allows you to include the phone in the group of phones that signal all calls for which no unique destination is defined.
2. Here you can activate **Access to Voice Mail**. To do this, set up voice mail number *50* in the user portal or your telephone.

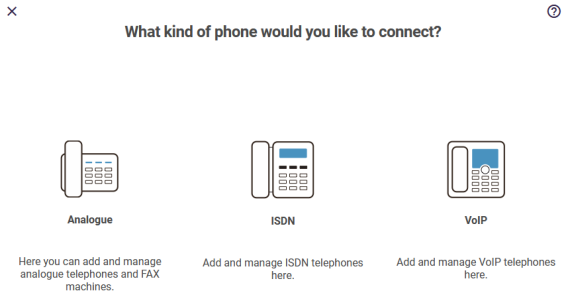
Click on **OK**.

7.4 Telephony / Terminals menu

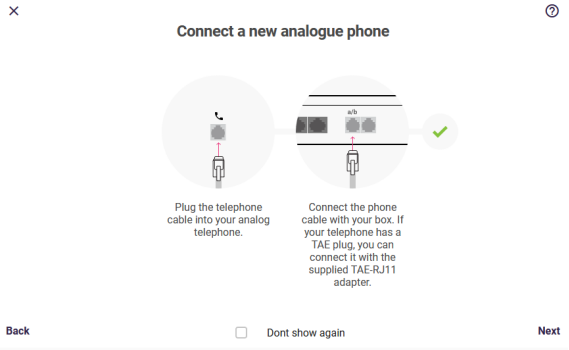
In this section you will be guided through all the settings required to set up a **terminal device**. In the overview, all terminals that have already been configured are displayed. You can delete or edit existing entries.

Use the **Add telephone** button to add a new device.

Selecting telephone type

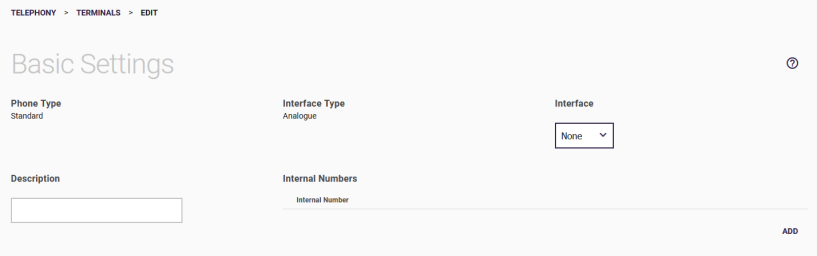


7.4.1 Connecting a new analog telephone



1. Connect your analog terminal device directly to an analog port (a/b1 to a/b4) of the be.IP swift. Use the cable supplied with the terminal device for this purpose.
2. Click on **Next**.

General settings



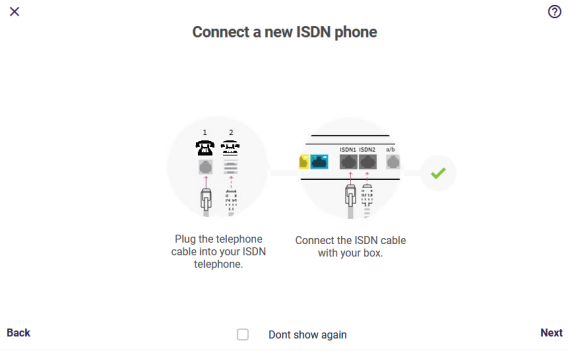
1. *Standard* is displayed as the **Phone Type**.
2. For Interface Type, the selected **Phone Type** *Analog* is displayed.
3. Select the **Interface** to which your analog telephone is connected (*a/b1* or *a/b2*).
4. Enter a description that the terminal device should show in its display, if applicable.

Use the **Add** button to add the internal number.

Click on **OK**.

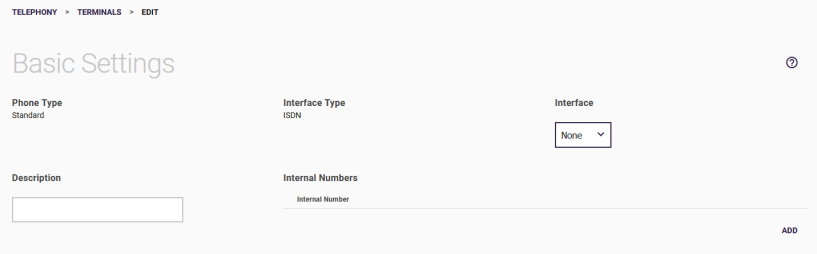
Use the **Add telephone** button to add more telephones.

7.4.2 Adding a new ISDN telephone



1. Connect your ISDN telephone to an internal ISDN port (**ISDN1** or **ISDN2**) of the be.IP swift.
2. Click on Next.

General settings

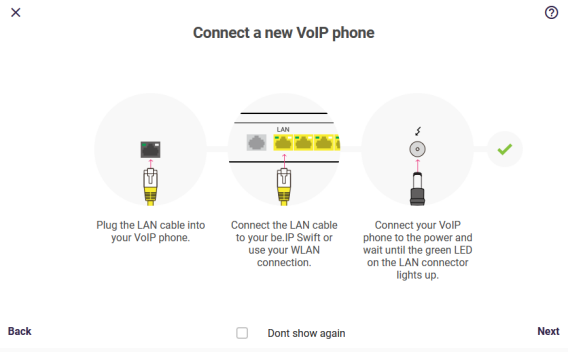


1. *Standard* is displayed as the **Phone Type**.
2. For Interface Type, the selected Phone Type *ISDN* is displayed.
3. Select the Interface to which your analog telephone is connected (*ISDN1* or *ISDN2*).
4. Enter a **description** that the terminal device should show in its display, if applicable.
5. Use the **Add** button to add the internal number.

Click on **OK**.

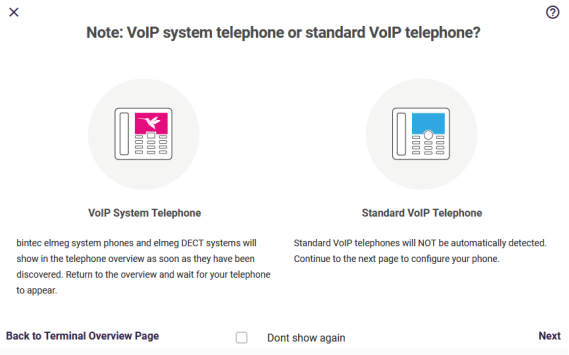
Use the **Add telephone** button to add more telephones.

7.4.3 Connecting a VoIP telephone



1. Connect your VoIP phone to a LAN port (LAN1 - LAN4) of the be.IP swift using the Ethernet cable.
2. Connect your VoIP phone with the power supply.
3. Click on Next.

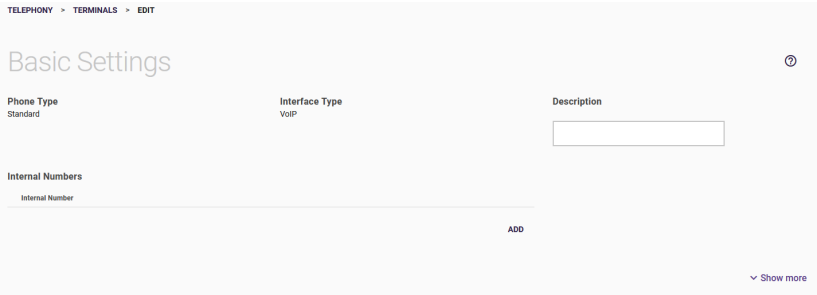
VoIP system telephone or standard VoIP telephone



Bintec-elmeg system telephones and elmeg DECT systems are automatically detected and displayed on the overview screen **Telephones / Terminals**. You can select the corresponding entry there and adapt it to your requirements. Standard VoIP phones are not automatically detected.

Click **Next** to enter the menu for setting up your phone.

General settings



1. *Standard* is displayed as the Phone Type. If a system telephone has been connected and automatically detected, the detected telephone type is displayed here.
2. For Interface Type, the selected Phone Type *VoIP* is displayed.

3. Provide a **Description** for the phone for better recognition.
4. Use the **Add** button to add the **Internal Number**.

Click on **Show more**.

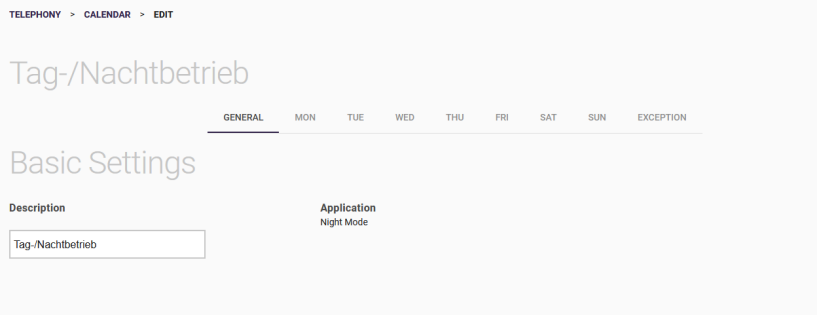
Select a **Location** for your VoIP telephone:

- *Not defined (registration only on private networks)*
- *LAN*: The subscriber is registered only when present at this location.

Click on **OK**.

Use the **Add telephone** button to add more telephones.

7.5 Telephony / Calendar menu



In this menu you can define calendar settings that control the day and night operation of your **be.IP swift**. When setting up a telephone, you define how it is to be reachable during the day or at night. In this menu you define the conditions for the corresponding operation.

1. Under **General** you just enter a description, then for each day of the week you can define at what time the night operation should start or end. For the days from Tuesday to Sunday, you can also apply the settings of another day. For Saturday and Sunday, individual setting options are also available.

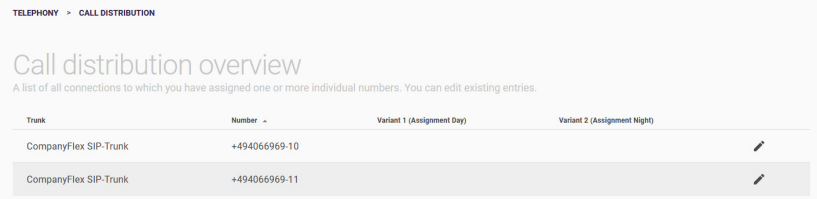
2. Under **Exception** you define if and which setting should be used for public holidays. The most important holidays are already preset under Show more, but you can also add or delete entries.

Click on **OK**.

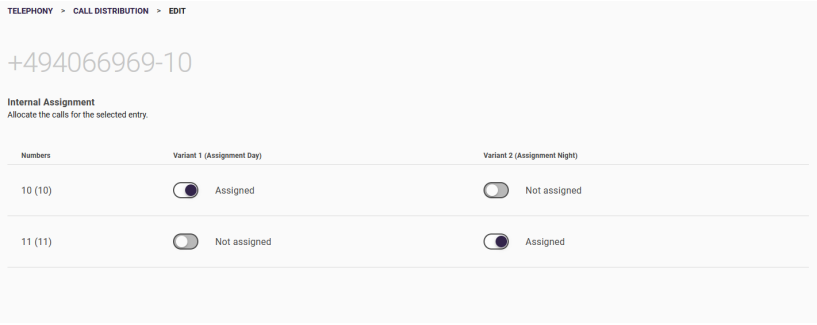
7.6 Telephony / Call distribution menu

In this section you define the distribution of incoming calls.

A list of all connections to which you have assigned one or more call numbers is displayed.



You can edit the individual entries using .

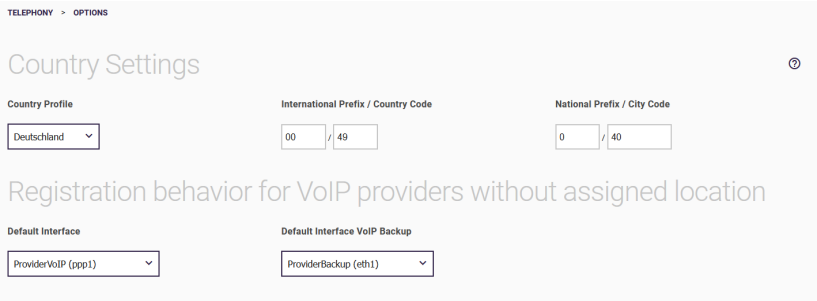


By default, **Variant 1 (Assignment Day)** is displayed for the selected entry for all displayed call numbers and *Unassigned* is displayed for **Variant 2 (Assignment Night)**.

You can define the times for day and night assignment in the **Telephony** / **Calendar** menu.

7.7 Telephony / Options menu

In the **Options** menu you specify the country settings, for example.



1. Select the country where the system is used. By default, the **Country setting** is preset to *Germany*.
2. The **International Prefix / Country Code** entry defaults to *00 / 49* for Germany.
3. Enter the **National Prefix / City code** for the location where your system is installed. By default, the national prefix is preset with *0*. You must enter the city code for your location yourself, e.g. *911* for Nuremberg.
4. VoIP providers that are not assigned a location require an interface for establishing a connection. In the section **Registration behavior for VoIP providers without assigned location**, you can set one of the created interfaces as the default for this case in the **Default Interface** field.
   In the **Default Interface VoIP Backup** field, you can also specify that a second Internet connection is used for a VoIP backup that has been set up.
5. You can use the option **Number of allowed simultaneous incoming calls** to keep call channels free for outgoing phone calls if the number of incoming calls is so high that outgoing calls could be blocked.
   The value applies to all configured VoIP connections and should therefore be smaller than the number of available call channels.

Click on **OK**.

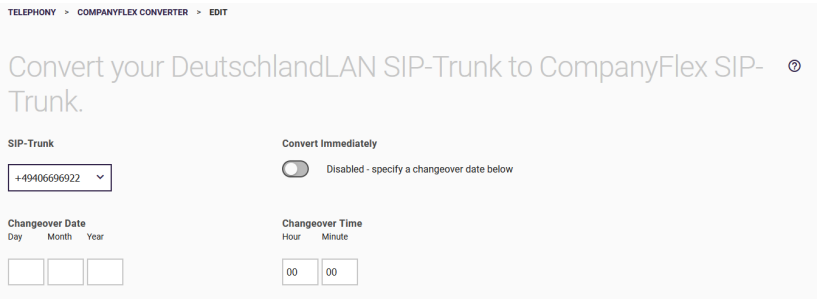
7.8 CompanyFlex Converter

Note

The wizard will only be displayed if a DeutschlandLAN SIP Trunk is set up on your be.IP swift that has not yet been converted, or if there are still entries in the list of conversion jobs.

The **CompanyFlex converter** function enables the conversion of one or more DeutschlandLAN SIP Trunks into a CompanyFlex SIP Trunk at any time. When you start the wizard, you will first be shown a list of existing conversion jobs. Both pending jobs and jobs that have already been completed are displayed:

If you create a new entry or edit an existing entry, you can select from the configured DeutschlandLAN SIP Trunks in the **SIP Trunk** field. If you activate the **Convert immediately** button, the conversion of the port will start immediately as soon as you confirm your entries on this screen. Otherwise, you can set the date and time of the conversion:

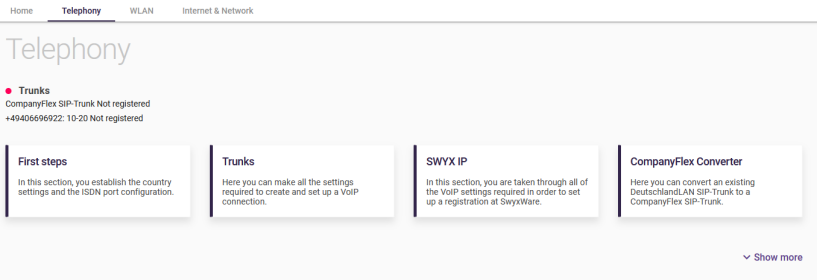


In the second section, enter the setup data of your CompanyFlex SIP Trunk. You will find it in your contract documents:

If you confirm your entries by clicking **Apply**, a corresponding entry will be created and the conversion will take place either immediately or at the time you set. If the conversion is completed successfully, the entry in the list of conversion jobs is not deleted, but remains for your information until you remove it yourself.

8 Telephony Menu in Operation as a Media Gateway

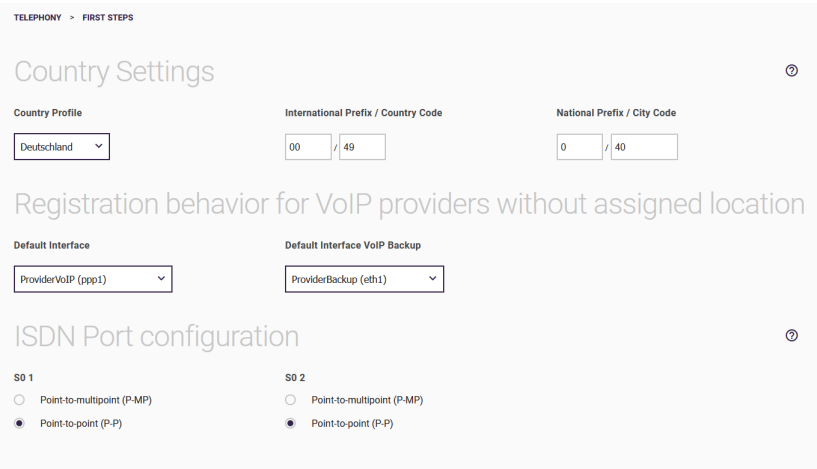
In the **Telephony** menu, you can make the settings required for a VoIP connection and define the country settings and the ISDN port configuration.



Click on the **First steps** button.

8.1 Telephony menu / First steps

In the **First steps** menu, you define the country settings and the default destination for incoming calls.



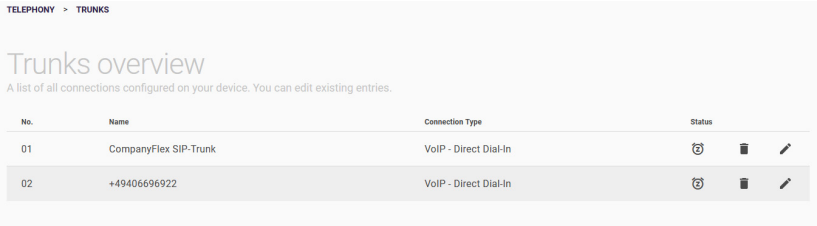
1. For the **country setting**, select the country in which you operate the be.IP swift.
2. The **International Prefix / Country Code** entry defaults to *00 / 49* for Germany.
3. Enter the **National Prefix / City Code** parameter for the location where your system is installed. By default, the prefix is preset with *0*. You must enter the city code for your location yourself, e.g. *911* for Nuremberg.
4. VoIP providers that are not assigned a location require an interface for establishing a connection. In the section **Registration behavior for VoIP providers without assigned location**, you can set one of the created interfaces as the default for this case in the **Default Interface** field.
   In the **Default Interface VoIP Backup** field, you can also specify that a second Internet connection is used for a VoIP backup that has been set up.
5. For **ISDN Port configuration**, select the port to which your telephone system is connected. For **ISDN 1 (bri-0)** and **ISDN 2 (bri-1)** below are available for selection: *Point-to-multipoint (multi-device connection) Point-to-point (system connection)*.

Click on **OK**.

8.2 Telephony menu / ports

The current tab guides you through the settings required to configure a port.

In the overview, all ports that have already been configured are displayed in a list.



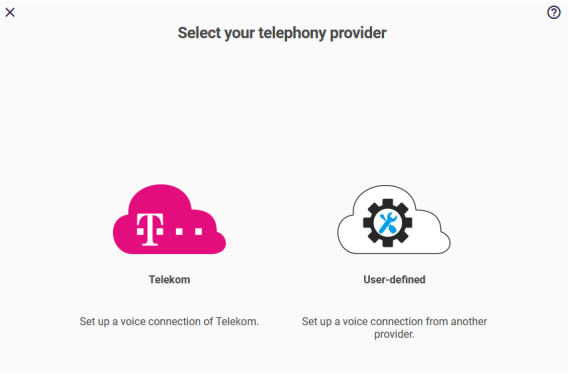
You can delete or edit existing entries.

Click on **Show more**.

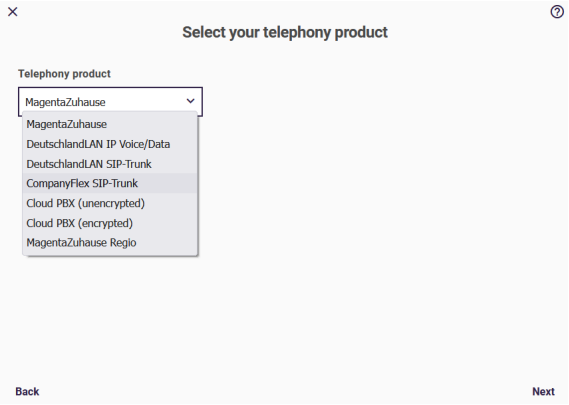
1. Select one from the list of configured ports. This **port** is always used as the default route when a terminal device without its own exchange number sets up a call.
2. The be.IP swift offers the option of converting call numbers that are transmitted incorrectly by a connected ISDN PBX into valid call numbers, so that the CO line number is signaled correctly for outgoing calls. This allows you, for example, to correct the outdated configuration of a telephone system that can no longer be changed and to continue to operate the telephone system with different call numbers even on a new port.
   Enter the phone number that is incorrectly signaled by the ISDN PBX on the ISDN line (**Incorrect CO line number**), as well as the correct CO line number (**Valid CO line number**) that is to be used for outgoing calls. Then select the ISDN line for which the rule is to apply.
   Note
   Enter the valid phone number without prefixes, as these are automatically added when the media gateway transforms the phone number.

Use the **New** button to add a new VoIP provider.

Selecting your telephony provider



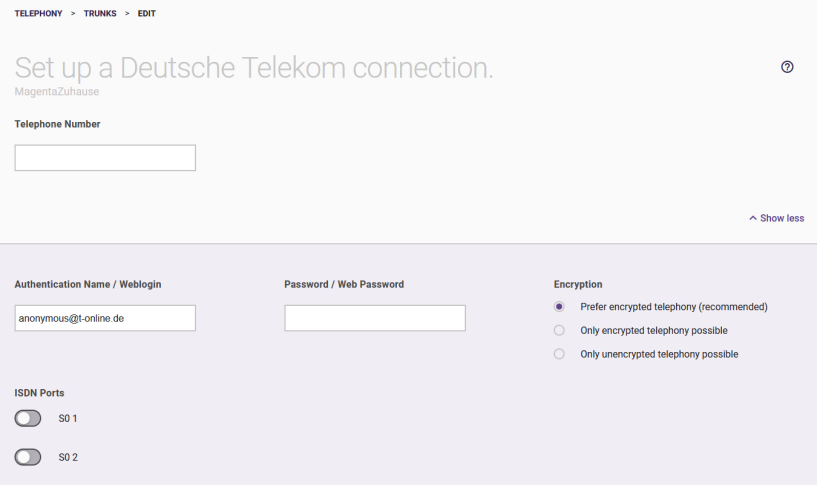
Selecting your telephony product



When you create a Telekom connection, you can choose between different variants:

- MagentaZuhause
- DeutschlandLAN IP Voice/Data
- DeutschlandLAN SIP Trunk
- Company Flex SIP Trunk
- Cloud PBX (unencrypted)
- Cloud PBX (encrypted)
- MagentaZuhause Regio

8.2.1 Configuration of MagentaZuhause and DeutschlandLAN Voice/Data



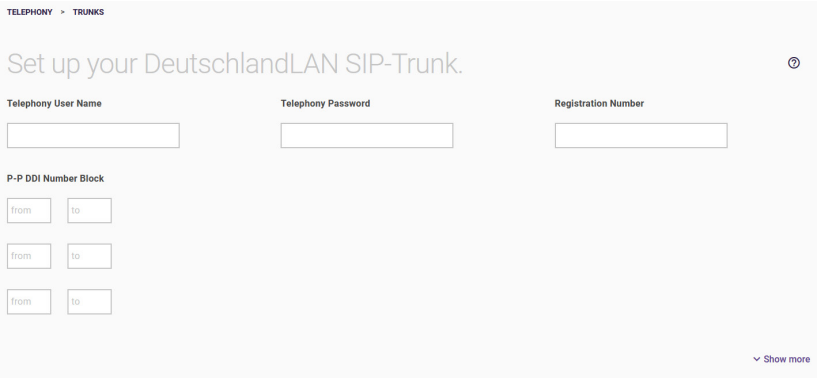
Enter the **phone number** given in your contract documents. Enter the *area code* and the *phone number*. The country code is automatically added.

Click on **Show more**.

1. Under **Authentication Name / Weblogin**, leave the default setting of Telekom *anonymous@t-online.de* if you want to make calls from your land line at home.
2. Assign a **Password / Web Password**.
3. In the **Encryption** section, you can specify whether telephone connections are to be established preferentially (this is the default setting), unconditionally or not encrypted.
4. Select the **ISDN port** to which your telephone system is connected.
5. If you have set up multiple Internet connections, you can select one of them for the **SIP interface binding** option; VoIP data traffic is then transmitted through this interface. By default, the primary Internet interface is selected here.

Click on **OK**.

8.2.2 Configuration of DeutschlandLAN SIP Trunk



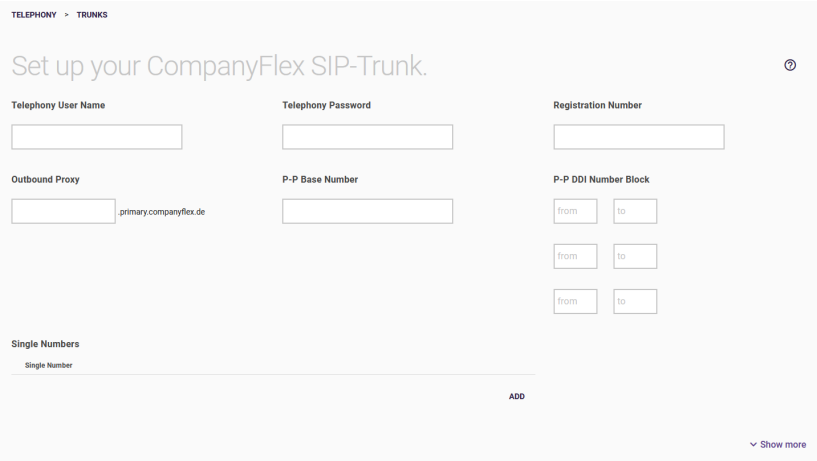
1. For **Telephony username**, enter the username you received from your provider.
2. For **Telephony password**, enter the telephony password you received from your provider.
3. Enter the international **registration number** you received from your provider.
4. A **PABX extension** refers to the last few digits assigned to extensions through the PBX (e.g. *00–29*). A call number consists of area code, direct dial-in number (basic call number) and PABX extension, e.g. *089 – 12345 – (00–29).*

Click on **Show more**.

1. In the **Encryption** section, you can specify whether telephone connections are to be established preferentially (this is the default setting), unconditionally or not encrypted.
2. Activate the **ISDN port** used for the connection.
3. If you have set up multiple Internet connections, you can select one of them for the **SIP interface binding** option; VoIP data traffic is then transmitted through this interface. By default, the primary Internet interface is selected here.

Click on **OK**.

8.2.3 Configuration of CompanyFlex SIP Trunk



1. For **Telephony username**, enter the telephony username for authentication from the configuration portal in this format *+49199296xxxxxxxxxxx@tel.t-online.de* .
2. Enter the default **Telephony password** from the configuration portal.
3. Enter the CompanyFlex SIP Trunk registration number from the configuration portal in this format *+49199296xxxxxxxxxxx*.
4. The outbound proxy must contain the 12-digit CompanyFlex-ID from the configuration portal. be.IP swift creates the necessary outbound proxy *<companyflex-id>.primary.companyflex.de* automatically.
5. If the CompanyFlex SIP Trunk is assigned a **Point to Point number**, enter the number in E.164 phone number format without extension in this field. If there is no assigned Point to Point number, the field remains empty.
   For example: The number *0228 / 12345678* - with the extension *00–29* requires input of *+4922812345678* in the Point to Point number field. The PABX extension can be entered in the field next to/below it.

6. If a Point to Point number is stored, you must enter the **PABX extension** in the fields **from** and **to**.
   For example: The number *0228 / 12345678 – 0* with extension *00–29* requires input of *00* in the first **from** and *29* in the first **to** field.
7. If one or more **single call numbers** are assigned to the CompanyFlex SIP Trunk in the configuration portal, you can store them in the E.164 call number format. You can enter more single numbers via **Add**. If no single phone numbers are assigned, this field remains empty.
   For example: The phone number *0228 / 111111111* requires input of *+4922811111111*.

Click on **Show more** to display more parameters.

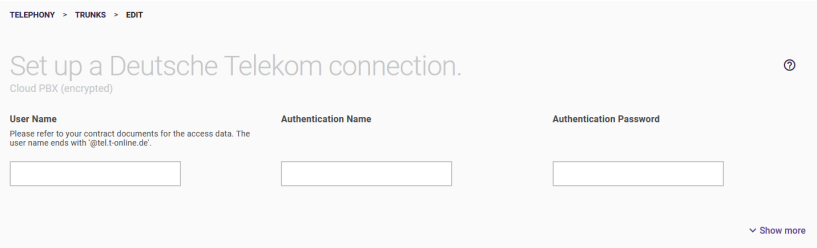
1. The **Activate additional access** option allows you to set up another CompanyFlex SIP Trunk that is used whenever the primary port is not available. The access data required for this second port can be found in your contract documents: There you may find a distinction between **Credentials Primary** and **Credentials Secondary**. To set up the backup port, you only need to enter the **Telephony user name**, **Telephony password**, and **Registration phone number**. The outgoing proxy is created automatically, and the phone numbers remain the same as for the primary port.
   If a second Internet connection is available for the backup telephony connection, it will be used. Which Internet connection is actually used is displayed under **SIP interface link**. In the **Telephony > First steps** menu, you can specify which interface is used, if necessary.
2. In the **Encryption** section, you can specify whether telephone connections are to be established preferentially (this is the default setting), unconditionally or not encrypted.
3. Activate the **ISDN port** used for the connection.

Click on **OK**.

8.2.4 Setting up a Cloud PBX port

A cloud PBX port makes it possible to make calls at different locations and with different terminals using a single telephone number.

Note
If you operate the port on a Telekom Internet connection, you can choose the unencrypted variant. On a port from a different provider, you must select the encrypted variant (Cloud PBX (encrypted)).



1. Enter your **User name**. It is made up of connection phone number in the format *+49<connection phone number><001...008>@tel.t-online.de*, e.g. *+49255111111111001@tel.t-online.de*. The *001...008* suffix allows the same account to be used on more than one terminal or location and to be reachable on the same phone number on all of them.
2. Enter your **Authentication ID**. You will find it in your contract documents.
3. Enter your **password**. You will find it in your contract documents.

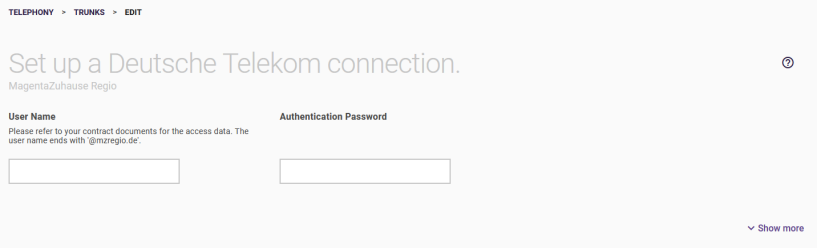
Click **Show More** to access more settings.

If you have set up multiple Internet connections, you can select one of them for the **SIP interface binding** option; VoIP data traffic is then transmitted through this interface. By default, the primary Internet interface is selected here.

Save your settings by clicking **OK**.

8.2.5 Setting up a MagentaZuhause-Regio port

A MagentaZuhause-Regio port provides you with a single phone number like a MagentaZuhause port:



Enter the **SIP user name** and the **password** from your contract documents. The user name corresponds to the telephone number of the connection with *@mzregio.de* appended, e.g. *+49911123456@mzregio.de*.

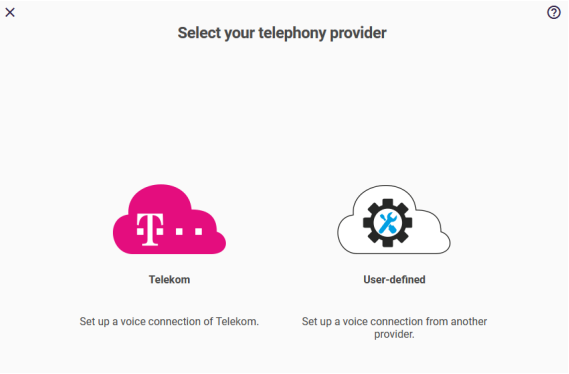
Click **Show More** to access more settings.

1. Select the ISDN port to which your telephone system is connected.
2. If you have set up multiple Internet connections, you can select one of them for the SIP interface binding option; VoIP data traffic is then transmitted through this interface. By default, the primary Internet interface is selected here.

8.2.6 Configuration of a user-defined VoIP provider (SIP single number)

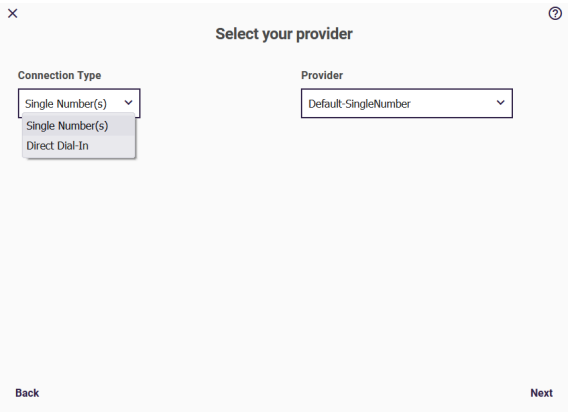
Here, you can configure a Point to Multipoint for any VoIP provider.

Select the **User-defined** telephony provider.



When you select a user-defined connection, you go to the select **Connection type** *Single number* or *Direct dial-in* and your **Provider**.

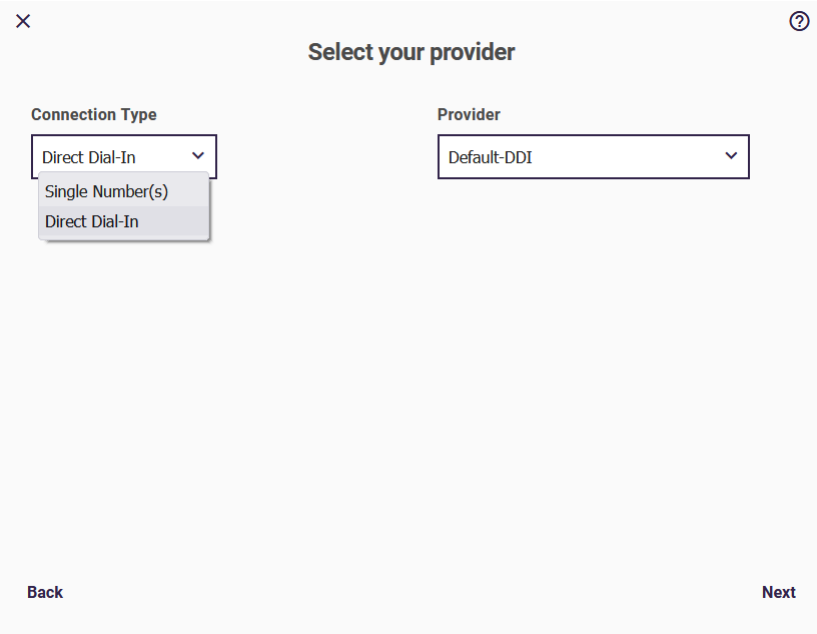
You can choose from a number of preset providers or create a provider by selecting the “Default” profile.



You will find more information about the **VoIP provider settings** and other settings in the Online Help.

8.2.7 Configuration of a user-defined VoIP provider (SIP Direct dial-in)

The **Direct dial-in** option corresponds with a Point to Point. Select **Connection Type** *Direct dial-in* and your **Provider**. You can choose from a number of preset providers or create a provider by selecting the “Default” profile.

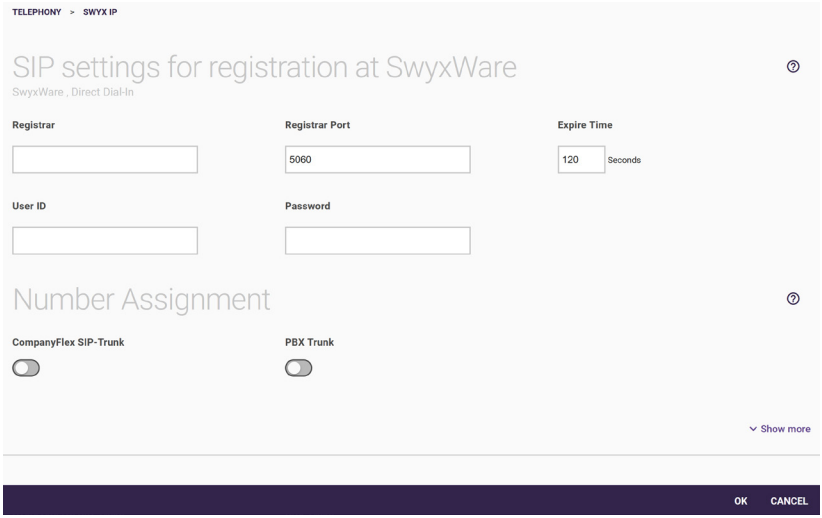


You will find more information about the **VoIP provider settings** and other settings in the Online Help.

8.3 Swyx IP

With **Swyx IP** you get a system that combines all the functions of a contemporary telephone system in a software-based solution. If you

want to connect your device to SWYX SIP servers, you can configure the necessary entries here:



Confirm your settings with OK.

The SIP settings for registration with SwyxWare are:

1. **Registrar**
   Enter the IP address or domain name (FQDN) of the SIP registrar (max. 40 characters).
2. **Registrar Port**
   Enter the port over which the data should be transferred.
3. **Expire Time**
   Specify how long the registration should be valid for the respective con-to (in seconds). Possible values are: 0 ... 99999.
4. **User ID**
   Enter the user ID for authentication.
5. **Password**
   Enter the password (max. 40 characters).
6. **Number Assignment**
   Select those of the configured phone numbers that are to be used for the connection via a Swyx server. Note that these

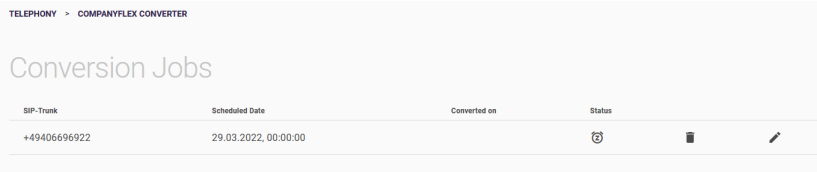
numbers will then no longer be available for (incoming) call distribution to the ISDN lines.

7. **Registration behavior**
   If you have set up multiple Internet connections, you can select one of them for the **SIP interface binding** option; VoIP data traffic is then transmitted through this interface. By default, the primary Internet interface is selected here. If you select *All sites*, all available Internet interfaces are used for the transfer.

8.4 CompanyFlex Converter

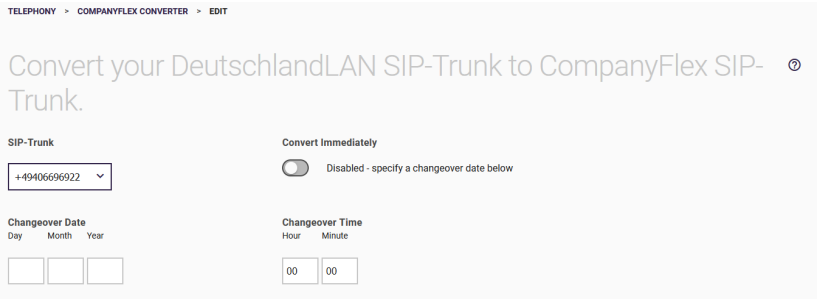
Note
The wizard will only be displayed if a DeutschlandLAN SIP Trunk is set up on your be.IP swift that has not yet been converted, or if there are still entries in the list of conversion jobs.

The **CompanyFlex converter** function enables the conversion of one or more DeutschlandLAN SIP Trunks into a CompanyFlex SIP Trunk at any time. When you start the wizard, you will first be shown a list of existing conversion jobs. Both pending jobs and jobs that have already been completed are displayed:



If you create a new entry or edit an existing entry, you can select from the configured DeutschlandLAN SIP Trunks in the **SIP Trunk** field. If you activate the **Convert immediately** button, the conversion of the port will start immediately as soon as you confirm your entries

on this screen. Otherwise, you can set the date and time of the conversion:

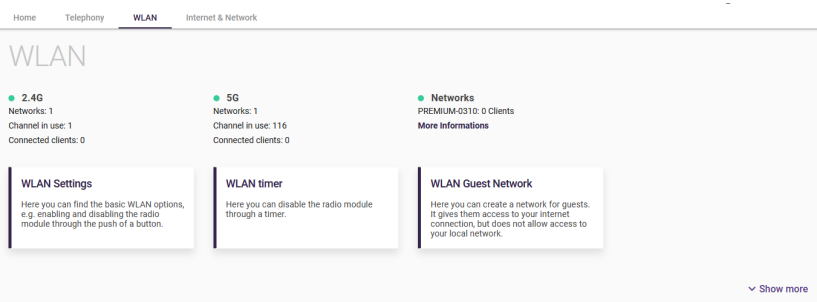


In the second section, enter the setup data of your CompanyFlex SIP Trunk. You will find it in your contract documents:

If you confirm your entries by clicking **Apply**, a corresponding entry will be created and the conversion will take place either immediately or at the time you set. If the conversion is completed successfully, the entry in the list of conversion jobs is not deleted, but remains for your information until you remove it yourself.

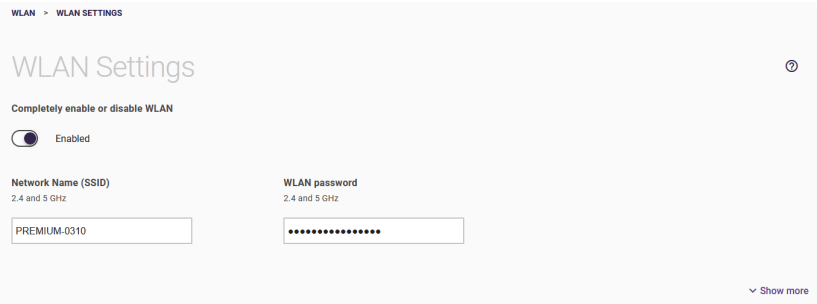
9 WLAN menu

Since a WLAN transmits via radio waves, the transmitted data can theoretically be intercepted and read by anyone with the appropriate equipment. Consequently, special attention must be paid to the security of the radio connection.



Click on **WLAN settings**.

9.1 WLAN menu / WLAN settings



In the **WLAN settings** menu, you make the basic settings for operating wireless networks in the 2.4 and 5GHz bands. In the default settings, the WLAN is enabled and provides the same network in both frequency bands. If you have not yet made any changes here, you can change the network name or disable the WLAN completely.

Note

Change the preset password. It must consist of at least eight characters and should contain upper- and lower-case letters as well as numbers and special characters.

In the Show more section of the menu, you can make further settings for one of the two frequency bands at a time. After clicking on the  icon, you can deactivate the corresponding radio module or assign a network name specific to the frequency band as well as a password of your own.

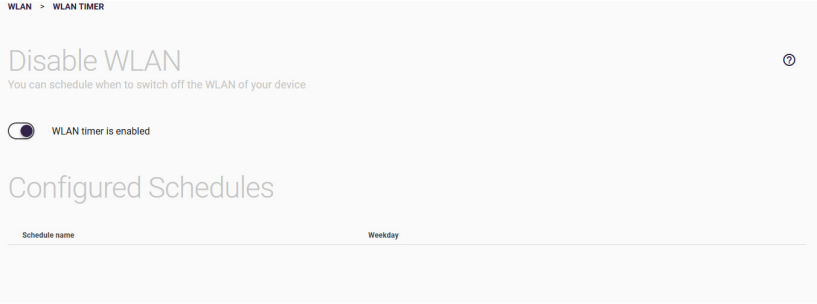
If you use different settings for the network name and password of the two frequency bands, the global options for the network name and password are hidden and the two menus for editing the frequency bands are permanently displayed.

You can also activate the **Band Steering** option. Your device can then automatically assign the more powerful frequency band to connected terminals to improve data transmission. This function requires that the same network name (SSID) be assigned to both frequency bands.

You also have the option to deactivate the WLAN button on the side of the device via a key lock, so that the WLAN function can neither be switched off nor on from the outside.

9.2 WLAN / WLAN Timer menu

In this menu, you can specify a time period for each day of the week when the WLAN base station is to be automatically deactivated:



1. To do this, toggle the **WLAN Timer is disabled** option.
2. Click **New** for a new rule.
3. Enter a name for the rule under **Schedule name**.
4. You can specify the **Start time** and **Expiry time** for each day of the week. The WLAN network is deactivated during the specified periods.

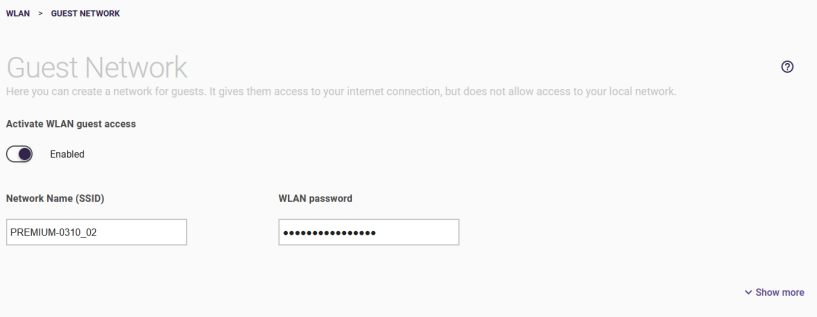
Click on **OK**.

For more rules, click the **New** button again.

9.3 WLAN guest network

If you want to give guests access to your Internet connection via the WLAN, but prevent them from accessing your local network, you can create a separate wireless network here. To do this, activate the **Activate WLAN guest access**. The guest network is activated with a **network name (SSID)** derived from the original name (noted on the router passport) of your main network and therefore easily recognizable. By default, the guest network is encrypted and accessible with the **WLAN password** that you can find on the router

passport. You should change it so that your own network is not accessible with the same password as the guest network.



In the **Show more** section you can select the **Encryption type** of the guest network. Keep in mind that the connection of the guest devices to the be.IP swift is not secured if you select Unencrypted here, and inform your guests accordingly.

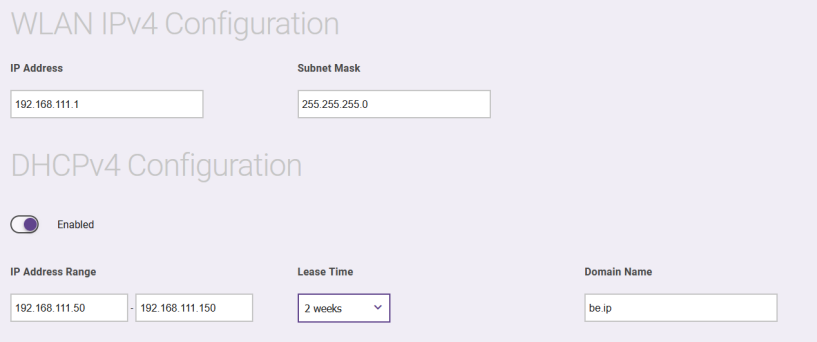
You can also **hide the SSID** here. The guest network will then not be displayed to WLAN clients in the list of available networks. However, this is not an effective way of securing the network, as it can still be discovered by other means.

If you enable **Client Isolation**, devices connected to the guest network will not be able to exchange data with each other.

WLAN IPv4 configuration

In order for your guests' devices to access the Internet, they need IP configuration. The necessary settings are already predefined, and

you can view and, if necessary, adjust them in the **WLAN IPv4 Configuration** area:

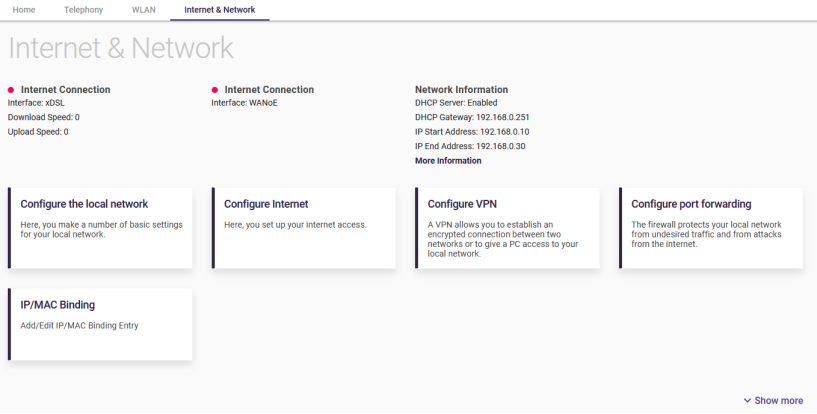


Note

If you upgrade to the current version from a software version without the guest network feature, the IP configuration data will not be automatically applied. The settings are then displayed in the upper part of the menu. If there is no overlap with your network configuration, you can simply accept the default values.

10 Internet & Network menu

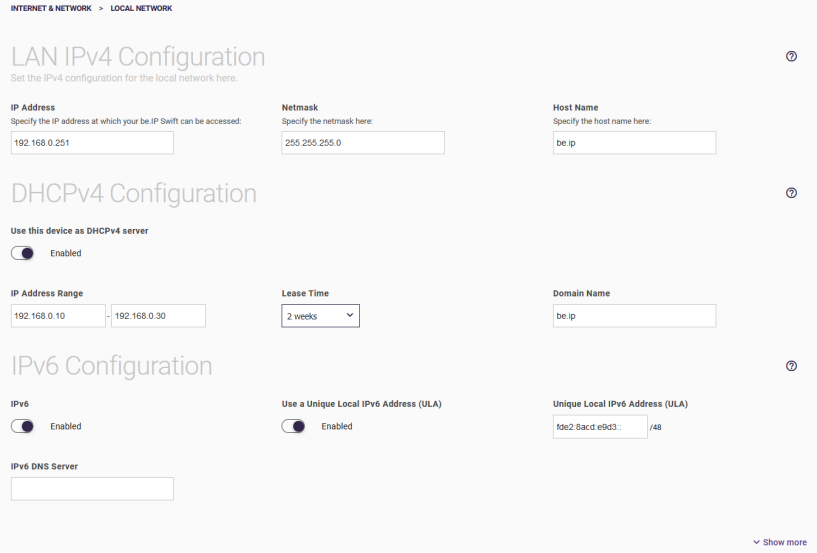
In this menu you can set up the local network, Internet connections, VPN connections and port forwarding.



10.1 Internet & Network / Local Network menu

Note

These settings may have a significant impact on your network. As a rule, you can leave it at the default values here.



1. Enter the **IP address** here at which your **be.IP swift** is accessible.
2. Enter the corresponding **netmask**.
3. Give your device a **host name** by which it should be accessible on the LAN.
4. Activate the **Use this device as DHCPv4 server** option if your device is to be used as a DHCPv4 server to dynamically assign an IP address to the devices within your network.
5. In the **IP address** range, enter the first and last IP addresses for the DHCP address pool.
6. Use **Lease Time** to specify how long the IP settings assigned to a device are valid. After the time has expired, a new assignment is made.
7. Assign a **Domain name** for the range of IP addresses. Clients that are assigned an IP address from this range can then be reached under the name *<host name>.<domain name>*.

8. Enable the **Ipv6** option to use IPv6 in addition to IPv4.
9. Enable the **Use a Unique Local IPv6 address (ULA)** option to automatically generate and use private addresses.
10. The **Unique Local IPv6 Address (ULA)** field displays the locally generated prefix that identifies a network.
11. Specify the address of the **IPv6 DNS server** on your local network.

Click on **Show more**.

Activate the option **Transfer provisioning server for elmeg IP/DECT** if connected elmeg system telephones are to automatically receive a base configuration and system software updates. The prerequisite for this is that the necessary system software files must be loaded onto the system. The update is then performed as entered in the configuration.

Click on **OK**.

10.2 Internet & Network / Internet Connections menu

You will see a list of configured Internet connections.

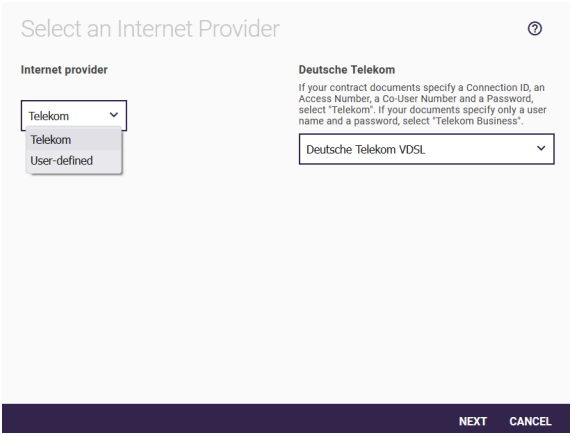
You can delete or edit existing entries. With the **Delete connection** button, you can first delete the existing Internet connections and then set them up again.

If you have set up an Internet connection that enables a backup connection via the WANoE port, you can use the **Enable WANoE Backup** button to set up another Internet connection. If a second connection has already been created, you will find a link here to the

menu for setting up **load balancing**. This is required if you want to use the second connection simultaneously with the first and not only as a backup.

10.2.1 Creating a new connection

Selecting an Internet provider



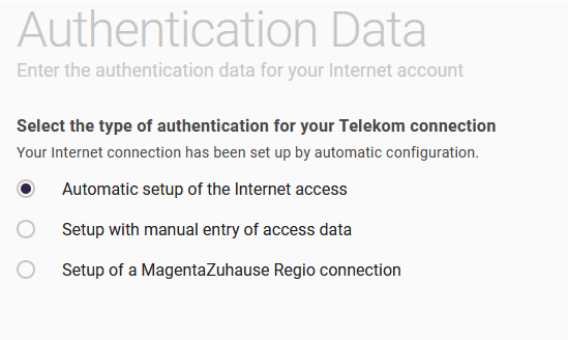
Internet access can be provided either directly via the be.IP swift, via a connected modem or by connecting to another gateway that provides Internet access.

Define how the Internet access is to be provided in your network. You can choose between preset Telekom connections or create a user-defined access. The following basic connection types are available:

- *Deutsche Telekom VDSL / ADSL*: The connection is provided by the integrated DSL modem via VDSL or ADSL.
- *Deutsche Telekom fiber optic SFP or external modem/fiber:* The connection is provided via an external modem connected to one of the Ethernet ports (usually LAN5) or via an SFP module.
- *G.Fast*: The connection is provided via the integrated DSL modem using g.fast. This option is only available if you set up a Telekom connection.

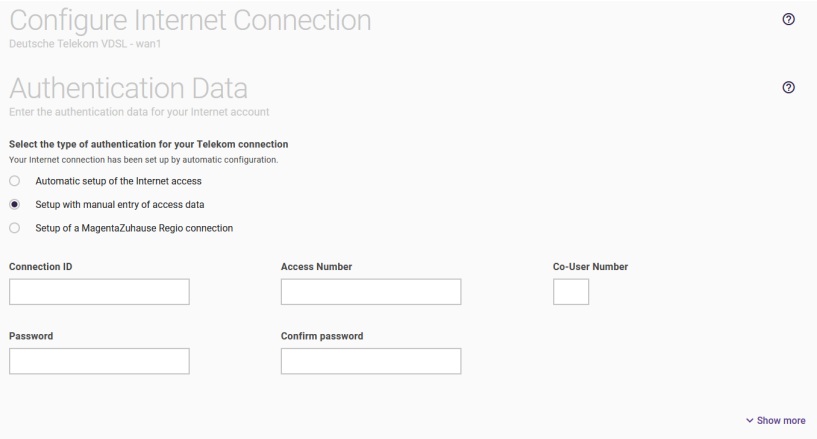
- *Deutsche Telekom Business Premium Access*: The connection is established via an upstream gateway. Public IP addresses provided by Deutsche Telekom are available for your network.

Click **Next** to confirm your selection and proceed to the next configuration step. Here you select whether the connection is to be set up without entering access data or whether you are to enter the relevant information yourself:



Setting up an Internet connection

Note
The data that you must enter to set up the Internet connection may differ depending on the provider and type of connection.



1. Enter the **authentication data**, the access identifiers sent by the Internet provider.
   Enter the access data **access name** and **password** for the Internet. Confirm the password in the **Confirm password** field. The password is not displayed in plain text for security reasons. Pay attention to the correct spelling and to upper and lower case. If you do not have the access data or the entered data is not accepted, please contact the Internet provider's customer service.
2. If you set up a connection via the WANoE port that has a static IP configuration, enter the IP address of the gateway via which the connection is realized under **Default gateway**; also the servers to be used for name resolution (**DNS server**). Under **Configured static IP addresses**, set up the corresponding IP address of your be.IP swift. You will find the corresponding information in the contract data of the Internet provider.
3. To set up **Deutsche Telekom Business Premium Access**, you also enter the **Default gateway** and the servers to be used for name resolution (**DNS servers**). In addition, you will be assigned public IP addresses by Deutsche Telekom, which you can enter in the **Public IP address configuration** area.

4. In a virtual LAN (VLAN), the physical network (DSL) is divided into several logical networks. These networks use one connection, but are logically separated and are addressed with the **VLAN ID**. The VLAN ID that your Internet provider has given you is entered here.
5. You may need to manually configure the VDSL settings according to your provider's requirements. Check with the ISP for the correct technical parameters.
   Enter the values for the **Virtual Path Identifier (VPI)** and **Virtual Channel Identifier (VCI)**.
6. Select the **IP version** to be used for the Internet connection. You can choose between *IPv6*, *Ipv4* or so-called *IPv4v6*, where IPv4 and IPv6 are used equally.
7. The **connection type** can only be specified if IPv6 is not offered by your provider. Specify if and when an existing Internet connection should be disconnected. The **Should your Internet connection be active all the time?** option is intended for users of an Internet flat rate. In this case, the be.IP swift remains permanently connected to the Internet.
   The **Disconnect after time without data traffic** setting allows you to have the Internet connection automatically disconnected from your device when no more data is being transferred.
8. The **Daily automatic disconnect** disconnects the be.IP swift from the Internet every day at a time you set yourself. This setting prevents the Internet provider from forcing the device to disconnect at a time that cannot be determined by the user.

Confirm your settings by clicking **OK**.

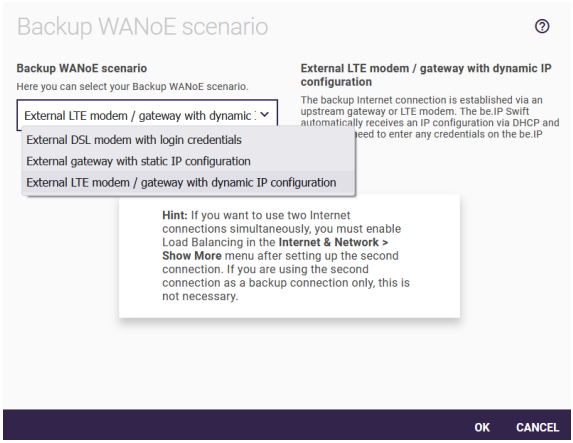
10.2.2 WANoE backup

If you want to set up a backup connection for your primary Internet access, e.g. via an LTE modem connected to the WANoE port, click the **Enable WANoE Backup** button on the Internet access overview page. If you have already set up a backup connection, it will be displayed in the overview as another Internet connection. You can then edit it if necessary.

If you set up the Internet connection via an SFP module, a backup connection is automatically created via any gateway or modem with dynamic IP configuration connected to the WANoE port. You cannot edit this entry here.

Note
*If you want to use two Internet connections at the same time, you must enable Load balancing in the **Internet & Network > Show More** menu after setting up the second connection.*
If you are only using the second connection as a backup connection in case of failure of the first, this is not necessary. If you have already created a second Internet connection, you will find a link into the menu at the bottom of the overview page.

Backup WANoE scenario



If you are editing an existing backup connection, you have the option here to deactivate it again. There are three options available for setting up a backup connection:

- *External DSL modem with access data:* The backup Internet connection is established via an external modem. On the be.IP swift, you enter the access data for authentication with your provider.

- *External gateway with static IP configuration:* The backup Internet connection is established via an upstream gateway. You enter a static IP configuration for the be.IP swift, but do not need any access data to enter on the be.IP swift.
- *External LTE modem / gateway with dynamic IP configuration:* The backup Internet connection is established via an upstream gateway or LTE modem. The be.IP swift automatically receives an IP configuration via DHCP and you do not need any access data to enter it on the be.IP swift.

The information required for the setup differs depending on the connection type and, if applicable, also on the connection provider. Please refer to the respective contract documents and setup instructions for the required information.

10.3 Setting up VPN menu

All the configured VPN configures will be displayed in a list. When this router is started up, the list is empty. When you click **Set up VPN** for the first time, you are taken directly to the scenario selection.

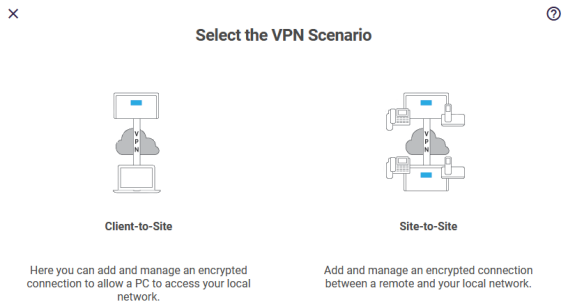
You can change the status by clicking on ^ or v, delete existing entries or edit them. Click **New** to add a new VPN connection.

In the **Show more** menu area, you can view a list of IP address pools available for VPN connections.

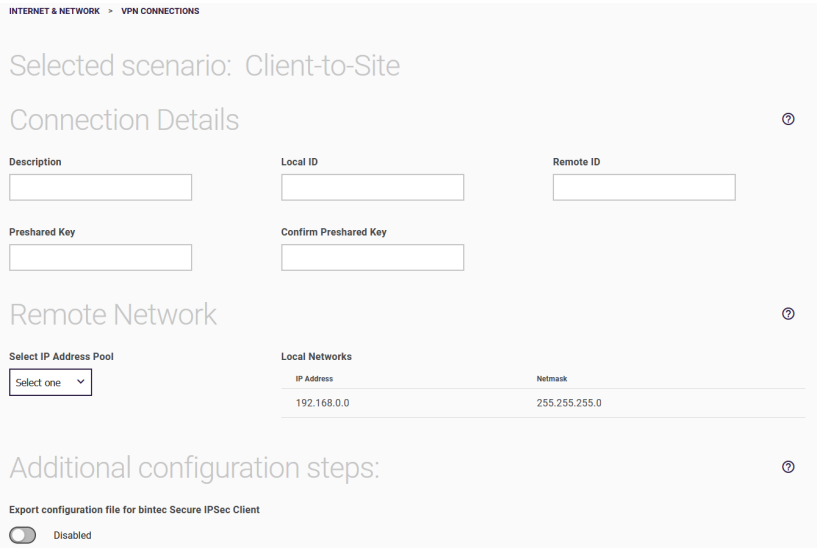
Selecting the VPN scenario

You can allow dial-up of a single host or connection between two networks.

Note
Please note that the selection of VPN connection options depends on the system-specific properties. Additional licenses can be purchased if necessary.



10.3.1 Scenario: Client to Site

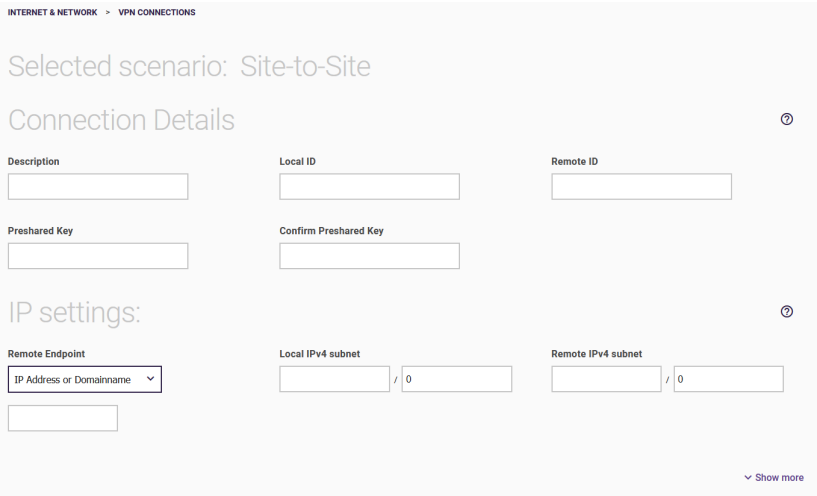


1. Enter a **description** for the connection.
2. Enter your own ID for **Local IPSec ID**.
3. Enter the remote **IPSec ID**.
   To establish an IPSec connection, each IPSec partner must be able to identify the ID of the other partner. Therefore, both IDs must be configured on both IPSec peers.

4. IPSec peers use preshared keys for authentication. The **Preshared key** must be configured identically on both sides.
5. Under **Select IP Address Pool**, the names of all configured IP address pools are listed. You can select an existing IP address pool or use **New** to configure a new IP address pool.
6. Enter a new **IP pool name**.
7. All configured **Local Networks** are listed here.
8. Enter a new **IP address range**. The pool must correspond to an existing network.
9. Select the **Export configuration file for bintec Secure IPSec Client** option to create a file with the corresponding data for importing to a bintec Secure IPSec Client.
   After confirming your settings with **OK**, the current peer description is displayed. You can enter the **Public Gateway address** of your device and then export the required data. If the gateway does not have a fixed public IP address, use the **Domain name of public gateway** option. Here you can enter a DynDNS name.

Click on **OK**.

10.3.2 Scenario: Site to Site



1. Enter a **description** for the connection.
2. The IPSec partners must identify and authenticate each other to establish an IPSec connection.
   Enter the **Local ID** of your own IPSec Gateway and that of the remote IPSec Gateway (**Remote ID**).
3. IPSec peers use preshared keys for authentication. The **Preshared key** must be configured identically on both sides.
4. For **Remote Endpoint**, enter the (public) IPv4 address or DNS name of the remote IPSec peer.
   If you select *Any (Responder only)* here, you do not have to specify a publicly reachable address for the remote endpoint. In this case, be.IP swift does not establish an IPSec connection to the partner by itself, but accepts incoming connections without checking the source address.
5. Enter the IPv4 address and netmask of the Local IPv4 subnet.
6. Enter the IPv4 address and netmask of the Remote IPv4 subnet.

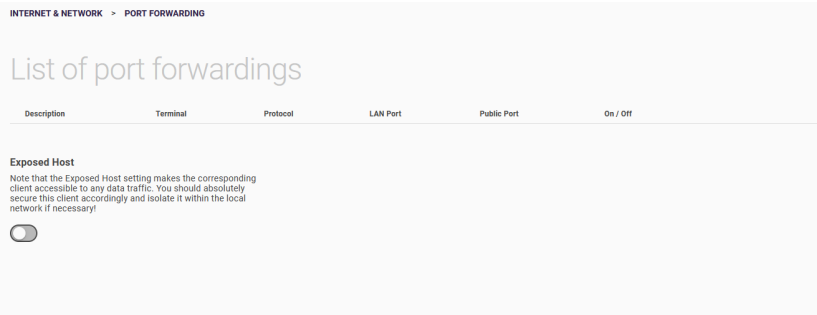
Confirm your settings by clicking **OK**.

10.4 Setting up port forwarding

Normally, your **be.IP swift** is protected by the firewall and Network Address Translation (NAT) against all connections that come in from the Internet for a destination in your local network but have not been requested from there. For certain purposes, however, it may be useful or even necessary to set up an exception for this protection, e.g. if you want to reach be.IP swift from the Internet while traveling. Some online games also require port forwarding in order to use multiplayer functions.

To ensure that there is no unchecked gap in the security of your network, port forwarding only ever allows certain incoming connections to a specific destination within your network.

You will first see a list of entries that have already been created.



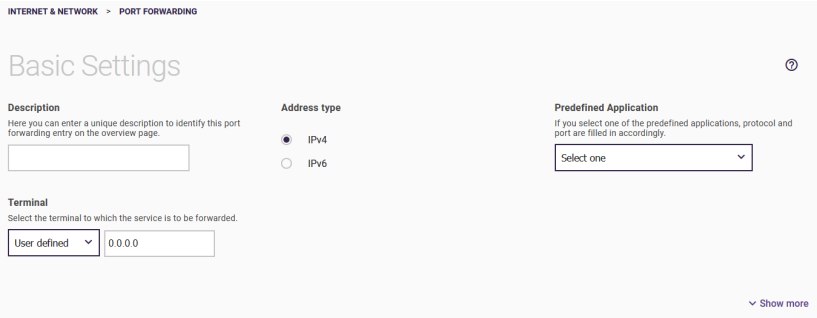
In addition to rules that forward specific traffic to specific destinations, you can also set up what is called an **Exposed Host**. A PC or server set up as an Exposed Host receives any type of traffic that is not previously forwarded to another destination by a specific rule.

Note
*The **Exposed Host** setting makes the corresponding client accessible to any data traffic. You should definitely secure this client accordingly and isolate it within the local network if necessary!*
The function is not available for backup connections!

You can delete or edit existing entries. Click **New** to create a new entry.

To allow incoming data traffic, you only need to specify a few parameters: The interface where the traffic reaches your network, the client (PC, server, or similar) on the local network to which the data should be transferred, and the type of traffic.

Basic settings



1. Enter a **description** that clearly characterizes the port forwarding.
2. Under **Address type** you can select whether you want to set up port forwarding based on IPv4 or IPv6 addresses. Basically the necessary settings do not differ, but for IPv6 some more options are available (see *Port forwarding with IPv6 addresses*).
3. Select a **Predefined application**. In each case, this specifies a combination of protocol(s) and corresponding ports that are commonly used for the applications. The combination used in each case is also displayed in the selection, e.g. *DNS Server (UDP:53)*.
4. Under **Terminal** you can select from the IP addresses of all devices connected to the be.IP swift to specify the device to which the traffic should be routed. If a device is not displayed, you can enter the corresponding IP address manually if you select *User-defined* here.

If you have not selected a predefined application but choose *User-defined* in the corresponding field, two more fields are available:

1. Select the **Protocol** that will be used for the connection to be shared.
2. Specify the port to which the connection from the Internet will be established.

In the **Show more** menu area, you can define the port forwarding rule in more detail:

1. **Public port:** If the connection on the local network is to be directed to a different port, uncheck **Original** here and specify the port on which the device on the local network will accept the connection.
2. **Remote IP address:** If necessary, specify a specific public IP address here from which connections will be allowed. Connection attempts from other addresses are then ignored. The default setting *0.0.0.0* means that no restriction is made.
3. **Source zone:** Here you can select over which Internet connection the port forwarding data is received.

Confirm your settings by clicking **OK**.

10.4.1 Port forwarding with Ipv6 addresses

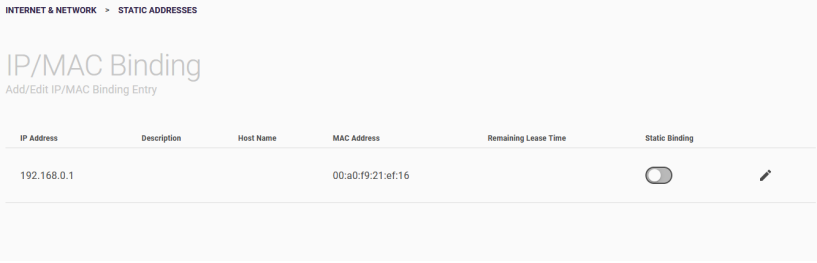
Basically, the settings you make for port forwarding with IPv6 addresses are the same as with IPv4 addresses. However, there are the following changes to the configuration page when you select IPv6 under Type of address:

- **Update prefix automatically**: An IPv6 address consists of a prefix assigned by the ISP and a host part that identifies a specific client. If the provider prefix changes, your device can update it automatically, and you only need to enter the client-specific part of the IPv6 address. If you enable this option, the field for entering the IP address (terminal) changes so that you do not enter the full IPv6 address.

- **Forwarding Behavior**: You can set up different types of forwarding with different levels of restriction:
    - *Specific device, specific port/application*—forwarding applies to exactly one device and one application or one port.
    - *Specific device, all ports/applications*—forwarding applies to exactly one device, but to all ports, so any type of traffic will be forwarded to the device.
    - *All devices, specific port/application*—forwarding applies to all devices on the local network, but only to a specific application or port.
- The **Remote IP Address** field changes to accommodate an IPv6 address. Entering ::0 allows all external sources.

10.5 IP/MAC Binding menu

The **IP/MAC Binding** menu displays a list of all clients connected to your be.IP swift. In the process, the remaining validity period of this configuration is displayed for the devices that have obtained an IP configuration from your be.IP swift:



You have the option to assign a desired IP address from the IP address pool of be.IP swift to certain devices via their MAC address. To do this, you can activate the **Static Binding** option in the list to apply a list entry as a fixed binding. You can also

manually create a fixed IP/MAC binding by setting it up in the **New** submenu:

1. Enter the **MAC** address to which the IP address specified in **IP address** should be assigned.
2. Also enter the name of the host to whose **MAC address** the **IP address** will be bound.

11 Video instructions

Do you need help with the configuration of your **be.IP swift**?

The videos offer quick solutions and instructions on topics related to Internet and telephony.

Numerous help videos explaining initial setup, commissioning and configuration in a simple and clear way can be found on the Internet at: *helpcenter.bintec-elmeg.com.*

12 Licenses and conformity

12.1 Open Source Code Licensing Notice

This product contains software that is licensed under Open Source Code Licenses and is provided to you under the terms of those licenses. A copy of the license text can also be found in the configuration interface of the be.IP swift.

On the Internet, you can find the license text in the *bintec elmeg download archive*. You can obtain a complete machine-readable copy of the source code from us within three years of the system software release being placed on the market by contacting us at *info@bintec-elmeg.com*.

12.2 EU Conformity

bintec elmeg GmbH hereby declares that the **be.IP swift** meets the Directive 2014/53/EU (RED), 2011/65/EU (RoHS) and 2009/125/EC (ErP). The full text of the EU Declaration of Conformity is available at the following address: *Declarations of conformity (bintec-elmeg.com)*.

CE

12.3 Safety-related data

12.3.1 Interfaces

DSL, ISDN, FXS, LAN/WANoE (Ethernet), USB

Classification according to DIN EN 62368-1, connection cable min. CAT. 5.

12.3.2 Mains connection

- Plug-in power supply WA-48B12FG

- Rated voltage 100–240 V ~
- Power consumption max. 1.5 A
- Rated frequency 50–60 Hz
- Output 12.0 V = 4.0 A

12.3.3 Ambient conditions

Storage: ETSI EN 300 019-1-1: Class 1.2
Temperature: -25 °C to 55 °C, humidity: 10 %RH to 100 %RH

Transportation: ETSI EN 300 019-1-2: Class 2.2
Temperature: -25 °C to 70 °C, humidity: 0 %RH to 95 %RH

Operation: ETSI EN 300 019-1-3: Class 3.1
Temperature: 5 °C to 40 °C, humidity: 5 %RH to 85 %RH without condensation

12.3.4 European regulations

The **be.IP swift** has been designed for operation in all countries of the European Union as well as Switzerland, Norway, Liechtenstein, and Iceland. Operation of this product in any other countries is not permitted.

Frequency bands of the integrated WLAN module

- 2,400–2,483.5 MHz: max. transmission power 100 mW
- 5,150–5,350 MHz: max. transmission power 200 mW (indoor operation only is permitted for this range)
- 5,470–5,725 MHz: max. transmission power 1,000 mW.

The maximum transmission powers of the **be.IP swift** comply with the legally prescribed exposure limits of the European Union.

12.3.5 Disposal

WEEE Reg. No. DE71587309

The product is marked with WEEE symbol: Used electronic products must not be disposed of with household waste! Take the router to the collection point of your municipal waste disposal service (e.g. recycling center) and make an active contribution to environmental protection.

Old devices often contain sensitive personal data. Before disposing of the router, you can permanently delete all personal data by restoring it to its factory settings.

13 Running services and their ports

According to the *BSI TR-03148 Secure Broadband Router* Directive of the German Federal Office for Information Security, you can find a list of services here executed by be.IP swift and the network ports that must be open to execute them. The availability of the services meets the requirements of the BSI.

The following services run on the local network and are **not** accessible from the Internet:

Protocol	Port	Service
TCP	80, 443	HTTP server for WEB GUI
TCP	18443	Gigaset provisioning server
UDP/TCP	53	DNS Relay
UDP/TCP	5060, 5061	SIP (VoIP telephony)
TCP	389	Telephone directory (LDAP server)
TCP	5002	TAPI server
UDP	123	NTP server
TCP	1900	UPnP IGD (disabled in delivery state)
UDP	67	DHCP server

You can disable the telephony services (No. 2, 4, 5, 6) if you do not need the corresponding functions. The protocol ports of disabled services will be closed and the system will no longer accept connections on them. The setting can be found in the **Telephony > Show more > Global settings > Show more > Telephony services menu**.

The following services are accessible from the Internet:

Protocol	Port	Service
TCP	443	HTTPS server for WEB GUI (disabled in delivery state)
UDP	5060	SIP (VoIP telephony–configuration-dependent)

UDP	10512-11022	RTP ports for voice transmission are dynamically selected from this range (disabled in delivery state)
TCP	7547	TR-069 (automatic configuration by the service provider)
UDP	500, 4500, and 68	VPN (disabled in delivery state)

14 Safety instructions

Important
Please read the safety instructions carefully before using this router.

Warning
Electrical voltage on power supply, telephone and network cables is dangerous! Failure to observe the safety instructions can lead to dangerous situations, which can also result in severe injury or death.

To prevent personal injury and damage to property as well as danger to domestic animals and livestock, the following must be observed when installing and operating the **be.IP swift**:

- The router must not be opened.
- Do not install the router or connect or disconnect any lines during a thunderstorm.
- Operation is only intended for dry rooms inside buildings.
- Choose a place for installation that is as far as possible out of the reach of domestic animals and livestock.
- The mains socket must be located close to the router and be easily accessible.
- Lay the cables so that no one can step on or trip over them.
- Connect cables only to the designated sockets, use only approved accessories.
- Do not allow liquids to infiltrate the interior of the router (risk of electric shock or short circuit).
- Avoid direct sunlight. Ensure sufficient ventilation.
- Avoid operating in the direct vicinity of a radiator.
- Before drilling, make sure that there is no domestic installation at the drilling site. Damage to gas, power, signal, or water lines may result in danger to life or property.
- Ventilation slots are required for cooling and must not be covered.
- The unit may only be operated with the enclosed plug-in power supply unit.

- The router is intended for use as an upright tabletop device. In this case, the router should stand on a smooth flat surface. A mounting bracket is included with the router for optional wall mounting.
- Only clean the **be.IP swift** with a soft, dry, anti-static cloth and do not use any cleaning agents or solvents.