bintec elmeg

Manual
be.IP

Workshops

Legal Notice

Warranty

This publication is subject to modifications.

bintec elmeg GmbHbintec elmeg GmbHbintec elmeg GmbHbintec elmeg GmbHbintec elmeg GmbH is not liable for the information in this manual. bintec elmeg GmbHbintec elmeg GmbHbintec elmeg GmbHbintec elmeg GmbHbintec elmeg GmbH accepts no liability for any direct, indirect, incidental, consequential or other damages associated with the distribution, provision or use of this manual.

Table of Contents

Chapter 1 Using be.IP as a VDSL modem

Requirements

- A **be.IP**
- A **be.IP plus**

Configuration destination

Using a **be.IP** as a VDSL modem and using other device functions

1.1 Preparation

1.1.1 Installation

(1) Open your web browser and enter the IP address *192.168.0.251* in your web browser's address field.

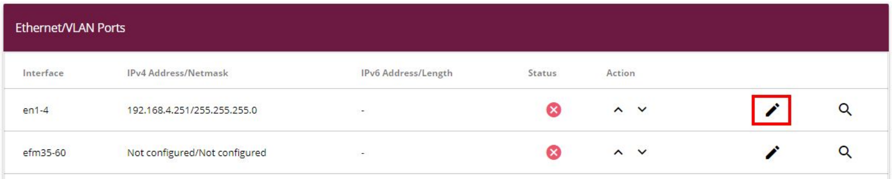
(2) Enter your login details in the fields **Login Name** and **password** and press **log in**.
The **Initial operation** wizard opens.

(3) Exit the **Initial operation** wizard by selecting *Full Access* in the header under **View**.

1.1.2 Deleting preconfigured addresses

Deleting preconfigured OP addresses in the *en1-4* interface (DMZ/WAN port, blue) enables further configuration in this IP area. The existence of the IP address has no effect on the actual function of the PPPoE on this interface.

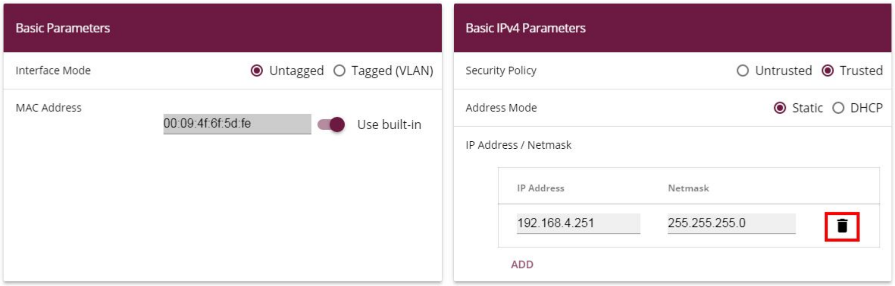
(1) Go to **LAN->IP Configuration->Interfaces->en1-4** ✎



Ethernet/VLAN Ports

Interface	IPv4 Address/Netmask	IPv6 Address/Length	Status	Action		
en1-4	192.168.4.251/255.255.255.0	-	⊗	^ ˅	✎	🔍
efm35-60	Not configured/Not configured	-	⊗	^ ˅	✎	🔍

(2) Click on the 🗑 symbol in the field **IP Address / Netmask** to delete the entry.



Basic Parameters

Interface Mode ● Untagged ○ Tagged (VLAN)

MAC Address 00:09:4f:6f:5d:fe Use built-in

Basic IPv4 Parameters

Security Policy ○ Untrusted ● Trusted

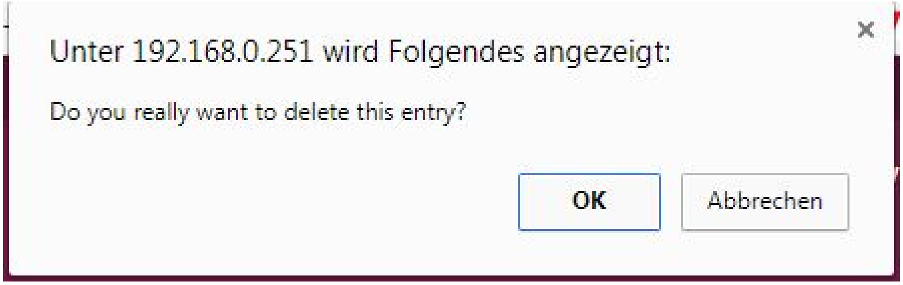
Address Mode ● Static ○ DHCP

IP Address / Netmask

IP Address	Netmask
192.168.4.251	255.255.255.0

(3) Press **OK** to confirm.

(4) A warning appears.



Unter 192.168.0.251 wird Folgendes angezeigt:

Do you really want to delete this entry?

(5) Press **OK** to confirm.

1.2 Configuration

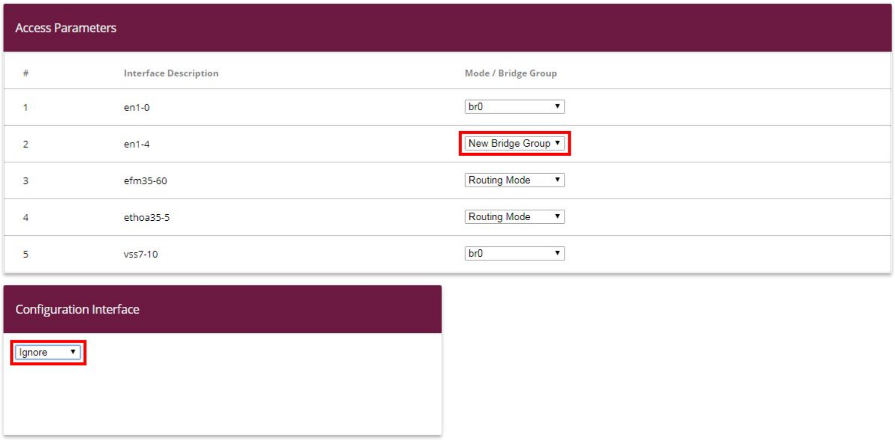
1.2.1 Connecting the VDSL modem and the ethernet interface

You connect the ethernet interface **en1-4** and the VDSL interface of the modem using a bridge group.

(1) Go to **System Management** -> **Interface Mode / Bridge Groups**-> **Interfaces**.

(2) Under **en1-4** select `New Bridge Group`.

(3) Under **Configuration Interface** select `Ignore`.



Access Parameters

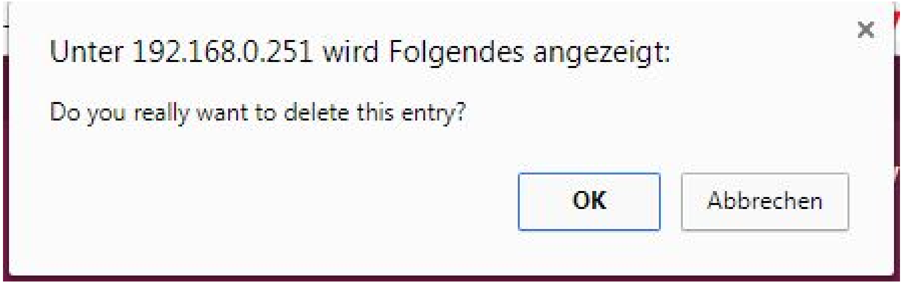
#	Interface Description	Mode / Bridge Group
1	en1-0	br0
2	en1-4	New Bridge Group
3	efm35-60	Routing Mode
4	ethoa35-5	Routing Mode
5	vss7-10	br0

Configuration Interface

Ignore

(4) Press **OK** to confirm.

A warning appears.



Unter 192.168.0.251 wird Folgendes angezeigt:

Do you really want to delete this entry?

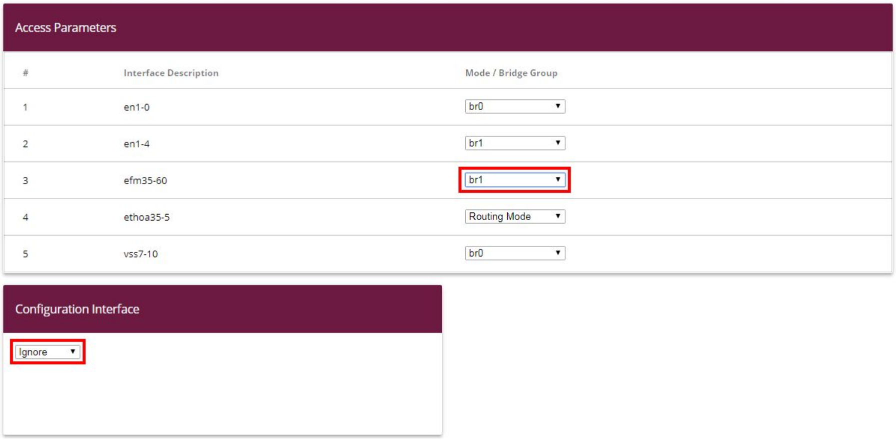
(5) Press **OK** to confirm.

en1-4 will be added to bridge group `br1`.

Add the interface **efm35-60** to bridge group `br1` in the same way.

(1) Under **efm35-60**, also add *New Bridge Group*.

(2) Under **Configuration Interface** select *Ignore*.



Access Parameters

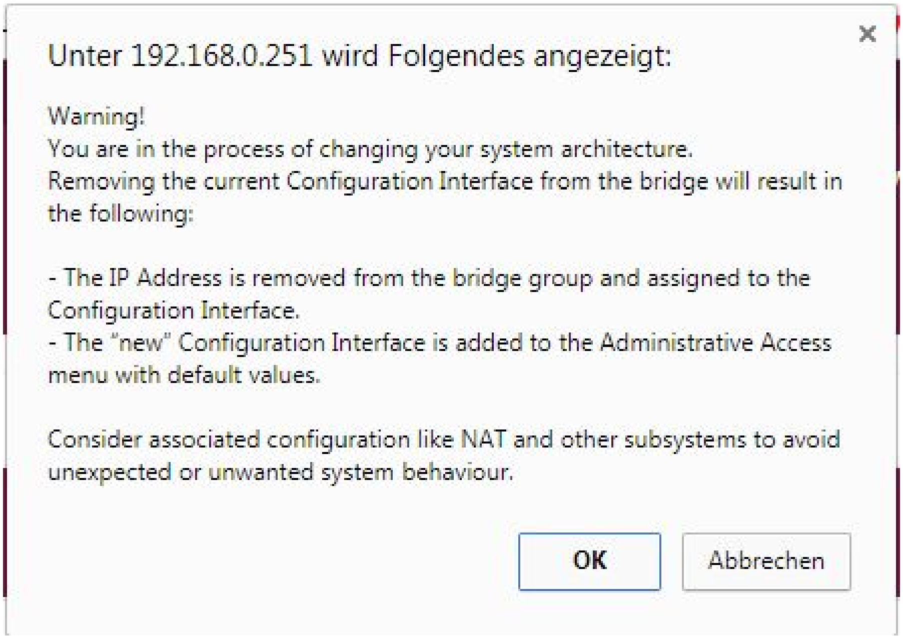
#	Interface Description	Mode / Bridge Group
1	en1-0	br0
2	en1-4	br1
3	efm35-60	br1
4	ethoa35-5	Routing Mode
5	vss7-10	br0

Configuration Interface

Ignore

(3) Press **OK** to confirm.

A warning appears.



Unter 192.168.0.251 wird Folgendes angezeigt:

Warning!
You are in the process of changing your system architecture.
Removing the current Configuration Interface from the bridge will result in the following:

- The IP Address is removed from the bridge group and assigned to the Configuration Interface.
- The "new" Configuration Interface is added to the Administrative Access menu with default values.

Consider associated configuration like NAT and other subsystems to avoid unexpected or unwanted system behaviour.

(4) Press **OK** to confirm.

efm35-60 will be added to bridge group `br1`.

The interface **en1-4** is available as the incoming interface for a PPPoE connection.

1.2.2 Configuration on the dial up router

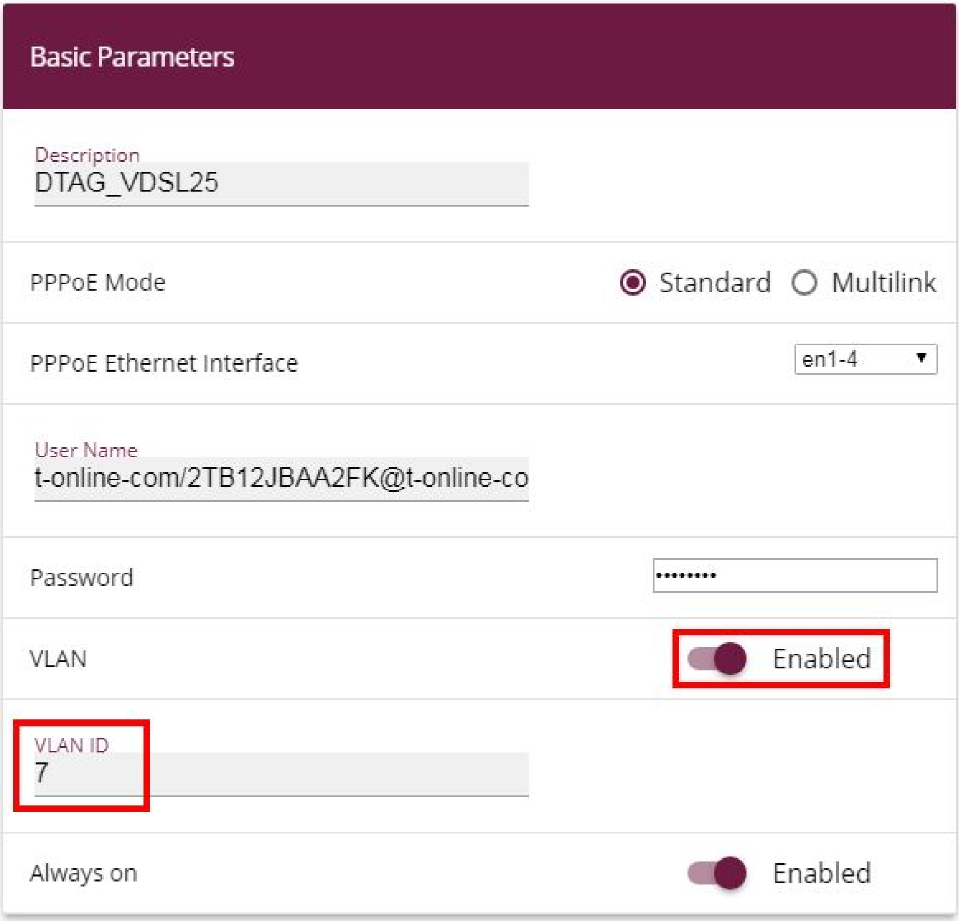
You configure **VLAN-ID** = `7` on the dial up router (i.e. on a **be.IP plus**).

(1) Go to **WAN**->**Internet + Dialup**->**PPPoE**->**<connection>**->✎

(2) Select **VLAN**.

(3) Enter **VLAN-ID** = `7`.

(4) Press **OK** to confirm.



Basic Parameters

Description
DTAG_VDSL25

PPPoE Mode ● Standard ○ Multilink

PPPoE Ethernet Interface en1-4

User Name
t-online-com/2TB12JBAA2FK@t-online-co

Password ••••••••

VLAN Enabled

VLAN ID
7

Always on Enabled

(1) Connect the interfaces **en1-4** from both devices with an ethernet cable.
The **be.IP** VDSL modem synchronises. The WAN partner on the **be.IP plus** dials up the **be.IP**.

1.2.3 Using further functions of the be.IP

You can use further functions of the **be.IP**.

To do this on the **be.IP** you must

- change your IP address
- deactivate the DHCP server
- set up the die standard route to **be.IP plus**
- enter **be.IP plus** as the DNS server.

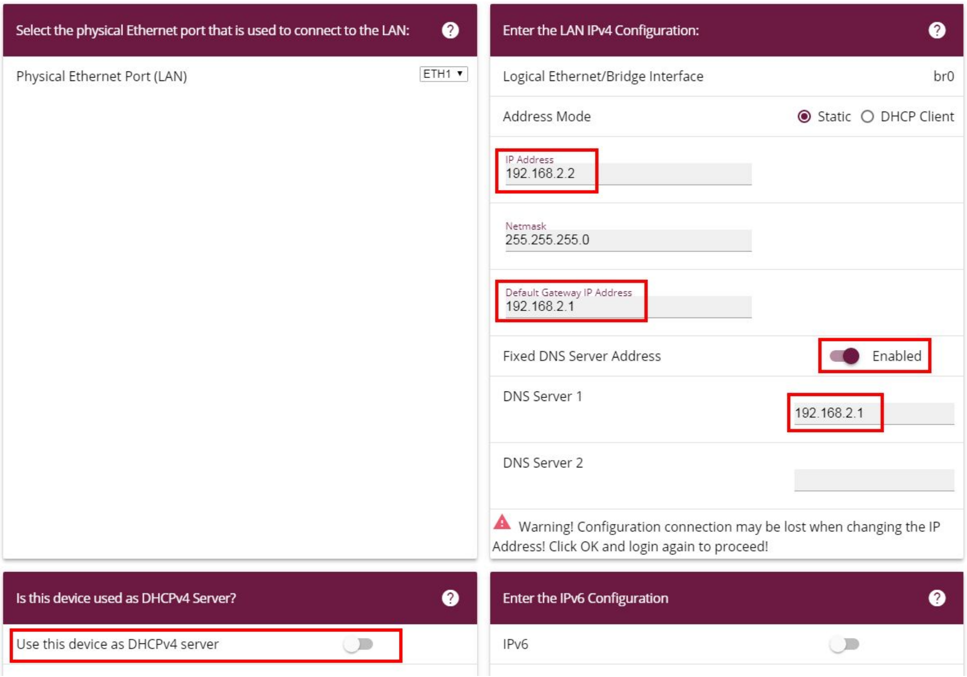
(1) Go to **Wizards** -> **Initial Steps** -> **Basic Settings**.

(2) Change your **IP Address**, e.g. into `192.168.2.2`.

(3) Deactivate **Use this device as DHCPv4 server**.

(4) Under **Default Gateway IP Address**, enter e.g. `192.168.2.1` to make the standard route show on the device with the PPPoE WAN partners.

(5) Under **DNS-Server 1**, enter the same IP address as above to add this device as a DNS server, e.g. `192.168.2.1`.



Select the physical Ethernet port that is used to connect to the LAN:

Physical Ethernet Port (LAN): ETH1

Enter the LAN IPv4 Configuration:

Logical Ethernet/Bridge Interface: br0

Address Mode: ● Static ○ DHCP Client

IP Address: 192.168.2.2

Netmask: 255.255.255.0

Default Gateway IP Address: 192.168.2.1

Fixed DNS Server Address: Enabled

DNS Server 1: 192.168.2.1

DNS Server 2

Warning! Configuration connection may be lost when changing the IP Address! Click OK and login again to proceed!

Is this device used as DHCPv4 Server?

Use this device as DHCPv4 server

Enter the IPv6 Configuration

IPv6

After plugging in, *br0*, for example, is available as a switch extension. You can also access the network from other functions like Access Point or IPSec.

1.3 Overview of Configuration Steps

Deleting preconfigured addresses

Field	Menu	Value
IP address / Netmask	**LAN->IP Configuration->Interfaces-> en1-4** ✎	🗑

Connecting the VDSL modem and the ethernet interface

Field	Menu	Value
en1-4	**System Administration -> Interface**	`New Bridge Group`

Field	Menu	Value
	Mode / Bridge Groups->Interfaces	
Configuration interface	**System Administration -> Interface Mode / Bridge Groups->Interfaces**	*Ignore*
efm35-60	**System Administration -> Interface Mode / Bridge Groups->Interfaces**	*br1*
Configuration interface	**System Administration -> Interface Mode / Bridge Groups->Interfaces**	*Ignore*

Configuration on the dial up router

Field	Menu	Value
VLAN	**WAN->Internet + Dialup->PPPoE-><connection>->** ✎	*Enabled*
VLAN ID	**WAN->Internet + Dialup->PPPoE-><connection>->** ✎	*7*

Using further functions of the be.IP

Field	Menu	Value
IP address	**Wizards -> Initial Steps -> Basic Settings**	e. g. *192.168.2.2*
Use this device as a DHCPv4 server	**Wizards -> Initial Steps -> Basic Settings**	*Enabled*
Standard Gateway IP Address	**Wizards -> Initial Steps -> Basic Settings**	e. g. *192.168.2.1*
DNS Server 1	**Wizards -> Initial Steps -> Basic Settings**	e. g. *192.168.2.1*

Chapter 2 Creating configuration access for the user and using special applications

2.1 Introduction

The system administrator can set up individual configuration access for all users. The user can thus display their most important personal settings and individually customise some of them. For this, a **user name** and **password** must be entered in the user HTML configuration, and personal access authorised.

Basically, there are two different kinds of user accounts: Users with access freely defined by the administrator, and users assigned to applications like system telephone book, connection data, hotel function and mini call centre. Users assigned by the administrator have access to a heavily reduced configuration screen. Users assigned to applications can view the menu corresponding to each application as it appears to the administrator.

You can access help on available configuration options via the online help system.

The **GUI** (Graphical User Interface) is used for configuring.

Requirements

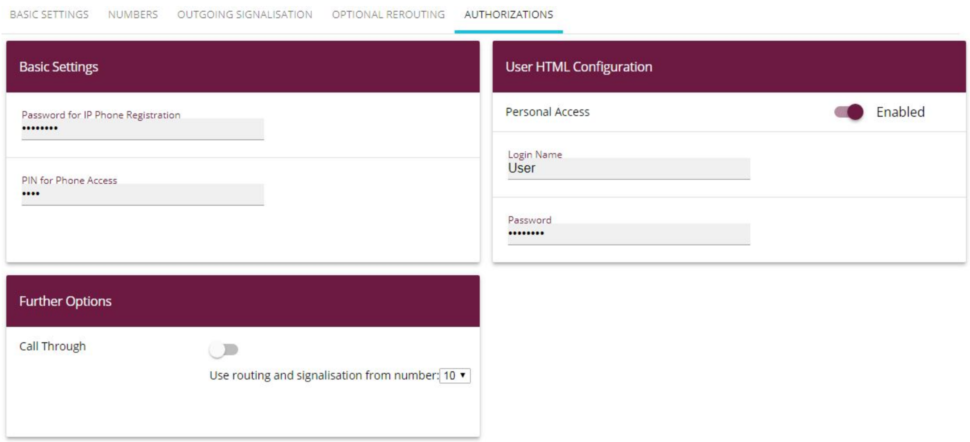
- A **be.IP** or a **be.IP plus**
- A configured baseline scenario for telephone services via VoIP or ISDN and an optional configured scenario for mini call centre. To configure baseline scenarios please note the instructions in the **quick reference guide** and the corresponding **workshops**.

2.2 Configuration

2.2.1 Access configuration for users (”user portal”)

Set up configuration access for each user on your system (known as a user portal), with which they can change their telephone service settings and retrieve status information.

(1) Go to **Numbering** -> **User Settings** -> **User** . Choose the ✎ icon to edit existing entri. Select the **Authorizations** menu.



BASIC SETTINGS | NUMBERS | OUTGOING SIGNALISATION | OPTIONAL REROUTING | AUTHORIZATIONS

Basic Settings

Password for IP Phone Registration: ••••••••

PIN for Phone Access: ••••

User HTML Configuration

Personal Access: Enabled

Login Name: User

Password: ••••••••

Further Options

Call Through

Use routing and signalisation from number: 10

Fig. 1: **Numbering** -> **User settings** -> **Users** -> ✎ -> **Authorizations**

Proceed as follows:

(1) Activate **Personal Access**.

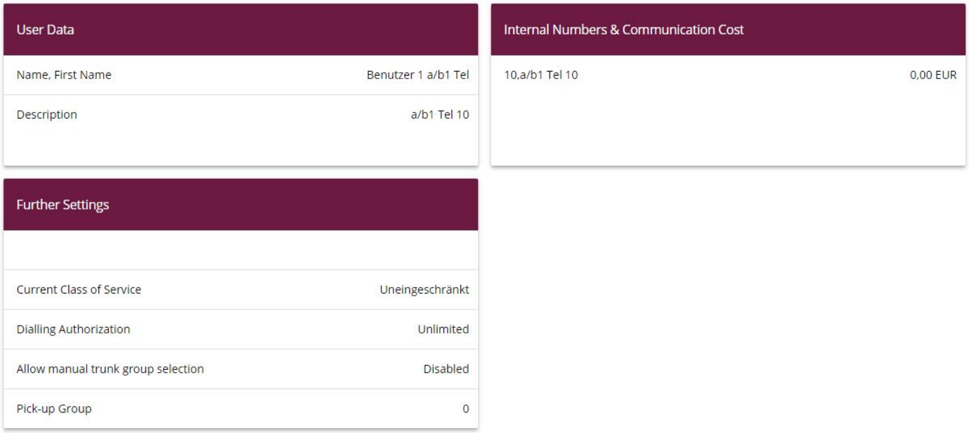
(2) Enter a **Login Name** for this user, e.g. `User`.

(3) Enter a **Password** for this user, e.g. `User`. These details are required for login on the user interface.

(4) Click **Apply**.

This concludes the configuration. The user can now login with the user name and password and configure certain things using the HTML configuration themselves.

Results:



User Data

Name, First Name	Benutzer 1 a/b1 Tel
Description	a/b1 Tel 10

Internal Numbers & Communication Cost

10,a/b1 Tel 10	0,00 EUR

Further Settings

Current Class of Service	Uneingeschränkt
Dialling Authorization	Unlimited
Allow manual trunk group selection	Disabled
Pick-up Group	0

Fig. 2: User configuration screen

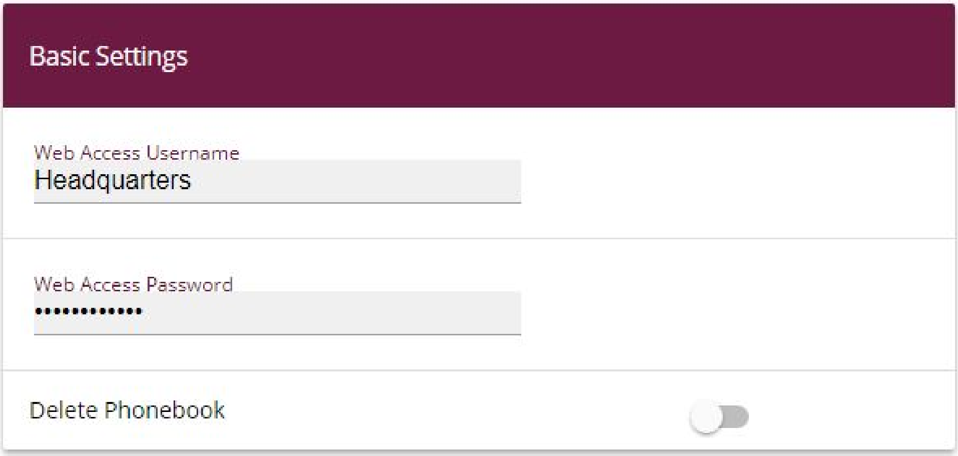
2.2.2 Applications

For the applications system telephone book, connection data and mini call centre management, configuration access can be set up by the administrator, allowing respective users to fulfil their particular tasks.

System Telephone Book

In the submenu **General** you define the user name and password for administration of the System Telephone Book.

(1) Go to **Applications** -> **System Phonebook** -> **General**.



Basic Settings

Web Access Username: Headquarters

Web Access Password: •••••••••••••

Delete Phonebook

Fig. 3: **Applications**-> **System Telephone Book** -> **General**

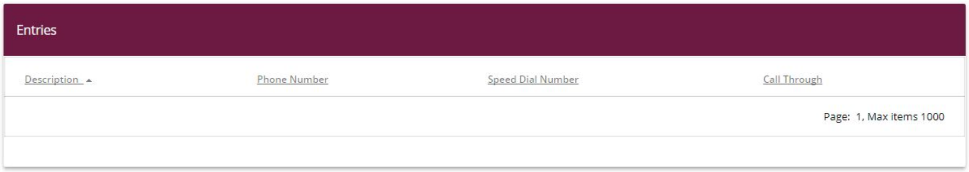
Proceed as follows:

(1) Enter a **Web Access Username** for the System Telephone Book administrator, e.g. `Headquarters`. In the phone book area, the administrator can view and modify the phone book, as well as import and export data.

(2) Enter a **Web Access Password** for the System Telephone Book administrator, e.g. `Headquarters`.

(3) Press **OK** to confirm your entries.

Results:



Entries

Description ▲	Phone Number	Speed Dial Number	Call Through

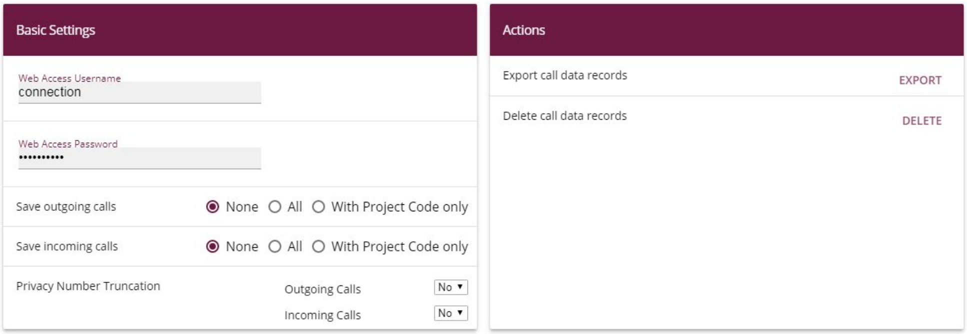
Page: 1, Max items 1000

Fig. 4: Access configuration for System Telephone Book administrator

Connection data

You can set up special configuration access for administration of **connection data**. This allows you to view the data collected on incoming and outgoing calls. The type and format of the collected data can also be configured and current records can be exported or deleted.

(1) Go to **Applications** ->**Call Data Records** -> **General**.



Basic Settings

Web Access Username: connection

Web Access Password: ••••••••••

Save outgoing calls: ● None ○ All ○ With Project Code only

Save incoming calls: ● None ○ All ○ With Project Code only

Privacy Number Truncation: Outgoing Calls: No ▾ Incoming Calls: No ▾

Actions

Export call data records: EXPORT

Delete call data records: DELETE

Fig. 5: **Applications** ->**Call Data Records** -> **General**

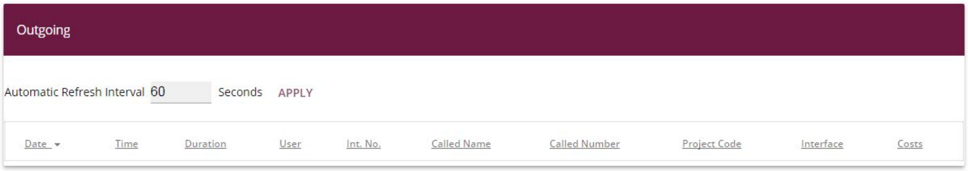
Proceed as follows:

(1) Enter a **Web Access Username** for the Connection Data administrator, e.g. `connection`.

(2) Enter a **Web Access Password** for the Connection Data administrator, e.g. `connection`.

(3) Press **OK** to confirm your entries.

Results:



Outgoing

Automatic Refresh Interval 60 Seconds APPLY

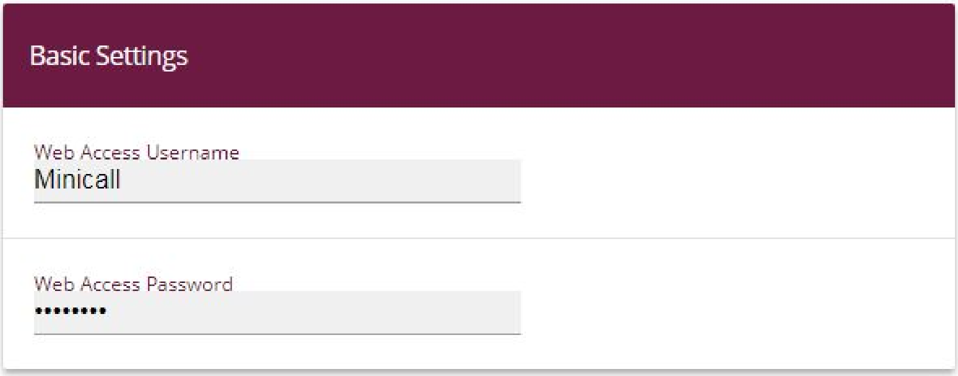
Date	Time	Duration	User	Int. No.	Called Name	Called Number	Project Code	Interface	Costs

Fig. 6: Access configuration for Connection Data administrator

Mini call centre

The mini call centre is an integrated call centre solution for up to 16 agents. In the submenu **General** you can set up an HTML web interface access for the mini call centre manager. The latter can then monitor the status of lines and agents, and modify the settings for lines and agents.

(1) Go to **Applications** -> **Mini Call Center**-> **General**.



Basic Settings

Web Access Username
Minicall

Web Access Password
••••••••

Fig. 7: **Applications** -> **Mini Call Center**-> **General**

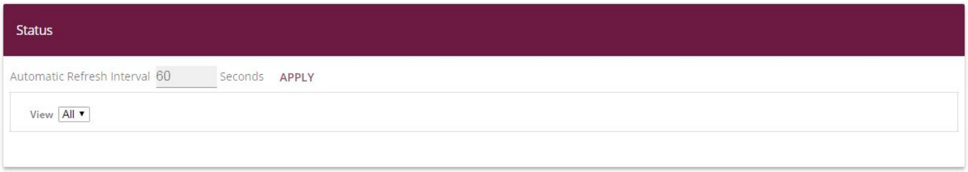
Proceed as follows:

(1) Enter a **Web Access Username** for the Mini Call Centre administrator, e.g. `Minicall`. When a user logs into the user interface under this name, he/she has access to the user interface with selected parameters for administration of the call centre.

(2) Enter a **Web Access Password** for the Mini Call Centre administrator, e.g. `Minicall`.

(3) Press **OK** to confirm your entries.

Results:



Status

Automatic Refresh Interval 60 Seconds APPLY

View All ▾

Fig. 8: Access configuration for Mini Call Center administrator

2.3 Overview of Configuration Steps

Access configuration for users

Field	Menu	Value
Personal Access	**Numbering -> User settings -> Users -> Authorizations**	`Enabled`
Login Name	**Numbering -> User settings -> Users -> Authorizations**	e.g. `User`
Password	**Numbering -> User settings -> Users -> Authorizations**	e.g. `User`

System Telephone Book administration

Field	Menu	Value
Web Access Username	**Applications-> System Phonebook -> General**	e. g. `Headquarters`
Web Access Password	**Applications-> System Phonebook -> General**	e. g. `Headquarters`

Connection data administration

Field	Menu	Value
Web Access Username	**Applications ->Call Data Records -> General**	e.g. `connection`
Web Access Password	**Applications ->Call Data Records -> General**	e.g. `connection`

Mini Call Centre administration

Field	Menu	Value
Web Access Username	**Applications -> Mini Call Center-> General**	e.g. `Minicall`

Field	Menu	Value
Web Access Password	**Applications** -> **Mini Call Center**-> **General**	e.g. *`Minicall`*

Chapter 3 Access from the WAN via HTTPS

3.1 Introduction

The following workshop describes how to configure access from the WAN via HTTPS to a **be.IP** / **be.IP plus**.

The **GUI** (Graphical User Interface) is used for configuring.

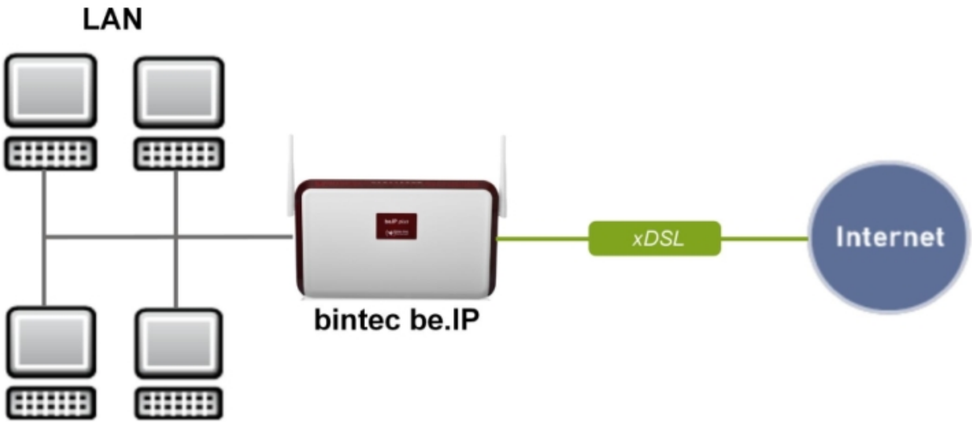


Fig. 9: Example scenario

Requirements

A **be.IP** or a **be.IP plus** with up to date firmware, a basic configuration and in the **View** = `Full Access`

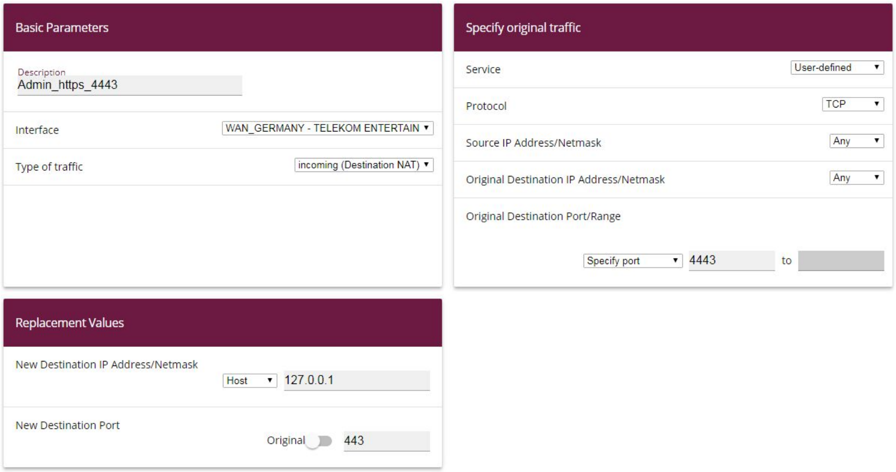
3.2 Configuration

3.2.1 Network Address Translation (NAT) / Port Address Translation (PAT)

Requests for the official address of the **be.IP** (WAN partner) are implemented by a rule and forwarded to the desired IPv4 address on the LAN (exposed host) or to a special DMZ (demilitarised zone, a separate interface monitored by additional firewall rules). In our example the destination for implementation is the **be.IP** itself. For this reason, localhost (127.0.0.1) is used.

In order to protect port scans on the current TCP ports (e.g. 22->ssh, 23->telnet, 80->http, 443->https) from attacks, configure a port address translation (PAT) from the external port 4443 to the internal port 443.

(1) Go to **Network**->**NAT**->**NAT Configuration**->**New**.



Basic Parameters

Description: Admin_https_4443

Interface: WAN_GERMANY - TELEKOM ENTERTAIN

Type of traffic: incoming (Destination NAT)

Specify original traffic

Service: User-defined

Protocol: TCP

Source IP Address/Netmask: Any

Original Destination IP Address/Netmask: Any

Original Destination Port/Range: Specify port 4443 to

Replacement Values

New Destination IP Address/Netmask: Host 127.0.0.1

New Destination Port: Original 443

Fig. 10: **Network**->**NAT**->**NAT Configuration**->**New**

(2) Enter a **Description**, e.g. `Admin_https_4443`.

(3) Select an **Interface**, e.g. `WAN_GERMANY - TELEKOM ENTERTAIN`.

(4) Leave the settings **Type of traffic** = `incoming (Destination NAT).`

(5) Leave**Service** as `User-defined`.

(6) Under **Protocol** select `TCP`.

(7) Select **Original Destination Port/Range** = `Specify port` and enter `4443`.

(8) For **New Destination IP Address/Netmask** = `Host` enter the value `127.0.0.1`.

(9) Under **New Destination Port** deactivate `Original` and enter `443`.

(10) Press **OK** to confirm your settings.

3.2.2 Stateful inspection firewall (SIF)

The firewall blocks packets that have passed through the NAT because the WAN partner is deemed “untrustworthy” in the default settings. No initial requests can therefore be made from this interface. Only requests from trustworthy interfaces can be answered. (All LAN interfaces are deemed trustworthy as standard.)

You have to configure a rule that enables the WAN partner access as an exception to default behaviour.

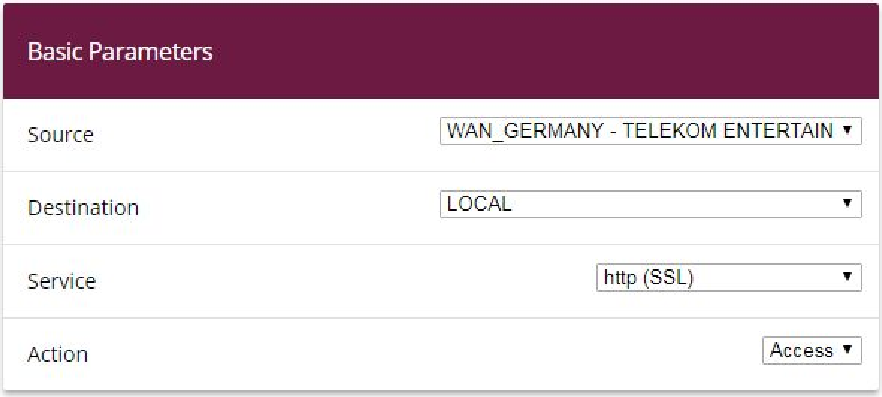
> **Note**
>
> In the firewall, a rule applies that packets enabled by a rule can subsequently no longer be prohibited and vice versa. The sequence of rules is crucial!

In our example the HTTPS service must be enabled for the WAN partner to gain access to the local interface `127.0.0.1`.

> **Note**
>
> HTTPS can be used because PAT has already been carried out.

In the example the service and all necessary interfaces are already predefined. In other circumstances a separate definition might be required beforehand under addresses or services.

(1) Go to **Firewall**->**Policies**->**IPv4 Filter Rules**->**New**.



Basic Parameters

Source	WAN_GERMANY - TELEKOM ENTERTAIN ▾
Destination	LOCAL ▾
Service	http (SSL) ▾
Action	Access ▾

Fig. 11: **Firewall**->**Policies**->**IPv4 Filter Rules**->**New**

(2) Select a **Source** e.g. *WAN_GERMANY_TELEKOM ENTERTAIN*.

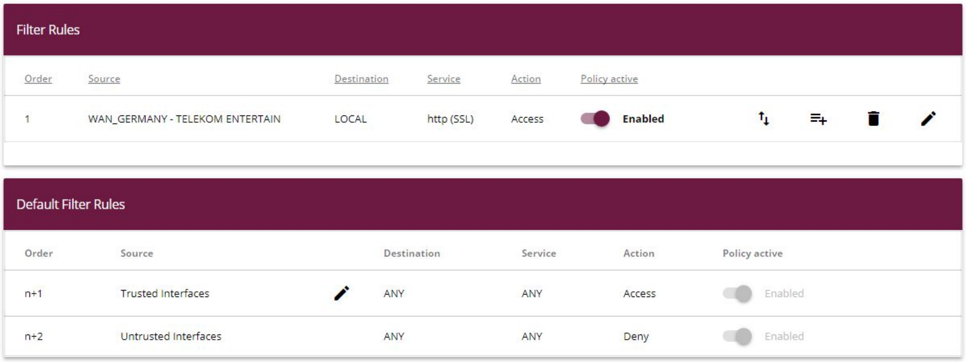
(3) Select the **Destination** *LAN_LOCAL* .

(4) Select the **Service** *http (SSL)*.

(5) Leave **Action** *Access*.

(6) Press **OK** to confirm your settings.

Under **Firewall**->**Policies**->**IPv4 Filter Rules** you will see the following overview:



Filter Rules

Order	Source	Destination	Service	Action	Policy active
1	WAN_GERMANY - TELEKOM ENTERTAIN	LOCAL	http (SSL)	Access	● Enabled

Default Filter Rules

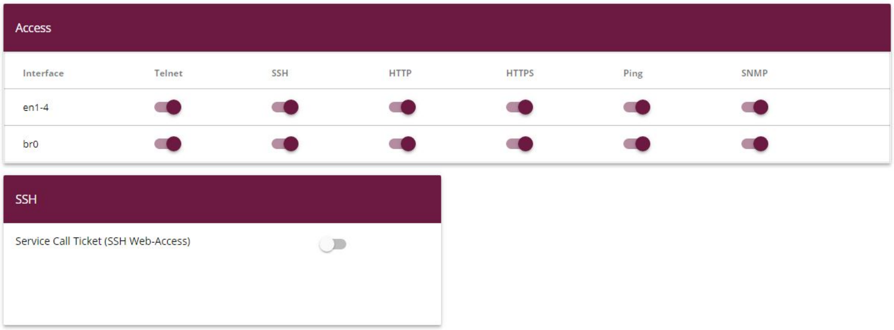
Order	Source	Destination	Service	Action	Policy active
n+1	Trusted Interfaces	ANY	ANY	Access	● Enabled
n+2	Untrusted Interfaces	ANY	ANY	Deny	● Enabled

Fig. 12: **Firewall**->**Policies**->**IPv4 Filter Rules**

3.2.3 Administrative access

Next, enable administrative access to the configuration screen for **be.IP** for the desired scenario. To do this, the WAN partner interface must first be added and then access via the *HTTPS* service enabled.

(1) Go to **System Management**->**Administrative Access**->**Access**.



Access

Interface	Telnet	SSH	HTTP	HTTPS	Ping	SNMP
en1-4	●	●	●	●	●	●
br0	●	●	●	●	●	●

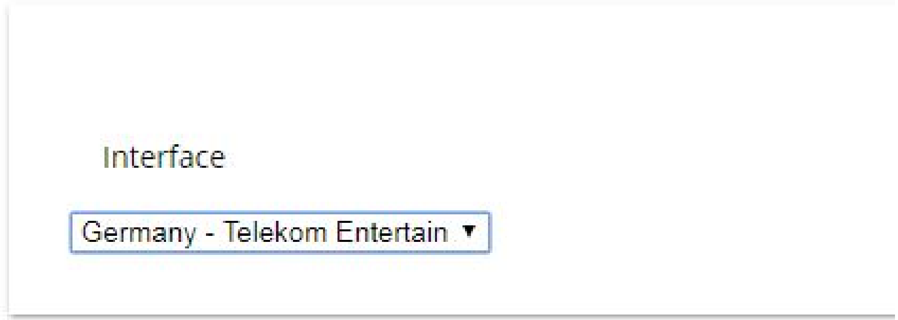
SSH

Service Call Ticket (SSH Web-Access) ○

Fig. 13: **System Management**->**Administrative Access**->**Access**

(2) Press **Add** to add the partner WAN interface.

(3) Select the WAN partner interface, e.g. `Germany - Telekom Business`.



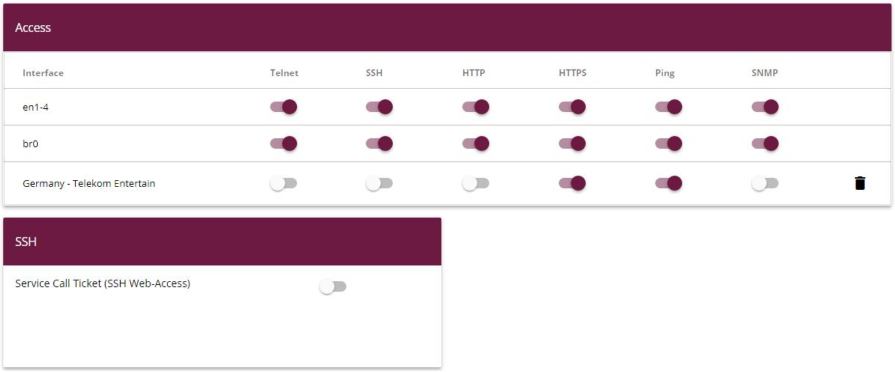
Interface

Germany - Telekom Entertain ▼

Fig. 14: **System Management**->**Administrative Access**->**Access**->**Add**

(4) Press **OK** to confirm your selection.

(5) Enable access via the HTTPS service.



Access

Interface	Telnet	SSH	HTTP	HTTPS	Ping	SNMP	
en1-4	●	●	●	●	●	●	
br0	●	●	●	●	●	●	
Germany - Telekom Entertain	○	○	○	●	●	○	🗑

SSH

Service Call Ticket (SSH Web-Access) ○

Fig. 15: **System Management**->**Administrative Access**->**Access**->**Add**

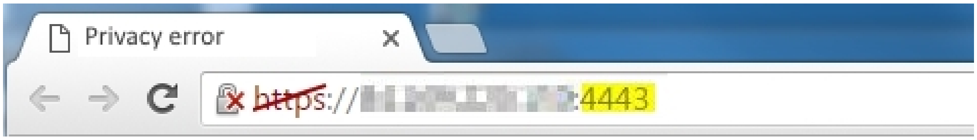
(6) In the row **Germany - Telekom Business**, check the box in the column *`HTTPS`*.

(7) Press **OK** to confirm your settings.

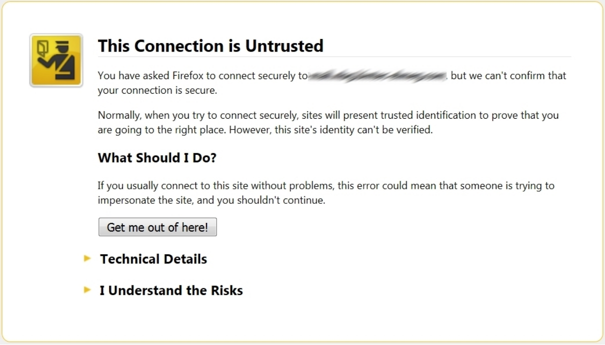
(8) Press **save configuration** to save the configuration.

3.2.4 Access from the WAN

Access from the WAN to the WAN partner's official IPv4 address with port 4443 produces a warning of an "insecure connection", since the browser cannot verify the certificate behind **be.IP** with a familiar CA.



https://[redacted]:4443



This Connection is Untrusted

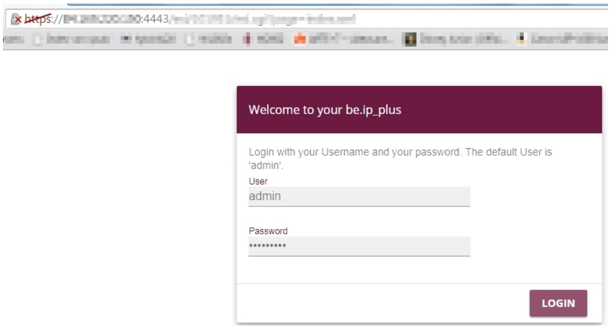
You have asked Firefox to connect securely to [redacted], but we can't confirm that your connection is secure.

Normally, when you try to connect securely, sites will present trusted identification to prove that you are going to the right place. However, this site's identity can't be verified.

What Should I Do?

If you usually connect to this site without problems, this error could mean that someone is trying to impersonate the site, and you shouldn't continue.

If you allow the connection anyway, you reach the login page for the **be.IP**.



https://[redacted]:4443/[redacted]

Welcome to your be.ip_plus

Login with your Username and your password. The default User is 'admin'.

User
admin

Password
•••••••••

Fig. 18: Login page for the **be.IP**

If the safety warning no longer appears, you must obtain a certificate that is deemed safe by the browser and store this in the **be.IP**.

3.3 Overview of Configuration Steps

NAT / PAT

Field	Menu	Value
Description	**Network->NAT->NAT Configuration->New**	e.g. *Admin_https_4443*
Interface	**Network->NAT->NAT Configuration->New**	e.g. *WAN_GERMANY_TELEKOM ENTERTAIN*
Type of traffic	**Network->NAT->NAT Configuration->New**	*incoming (destination NAT)*
Service	**Network->NAT->NAT Configuration->New**	*User-defined*
Protocol	**Network->NAT->NAT Configuration->New**	*TCP*
Original Destination Port/Range	**Network->NAT->NAT Configuration->New**	*Specify Port*: *4443*
New Destination IP Address/Netmask	**Network->NAT->NAT Configuration->New**	*Host*: *127.0.0.1*
New Destination Port	**Network->NAT->NAT Configuration->New**	*Original* deactivate, *443*

SIF

Field	Menu	Value
Source	**Firewall->Policies->IPv4 Filter Rules->New**	e.g. *WAN_GERMANY_TELEKOM ENTERTAIN*
Destination	**Firewall->Policies->IPv4 Filter Rules->New**	*LAN_LOCAL*
Service	**Firewall->Policies->IPv4 Filter Rules->New**	*http (SSL)*
Action	**Firewall->Policies->IPv4 Filter Rules->New**	*Access*

Administrative Access

Field	Menu	Value
Interface	**System Management->Administrative Access->Access->Add**	e.g. *Germany - Telekom Business*

Field	Menu	Value
Germany - Telekom Business	**System Management**->**Administrative Access**->**Access**	`HTTPS` activated.

Chapter 4 Access from the WAN to a web server in the LAN

4.1 Introduction

The following workshop describes how to configure access from the WAN via HTTPS to a web server.

The **GUI** (Graphical User Interface) is used for configuring.

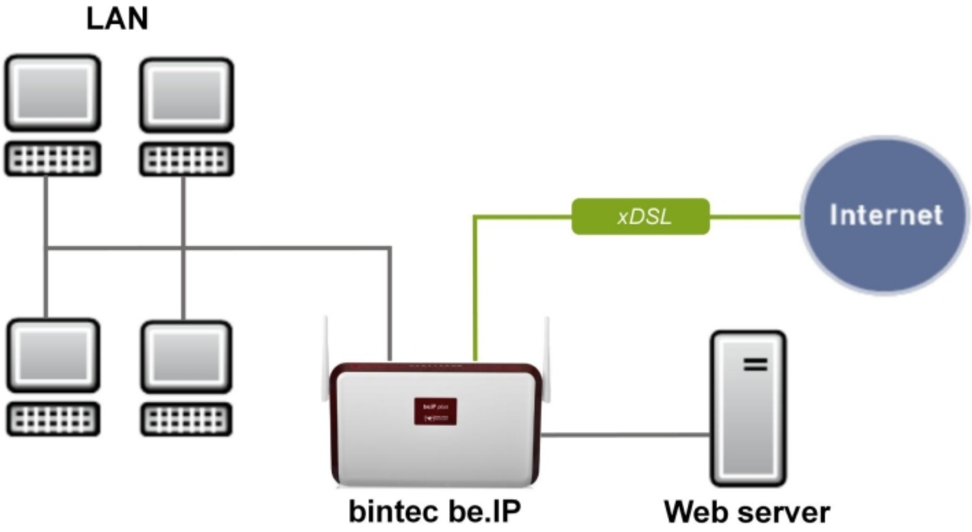


Fig. 19: Example scenario

Requirements

A **be.IP** or a **be.IP plus** with up to date firmware, a basic configuration and in the **View** = `Full Access`

4.2 Configuration

4.2.1 Network Address Translation (NAT) / Port Address Trans-

lation (PAT)

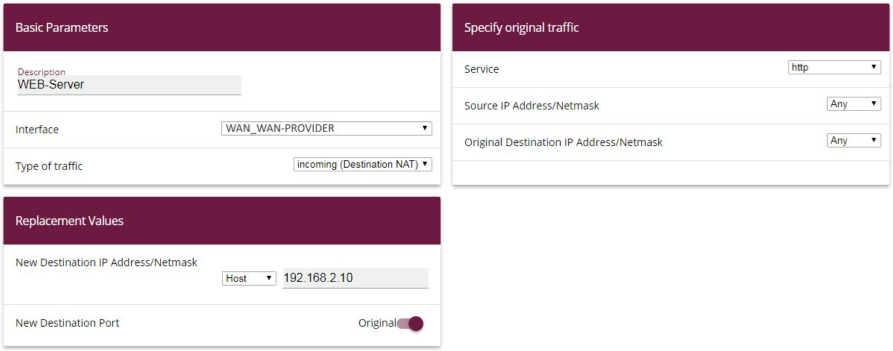
Requests for the official address of the **be.IP** (WAN partner) are implemented by a rule and forwarded to the desired IPv4 address on the LAN (exposed host) or to a special DMZ (demilitarised zone; a separate interface monitored by additional firewall rules). In our example the destination for implementation is a web server.

In order to protect port scans on the current TCP ports (e.g. 22->ssh, 23->telnet, 80->http, 443->https) from attacks, you can configure a port address translation (PAT) from the external port 8080 to the internal port 80. However, this is not a requirement for further configuration.

Configuration without PAT

To configure without PAT, proceed as follows:

(1) Go to **Network**->**NAT**->**NAT Configuration**->**New**.



Basic Parameters

Description
WEB-Server

Interface WAN_WAN-PROVIDER

Type of traffic incoming (Destination NAT)

Specify original traffic

Service http

Source IP Address/Netmask Any

Original Destination IP Address/Netmask Any

Replacement Values

New Destination IP Address/Netmask Host 192.168.2.10

New Destination Port Original

Fig. 20: **Network**->**NAT**->**NAT Configuration**->**New**

(2) Enter a **Description** e.g. *WEB-Server*.

(3) Select an **Interface**, e.g. *WAN_WAN-Provider* as the WAN partner's interface.

(4) Leave the settings **Type of traffic** = *incoming (Destination NAT)*.

(5) Select **Service** = *http*.

(6) In **New Destination IP Address/Netmask** = *Host* enter the value *192.168.2.10* as the web server's IP address.

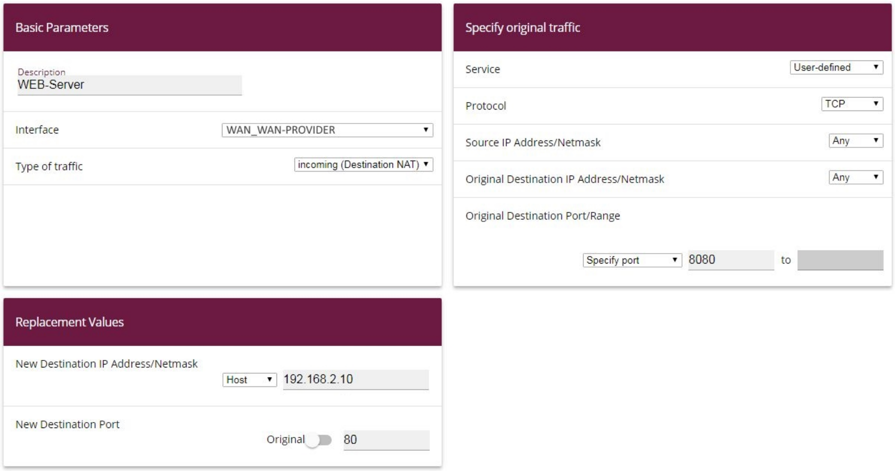
(7) Leave **New Destination Port** = *Original*.

(8) Press **OK** to confirm your settings.

Configuration with PAT

As an alternative to configuring without PAT, configure with PAT as follows:

(1) Go to **Network**->**NAT**->**NAT Configuration**->**New**.



Basic Parameters

Description
WEB-Server

Interface WAN_WAN-PROVIDER

Type of traffic incoming (Destination NAT)

Specify original traffic

Service User-defined

Protocol TCP

Source IP Address/Netmask Any

Original Destination IP Address/Netmask Any

Original Destination Port/Range

Specify port 8080 to

Replacement Values

New Destination IP Address/Netmask Host 192.168.2.10

New Destination Port Original 80

Fig. 21: **Network**->**NAT**->**NAT Configuration**->**New**

(2) Enter a **Description**, e.g. *WEB-Server*.

(3) Select an **Interface**, e.g. *WAN_WAN-Provider* as the WAN partner's interface.

(4) Leave the settings **Type of traffic** = *incoming (Destination NAT)*.

(5) Leave **Service** as *User-defined*.

(6) Under **Protocol** select *TCP*.

(7) Select **Original Destination Port/Range** = *Specify port* and enter *8080*.

(8) In **New Destination IP Address/Netmask** = *Host* enter the value *192.168.2.10* as the web server's IP address.

(9) Under **New Destination Port** deactivate *Original* and enter *80*.

(10) Press **OK** to confirm your settings.

4.2.2 Stateful inspection firewall (SIF)

The firewall blocks packets that have passed through the NAT, since the WAN partner is deemed "untrustworthy" in the default settings. No initial requests can therefore be made from this interface. Only requests from trustworthy interfaces can be answered. (All LAN interfaces are deemed trustworthy as standard.)

You have to configure a rule that enables the WAN partner access as an exception to default behaviour.

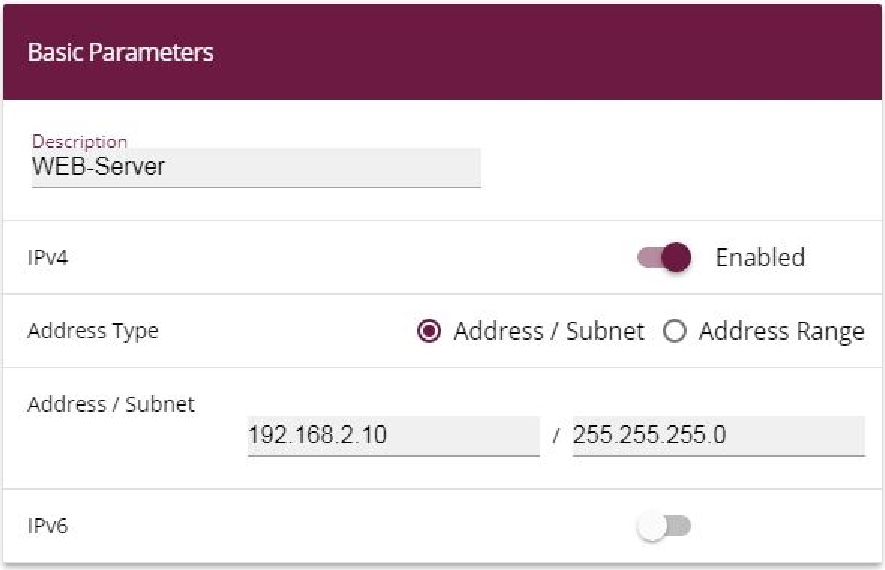
Note

In the firewall, a rule applies that packets enabled by a rule can no longer be prohibited later and vice versa. The sequence of rules is crucial!

In our example the HTTP service must be enabled for the WAN partner to gain access to the local interface `192.168.0.1`.

In the example, all necessary interfaces and the service are already predefined. In other circumstances a separate definition might be required beforehand under addresses or services.

(1) Go to **Firewall**->**Addresses**->**Address List**->**New**.



Basic Parameters

Description: WEB-Server

IPv4: Enabled

Address Type: ● Address / Subnet ○ Address Range

Address / Subnet: 192.168.2.10 / 255.255.255.0

IPv6

Fig. 22: **Firewall**->**Addresses**->**Address List**->**New**

(2) Enter a **Description** e.g. *`WEB-Server`*.

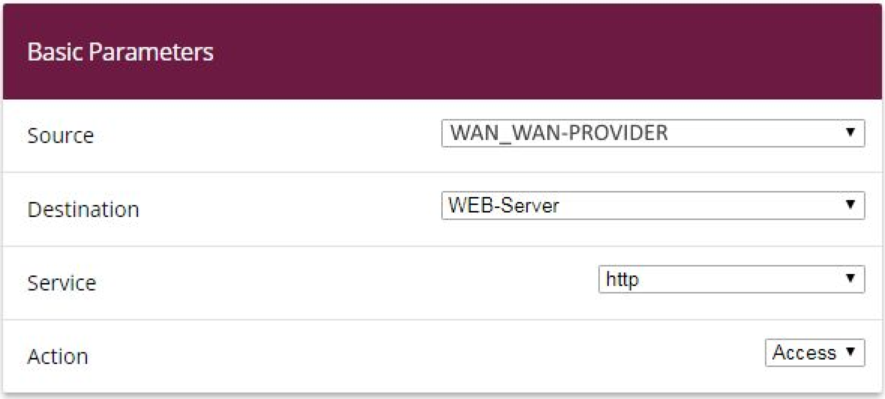
(3) Leave **IPv4** *`Enabled`*.

(4) Leave **Address Type** = *`Address / Subnet`*.

(5) Under **Address / Subnet** enter e.g. *`192.168.2.10`* as the web server's address.

(6) Press **OK** to confirm your settings.

(1) Go to **Firewall**->**Policies**->**IPv4 Filter Rules**->**New**.



Basic Parameters

Source	WAN_WAN-PROVIDER ▼
Destination	WEB-Server ▼
Service	http ▼
Action	Access ▼

Fig. 23: **Firewall**->**Policies**->**IPv4 Filter Rules**->**New**

(2) Select a **Source**, e.g. *WAN_WAN-PROVIDER*.

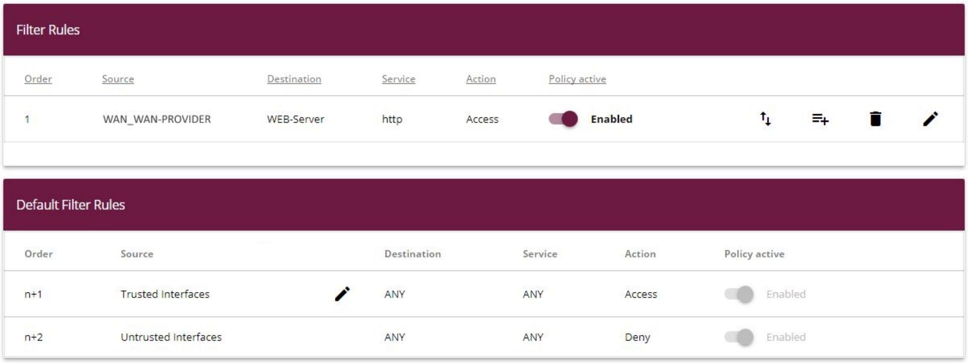
(3) Select the **Destination** *WEB-Server* .

(4) Select the **Service** *http*.

(5) Leave **Action** *Access*.

(6) Press **OK** to confirm your settings.

Under **Firewall**->**Policies**->**IPv4 Filter Rules** you will see the following overview:



Filter Rules

Order	Source	Destination	Service	Action	Policy active
1	WAN_WAN-PROVIDER	WEB-Server	http	Access	Enabled

Default Filter Rules

Order	Source	Destination	Service	Action	Policy active
n+1	Trusted Interfaces	ANY	ANY	Access	Enabled
n+2	Untrusted Interfaces	ANY	ANY	Deny	Enabled

Fig. 24: **Firewall**->**Policies**->**IPv4 Filter Rules**

4.3 Overview of Configuration Steps

NAT / without PAT

Field	Menu	Value
Description	**Network->NAT->NAT Configuration->New**	e. g. WEB-Server
Interface	**Network->NAT->NAT Configuration->New**	e.g. WAN_WAN-Provider
Type of traffic	**Network->NAT->NAT Configuration->New**	incoming (destination NAT)
Service	**Network->NAT->NAT Configuration->New**	http
New Destination IP Address/Netmask	**Network->NAT->NAT Configuration->New**	Host: 192.168.2.10
New Destination Port	**Network->NAT->NAT Configuration->New**	Original

NAT / with PAT

Field	Menu	Value
Description	**Network->NAT->NAT Configuration->New**	e. g. WEB-Server
Interface	**Network->NAT->NAT Configuration->New**	e.g. WAN_WAN-Provider
Type of traffic	**Network->NAT->NAT Configuration->New**	incoming (destination NAT)
Service	**Network->NAT->NAT Configuration->New**	User-defined
Protocol	**Network->NAT->NAT Configuration->New**	TCP
Original Destination Port/Range	**Network->NAT->NAT Configuration->New**	Specify port: 8080
New Destination IP Address/Netmask	**Network->NAT->NAT Configuration->New**	Host: 192.168.2.10
New Destination Port	**Network->NAT->NAT Configuration->New**	Original deactivate, 80

SIF

Field	Menu	Value
Description	**Firewall**->**Addresses**->**Address List**->**NewNew**	*WEB-Server*
IPv4	**Firewall**->**Addresses**->**Address List**->**New**	*Enabled*
Address Type	**Firewall**->**Addresses**->**Address List**->**New**	*Address / Subnet*
Address / Subnet	**Firewall**->**Addresses**->**Address List**->**New**	e.g. *192.168.2.10*/ *255.255.255.0*
Source	**Firewall**->**Policies**->**IPv4 Filter Rules**->**New**	e.g. *WAN_WAN-PROVIDER*
Destination	**Firewall**->**Policies**->**IPv4 Filter Rules**->**New**	*WEB-Server*
Service	**Firewall**->**Policies**->**IPv4 Filter Rules**->**New**	*http*
Action	**Firewall**->**Policies**->**IPv4 Filter Rules**->**New**	*Access*

Chapter 5 Dialling in of an iPhone to a be.IP

5.1 Introduction

The following text covers how an iPhone dials via an IPSec-VPN tunnel to a **be.IP** or a **be.IP plus**.

The **GUI** (Graphical User Interface) is used for configuring.

Requirements

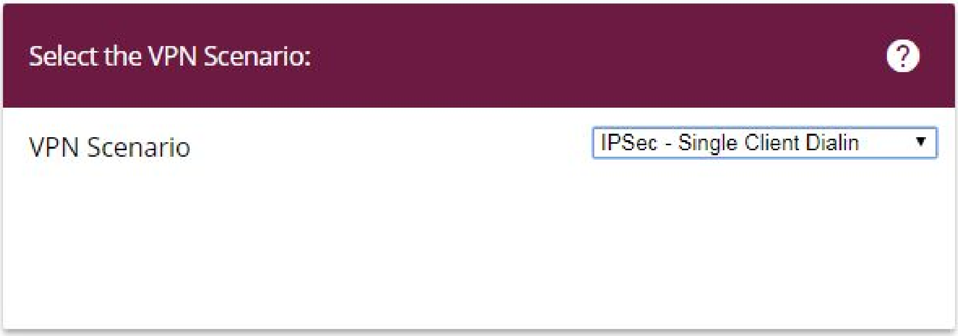
- A **be.IP** or a **be.IP plus**
- An existing configuration as set up by a completed **Quick Start assistant**.
- BOSS version V.10.1 Rev. 5 or higher. The BOSS version of your **be.IP** can be checked in the menu **System Administration** -> **Status**.

5.2 Configuration

5.2.1 Setting up the dialling profile via the Assistant

Leave the **Initial operation** assistant by selecting **View** `Full Access` in the header. First, create the VPN connection.

To do so, go to the **Assistants**->**VPN**->**VPN Connections**->**New** menu.



Select the VPN Scenario:

VPN Scenario: IPSec - Single Client Dialin

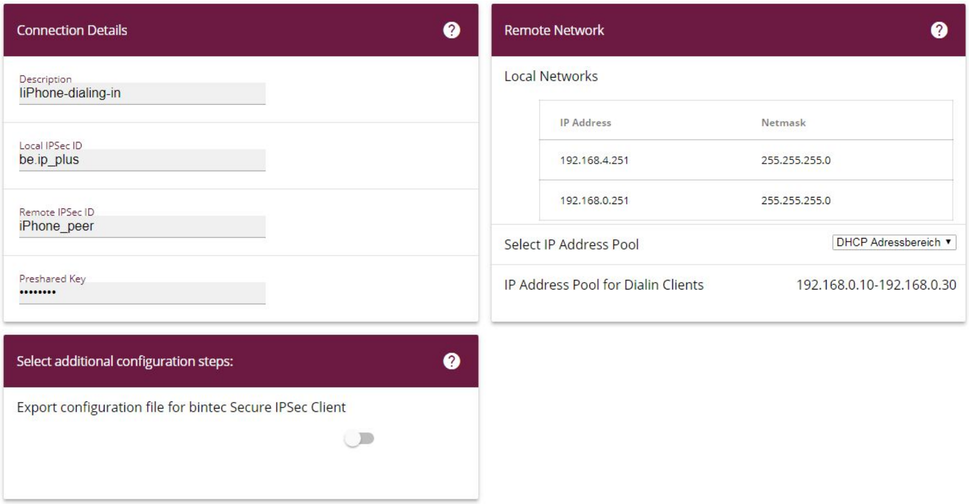
Fig. 25: **Assistants**->**VPN**->**VPN Connections**->**New**

Proceed as follows:

(1) Under **VPN Scenario** select `IPSec - Single Client Dialin`.

(2) Click **Next** to confirm your selection.

Enter the required data for the IPSec scenario in the next step.



Connection Details

Description: liPhone-dialing-in

Local IPSec ID: be.ip_plus

Remote IPSec ID: iPhone_peer

Preshared Key: ••••••••

Remote Network

Local Networks

IP Address	Netmask
192.168.4.251	255.255.255.0
192.168.0.251	255.255.255.0

Select IP Address Pool: DHCP Adressbereich ▾

IP Address Pool for Dialin Clients: 192.168.0.10-192.168.0.30

Select additional configuration steps:

Export configuration file for bintec Secure IPSec Client

Fig. 26: **Assistants**->**VPN**->**VPN Connections**->**Next**

Proceed as follows:

(1) Under **Description** enter a name for the connection, e. g. `iPhone dial-in`.

(2) Under **Remote IPSec ID** enter the ID of the remote IPSec peer, e.g. `iPhone_peer`.

(3) A **Preshared Key** is used for authentication. A combination of letters, numbers and special characters is recommended.

(4) Under **Select IP Address Pool** select `Internal DHCP address range`.

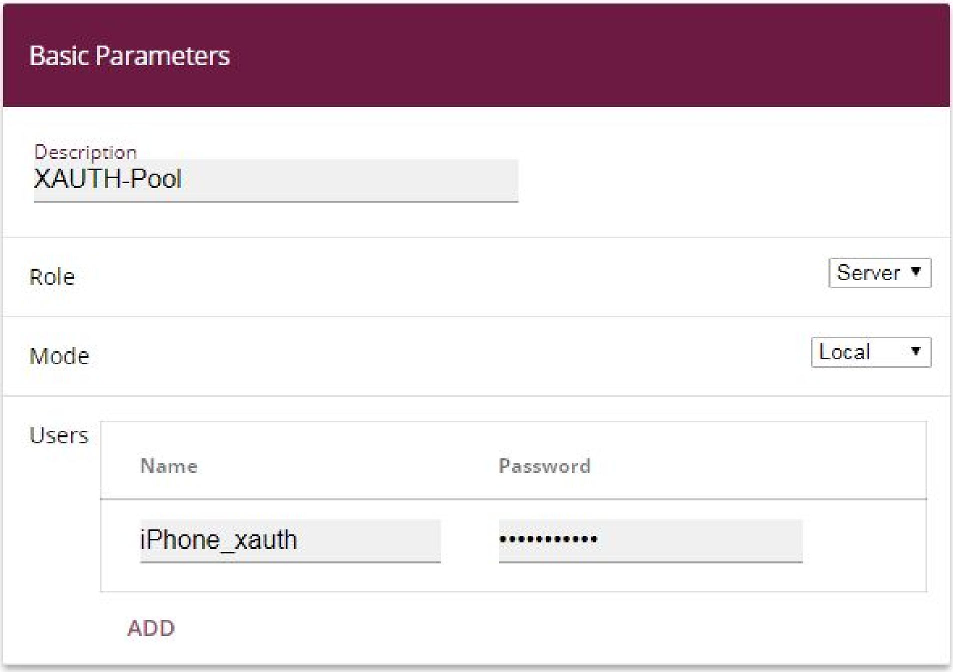
(5) Please leave the **Local IPSec ID** unchanged.

(6) Click **OK** to confirm your entries.

5.2.2 Creating / changing iPhone-specific parameters

The iPhone requires special IPSec settings as well as a XAUTH profile.

Go to the **VPN**->**IPSec**->**XAUTH Profiles**->**New** menu.



Basic Parameters

Description: XAUTH-Pool

Role: Server

Mode: Local

Users

Name	Password
iPhone_xauth	••••••••••••

Fig. 27: **VPN**->**IPSec**->**XAUTH Profiles**->**New**

Proceed as follows:

(1) Enter a **Description** for the XAUTH profile, e.g. *XAUTH-Pool*.

(2) Regarding the **Role**, select *Server*.

(3) Regarding the **Mode**, select *Local*.

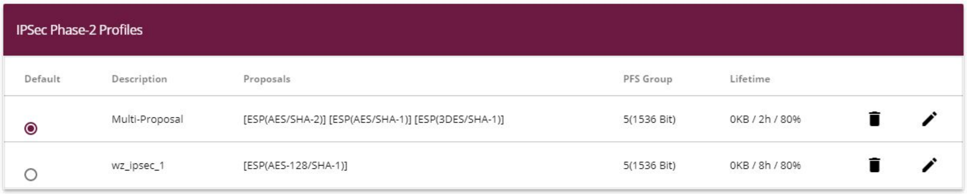
(4) To better distinguish between the names of the IPSec peers, when under **Users** and then **Name** enter e.g. *iPhone_xauth*.

(5) Enter the authentication password (**Password**).

(6) Confirm with **OK**.

In the next step, it is necessary to adjust the profile for phase 2.

Go to the **VPN**->**IPSec**->**Phase-2 Profiles** menu.

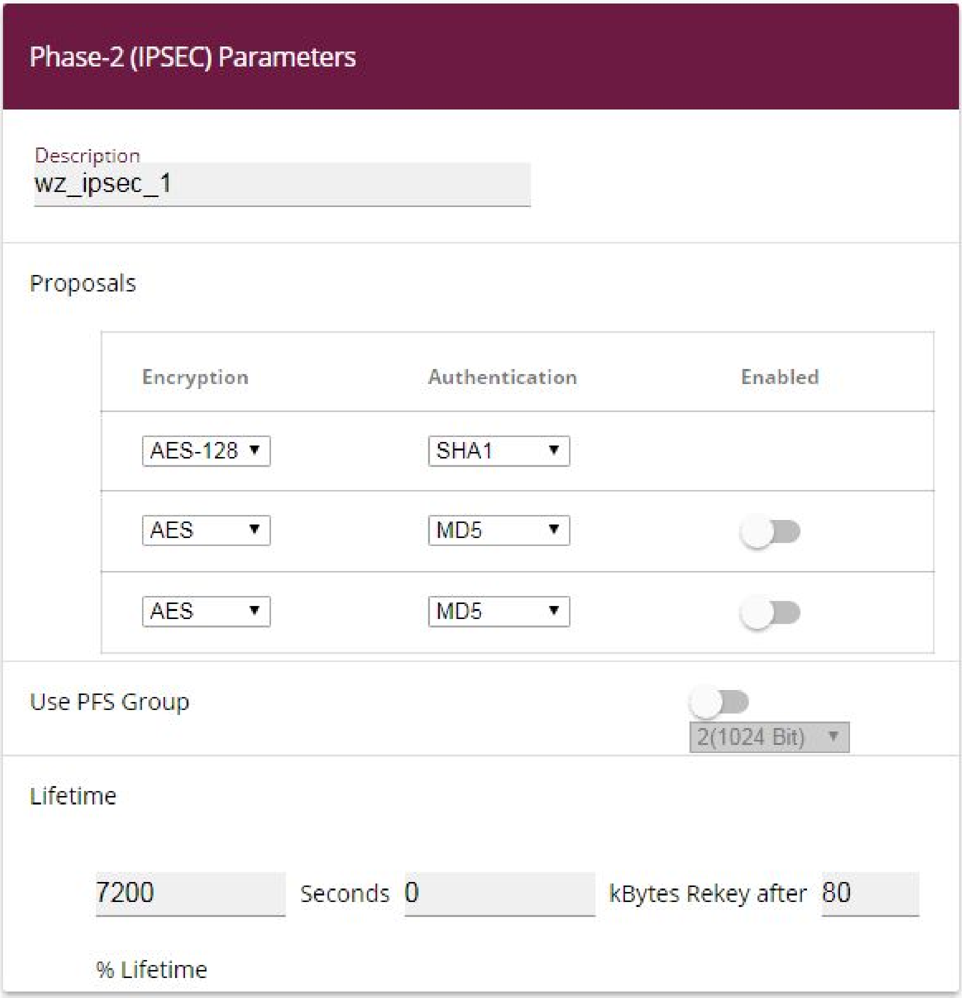


IPSec Phase-2 Profiles

Default	Description	Proposals	PFS Group	Lifetime		
●	Multi-Proposal	[ESP(AES/SHA-2)] [ESP(AES/SHA-1)] [ESP(3DES/SHA-1)]	5(1536 Bit)	0KB / 2h / 80%	🗑	✎
○	wz_ipsec_1	[ESP(AES-128/SHA-1)]	5(1536 Bit)	0KB / 8h / 80%	🗑	✎

Fig. 28: **VPN**->**IPSec**->**Phase-2 Profiles**

Click on the ✎ symbol to process the configured *`wz_ipsec_1`* profile.



Phase-2 (IPSEC) Parameters

Description: wz_ipsec_1

Proposals

Encryption	Authentication	Enabled
AES-128 ▼	SHA1 ▼	
AES ▼	MD5 ▼	○
AES ▼	MD5 ▼	○

Use PFS Group ○ 2(1024 Bit) ▼

Lifetime

7200 Seconds 0 kBytes Rekey after 80 % Lifetime

Fig. 29: **VPN**->**IPSec**->**Phase-2 Profiles** ✎

Proceed as follows:

(1) When on **Proposals** select **Authentication** *SHA1*.

Note

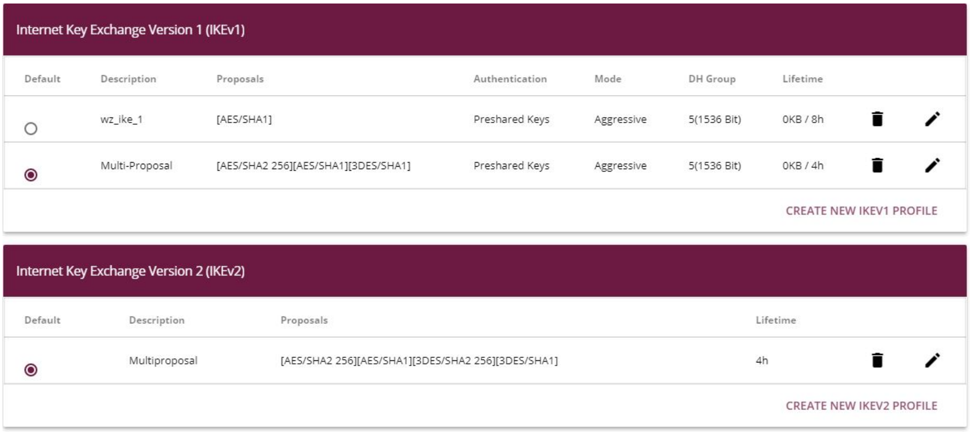
It is important NOT to select SHA2!

(2) Disable the **Use PFS Group** option.

(3) Click **OK** to confirm your entries.

The profile for phase 2 must also be adapted just as for phase 1.

Go to the **VPN**->**IPSec**->**Phase-1 Profiles** menu.



Internet Key Exchange Version 1 (IKEv1)

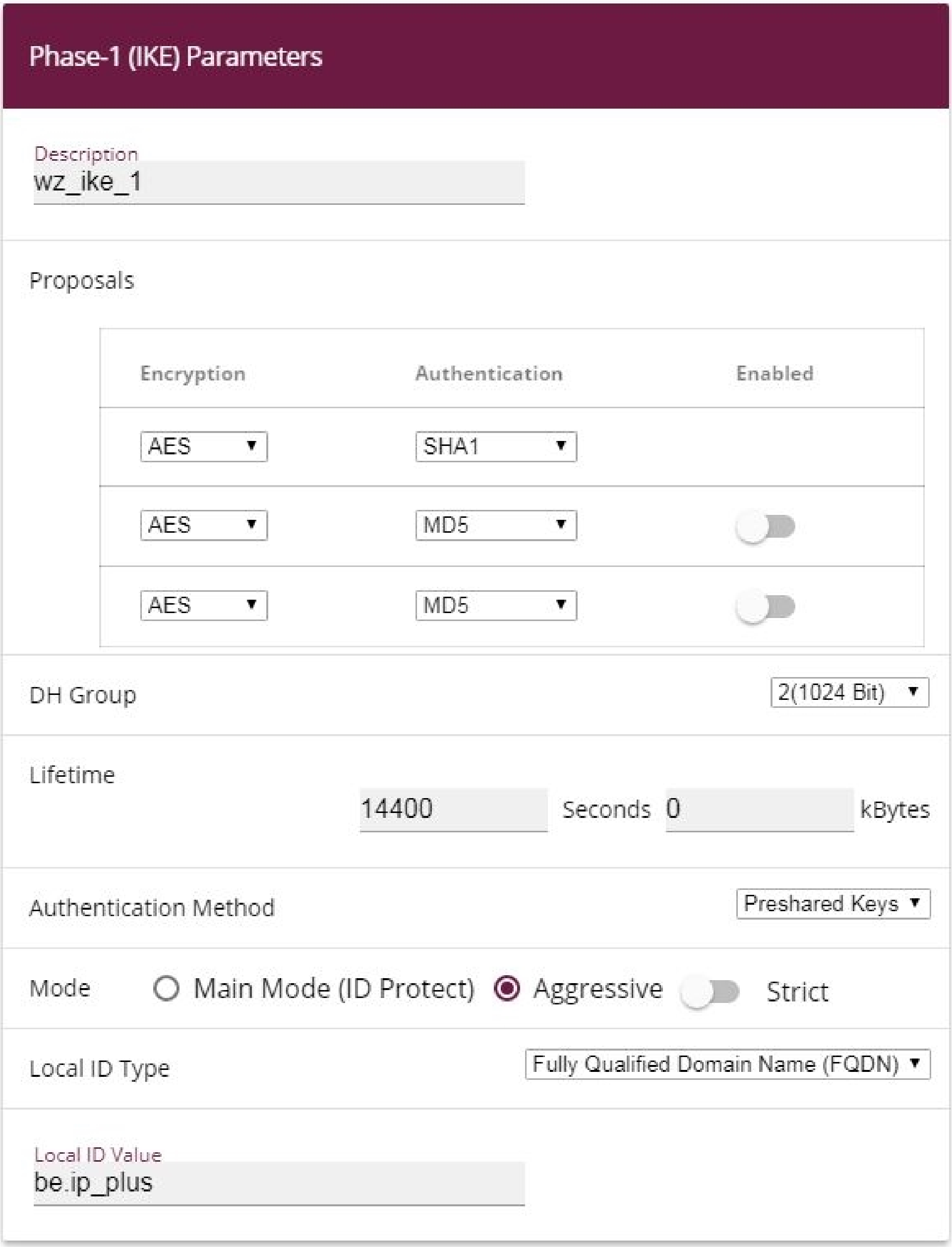
Default	Description	Proposals	Authentication	Mode	DH Group	Lifetime
○	wz_ike_1	[AES/SHA1]	Preshared Keys	Aggressive	5(1536 Bit)	0KB / 8h
●	Multi-Proposal	[AES/SHA2 256][AES/SHA1][3DES/SHA1]	Preshared Keys	Aggressive	5(1536 Bit)	0KB / 4h

Internet Key Exchange Version 2 (IKEv2)

Default	Description	Proposals	Lifetime
●	Multiproposal	[AES/SHA2 256][AES/SHA1][3DES/SHA2 256][3DES/SHA1]	4h

Fig. 30: **VPN**->**IPSec**->**Phase-1 Profiles**

Click on the ✎ symbol to process the configured *wz_ike_1* profile.



Phase-1 (IKE) Parameters

Description: wz_ike_1

Proposals

Encryption	Authentication	Enabled
AES ▾	SHA1 ▾	
AES ▾	MD5 ▾	○
AES ▾	MD5 ▾	○

DH Group: 2(1024 Bit) ▾

Lifetime: 14400 Seconds 0 kBytes

Authentication Method: Preshared Keys ▾

Mode: ○ Main Mode (ID Protect) ● Aggressive ○ Strict

Local ID Type: Fully Qualified Domain Name (FQDN) ▾

Local ID Value: be.ip_plus

Fig. 31: **VPN**->**IPSec**->**Phase-1 Profiles** ✎

Proceed as follows:

(1) When on **Proposals** select **Authentication** *SHA1*.

Note

It is important NOT to select SHA2!

(2) Select **DH Group** *2 (1024 Bit)*.

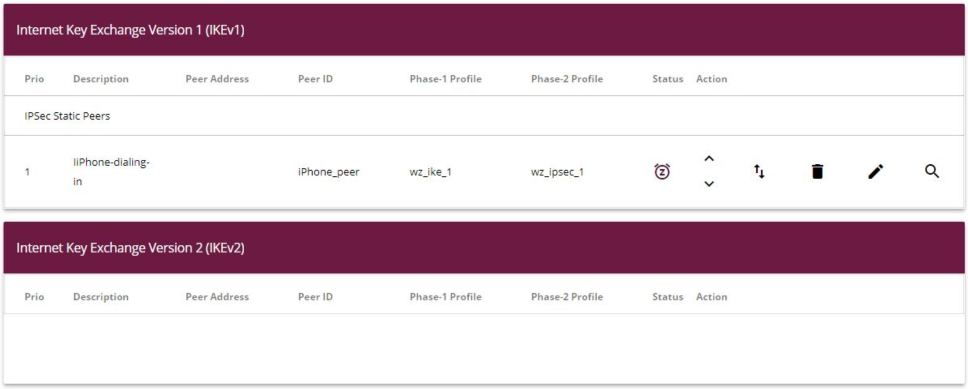
(3) Click **Advanced Settings**.

(4) Under **Alive Check** select the *Dead Peer Detection (Idle)* option.

(5) Click **OK** to confirm your entries.

The IPSec peer must then be adapted.

Go to the **VPN**->**IPSec**->**IPSec Peers** menu.



Internet Key Exchange Version 1 (IKEv1)

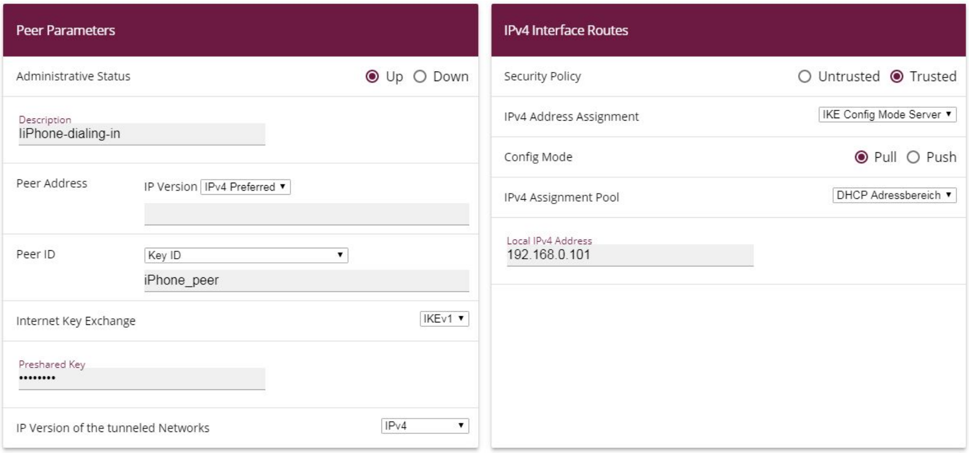
Prio	Description	Peer Address	Peer ID	Phase-1 Profile	Phase-2 Profile	Status	Action
IPSec Static Peers							
1	IiPhone-dialing-in		iPhone_peer	wz_ike_1	wz_ipsec_1		

Internet Key Exchange Version 2 (IKEv2)

Prio	Description	Peer Address	Peer ID	Phase-1 Profile	Phase-2 Profile	Status	Action

Fig. 32: **VPN**->**IPSec**->**IPSec Peers**

Click on the ✎ symbol to process the configured *iPhone dial-in* profile.



Peer Parameters

Administrative Status ● Up ○ Down

Description
liPhone-dialing-in

Peer Address IP Version IPv4 Preferred ▾

Peer ID Key ID ▾
iPhone_peer

Internet Key Exchange IKEv1 ▾

Preshared Key
••••••••

IP Version of the tunneled Networks IPv4 ▾

IPv4 Interface Routes

Security Policy ○ Untrusted ● Trusted

IPv4 Address Assignment IKE Config Mode Server ▾

Config Mode ● Pull ○ Push

IPv4 Assignment Pool DHCP Adressbereich ▾

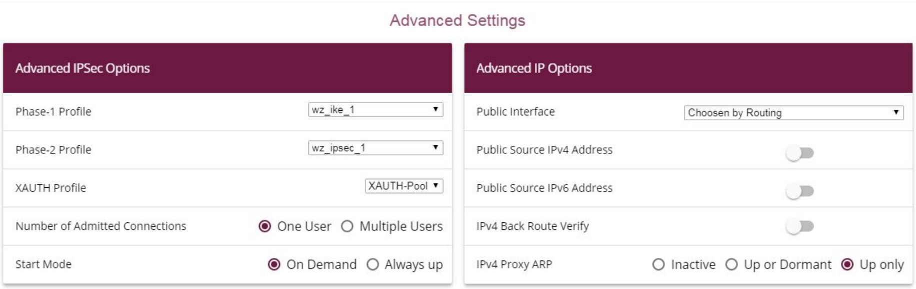
Local IPv4 Address
192.168.0.101

Fig. 33: **VPN**->**IPSec**->**IPSec Peers** ✎

Proceed as follows:

(1) Using the drop-down menu in **Peer ID** select the `Key ID` value.

(2) Click **Advanced Settings**.



Advanced Settings

Advanced IPSec Options

Phase-1 Profile wz_ike_1 ▾

Phase-2 Profile wz_ipsec_1 ▾

XAUTH Profile XAUTH-Pool ▾

Number of Admitted Connections ● One User ○ Multiple Users

Start Mode ● On Demand ○ Always up

Advanced IP Options

Public Interface Choosen by Routing ▾

Public Source IPv4 Address

Public Source IPv6 Address

IPv4 Back Route Verify

IPv4 Proxy ARP ○ Inactive ○ Up or Dormant ● Up only

Fig. 34: **VPN**->**IPSec**->**IPSec Peers**-> ✎ ->**Advanced Settings**

(3) Check whether the following values were selected:

(4) **Phase-1 Profile**: *wz_ike_1*

(5) **Phase-2 Profile**: *wz_ipsec_1*

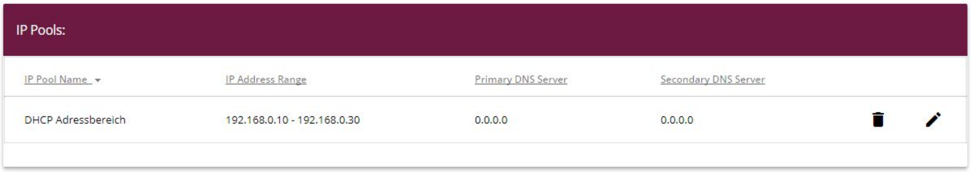
(6) **XAUTH Profile**: in this case *XAUTH pool* (the XAUTH profile that was set up)

(7) Under **IPv4 Proxy ARP** select the *Up only* option.

(8) Click **OK** to confirm your entries.

The DNS server must be entered into the DHCP pool so that the iPhone can carry out a DNS resolution.

To do so, go to the **Local Services**->**DHCP Server**->**IP Pool Configuration** menu.

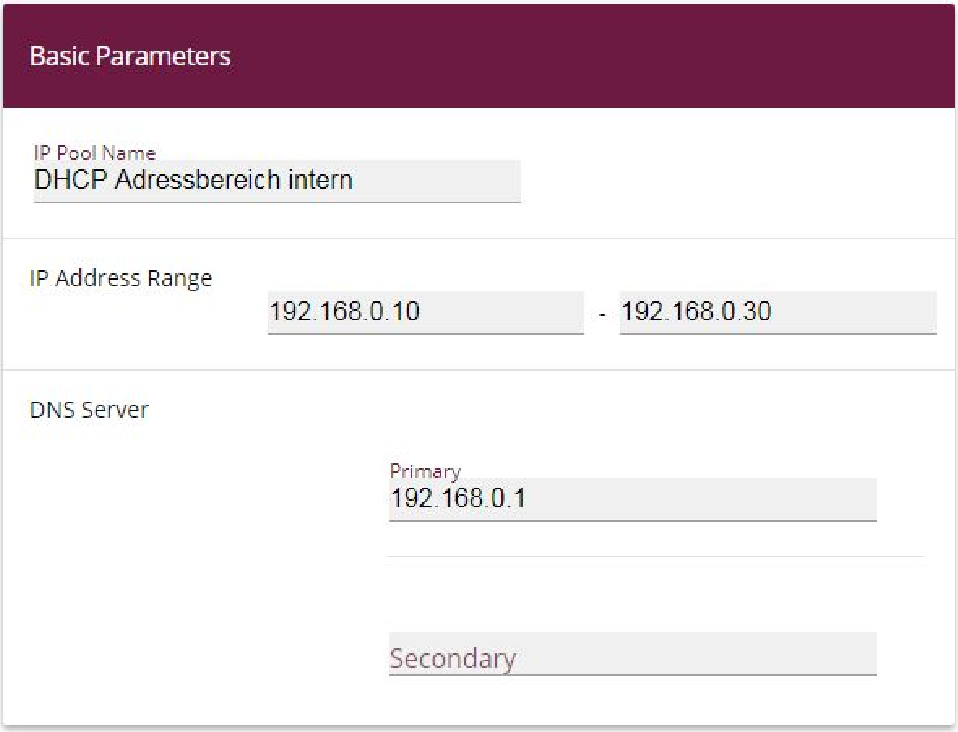


IP Pools:

IP Pool Name	IP Address Range	Primary DNS Server	Secondary DNS Server
DHCP Adressbereich	192.168.0.10 - 192.168.0.30	0.0.0.0	0.0.0.0

Fig. 35: **Local Services**->**DHCP Server**->**IP Pool Configuration**

Click the ✎ symbol to edit the `internal DHCP address range`.



Basic Parameters

IP Pool Name: DHCP Adressbereich intern

IP Address Range: 192.168.0.10 - 192.168.0.30

DNS Server

Primary: 192.168.0.1

Secondary

Fig. 36: **Local Services**->**DHCP Server**->**IP Pool Configuration** ✎

Proceed as follows:

(1) Under **DNS Server** enter the primary IP address of the DNS server. Under normal circumstances this is the **be.IP** IP address. The IP address is `192.168.0.1` as a default.

(2) Click **OK** to confirm your entries.

This concludes the configuration. Save the current configuration using the button **Save configuration** as a boot configuration.

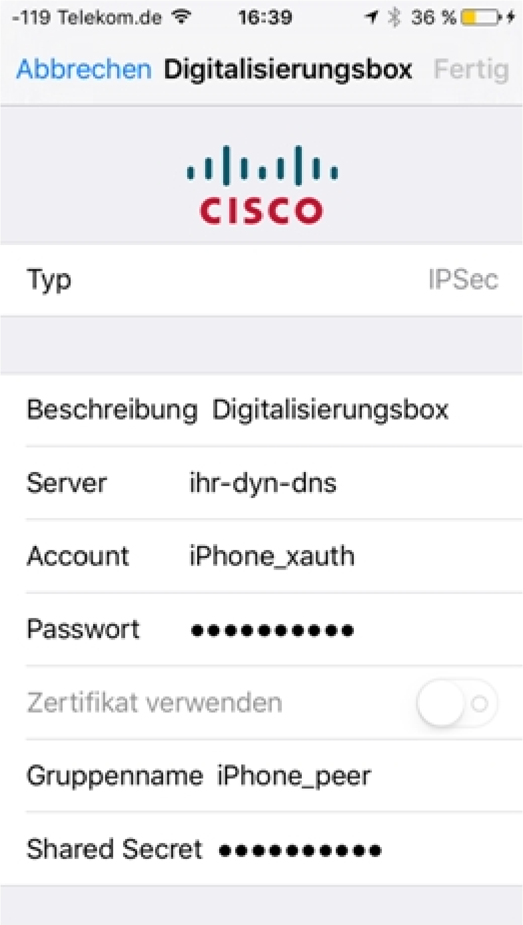
5.3 Setting up the dialling profile on the iPhone

The IPSec profile is now set up on the iPhone in the final step.

To do so, select **Settings**-> **VPN** -> **Add VPN**.

Note

Note that as of iOS 10 the default selection for VPN profiles is `IKEv2`. `IKEv1` is still available, however. Tap on the **Type** menu and choose `IPSec` in the following selection. After this change all options used in the following instructions are available again.



-119 Telekom.de 16:39 36 %

Abbrechen Digitalisierungsbox Fertig

Typ IPSec

Beschreibung Digitalisierungsbox

Server ihr-dyn-dns

Account iPhone_xauth

Passwort ●●●●●●●●●●●

Zertifikat verwenden ○

Gruppenname iPhone_peer

Shared Secret ●●●●●●●●●●●

Fig. 37: **Settings** -> **VPN** -> **Add VPN**

You will see the following data on your display:

Type: IPSec

Server: Your fixed public IP address or DynDNS

Password: XAUTH profile user's password

Group name: Name of the IPSec peer that was created under IPSec Peers

Shared Secret: Password that was used for the IPSec peer

5.4 Overview of Configuration Steps

Setting up the dialling profile via the Assistant

Field	Menu	Value
VPN Scenario	**Assistants->VPN->VPN Connections->New**	*IPSec - Individual Client Dial-In*
Description	**Assistants->VPN->VPN Connections->Next**	e.g. *iPhone dial-in*
Remote IPSec ID	**Assistants->VPN->VPN Connections->Next**	e.g. *iPhone_peer*
Preshared Key	**Assistants->VPN->VPN Connections->Next**	e.g. *SuperSecret*
Select IP Address Pool	**Assistants->VPN->VPN Connections->Next**	*Internal DHCP address range*

Creating / modifying the iPhone-specific parameters

Field	Menu	Value
Description	**VPN->IPSec->XAUTH Profiles->New**	e.g. *XAUTH pool*
Role	**VPN->IPSec->XAUTH Profiles->New**	*Server*
Mode	**VPN->IPSec->XAUTH Profiles->New**	*Local*
Users	**VPN->IPSec->XAUTH Profiles->New**	**Name** e.g. *iPhone_xauth* **Password** e.g. *SuperSecret*

Changing the Phase-2 profile

Field	Menu	Value
Proposals	**VPN->IPSec->Phase-1 Profiles->New**	**Authentication** *SHA1*
Use PFS Group	**VPN->IPSec->Phase-1 Profiles->New**	*Disabled*

Changing the Phase-1 profile

Field	Menu	Value
Proposals	**VPN->IPSec->Phase-1 Profiles->New**	**Authentication** *SHA1*
DH Group	**VPN->IPSec->Phase-1 Profiles->New**	*2 (1024 Bit)*
Alive Check	**VPN->IPSec->Phase-1 Profiles->New->Advanced Settings**	*Dead Peer Detection (Idle)*

Modifying IPSec Peers

Field	Menu	Value
Peer ID	**VPN->IPSec->IPSec Peers->New**	*Key ID*
IPv4 Proxy ARP	**VPN->IPSec->IPSec Peers->New->Advanced Settings**	*Up only*

Configuring the IP pool

Field	Menu	Value
DNS Server	**Local Services->DHCP Server->IP Pool Configuration->New**	**Primary** e.g. *192.168.0.1*

Chapter 6 Access from WAN via the PPPoE-WAN connection

6.1 Introduction

The NAT and firewall settings are described in the following using the example of an "exposed host" for IPv4 access from WAN to an Internet gateway via the PPPoE-WAN connection of a **be.IP**.

Requirements

- A **be.IP** with current firmware version in the **View** = `Full Access`.
- An existing Internet gateway (e.g. firewall appliance) should also be reachable on the Internet for all services (e.g. for IPSec), and act as a default gateway and firewall for data traffic in the existing network, IP telephony and all associated mechanisms (e.g. QoS on the WAN connection) should be taken over by the **be.IP**. In this case the following systems are passed through regarding connections from WAN and must therefore be prepared accordingly:

  - Network Address Translation (NAT/PAT)

  - Stateful Inspection Firewall (SIF).
- This also applies to services that may require a constant source port and is configured by an outgoing NAT rule. This assumes that there is a "normal" WAN configuration with no load distribution scenario and without extended routing with the current firmware version.

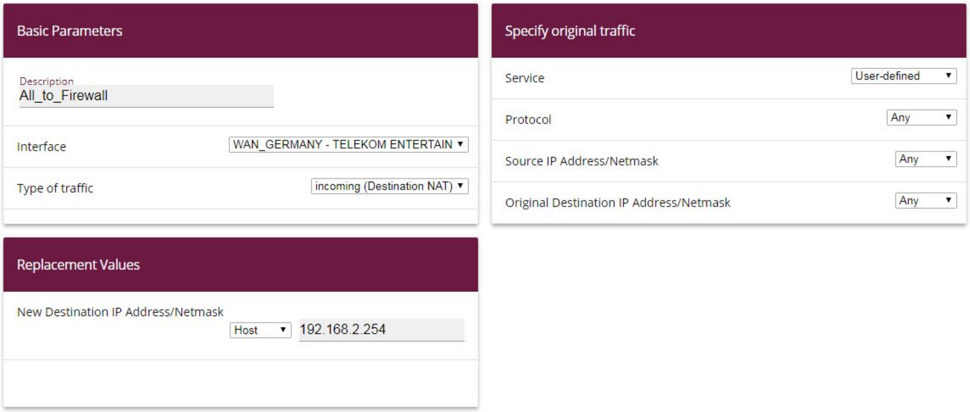
6.2 Configuration

6.2.1 Network Address Translation (NAT) / Port Address Translation (PAT)

The first subsystem that is passed through with IPv4 access from WAN is the Network Address Translation (NAT).

The request is sent to the official IPv4 address of the **be.IP** (that of the WAN connection) and then forwarded to the desired IPv4 address in LAN (exposed host) or to a server in a special DMZ (demilitarized zone, an interface that is separate and monitored by additional firewall rules). In our example the target is implementation in the LAN that is connected to br0 (IPv4 address 192.168.2.254). For this reason, the designation "Exposed Host" is used.

Go to the **Network**->**NAT**->**NAT Configuration**->**New** menu.



Basic Parameters

Description: All_to_Firewall

Interface: WAN_GERMANY - TELEKOM ENTERTAIN

Type of traffic: incoming (Destination NAT)

Specify original traffic

Service: User-defined

Protocol: Any

Source IP Address/Netmask: Any

Original Destination IP Address/Netmask: Any

Replacement Values

New Destination IP Address/Netmask: Host 192.168.2.254

Fig. 38: **Network**->**NAT**->**NAT Configuration**->**New**

Proceed as follows:

(1) Enter a **Description** such as, e.g. *All_to_Firewall*.

(2) Select a **Interface** such as *WAN_GERMANY - TELEKOM ENTERTAIN*.

(3) Leave the settings **Type of traffic** = *incoming (Destination NAT)*.

(4) Leave the **Service** settings as *User-defined*.

(5) Leave the **Protocol** settings as *Any*.

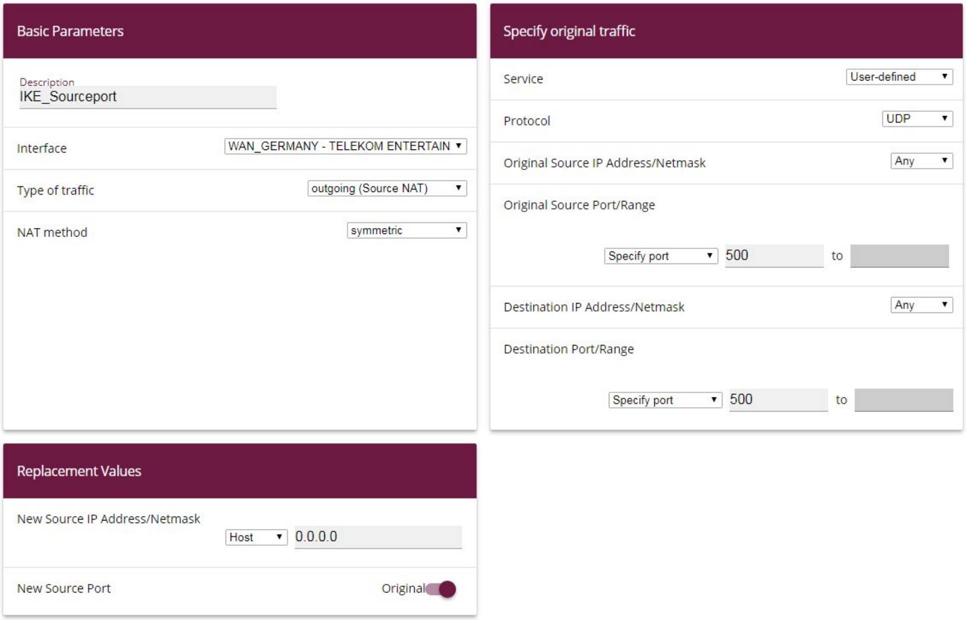
(6) Ensure that at the option **New Destination IP Address/Netmask** = *host* and that the IPv4 address is *192.168.2.254*.

This rule means that all IPv4 traffic arriving at the PPPoE-WAN interface will be forwarded to the IP address 192.168.2.254.

(7) Click **OK** to confirm your settings.

The outgoing source ports must now be set for the outgoing traffic regarding sensitive data. This is, for example, necessary for a few manufacturers (LANCOM, Sophos UTM, ...) for starting phase 1 (IKE) of an IPSec connection. This step for IPSec is not necessary if a **be.IP** or a device from bintec elmeg GmbH is in use.

Go to the **Network**->**NAT**->**NAT Configuration**->**New** menu.



Basic Parameters

Description: IKE_Sourceport

Interface: WAN_GERMANY - TELEKOM ENTERTAIN

Type of traffic: outgoing (Source NAT)

NAT method: symmetric

Specify original traffic

Service: User-defined

Protocol: UDP

Original Source IP Address/Netmask: Any

Original Source Port/Range: Specify port 500 to

Destination IP Address/Netmask: Any

Destination Port/Range: Specify port 500 to

Replacement Values

New Source IP Address/Netmask: Host 0.0.0.0

New Source Port: Original

Fig. 39: **Network**->**NAT**->**NAT Configuration**->**New**

Proceed as follows:

(1) Enter a **Description** such as, e.g. `IKE_Sourceport`.

(2) Select a **Interface** such as `WAN_GERMANY - TELEKOM ENTERTAIN`.

(3) Select the **Type of traffic** = `outgoing (Source NAT)`setting.

(4) For the **NAT method** select `symmetrical` .

(5) Leave the **Service** settings as `User-defined`.

(6) Under **Protocol** select `UDP`.

(7) Select **Original Source Port/Range** = `Specify port` then enter `500`.

(8) Select **New Destination IP Address/Netmask** = `Specify port` then enter `500`.

(9) The **New Source IP Address/Netmask** given as `0.0.0.0` acts as a placeholder for the dynamically assigned WAN interface IP address If a "fixed" official IP address is available, then this can be entered here.

(10) Under **New Source Port** enable `Original`.

(11) Click **OK** to confirm your settings.

For other services that require retention of the **Source Port** then please use the same procedure as the above example. Select the corresponding **Protocol** then enter **Port**.

6.2.2 Stateful Inspection Firewall (SIF)

The next subsystem that the packets move through, after the NAT, is the Stateful Inspection Firewall. As the status of the WAN interface is "not trustworthy" no initial requests may be placed in the default settings for this interface, instead only corresponding requests from "trustworthy" interfaces (initially all LAN interfaces) will be answered. Initially, the requests continue to be blocked, this time from the SIF.

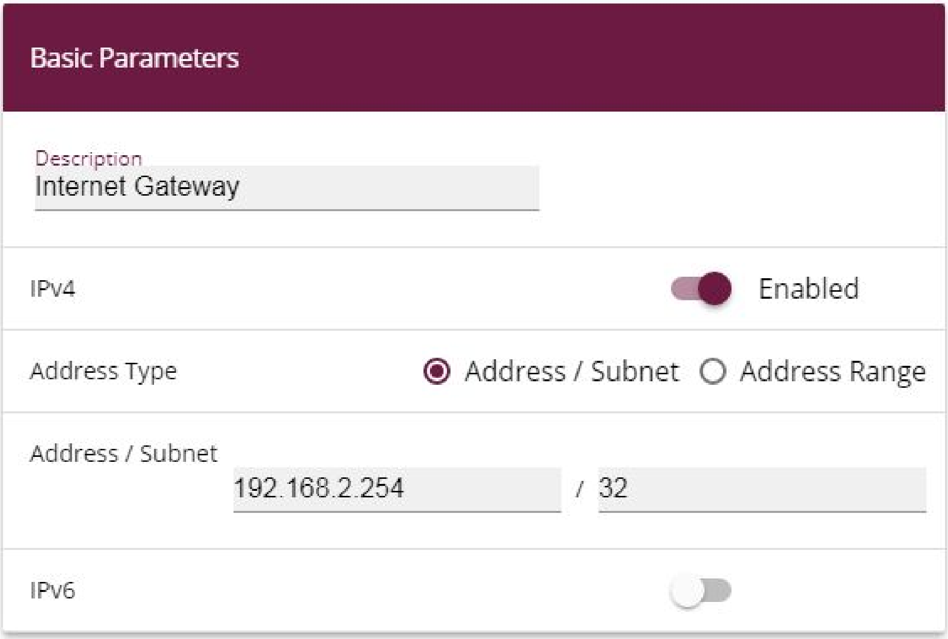
A rule that enables this access to be an exception to output behaviour must be created.

Note

With the Stateful Inspection Firewall the rule applies that packages that are permitted due to a rule cannot be subsequently forbidden, and vice versa. If necessary, the sequence of the rules that have been passed through must be observed!

In our example, all protocols and ports for access from the WAN to the IP address of the Internet gateway (192.168.2.254) must be enabled. The required interfaces and the service summary "any" have already been predefined, only the Internet gateway IP address requires definition.

Go to the **Firewall**->**Addresses**->**Address List**->**New** menu.



Basic Parameters

Description: Internet Gateway

IPv4: Enabled

Address Type: ● Address / Subnet ○ Address Range

Address / Subnet: 192.168.2.254 / 32

IPv6

Fig. 40: **Firewall**->**Addresses**->**Address List**->**New**

Proceed as follows:

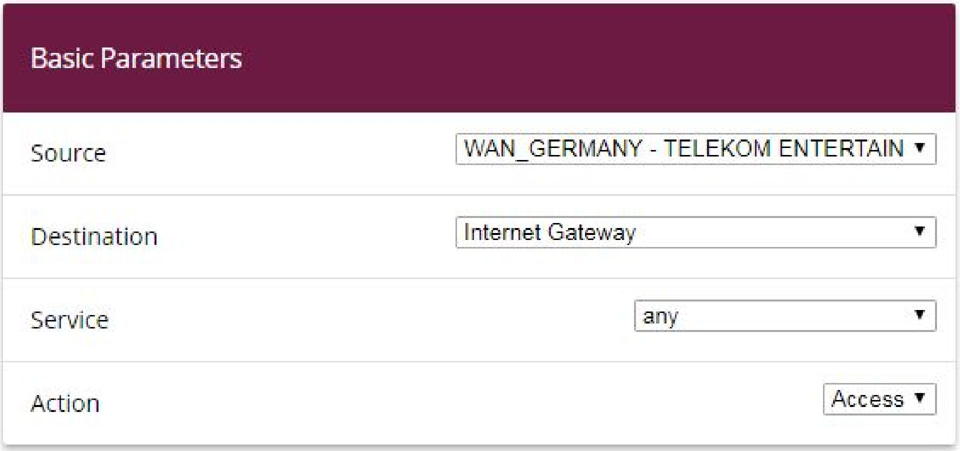
(a) Enter a **Description** such as `Internet Gateway`.

(b) Under **Address / Subnet** enter the IP address of the Internet gateway `192.168.2.254` and the sub-network `32`.

(c) Click **OK** to confirm your settings.

As a new rule access from the WAN interface to the IPv4 address of the Internet gateway is defined for every service and for all protocols.

Go to the **Firewall**->**Policies**->**IPv4 Filter Rules**->**New** menu.



Basic Parameters

Source	WAN_GERMANY - TELEKOM ENTERTAIN ▾
Destination	Internet Gateway ▾
Service	any ▾
Action	Access ▾

Fig. 41: **Firewall**->**Policies**->**IPv4 Filter Rules**->**New**

Proceed as follows:

(a) Select a **Source** such as `WAN_GERMANY - TELEKOM ENTERTAIN`.

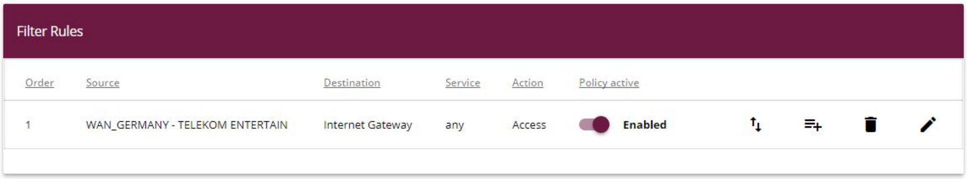
(b) Select the **Destination** = `Intern Gateway`.

(c) Select the **Service** `any`.

(d) Leave **Action** `Access`.

(e) Click **OK** to confirm your settings.

A list of all configured IPv4 filter rules is displayed in the **Firewall**->**Policies**->**IPv4 Filter Rules** menu.



Filter Rules

Order	Source	Destination	Service	Action	Policy active
1	WAN_GERMANY - TELEKOM ENTERTAIN	Internet Gateway	any	Access	● Enabled

Fig. 42: **Firewall**->**Policies**->**IPv4 Filter Rules**

6.2.3 Changes to Internet gateway

Regarding the Internet gateway, it is now necessary to adjust the default route and the DNS server, if necessary, to the **be.IP** IP address. The role of time server can also be taken over by the **be.IP**.

6.2.4 Final note

The scenario is also due to the fact that dialling in of several PPPoE connections to one DTAG xDSL connection has been forbidden since January 2015. A routing connection of the **be.IP** could also be configured via the previous PPPoE dial-in of the Internet gateway, however mechanisms that are automatically performed by the **be.IP** for VoIP must be taken over by the Internet gateway. These serve as examples:

- Quality of Service (prioritisation) for telephony packages

- Releases in the firewall for telephony

- NAT mechanisms for the unconnected ports of RTP data

- SRV requests via DNS (for tel.t-online.de) must be properly resolved.

The extremely comprehensive settings in NAT and SIF for forwarding all traffic from the Internet can, of course, be fine-tuned and limited to a greater extent.

This description is based on a completed Quick Start assistant, and if there are already port forwardings in the NAT, then the sequence should be observed, if necessary!

6.3 Overview of Configuration Steps

NAT configuration (target NAT)

Field	Menu	Value
Description	**Network->NAT->NAT Configuration->New**	e.g. *All_to_Firewall*
Interface	**Network->NAT->NAT Configuration->New**	e.g. *WAN_GERMAN - TELEKOM ENTERTAIN*
Type of traffic	**Network->NAT->NAT Configuration->New**	*incoming (Destination NAT)*
Service	**Network->NAT->NAT Configuration->New**	*User-defined*
Protocol	**Network->NAT->NAT Configuration->New**	*ANY*
Source IP Address/ Netmask	**Network->NAT->NAT Configuration->New**	*ANY*
Original Destination IP Address/Netmask	**Network->NAT->NAT Configuration->New**	*ANY*
New Destination IP Address/Netmask	**Network->NAT->NAT Configuration->New**	*Host: 192,168.2,254*

NAT configuration (Source NAT)

Field	Menu	Value
Description	**Network->NAT->NAT Configuration->New**	e.g. *IKE_Sourceport*
Interface	**Network->NAT->NAT Configuration->New**	e.g. *WAN_GERMAN - TELEKOM ENTERTAIN*
Type of traffic	**Network->NAT->NAT Configuration->New**	*outgoing (Source NAT)*
NAT method	**Network->NAT->NAT Configuration->New**	*symmetric*
Protocol	**Network->NAT->NAT Configuration->New**	*UDP*
Original Source Port/ Range	**Network->NAT->NAT Configuration->New**	*Specify port: 500*
Destination Port/Range	**Network->NAT->NAT Configuration->New**	*Specify port: 500*

Field	Menu	Value
New Source IP Address/Netmask	**Network**->**NAT**->**NAT Configuration**->**New**	*Host: 0.0.0.0*
New Source Port	**Network**->**NAT**->**NAT Configuration**->**New**	*Original*

Stateful Inspection Firewall (SIF)

Field	Menu	Value
Description	**Firewall**->**Addresses**->**Address List**->**New**	e.g. *Internet Gateway*
IPv4	**Firewall**->**Addresses**->**Address List**->**New**	*Enabled*
Address Type	**Firewall**->**Addresses**->**Address List**->**New**	*Address / Subnet*
Address / Subnet	**Firewall**->**Addresses**->**Address List**->**New**	e.g. *192.168.2.254 / 32*

IPv4 Filter Rules

Field	Menu	Value
Source	**Firewall**->**Policies**->**IPv4 Filter Rules**->**New**	*WAN_GERMAN - TELEKOM ENTERTAIN*
Destination	**Firewall**->**Policies**->**IPv4 Filter Rules**->**New**	*Internet Gateway*
Service	**Firewall**->**Policies**->**IPv4 Filter Rules**->**New**	*any*
Action	**Firewall**->**Policies**->**IPv4 Filter Rules**->**New**	*Access*

Chapter 7 be.IP Secure Client: Configuration of VPN remote access

7.1 Introduction

The following passage shows how an IPSec tunnel between a bintec be.IP media and VPN gateway (from software 10.1.5 patch 3 and above) and a be.IP Secure Client (from version 3.04, build 26471 and above) is configured.

The graphical user interface (**GUI**) is used for configuration. You can access help on available configuration options via the online help system.

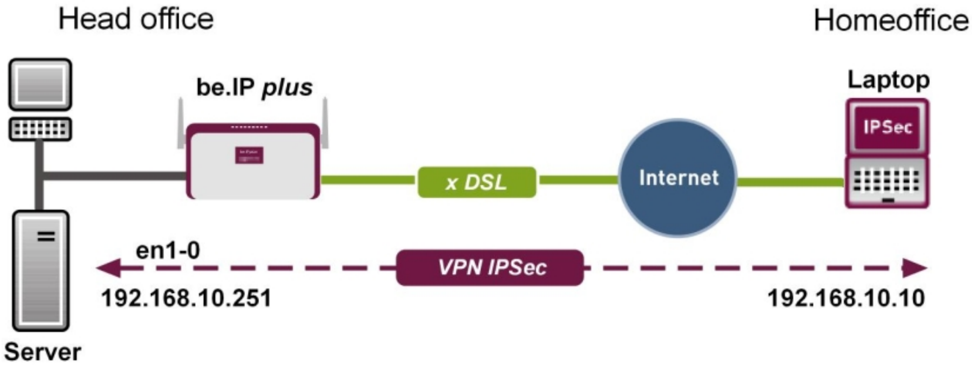


Fig. 43: Example scenario

Requirements

- A **be.IP** or a **be.IP plus**, which can be reached via an official IP address or via DynDNS, as well as with an active Internet connection
- A PC or a laptop with an active Internet connection on which the be.IP Secure Client will be installed.
- Licence key and serial number for activation of the be.IP Secure Client

7.2 Configuration

7.2.1 Start Gateway

(1) Open a Web browser, enter the IP address of your device into the address field on your Web browser and confirm by pressing Return.
The **Welcome** window opens.

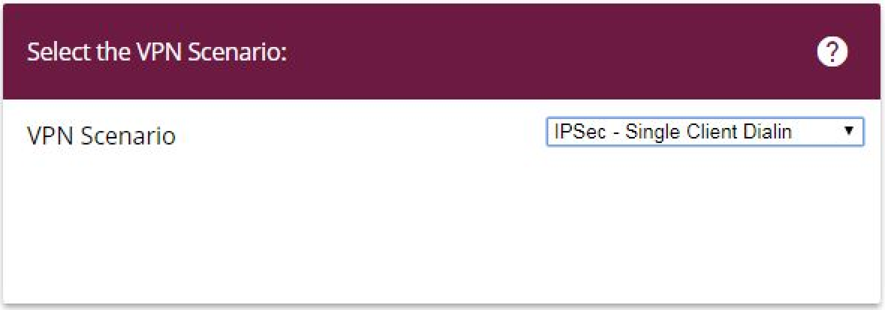
(2) Enter your login details in the **User** and **Password** fields, then click on **Login**.
The status page of the user interface opens in the **View** *`User`*.

7.2.2 Configure tunnel with the Assistant VPN

In order to configure the tunnel, use **AssistantsVPN**.

(1) Go to **Assistants**->**VPN**->**VPN Connections**->**New**.

(2) Select **VPN Scenario** *`IPSec - Single Client Dialin`*.



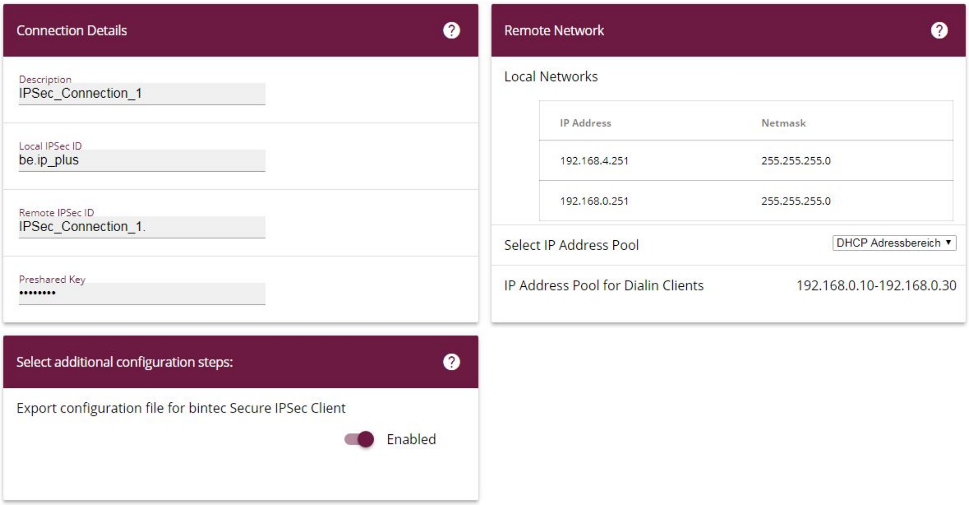
Select the VPN Scenario:

VPN Scenario: IPSec - Single Client Dialin

Fig. 44: **Assistants**->**VPN**->**VPN Connections**->**New**

(3) Click **Next** to confirm your selection.

Enter the required data for the IPSec scenario in the next step.



Connection Details

Description
IPSec_Connection_1

Local IPSec ID
be.ip_plus

Remote IPSec ID
IPSec_Connection_1.

Preshared Key
••••••••

Remote Network

Local Networks

IP Address	Netmask
192.168.4.251	255.255.255.0
192.168.0.251	255.255.255.0

Select IP Address Pool: DHCP Adressbereich ▾

IP Address Pool for Dialin Clients: 192.168.0.10-192.168.0.30

Select additional configuration steps:

Export configuration file for bintec Secure IPSec Client

Enabled

Fig. 45: **Assistants**->**VPN**->**VPN Connections**->**New**->**Next**

Proceed as follows:

(1) Under **Description** enter a name for the connection, e. g. `IPSec_Connection_1` .

(2) Leave the **Local IPSec ID** unchanged.

(3) At **Remote IPSec ID** enter the ID of the remote IPSec peer, e.g. `IPSec_Connection_1`.

(4) A **Preshared Key** is used for authentication.

> **Note**
>
> As **Preshared Key** we recommend using a combination of letters, numbers, and symbols.

(5) Under **Select IP Address Pool** select a suitable IP address range such as `DHCP address range` or configure a new address range under **WAN**->**Internet + Dialup**->**IP Pools**->**New**. In order to configure a new address range, use **View** `Full Access`.

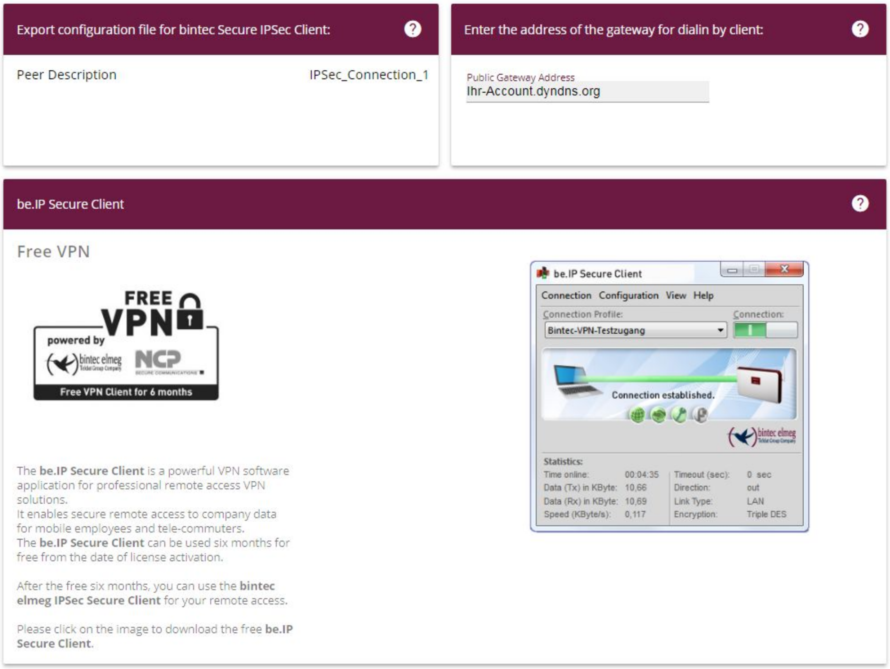
> **Note**
>
> We recommend using an IP pool with addresses from the gateway's internal network.

(6) Activate **Export configuration file for bintec Secure IPSec Client**.

Note

The exported *.ini file can be imported into a be.IP Secure Client as well as into a bintec elmeg IPSec Secure Client.

(7) Click **OK** to confirm your entries.
 The following window opens:



Export configuration file for bintec Secure IPSec Client:

Peer Description IPSec_Connection_1

Enter the address of the gateway for dialin by client:

Public Gateway Address Ihr-Account.dyndns.org

be.IP Secure Client

Free VPN

The **be.IP Secure Client** is a powerful VPN software application for professional remote access VPN solutions.
It enables secure remote access to company data for mobile employees and tele-commuters.
The **be.IP Secure Client** can be used six months for free from the date of license activation.

After the free six months, you can use the **bintec elmeg IPSec Secure Client** for your remote access.

Please click on the image to download the free **be.IP Secure Client**.

Connection Profile: Bintec-VPN-Testzugang

Connection:

Connection established.

Statistics:

```
Time online:          00:04:35   Timeout (sec):  0  sec
Data (Tx) in KByte:   10,66      Direction:      out
Data (Rx) in KByte:   10,69      Link Type:      LAN
Speed (KByte/s):      0,117      Encryption:     Triple DES
```

Fig. 46: **Assistants**->**VPN**->**VPN Connections**->**New**->**Next**->**OK**

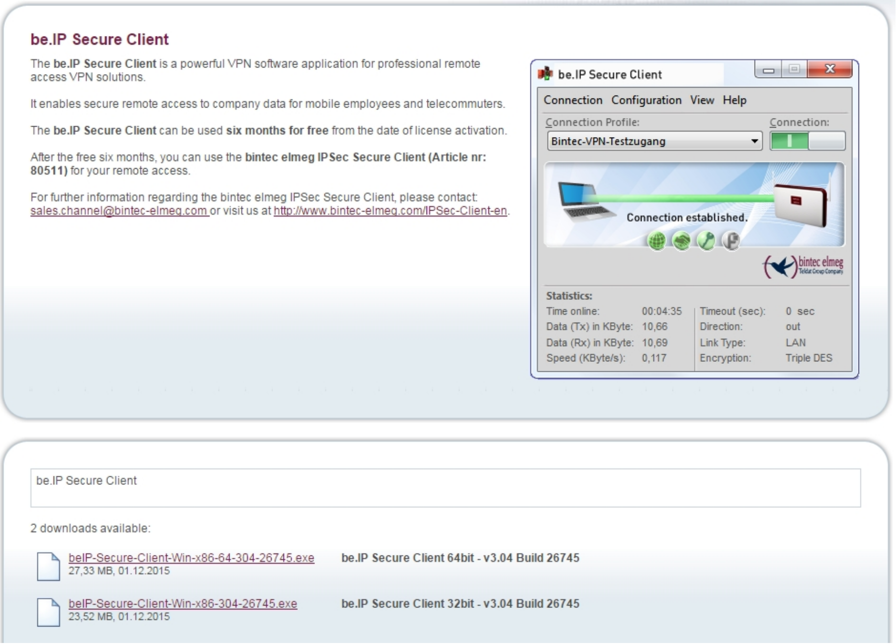
(8) Click **Export**.
 An addition window opens.

(9) Select **Save File** then click **OK**.
 The ini file is saved.

7.2.3 Download the be.IP Secure Client

(1) Click the **be.IP Secure Client** link or the graphic.

The bintec elmeg home page opens at the corresponding point.



be.IP Secure Client

The **be.IP Secure Client** is a powerful VPN software application for professional remote access VPN solutions.

It enables secure remote access to company data for mobile employees and telecommuters.

The **be.IP Secure Client** can be used **six months for free** from the date of license activation.

After the free six months, you can use the **bintec elmeg IPSec Secure Client (Article nr: 80511)** for your remote access.

For further information regarding the bintec elmeg IPSec Secure Client, please contact: sales.channel@bintec-elmeg.com or visit us at http://www.bintec-elmeg.com/IPSec-Client-en.

Connection Profile: Bintec-VPN-Testzugang
Connection:

Statistics:

Time online:	00:04:35	Timeout (sec):	0 sec
Data (Tx) in KByte:	10,66	Direction:	out
Data (Rx) in KByte:	10,69	Link Type:	LAN
Speed (KByte/s):	0,117	Encryption:	Triple DES

be.IP Secure Client

2 downloads available:

beIP-Secure-Client-Win-x86-64-304-26745.exe 27,33 MB, 01.12.2015	**be.IP Secure Client 64bit - v3.04 Build 26745**
beIP-Secure-Client-Win-x86-304-26745.exe 23,52 MB, 01.12.2015	**be.IP Secure Client 32bit - v3.04 Build 26745**

Fig. 47: Download page for the be.IP Secure Client

(2) Download the installation file for the be.IP Secure Client from this homepage and save the desired version of the .exe file (32 bit version or 64 bit version, suitable for your operating system) to your PC.

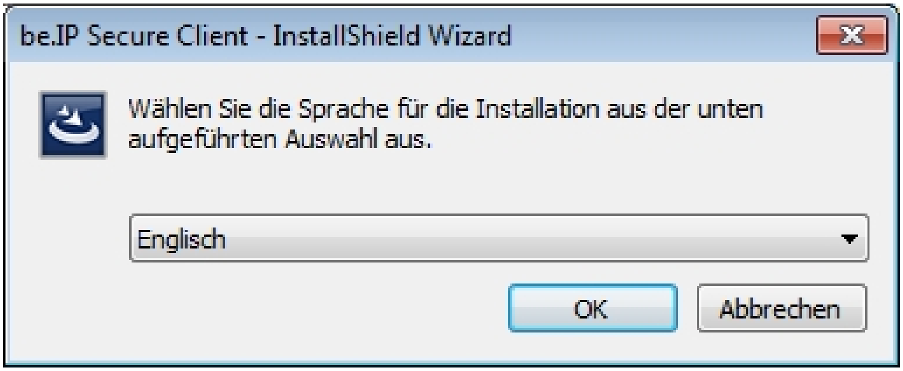
(3) Save the configuration of your gateway via **Save configuration** button.

7.2.4 Install and configure the be.IP Secure Client

An Assistant is available for installing the be.IP Secure Client.

(1) Click the exe file that was downloaded from the bintec-elmeg homepage.

The **be.IP Secure Client - InstallShield Wizard** window opens.

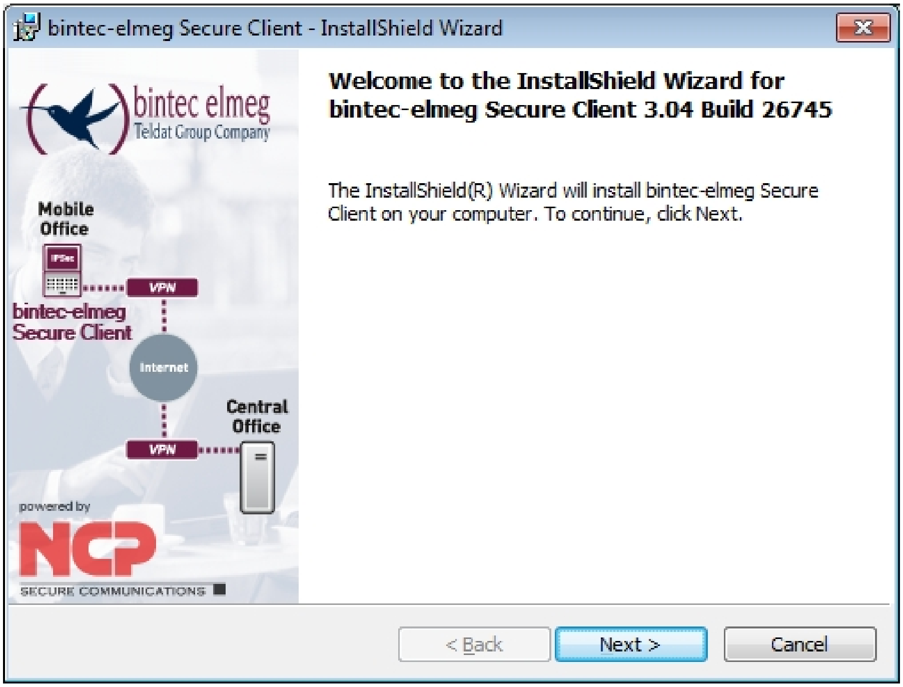

be.IP Secure Client - InstallShield Wizard

Wählen Sie die Sprache für die Installation aus der unten aufgeführten Auswahl aus.

Englisch

Fig. 48: Language selection in **InstallShield wizard**

(2) Select the installation language, e.g. `German` and then click **OK**.
The file is unpacked, you are greeted.

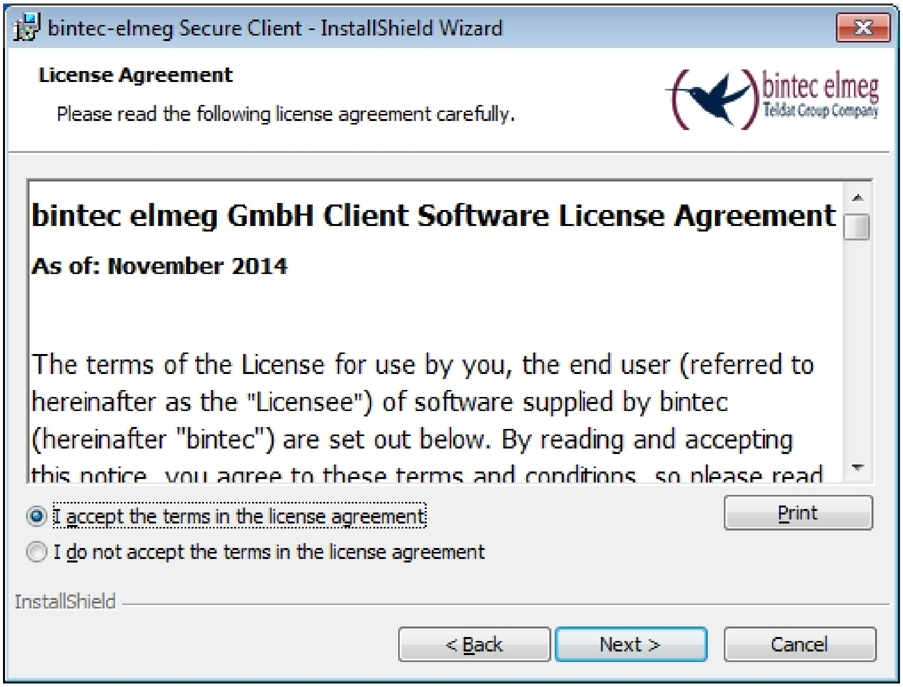

bintec-elmeg Secure Client - InstallShield Wizard

Welcome to the InstallShield Wizard for bintec-elmeg Secure Client 3.04 Build 26745

The InstallShield(R) Wizard will install bintec-elmeg Secure Client on your computer. To continue, click Next.

Fig. 49: Welcome page in **InstallShield wizard**

(3) Click **Next**.



License Agreement

Please read the following license agreement carefully.

bintec elmeg GmbH Client Software License Agreement

As of: November 2014

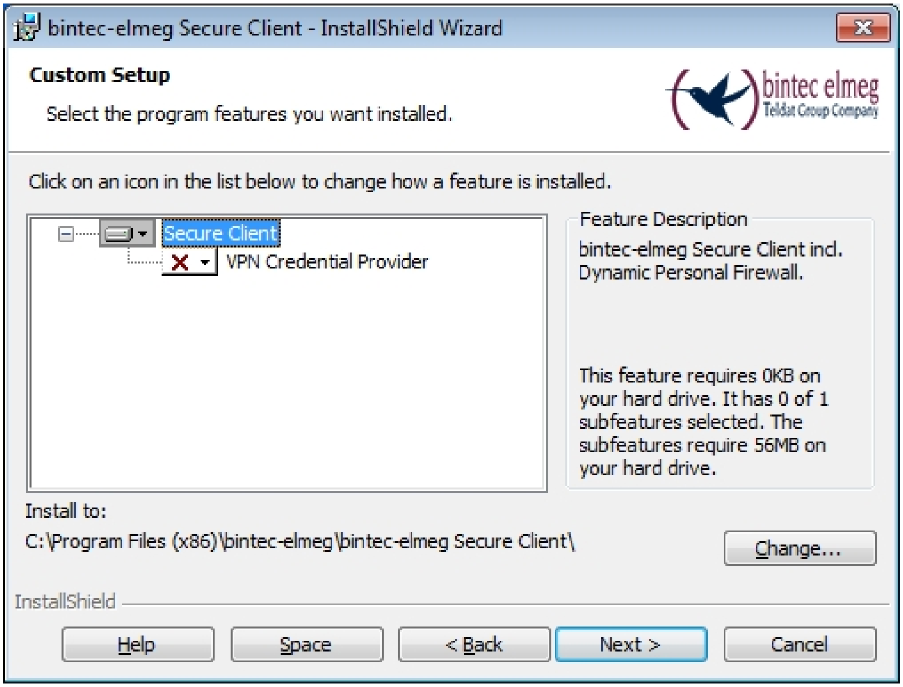
The terms of the License for use by you, the end user (referred to hereinafter as the "Licensee") of software supplied by bintec (hereinafter "bintec") are set out below. By reading and accepting this notice, you agree to these terms and conditions, so please read

● I accept the terms in the license agreement

○ I do not accept the terms in the license agreement

Fig. 50: Licence agreement in **InstallShield wizard**

(4) Read the licence conditions. Enable `I accept the terms of the licensing agreement` then click **Next**.



bintec-elmeg Secure Client - InstallShield Wizard

Custom Setup

Select the program features you want installed.

Click on an icon in the list below to change how a feature is installed.

- Secure Client
  - VPN Credential Provider

Feature Description

bintec-elmeg Secure Client incl. Dynamic Personal Firewall.

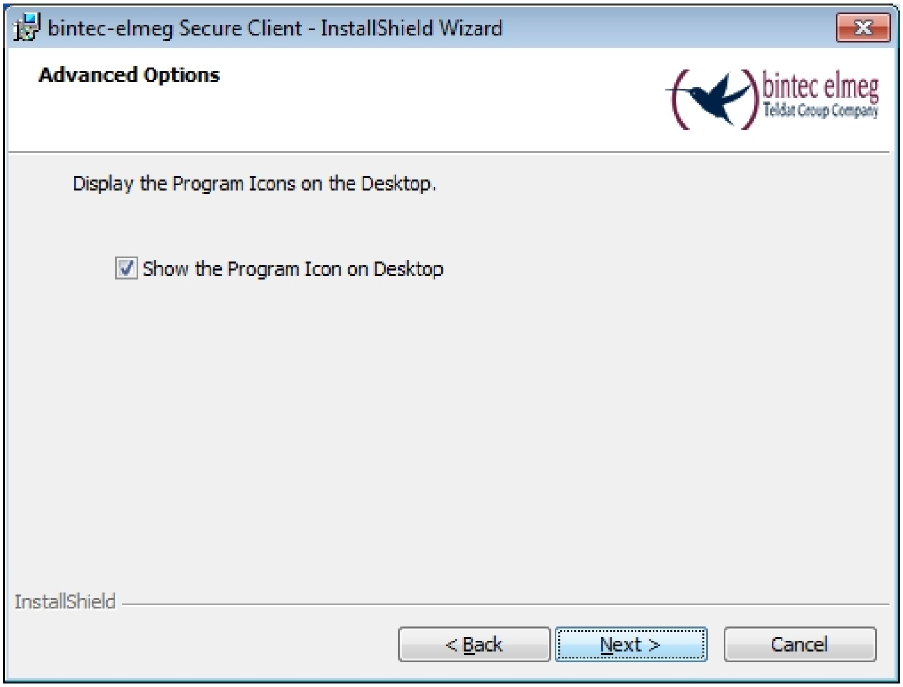
This feature requires 0KB on your hard drive. It has 0 of 1 subfeatures selected. The subfeatures require 56MB on your hard drive.

Install to:

C:\Program Files (x86)\bintec-elmeg\bintec-elmeg Secure Client\

Fig. 51: Setup in the **InstallShield wizard**

(5) Keep the setting **Secure Client** then click **Next**.



bintec-elmeg Secure Client - InstallShield Wizard

Advanced Options

Display the Program Icons on the Desktop.

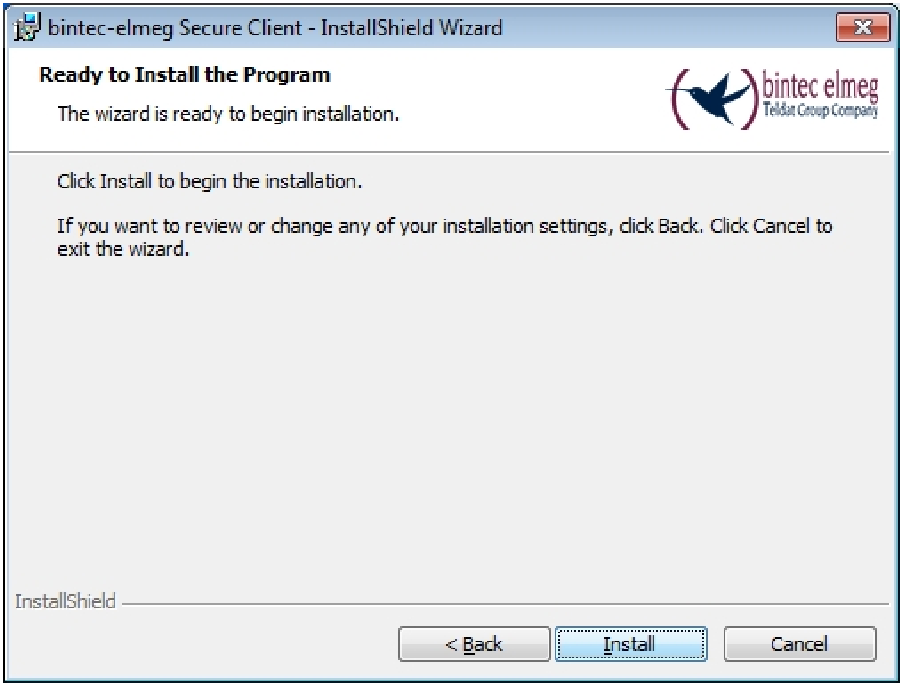
☑ Show the Program Icon on Desktop

Fig. 52: Allow the icon to be displayed in **InstallShield wizard**

(6) If you want an icon to be displayed on your PC desktop for be.IP Secure Client, enable the `Display program icons on desktop` then click **Next**.

Preparations for installation are complete.

(7) Click **Install**.



bintec-elmeg Secure Client - InstallShield Wizard

Ready to Install the Program

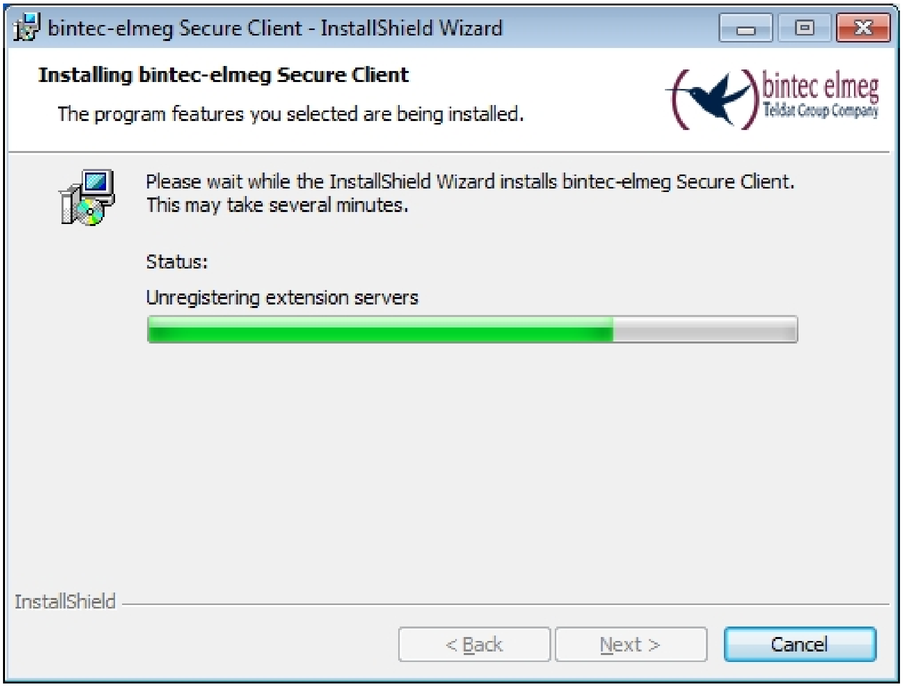
The wizard is ready to begin installation.

Click Install to begin the installation.

If you want to review or change any of your installation settings, click Back. Click Cancel to exit the wizard.

Fig. 53: End of preparations in the **InstallShield wizards**

The be.IP Secure Client is installed.



bintec-elmeg Secure Client - InstallShield Wizard

Installing bintec-elmeg Secure Client

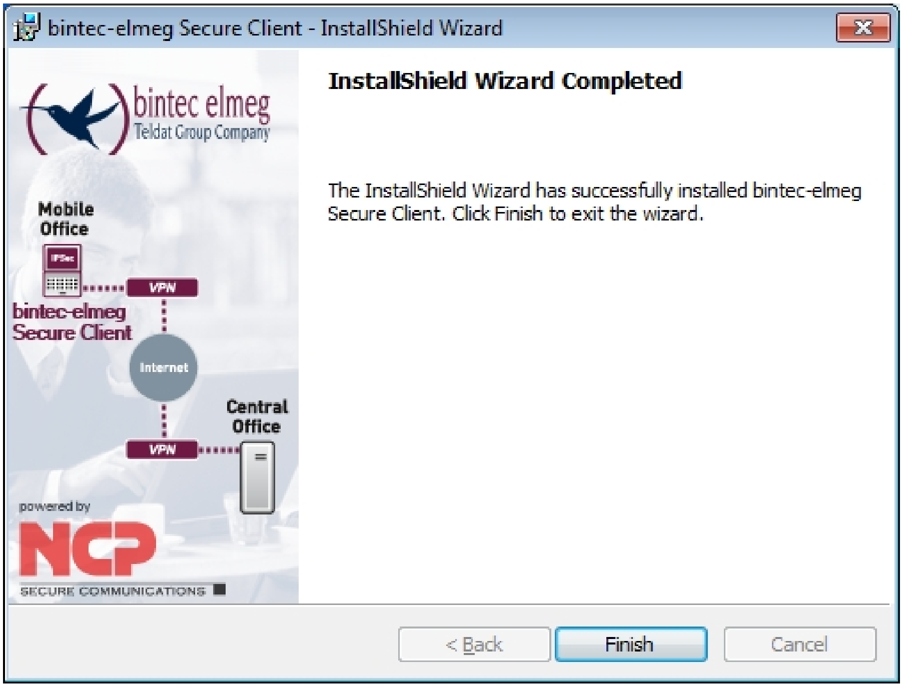
The program features you selected are being installed.

Please wait while the InstallShield Wizard installs bintec-elmeg Secure Client. This may take several minutes.

Status:

Unregistering extension servers

Fig. 54: Install be.IP Secure Client in **InstallShield wizard**



bintec-elmeg Secure Client - InstallShield Wizard

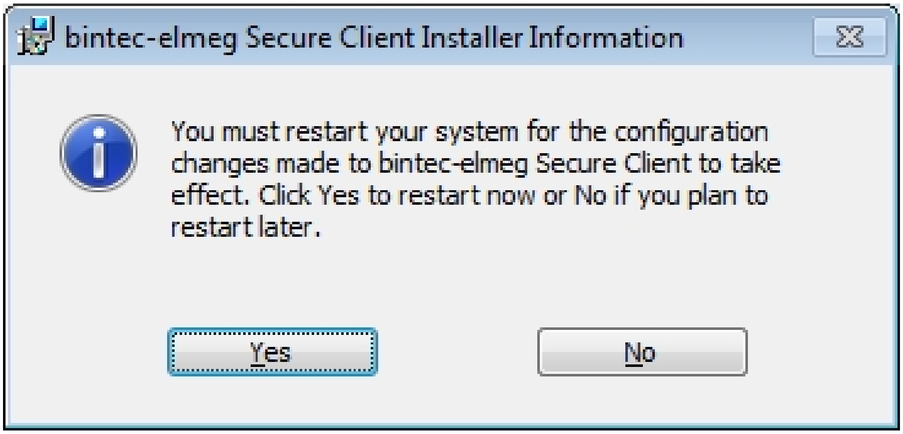
InstallShield Wizard Completed

The InstallShield Wizard has successfully installed bintec-elmeg Secure Client. Click Finish to exit the wizard.

Fig. 55: be.IP Secure Client is installed

Installation is complete.

(8) Click on **Complete**.



bintec-elmeg Secure Client Installer Information

You must restart your system for the configuration changes made to bintec-elmeg Secure Client to take effect. Click Yes to restart now or No if you plan to restart later.

Fig. 56: Installation information for the **be.IP Secure Client**

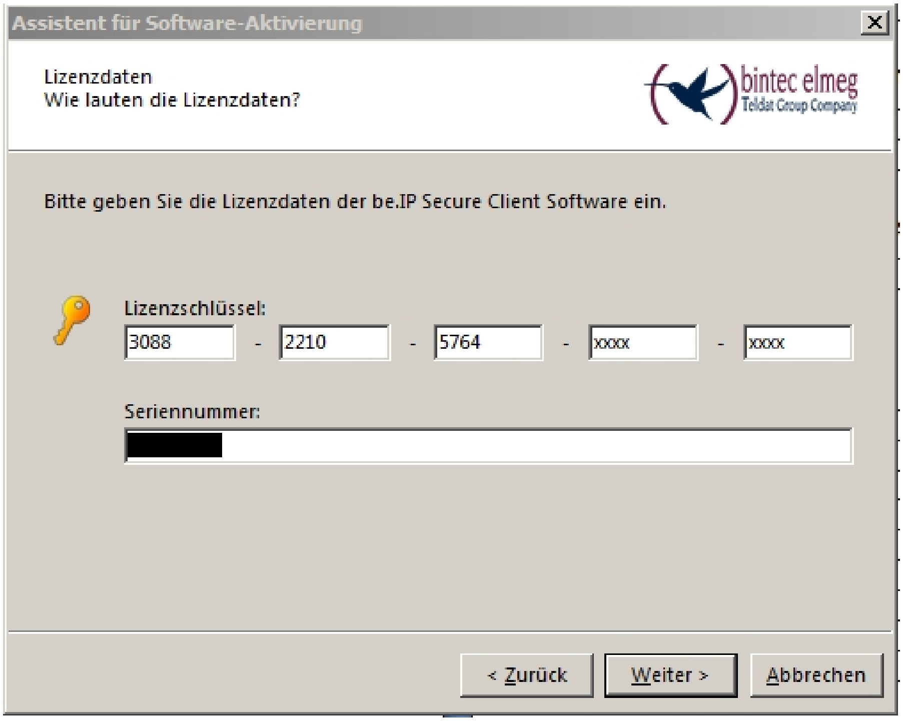
(9) Click **Yes** to restart your PC.

7.2.5 Enable software and load file

The be.IP Secure Client and the assistant for software enabling automatically start after the PC is rebooted. An active internet connection is required for software activation.

(1) Enter the licence data.

> **Note**
>
> The serial number of a be.IP Client license consists of eight digits and begins with `300`.



Assistent für Software-Aktivierung

Lizenzdaten
Wie lauten die Lizenzdaten?

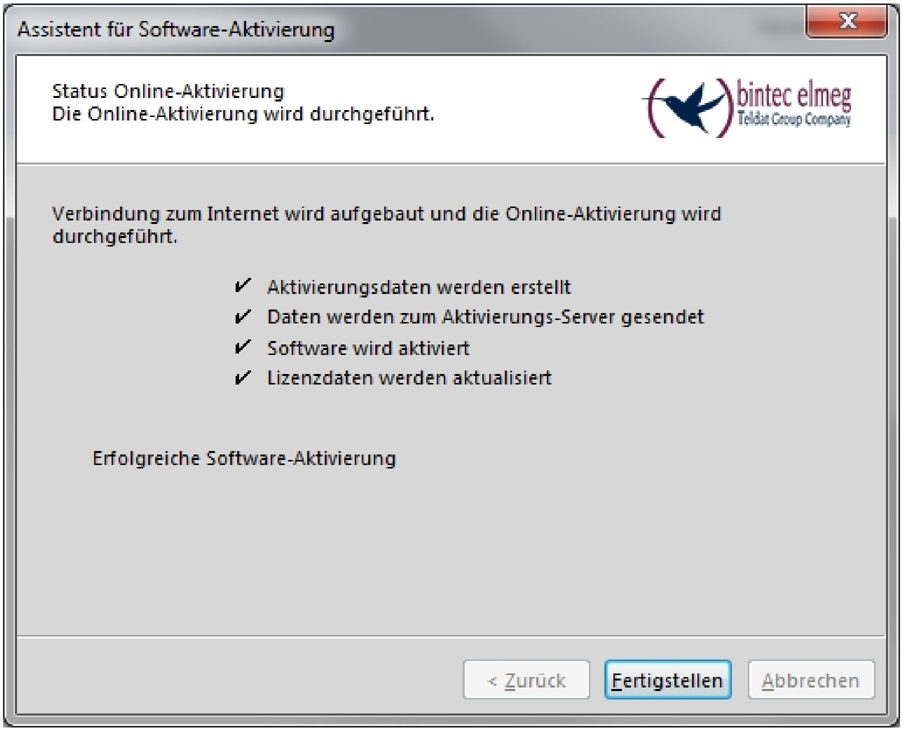
Bitte geben Sie die Lizenzdaten der be.IP Secure Client Software ein.

Lizenzschlüssel: 3088 - 2210 - 5764 - xxxx - xxxx

Seriennummer: [redacted]

Fig. 57: Assistant for software enabling: Enter license data

(2) Click **Next**.
Online activation of the software is carried out.



Assistent für Software-Aktivierung

Status Online-Aktivierung
Die Online-Aktivierung wird durchgeführt.

Verbindung zum Internet wird aufgebaut und die Online-Aktivierung wird durchgeführt.

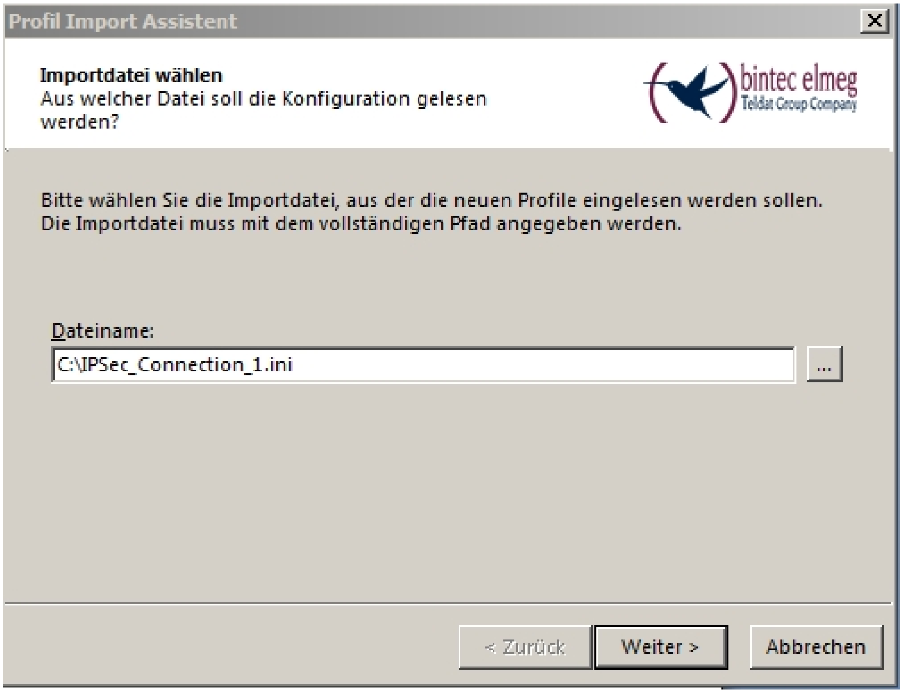
- ✓ Aktivierungsdaten werden erstellt
- ✓ Daten werden zum Aktivierungs-Server gesendet
- ✓ Software wird aktiviert
- ✓ Lizenzdaten werden aktualisiert

Erfolgreiche Software-Aktivierung

Fig. 58: Successful software activation

(3) When the software is successfully enabled, click **Finish**.

(4) When the software is enabled, load the ini file that was created using the gateway.



Profil Import Assistent

Importdatei wählen
Aus welcher Datei soll die Konfiguration gelesen werden?

Bitte wählen Sie die Importdatei, aus der die neuen Profile eingelesen werden sollen.
Die Importdatei muss mit dem vollständigen Pfad angegeben werden.

Dateiname: C:\IPSec_Connection_1.ini

Fig. 59: Load ini file

(5) Select the required file, e.g. `IPSec_Connection_1.ini` and click **Next**.

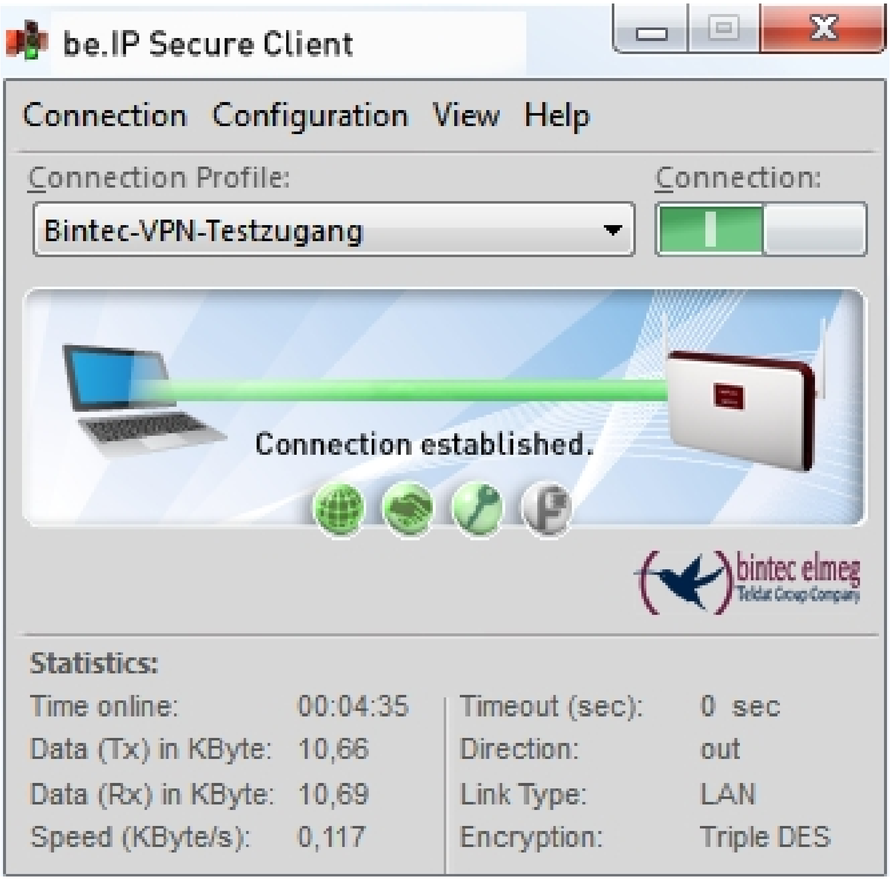
(6) Click **Finish**.

7.2.6 Establish IPSec connection

The IPSec connection can be established when enabling is complete and an ini file has been loaded.

(1) For this purpose, select **be.IP Secure Client** from the **Connection Profile** the profile you have loaded, e.g. `IPSec_Connection_1`.

(2) Click the **Connection** field.
The connection is established. The colour of the field changes from red to green.



Connection Profile: Bintec-VPN-Testzugang

Statistics:

Time online:	00:04:35	Timeout (sec):	0 sec
Data (Tx) in KByte:	10,66	Direction:	out
Data (Rx) in KByte:	10,69	Link Type:	LAN
Speed (KByte/s):	0,117	Encryption:	Triple DES

Fig. 60: IPSec connection is created

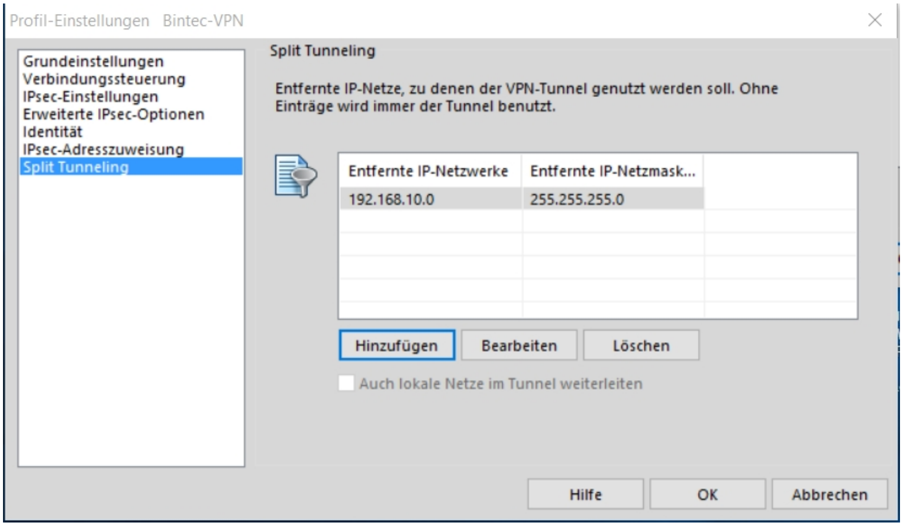
7.2.7 Split tunnel

By default the client sends all data packets into the active tunnel. If you want access to a specific destination network, then you must enter the IP address of this private destination network.

(1) For this purpose, go to **be.IP Secure Client Configuration**->**Profiles** in the menu.
The **Profiles** window opens.

(2) Double-click on the profile you have set up, e.g. `IPSec_Connection_1`.
The **profile settings IPSec_Connection_1** window opens.

(3) Click **Split Tunneling** on the left-hand side of the list.



Profil-Einstellungen Bintec-VPN

Split Tunneling

Entfernte IP-Netze, zu denen der VPN-Tunnel genutzt werden soll. Ohne Einträge wird immer der Tunnel benutzt.

Entfernte IP-Netzwerke	Entfernte IP-Netzmask...
192.168.10.0	255.255.255.0

□ Auch lokale Netze im Tunnel weiterleiten

Fig. 61: Split Tunneling

(4) Click **Add**.

The **IP networks** window opens.

(5) Enter the IP address and the netmasks of your private network, e.g. `192.168.10.0` and `255.255.255.0` and click **OK**.

Your network is displayed in the list.

(6) Click **OK**.

The **IP networks** window closes.

(7) Click **OK**.

The **Profiles** window closes.

7.3 Overview of Configuration Steps

Start Gateway

Field	Window	Value
User	Welcome	e.g. `admin`
Password	Welcome	e.g. `User`

Configure tunnel with the Assistant VPN

Field	Menu	Value
VPN Scenario	**Assistants->VPN->VPN Connections->New**	e.g. `IPSec - Single Client Dialin`
Description	**Assistants->VPN->VPN**	e. g.

Field	**Menu**	**Value**
	Connections->**New**->**Continue**	*IPSec_Connection_1*
Local IPSec ID	**Assistants**->**VPN**->**VPN Connections**->**New**->**Continue**	Leave the displayed value unchanged, e.g. *be.IP+*
Remote IPSec ID	**Assistants**->**VPN**->**VPN Connections**->**New**->**Continue**	e. g. *IPSec_Connection_1*
Preshared Key	**Assistants**->**VPN**->**VPN Connections**->**New**->**Continue**	e.g. *Secret_1*
Select IP Address Pool	**Assistants**->**VPN**->**VPN Connections**->**New**->**Continue**	e.g. *DHCP address range*
Export configuration file for bintec Secure IPSec Client	**Assistants**->**VPN**->**VPN Connections**->**New**->**Next**->**OK**	*Enabled*

bintec-elmeg Secure Client - InstallShield wizard

Field	**Menu**	**Value**
Language	**OK**	e. g. *German*
I accept the conditions of the licence agreement	**OK**->**Next**	*Enabled*
Secure Client	**OK**->**Next**->**Next**	*Enabled*
Display program icons on the desktop	**OK** ->**Next**->**Next**->**Next**->**Install**->**Finish**->**Yes**	e.g. *enabled*

Software enabling assistant

Field	**Menu**	**Value**
Online activation	**Activation**	**Enabled**
Licence Key	**Activation** ->**Activation**->**Next**	e.g. *3088 - 2210 - 5764 - 6789 - 1234*
Serial number	**Activation** ->**Activation**->**Next**	e.g. *30001234*
Select import file	**Activation** ->**Activation** ->**Next** ->**Next**	e.g. *C:\IPSec_Connection_1.ini*

be.IP Secure Client: Establish IPSec connection

Field	Menu	Value
Connection profile	Window **be.IP Secure Client**	e. g. *IPSec_Connection_1*

be.IP Secure Client: Share tunnel

Field	Menu	Value
Available Profiles	**Configuration** ->**profiles**	e.g. double-click on *IPSec_Connection_1*
List on left-hand side	**Configuration** ->**Profiles** ->**Add**	Split Tunneling
IP network	**Configuration** ->**Profiles** ->**Add**	e.g. *192.168.10.0*
Netmask	**Configuration** ->**Profiles** ->**Add** ->**OK**->**OK**->**OK**	e.g. *255.255.255.0*

Chapter 8 be.IP plus as PBX with two xDSL connections

8.1 Introduction

The following workshop describes the configuration of a **be.IP plus** as a telephone system with two xDSL connections by means of load distribution and permanently assigned SIP lines (no nomadic use).

It is possible to link individual VoIP connections to a specific WAN connection from firmware status 10.1.5 onwards. This is made possible via the mechanism for **locations** that is already used for registrations and also defines the outgoing interface for VoIP packages of a SIP connection.

This state is necessary due to the lack of other decision-making criteria, as the registrar IP address, ports, and DSCP values are identical. In addition, it should be taken into account that IPv6 is activated with only one of the WAN connections, as all operating systems and their applications such as, e.g. MS Windows are not capable of using several IPv6 prefixes in load distribution scenarios, and that this task cannot be taken over by the **be.IP** as there is no NAT either.

The **GUI** (Graphical User Interface) is used for configuring.

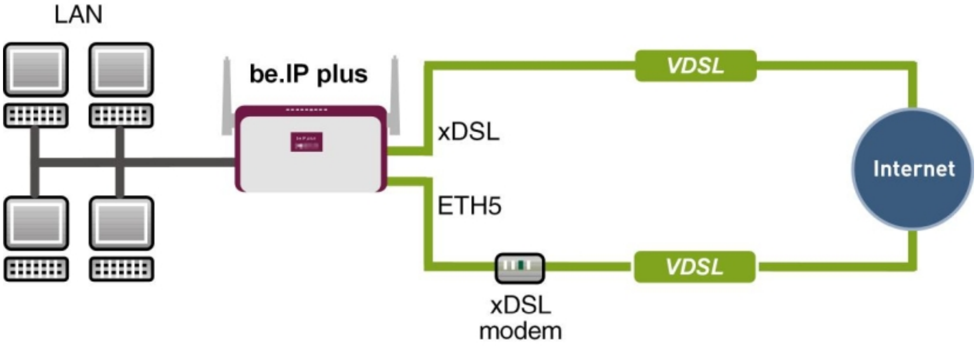


Fig. 62: Example scenario

Requirements

The following prerequisites for configuration must be met:

- A **be.IP plus** with system software 10.1.5 patch 6
- Two independent VDSL internet connections
- An external VDSL modem that is connected to eth1-4 (physical port LAN5) of the **be.IP**

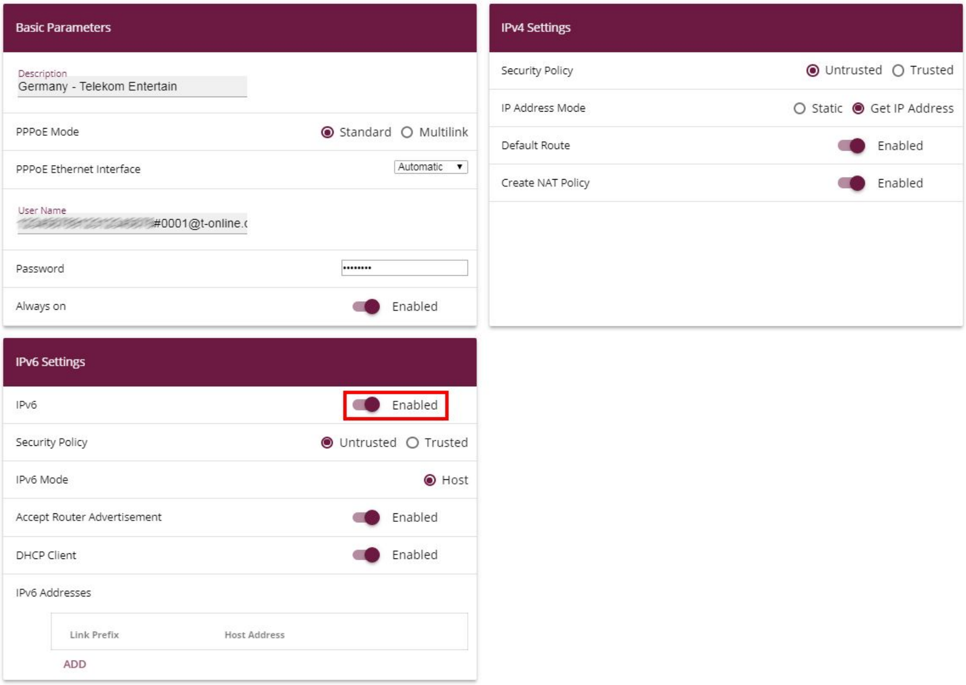
8.2 Configuration

8.2.1 Setting up the WAN connection

Both WAN connections must be set up first. Follow the **Initial operation Telekom** steps for the WAN connection via the internal VDSL modem (for a connection to Deutsche Telekom). Use the **Next** button to carry out the individual steps.

WAN connection via the internal modem of the be.IP

The connection to Deutsche Telekom that is configured via the Quick Start wizard can be seen in the menu **WAN**->**Internet + Dialup**->**PPPoE**->**Germany - Telekom Entertain** -> ✎ . The **IPv6** option is activated.



Basic Parameters

Description: Germany - Telekom Entertain

PPPoE Mode: ● Standard ○ Multilink

PPPoE Ethernet Interface: Automatic ▾

User Name: [redacted]#0001@t-online.c

Password: ••••••••

Always on: Enabled

IPv4 Settings

Security Policy: ● Untrusted ○ Trusted

IP Address Mode: ○ Static ● Get IP Address

Default Route: Enabled

Create NAT Policy: Enabled

IPv6 Settings

IPv6: Enabled

Security Policy: ● Untrusted ○ Trusted

IPv6 Mode: ● Host

Accept Router Advertisement: Enabled

DHCP Client: Enabled

IPv6 Addresses

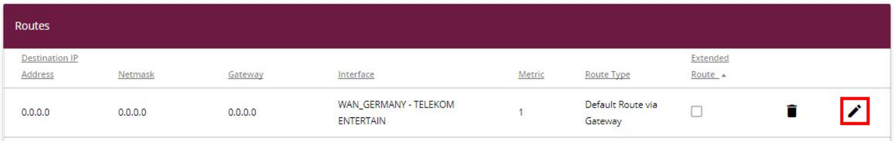
Link Prefix	Host Address

ADD

Fig. 63: **WAN**->**Internet + Dialup**->**PPPoE**->**Germany - Telekom Entertain** -> ✎

In order to avoid disruptions of the first existing VDSL-WAN path via the internal modem, the **Metric** of the standard route must initially be set to *0* via the relevant WAN interface. As the **be.IP** also receives a standard route together with the WAN-IP via the second xDSL route - albeit with metric *1* - this step is expedient (particularly with remote configuration).

(1) Go to the **Network**->**Routes**->**IPv4 Route Configuration** menu.

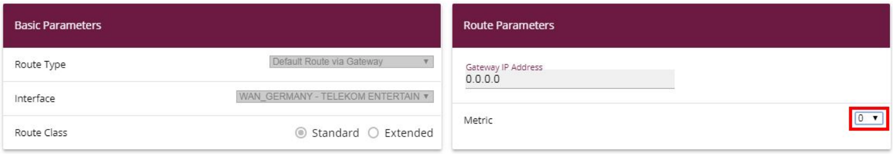


Routes

Destination IP Address	Netmask	Gateway	Interface	Metric	Route Type	Extended Route ▲		
0.0.0.0	0.0.0.0	0.0.0.0	WAN_GERMANY - TELEKOM ENTERTAIN	1	Default Route via Gateway	□	🗑	✎

Fig. 64: **Network**->**Routes**->**IPv4 Route Configuration**

(2) Select the ✎ symbol so that the *WAN_GERMANY - TELEKOM ENTERTAIN* entry can be processed.



Basic Parameters

Route Type: Default Route via Gateway ▼

Interface: WAN_GERMANY - TELEKOM ENTERTAIN ▼

Route Class: ● Standard ○ Extended

Route Parameters

Gateway IP Address: 0.0.0.0

Metric: 0 ▼

Fig. 65: **Network**->**Routes**->**IPv4 Route Configuration** ✎

(3) Under **Metric** select the priority of the route, which is *0* in our example.

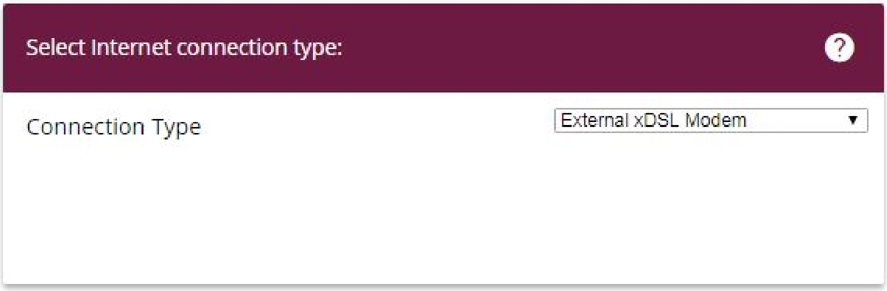
(4) Click **OK** to confirm your entries.

WAN connection via the external modem to en1-4 (physical port LAN5)

The second connection is created via the external modem to en1-4 with the aid of **Assistants**.

(1) To do so, go to the **Assistants**->**Internet**->**Internet Connections**->**New** menu.

(2) For **Connection Type**, select *External xDSL Modem*.



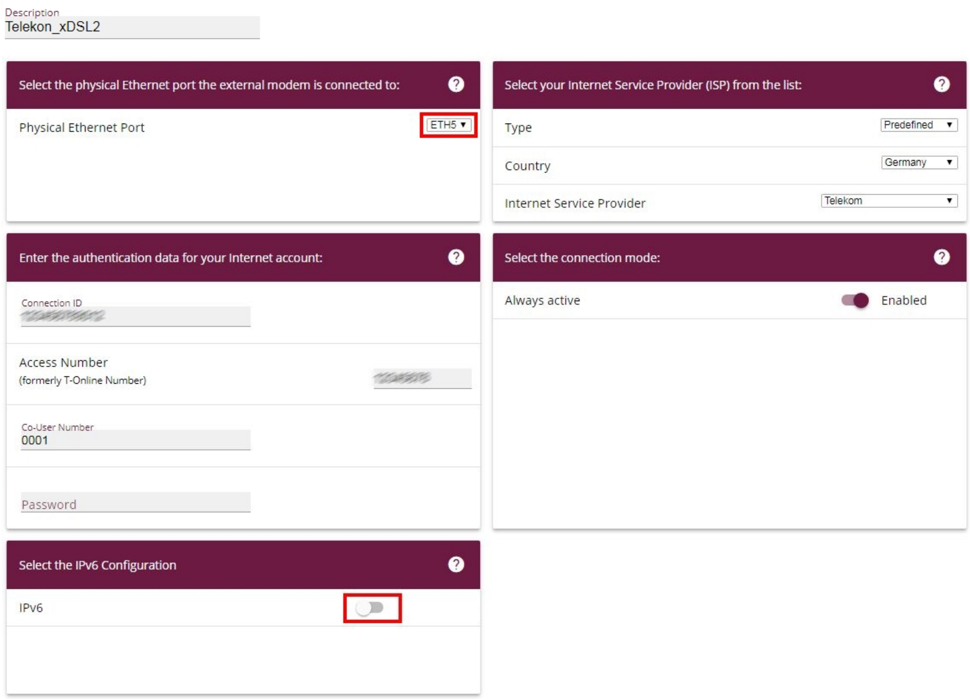
Select Internet connection type: ?

Connection Type: External xDSL Modem ▼

Fig. 66: **Assistants**->**Internet**->**Internet Connections**->**New**

(3) Click on **Next** to configure a new internet connection.

(4) Enter the required data for the connection.



Description: Telekon_xDSL2

Select the physical Ethernet port the external modem is connected to:

Physical Ethernet Port: ETH5

Select your Internet Service Provider (ISP) from the list:

Type: Predefined

Country: Germany

Internet Service Provider: Telekom

Enter the authentication data for your Internet account:

Connection ID: [redacted]

Access Number (formerly T-Online Number): [redacted]

Co-User Number: 0001

Password

Select the connection mode:

Always active: Enabled

Select the IPv6 Configuration

IPv6: ○

Fig. 67: **Assistants**->**Internet Access**->**Internet Connections**->**New**->**Next**

Note

The message you get when you create the second DSL connection may be ignored. The IP load distribution avoids routing conflicts due to multiple standard routes!

Proceed as follows:

(1) Under **Description** enter any name for the Internet connection, e.g. `Telekom_xDSL2` .

(2) Under **Physical Ethernet Port** select the port that is connected to the xDSL modem, in this case `ETH5` (this corresponds to the LAN5 connection of the device).

(3) Under **Type** select the option `Predefined`.

(4) Select the **Country** where Internet access should be set up, in this case `Germany`.

(5) Select your **Internet Service Provider** from the list, in this case `Telekom`.

(6) Under **Connection ID** enter the 12-digit user account obtained from your provider,

e.g. `123456789012`.

(7) Enter the usually 12-digit **Access Number** that you have received from your provider, e.g. `123456789012`.

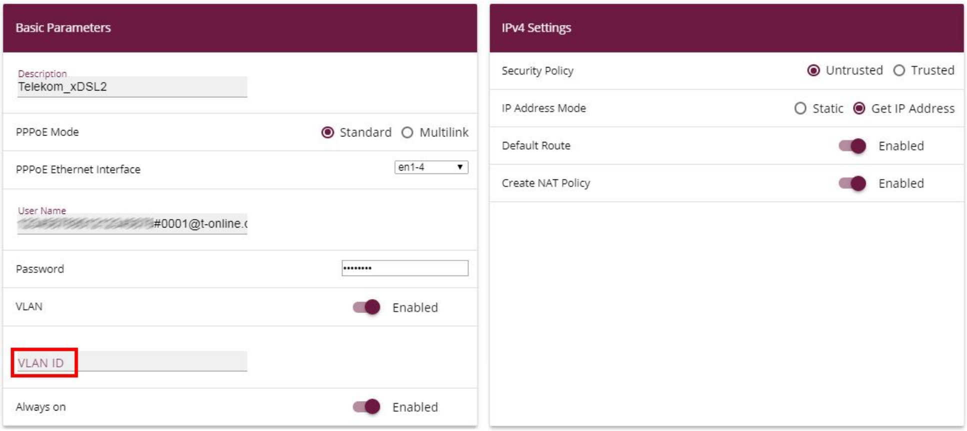
(8) Enter the **Password** that your provider has given you, e.g. `test12345`.

(9) In the **Always on** field, specify whether or not the Internet connection should always be active. Only select this option if you have flatrate Internet access.

(10) The control box **IPv6** remains deactivated.

(11) Click **OK** to confirm your entries.

Depending on the setting of the upstream modem, the **VLAN ID** `7` in the menu **WAN**->**Internet + Dialup**->**PPPoE**->✎ -> **Telekom_xDSL2** may have to be removed.



Basic Parameters

Description: Telekom_xDSL2

PPPoE Mode: ● Standard ○ Multilink

PPPoE Ethernet Interface: en1-4

User Name: [redacted]#0001@t-online.c

Password: ••••••••

VLAN: Enabled

VLAN ID

Always on: Enabled

IPv4 Settings

Security Policy: ● Untrusted ○ Trusted

IP Address Mode: ○ Static ● Get IP Address

Default Route: Enabled

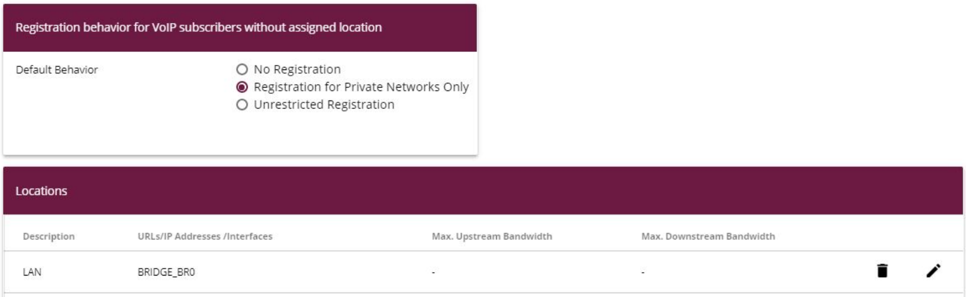
Create NAT Policy: Enabled

Fig. 68: **WAN**->**Internet + Dialup**->**PPPoE**->✎ -> **Telekom_xDSL2**

8.2.2 Setting up the WAN interface for the SIP connection

The SIP connections must still be fixedly linked to the relevant xDSL-WAN interfaces in the next step.

For connection via the internal modem of the **be.IP**, go to the menu **VoIP**->**Settings**->**Locations**.



Registration behavior for VoIP subscribers without assigned location

Default Behavior
○ No Registration
● Registration for Private Networks Only
○ Unrestricted Registration

Locations

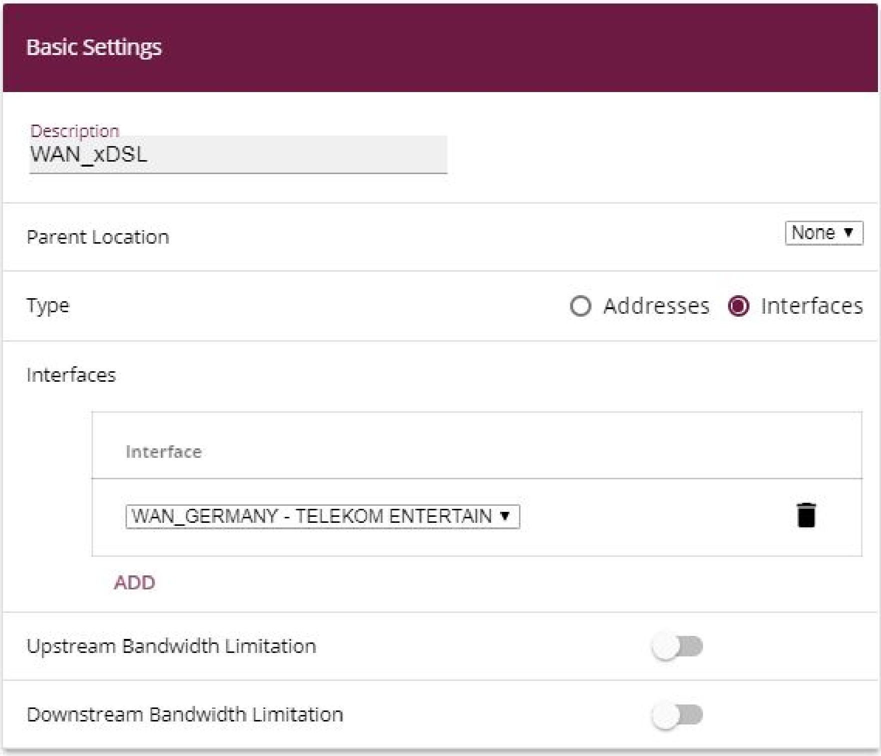
Description	URLs/IP Addresses /Interfaces	Max. Upstream Bandwidth	Max. Downstream Bandwidth
LAN	BRIDGE_BR0	-	-

Fig. 69: **VoIP**->**Settings**->**Locations**

Proceed as follows:

(1) When in **Default Behavior** keep the setting *Registration for Private Networks Only*.

(2) Click on **New** to create new entries.



Basic Settings

Description: WAN_xDSL

Parent Location: None ▾

Type: ○ Addresses ● Interfaces

Interfaces

Interface
WAN_GERMANY - TELEKOM ENTERTAIN ▾

ADD

Upstream Bandwidth Limitation

Downstream Bandwidth Limitation

Fig. 70: **VoIP**->**Settings**->**Locations**->**New**

(3) State a **Description** for the entry, in this case *WAN_xDSL*.

(4) Under **Type** select the *Interface* option. The SIP location is defined via the avail-

able interfaces.

(5) Under **Interfaces** click **Add** and select the desired interface, in this case *WAN_GERMANY - TELEKOM ENTERTAIN*.

(6) Click **OK** to confirm your entries.

The configuration must be carried out for **both** xDSL-WAN connections and the associated SIP connections. Configure the external xDSL modem in the same manner as configuring the internal modem.

(1) State a **Description** for the entry, in this case *Telekom_xDSL2*.

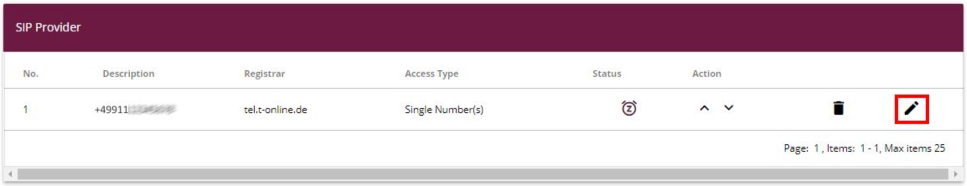
(2) Under **Type** select the *Interface* option.

(3) Under **Interfaces** click **Add** and select the desired interface, in this case *WAN_TELEKOM_xDSL2*.

(4) Click **OK** to confirm your entries.

Now select the newly defined **Location** regarding the connection to Deutsche Telekom.

To do so, go to the **VoIP**->**Settings**->**SIP Provider** menu.



SIP Provider

No.	Description	Registrar	Access Type	Status	Action		
1	+49911[redacted]	tel.t-online.de	Single Number(s)	ⓩ	^ v	🗑	✎

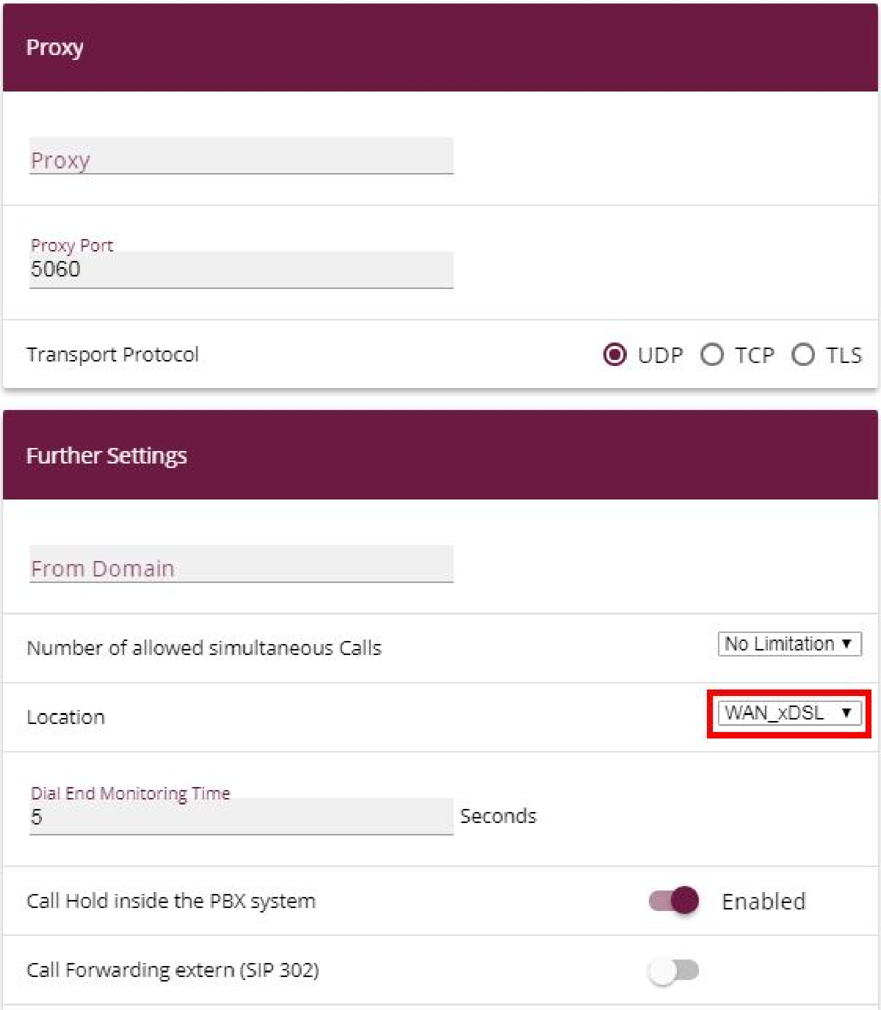
Page: 1 , Items: 1 - 1, Max items 25

Fig. 71: **VoIP**->**Settings**->**SIP Provider**

Proceed as follows:

(1) Select the ✎ symbol to process the SIP provider.

(2) Click **Advanced Settings**.



Proxy

Proxy

Proxy Port
5060

Transport Protocol ● UDP ○ TCP ○ TLS

Further Settings

From Domain

Number of allowed simultaneous Calls: No Limitation ▾

Location: WAN_xDSL ▾

Dial End Monitoring Time
5 Seconds

Call Hold inside the PBX system: Enabled

Call Forwarding extern (SIP 302)

Fig. 72: **VoIP**->**Settings**->**SIP Provider**->**New**+**Advanced Settings**

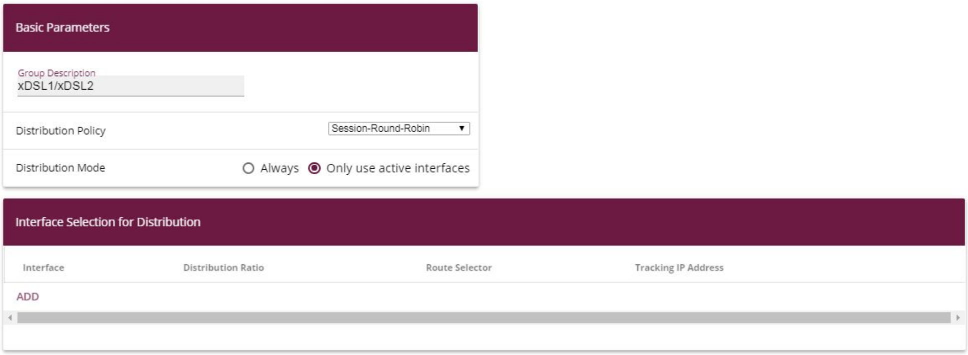
(3) Select the newly defined **Location** of the SIP provider, in this case `WAN_xDSL`.

(4) Click **OK** to confirm your entries.

8.2.3 Setting up the load distribution

A **Load Balancing Group** needs to have been created before you can set up the load distribution.

Go to the **Network**->**Load Balancing**->**Load Balancing Groups**->**New** menu.



Basic Parameters

Group Description xDSL1/xDSL2

Distribution Policy Session-Round-Robin ▾

Distribution Mode ○ Always ● Only use active interfaces

Interface Selection for Distribution

Interface	Distribution Ratio	Route Selector	Tracking IP Address

ADD

Fig. 73: **Network**->**Load Balancing**->**Load Balancing Groups**->**New**

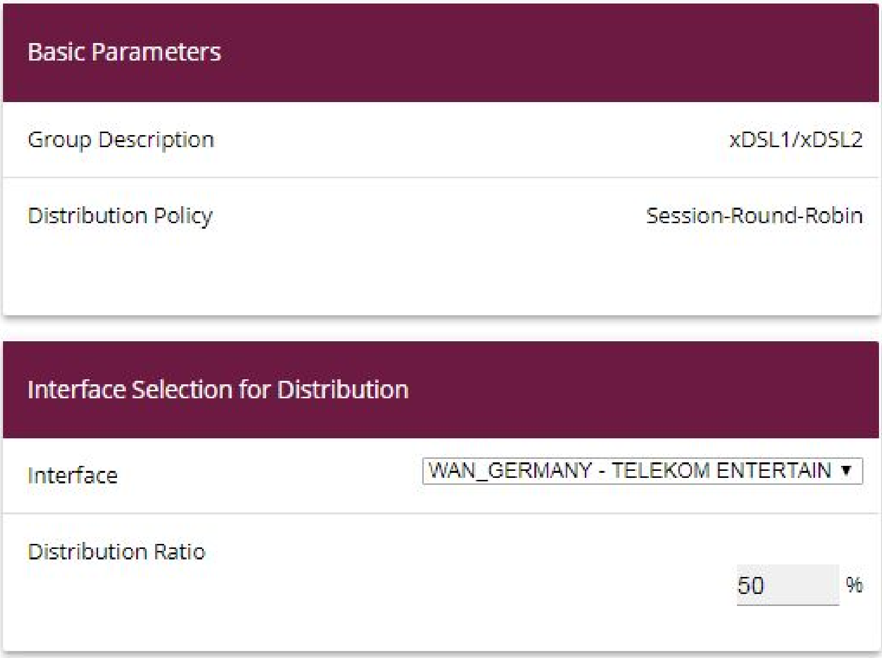
Proceed as follows:

(1) Enter any **Group Description** such as, e.g. *xDSL1/xDSL2*.

(2) Under **Distribution Policy** select the process according to which the data are distributed, in this case *Session-Round-Robin* .

The two xDSL Internet accesses can then be added to this load balancing group.

(3) To do so, click **Add**.



Basic Parameters

Group Description xDSL1/xDSL2

Distribution Policy Session-Round-Robin

Interface Selection for Distribution

Interface WAN_GERMANY - TELEKOM ENTERTAIN ▾

Distribution Ratio 50 %

Fig. 74: **Network**->**Load Balancing**->**Load Balancing Groups**->**New**->**Add**

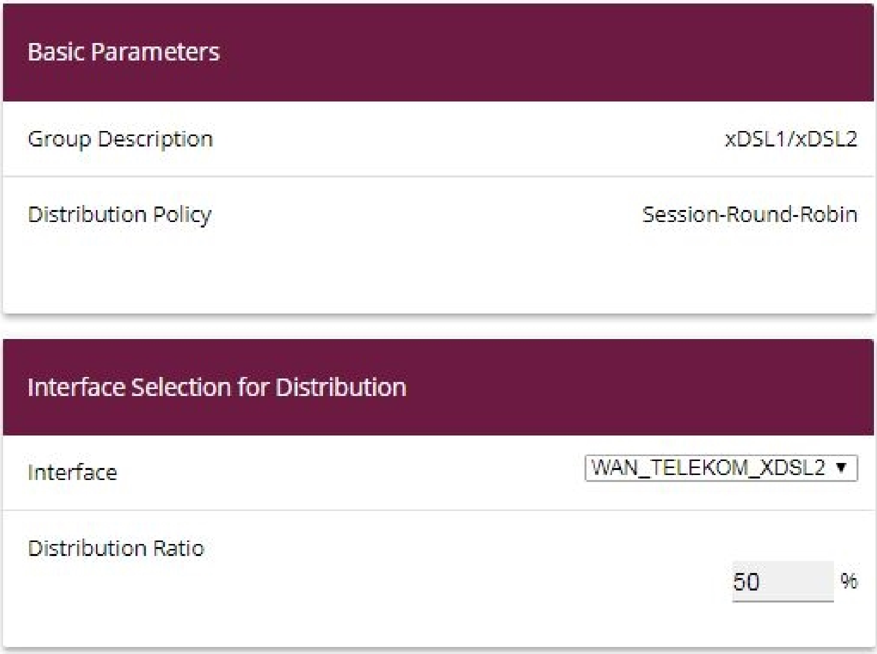
(4) Under **Interface** select the first xDSL access *WAN_GERMANY - TELEKOM ENTER-*

TAIN.

(5) In **Distribution Ratio** enter the percentage of the data traffic to be assigned to an interface. It is *50 %* in our example.

(6) Click **Apply**.

(7) Use **Add** to add the second xDSL line.



Basic Parameters

Group Description	xDSL1/xDSL2
Distribution Policy	Session-Round-Robin

Interface Selection for Distribution

Interface	WAN_TELEKOM_XDSL2 ▾
Distribution Ratio	50 %

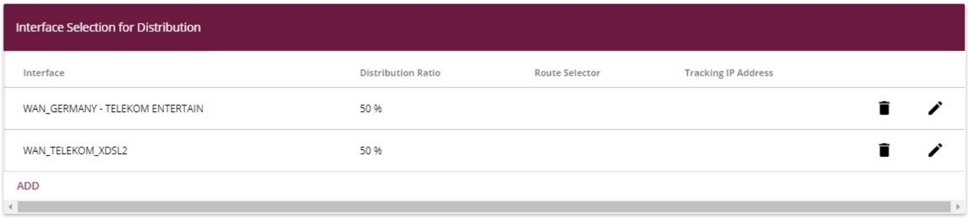
Fig. 75: **Network**->**Load Balancing**->**Load Balancing Groups**->**New**->**Add**

(8) Under **Interface** select the second xDSL access *WAN_TELEKOM_XDSL2*.

(9) When on **Distribution Ratio** enter *50 %*.

(10) Click **Apply**.

After this configuration step, the two Internet connections can be used with the load distribution.



Interface Selection for Distribution

Interface	Distribution Ratio	Route Selector	Tracking IP Address		
WAN_GERMANY - TELEKOM ENTERTAIN	50 %			🗑	✎
WAN_TELEKOM_XDSL2	50 %			🗑	✎

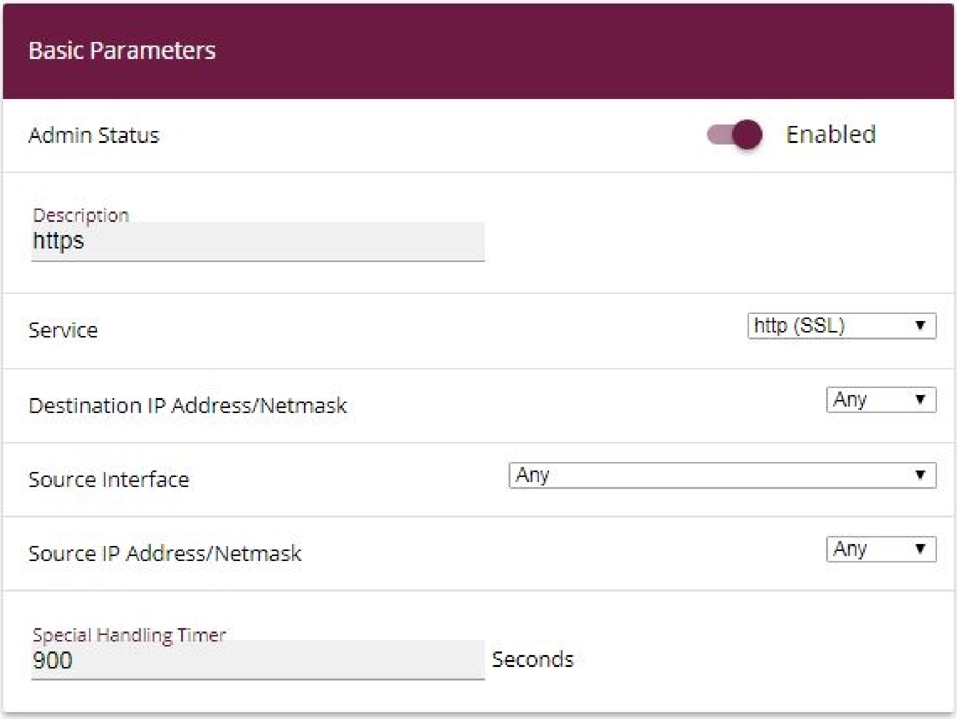
Fig. 76: **Network**->**Load Balancing**->**Load Balancing Groups**

Distribution ratios shall be adjusted accordingly in case of differing speeds on WAN routes or in case of a larger number of WAN routes involved in load distribution.

8.2.4 Special load distribution handling for encrypted connections

With the configuration now complete, IP sessions are distributed half and half to the two xDSL lines. This behaviour can lead to problems and losses of connection with certain protocols (e. g. encrypted HTTPS connections). The reason for these connection problems lies in the different Internet IP address of the two xDSL connections. With parallel connections to the same server, the two xDSL lines would be used alternately. To get around this difficulty, IP sessions that are associated can temporarily be connected to one of the Internet connections. This type of critical connection is configured in the **Special Session Handling** menu.

Go to the **Network**->**Load Balancing**->**Special Session Handling**->**New** menu.



Basic Parameters

Admin Status: Enabled

Description: https

Service: http (SSL)

Destination IP Address/Netmask: Any

Source Interface: Any

Source IP Address/Netmask: Any

Special Handling Timer: 900 Seconds

Fig. 77: **Network**->**Load Balancing**->**Special Session Handling**->**New**

Proceed as follows:

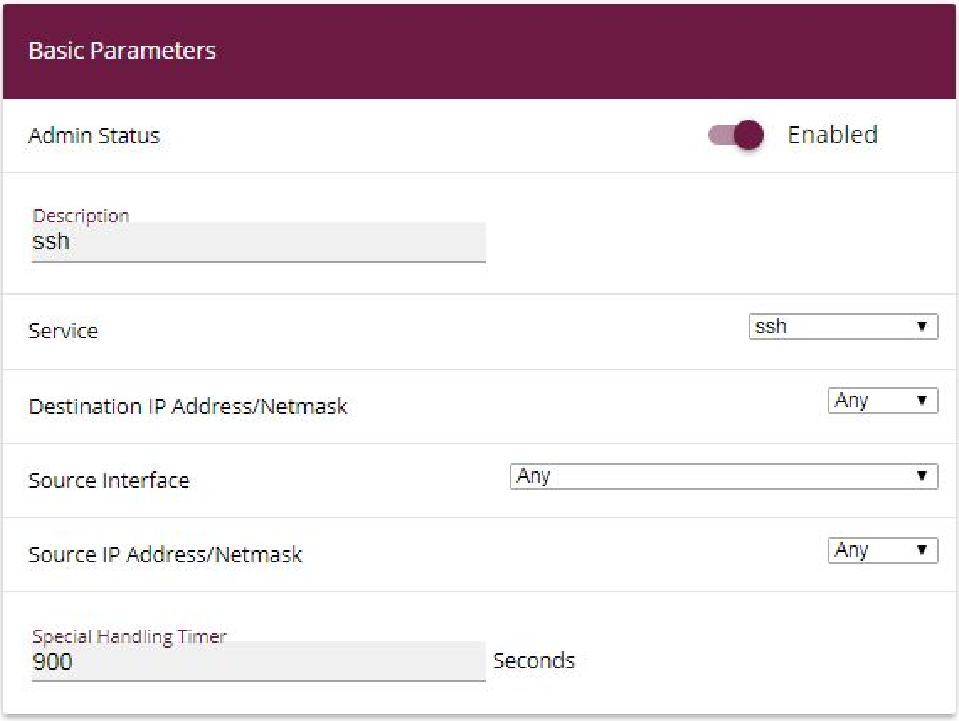
(1) Under **Description** enter a name for the entry, e.g. `https` ein.

(2) Under **Service** select `http (SSL)`.

(3) The **Special Handling Timer** should be set to `900` seconds.

(4) Leave the remaining settings unchanged and confirm them with **OK**.

(5) Click **New** again.



Basic Parameters

Admin Status: Enabled

Description: ssh

Service: ssh

Destination IP Address/Netmask: Any

Source Interface: Any

Source IP Address/Netmask: Any

Special Handling Timer: 900 Seconds

Fig. 78: **Network**->**Load Balancing**->**Special Session Handling**->**New**

(1) State a **Description** for the entry, e.g. `ssh`.

(2) Select **Service** `ssh`.

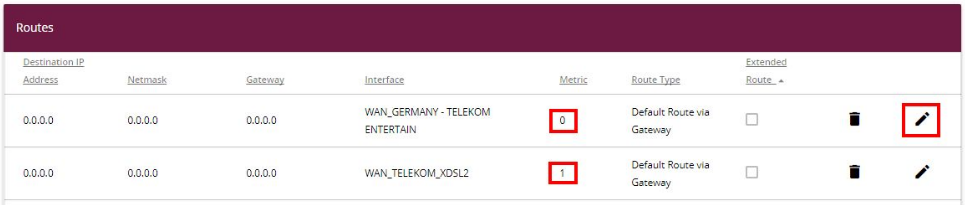
(3) The **Special Handling Timer** should be set to `900` seconds.

(4) Leave the remaining settings unchanged and confirm them with **OK**.

8.2.5 Adjusting the metric

As a load distribution group only becomes active when the default routers belonging to the WAN connections have the same metric, the WAN connection metric that was changed to `0` in an earlier step must now be reset back to metric `1` instead.

Go to the **Network**->**Routes**->**IPv4 Route Configuration** menu.

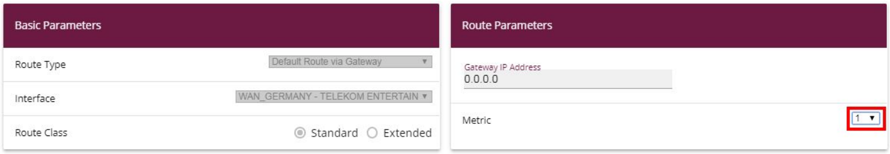


Routes

Destination IP Address	Netmask	Gateway	Interface	Metric	Route Type	Extended Route ▲		
0.0.0.0	0.0.0.0	0.0.0.0	WAN_GERMANY - TELEKOM ENTERTAIN	0	Default Route via Gateway	☐	🗑	✎
0.0.0.0	0.0.0.0	0.0.0.0	WAN_TELEKOM_XDSL2	1	Default Route via Gateway	☐	🗑	✎

Fig. 79: **Network**->**Routes**->**IPv4 Route Configuration**

(1) Click on the ✎ symbol to edit the entry.



Basic Parameters

Route Type: Default Route via Gateway ▾

Interface: WAN_GERMANY - TELEKOM ENTERTAIN ▾

Route Class: ● Standard ○ Extended

Route Parameters

Gateway IP Address: 0.0.0.0

Metric: 1 ▾

Fig. 80: **Network**->**Routes**->**IPv4 Route Configuration**->✎

(2) Under **Metric** select the priority of the route, which is *1* in our example.

(3) Confirm with **OK**.

The load distribution between both xDSL connections is now active.

8.3 Concluding notes

If IPSec tunnels are initiated from a specific interface active with the load distribution group, this must be specified in the **Advanced Settings** for the respective tunnel under the IPSec menu.

The identical WAN interface via which the request was made is again selected automatically in response for forwarding via NAT/PAT. No further configuration steps are required.

IPv6 data traffic is, for example, only routed using the first xDSL-WAN connection, but is also included in the load on the interface.

If both WAN connections support an IPv6 load distribution group, then it must be deactivated on one or the two. In IPv6 there is no NAT mechanism and no proprietary "prefix masking" is implemented. As the selection of the source IP is a matter for the network client behind the **be.IP** it is not otherwise possible to guarantee trouble-free function of services.

8.4 Overview of Configuration Steps

Setting up WAN connection via the internal modem

Field	Menu	Value
IPv6	**WAN**->**Internet + Dialup**->**PPPoE**->**Germany - Telekom Entertain** ->✎	*Enabled*
Metric	**Network**->**Routes**->**IPv4 Route Configuration**->✎	*0*

Setting up WAN connection via the external modem

Field	Menu	Value
Connection Type	**Assistants**->**Internet Access**->**Internet Connections**->**New**	*External xDSL Modem*
Description	**Assistants**->**Internet Access**->**Internet Connections**->**New**->**Next**	e.g. *Telekom_xDSL2*
Physical Ethernet Port	**Assistants**->**Internet Access**->**Internet Connections**->**New**->**Next**	e.g. *ETH5*
Type	**Assistants**->**Internet Access**->**Internet Connections**->**New**->**Next**	*Predefined*
Country	**Assistants**->**Internet Access**->**Internet Connections**->**New**->**Next**	*Germany*
Internet Service Provider	**Assistants**->**Internet Access**->**Internet Connections**->**New**->**Next**	e.g. *Telekom*
Connection ID	**Assistants**->**Internet Access**->**Internet Connections**->**New**->**Next**	e.g. *123456789012*
Access Number	**Assistants**->**Internet Access**->**Internet Connections**->**New**->**Next**	e.g. *123456789012*
Co-User Number	**Assistants**->**Internet Access**->**Internet Connections**->**New**->**Next**	*0001*
Password	**Assistants**->**Internet Access**->**Internet Connections**->**New**->**Next**	e. g. *test12345*
Always on	**Assistants**->**Internet Access**->**Internet Connections**->**New**->**Next**	*Enabled*
IPv6	**Assistants**->**Internet Access**->**Internet Connections**->**New**->**Next**	*Disabled*

Setting up WAN connection via the external modem

Field	Menu	Value
Default Behavior	**VoIP**->**Settings**->**Locations**	*Registration for Private Networks Only*
Description	**VoIP**->**Settings**->**Locations**->**New**	e.g. *WAN_xDSL*
Type	**VoIP**->**Settings**->**Locations**->**New**	*Interfaces*
Interfaces	**VoIP**->**Settings**->**Locations**->**New**	**Add** and *WAN_GERMANY - TELEKOM ENTERTAIN*
Location	**VoIP**->**Settings**->**SIP Provider**->**New**+**Advanced Settings**	*WAN_xDSL*
Description	**VoIP**->**Settings**->**Locations**->**New**	e.g. *Telekom_xDSL2*
Type	**VoIP**->**Settings**->**Locations**->**New**	*Interfaces*
Interfaces	**VoIP**->**Settings**->**Locations**->**New**	**Add** and *WAN_TELEKOM_XDSL2*

Setting up the load distribution

Field	Menu	Value
Group Description	**Network**->**Load Balancing**->**Load Balancing Groups**->**New**	e.g. *xDSL1 / xDSL2*
Distribution Policy	**Network**->**Load Balancing**->**Load Balancing Groups**->**New**	*Session-Round-Robin*
Interface	**Network**->**Load Balancing**->**Load Balancing Groups**->**New**->**Add**	*WAN_GERMANY - TELEKOM ENTERTAIN*
Distribution Ratio	**Network**->**Load Balancing**->**Load Balancing Groups**->**New**->**Add**	*50* %
Interface	**Network**->**Load Balancing**->**Load Balancing Groups**->**New**->**Add**	*WAN_TELEKOM_XDSL2*
Distribution Ratio	**Network**->**Load Balancing**->**Load Balancing Groups**->**New**->**Add**	*50* %
Description	**Network**->**Load Balancing**->**Special Session Handling**->**New**	e.g. *https*
Service	**Network**->**Load Balancing**->**Special Session Handling**->**New**	*http (SSL)*
Special Handling Timer	**Network**->**Load Balancing**->**Special Session Handling**->**New**	*900* seconds

Field	Menu	Value
Description	**Network**->**Load Balancing**->**Special Session Handling**->**New**	e.g. *ssh*
Service	**Network**->**Load Balancing**->**Special Session Handling**->**New**	*ssh*
Special Handling Timer	**Network**->**Load Balancing**->**Special Session Handling**->**New**	*900* seconds

Adjusting the metric

Field	Menu	Value
Metric	**Network**->**Routes**->**IPv4 Route Configuration**->✎	*1*

Chapter 9 Telephoning via a SIP provider using the be.IP plus

9.1 Introduction

The following describes how to set up a SIP provider in the **be.IP plus**.

Note

The pictured information is only provided as an example. Please use the data obtained from your SIP provider.

An overview of the SIP providers tested so far can be found on the internet at http://faq.bintec-elmeg.com/index.php/Konfiguration_SIP_Provider.

Certain presettings are of importance when using a domestic SIP provider in order, for example, to ensure that only the number is entered, as opposed to the entire area code and number, when making a local call.

Variant 1

In this example, the **be.IP plus** are connected directly to the Internet via your internal DSL modem.

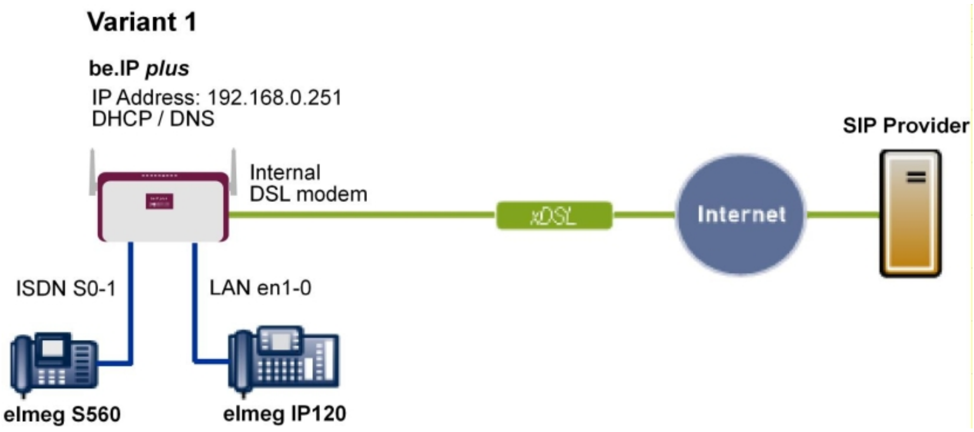


Fig. 81: Example scenario

Requirements

- Internet access via the integrated ADSL/ADSL2+ modem
- An **be.IP plus** as of system software version 10.1, Rev. 5, is used as a DHCP and DNS server in the network.
- **elmeg IP120** telephone as of firmware version 01.00.04
- **elmeg S560** telephone as of firmware version 1.400
- Connecting the **be.IP plus** to all terminals and connections as indicated in the circuit diagram

Variant 2

This example describes how to integrate an **be.IP plus** into an existing network with a gateway, e.g. **bintec RS353jw**.

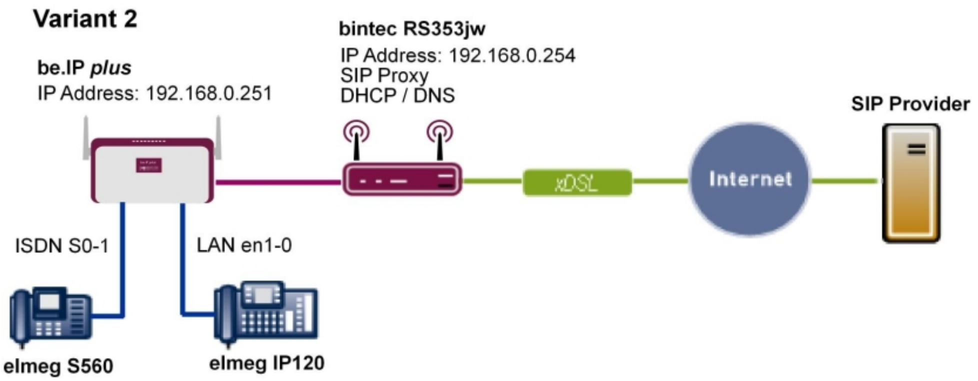


Fig. 82: Example scenario

Requirements

- An existing network with **bintec RS353jw** gateway, as of system software version 10.1, Rev. 4. The **bintec RS353jw** gateway is used as a DHCP and DNS server in the network.
- An **be.IP plus** as of system software version 10.1, Rev. 5
- **elmeg IP120** telephone as of firmware version 01.00.04
- **elmeg S560** telephone as of firmware version 1.400
- Connecting the **be.IP plus** to all terminals and connections as indicated in the circuit diagram

9.2 Basic Configuration

Note

Follow the **Initial Steps** and **Internet Access** Wizards for the general network configuration.

9.2.1 Variant 1: Network configuration with direct Internet connection

9.2.1.1 Configuration of be.IP plus

You must configure your **be.IP plus**as a DHCP server.

Note

In order to configure the **be.IP plus** as a DHCP server, please read the chapter on Variant 3 of the "Connecting **elmeg** telephones" telephony workshop.

9.2.2 Variant 2: Network configuration with gateway

9.2.2.1 Configuration of the gateway (bintec RS353jw)

You must change the VoIP settings of the gateway. The configuration is done using the gateway GUI. A DHCP server must also be set up.

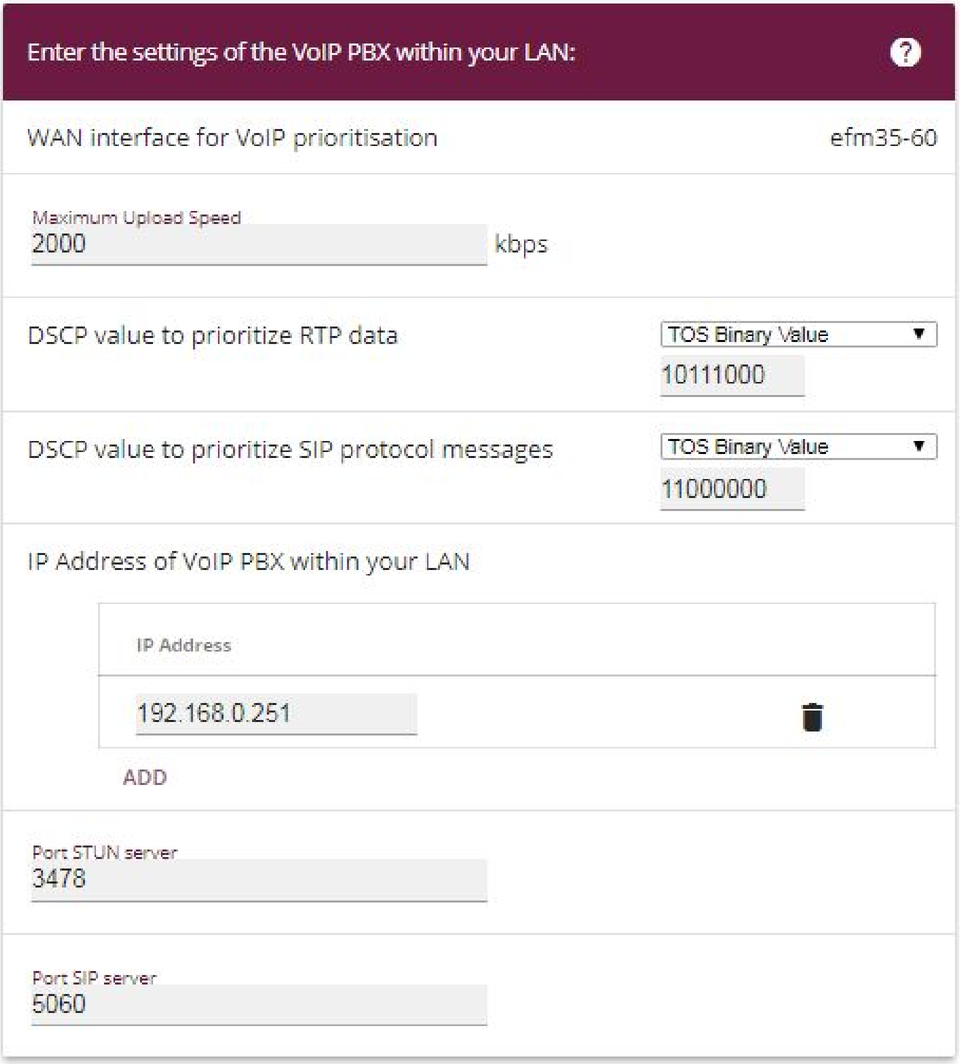
Note

In order to configure the DHCP server, please read the chapter on Variants 1 and 2 of the "Connecting **elmeg** telephones" telephony workshop.

(1) Go to **Assistants**->**VoIP PBX in LAN**->**New**.

(2) Select the **WAN interface for VoIP prioritisation** to be used by the VoIP PBX to access the internet in the LAN, e.g. *Internet-PPPoE*.

(3) Click Next.



Enter the settings of the VoIP PBX within your LAN:

WAN interface for VoIP prioritisation efm35-60

Maximum Upload Speed 2000 kbps

DSCP value to prioritize RTP data TOS Binary Value 10111000

DSCP value to prioritize SIP protocol messages TOS Binary Value 11000000

IP Address of VoIP PBX within your LAN

IP Address
192.168.0.251

Port STUN server 3478

Port SIP server 5060

Fig. 83: **Assistants**->**VoIP PBX in LAN**->**New**

Proceed as follows to make the SIP settings:

(1) Enter the **Maximum Upload Speed** for you internet connection, here e.g. `2000` kbps.

(2) The parameters **DSCP value to prioritize RTP data** and **DSCP value to prioritize SIP protocol messages** are to be found by the manufacturer of the PBX or the VoIP telephone.

(3) Enter the **IP Address of VoIP PBX within your LAN** , e.g. `192.168.0.251`.

(4) Leave the remaining settings unchanged and confirm them with **OK**.

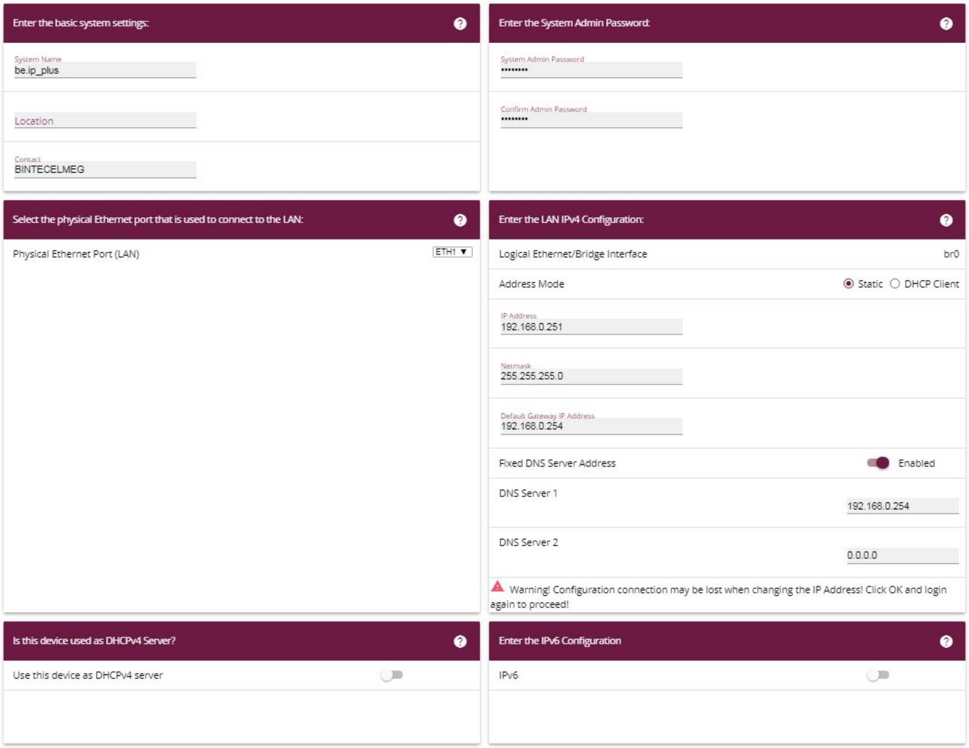
Note

Ensure you make the above settings in any case as otherwise it may lead to problems when making calls via a SIP provider.

9.2.2.2 Configuration of be.IP plus

You must configure the gateway and the DNS server settings of the **be.IP plus**. The configuration is done using the **be.IP plus** GUI.

(1) Go to **Assistants**->**First steps**->**Basic Setup**.



Enter the basic system settings:

System Name: be.ip_plus

Location

Contact: BINTECELMEG

Enter the System Admin Password:

System Admin Password: ••••••••

Confirm Admin Password: ••••••••

Select the physical Ethernet port that is used to connect to the LAN:

Physical Ethernet Port (LAN): ETH1 ▼

Enter the LAN IPv4 Configuration:

Logical Ethernet/Bridge Interface: br0

Address Mode: ● Static ○ DHCP Client

IP Address: 192.168.0.251

Netmask: 255.255.255.0

Default Gateway IP Address: 192.168.0.254

Fixed DNS Server Address: Enabled

DNS Server 1: 192.168.0.254

DNS Server 2: 0.0.0.0

Warning! Configuration connection may be lost when changing the IP Address! Click OK and login again to proceed!

Is this device used as DHCPv4 Server?

Use this device as DHCPv4 server

Enter the IPv6 Configuration

IPv6

Fig. 84: **Assistants**->**First steps**->**Basic Setup**

Proceed as follows to make the gateway and DNS settings:

(1) Enter the IP address of your gateway that you use to provide Internet access under **Default Gateway IP Address**, e.g. `192.168.0.254`.

(2) Enable **Fixed DNS Server Address**.

(3) Enter the IP address of the name server for Internet address name resolution under

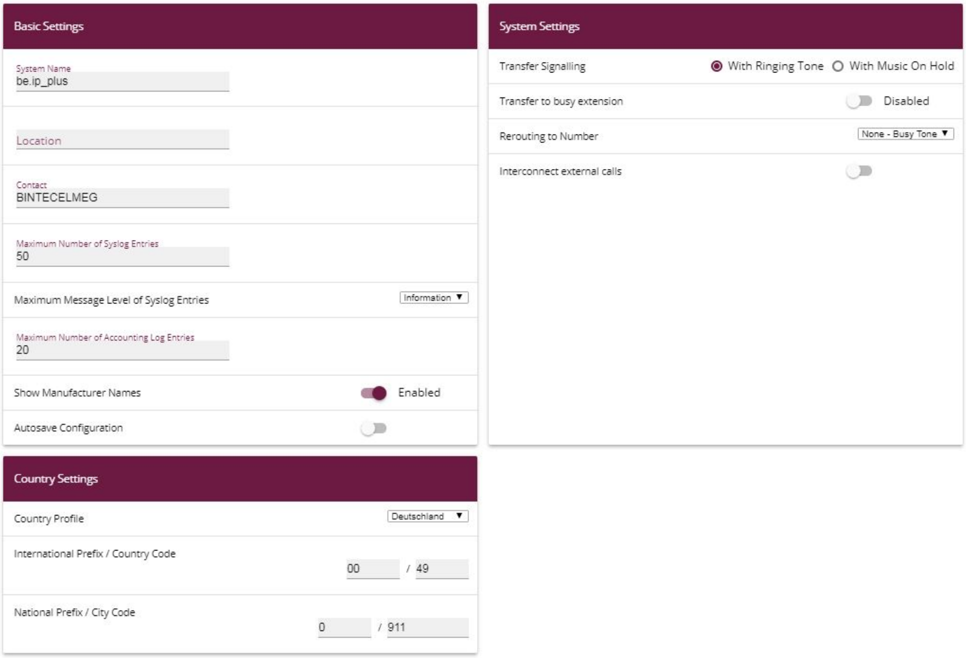
DNS Server1; here it is `192.168.0.254`.

(4) Leave the remaining settings unchanged and confirm them with **OK**.

9.2.3 Variants 1 + 2: Configuration of country settings in the be.IP plus

By setting the parameters **International Prefix / Country Code**/**Country Code** and **National Prefix / City Code**/**Area Code**, international and national numbers are automatically generated without the need for any additional entries when dialling them via the SIP provider. Such configuration also allows the correct distribution of calls for incoming call via the SIP provider.

(1) Go to **System Management**->**Global Settings**->**System**.



Basic Settings

System Name: be.ip_plus

Location

Contact: BINTECELMEG

Maximum Number of Syslog Entries: 50

Maximum Message Level of Syslog Entries: Information ▼

Maximum Number of Accounting Log Entries: 20

Show Manufacturer Names: Enabled

Autosave Configuration

System Settings

Transfer Signalling: ● With Ringing Tone ○ With Music On Hold

Transfer to busy extension: Disabled

Rerouting to Number: None - Busy Tone ▼

Interconnect external calls

Country Settings

Country Profile: Deutschland ▼

International Prefix / Country Code: 00 / 49

National Prefix / City Code: 0 / 911

Fig. 85: **System Management**->**Global Settings**->**System**

Proceed as follows to configure the codes:

(1) Enter the country code under **International Prefix / Country Code**, e.g. `49` for Germany. If this is not entered, then the full number along with the country code must always be dialled when using SIP providers.

(2) Enter the area code for the location where your system is installed under **National Prefix / City Code**, e.g. `911` for Nuremberg. If this is not entered, then the number

along with the national prefix/area code must be dialled for local calls when using SIP providers.

(3) Leave the remaining settings unchanged and confirm them with **OK**.

9.3 Variants 1 + 2: Configuration of SIP provider in the be.IP plus

A VoIP connection can be configured as an individual number or extension connection. These names refer to ISDN point-to-multipoint and point-to-point connections.

For an individual number connection, you receive one or more numbers from the SIP provider.

For an extension connection, you receive a main number with several extension numbers (extension number range) from the SIP provider. Example: Main number = 1234; Extension numbers: 1, 2, ...; Numbers: 1234 - 1, 1234 - 2, ...

9.3.1 SIP provider (individual number)

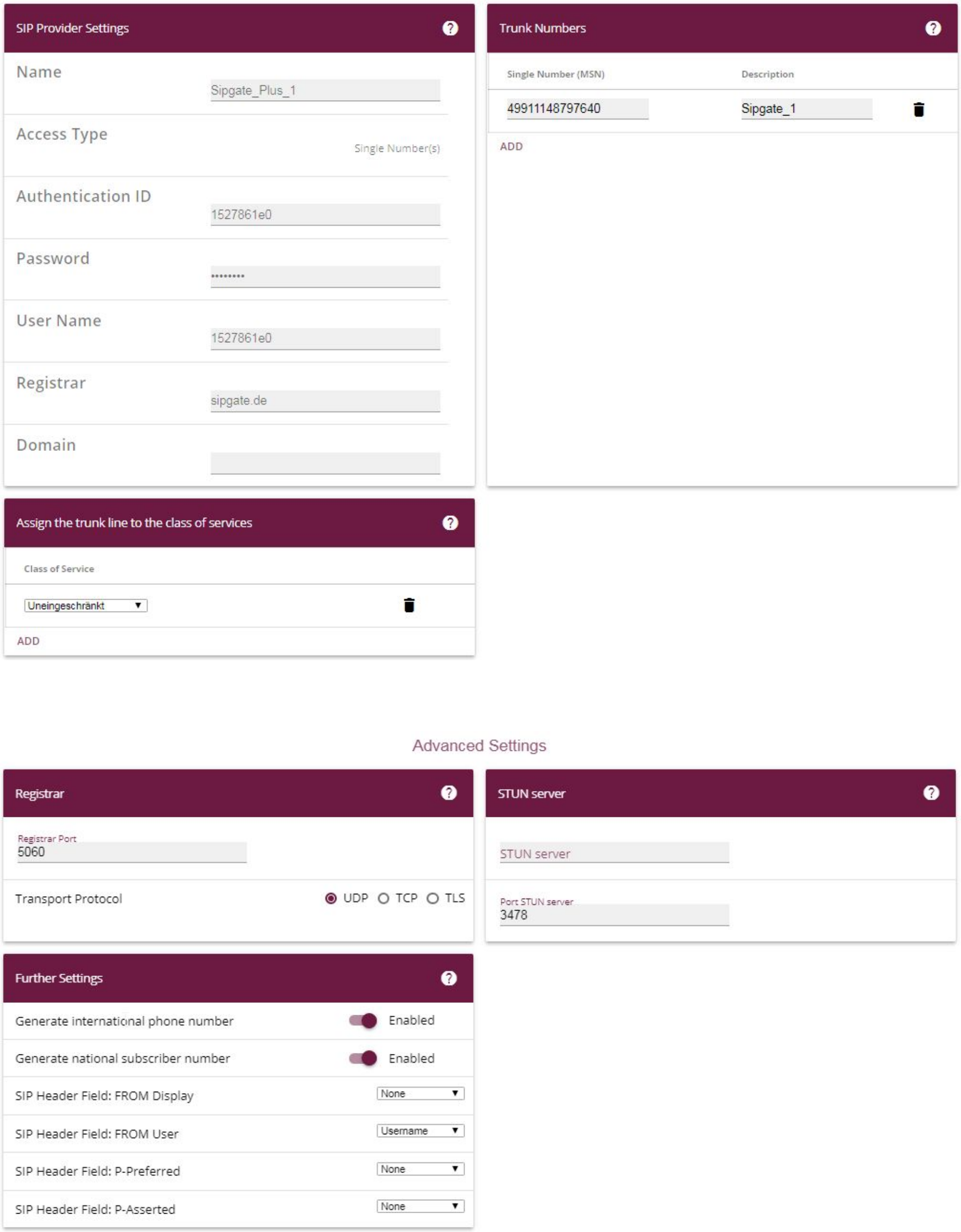
The following describes how to set up a SIP provider when using an individual number connection.

(1) Go to **Assistants**->**Telephony**->**Trunks**->**New**.

(2) Select *SIP Single Number* under **Connection Type**.

(3) Under **Type** select *User-defined*.

(4) Click **Next**.



SIP Provider Settings

Name: Sipgate_Plus_1

Access Type: Single Number(s)

Authentication ID: 1527861e0

Password: ••••••••

User Name: 1527861e0

Registrar: sipgate.de

Domain:

Trunk Numbers

Single Number (MSN)	Description
49911148797640	Sipgate_1

ADD

Assign the trunk line to the class of services

Class of Service
Uneingeschränkt

ADD

Advanced Settings

Registrar

Registrar Port: 5060

Transport Protocol: ● UDP ○ TCP ○ TLS

STUN server

STUN server

Port STUN server: 3478

Further Settings

Generate international phone number: Enabled

Generate national subscriber number: Enabled

SIP Header Field: FROM Display: None

SIP Header Field: FROM User: Username

SIP Header Field: P-Preferred: None

SIP Header Field: P-Asserted: None

Fig. 87: **Assistants**->**Telephony**->**Trunks**->**New**-> **<SIP Provider>**

Proceed as follows to save the login information of the SIP provider:

Note

For certain SIP providers, a **STUN server** must be configured for gateways with established VoIP PBX in LAN assistant.

(1) Enter a name for the SIP provider under **Name**, e.g. `Sipgate_Plus_1`.

(2) Enter your provider's **Authentication ID** (SIP-ID), e. g. `1527861e0`.

(3) Enter the **Password** you received from your VoIP provider.

(4) For **Login Name**, enter the name that your VoIP provider has sent you, e. g. `1527861e0`. This is the SIP-ID for the providers Sipgate, 1&1, QSC and Toplink.

(5) Enter an IP address or a domain name as the SIP **Registrar**.

- For Sipgate Basic/Plus: `sipgate.de`
- For 1&1: `sip.1und1.de`
- For QSC-IPfonie basic: `sip.qsc.de`
- When connecting the Deutsche Telekom Call & Surf Comfort IP connection: `tel.t-online.de`
- For Toplink: `toplink-voice.de`

(6) Use **Add** under **Single Number (MSN)** to create a new entry.
Enter the number that your VoIP provider has given you under **Single Number (MSN)**, e.g. `4911148797640`.
Enter a name for the connection under **Displayed Name**, e.g. `Sipgate_1`. This is displayed on the system telephone for incoming calls.

Note

Several numbers can be configured here for the providers QSC-IPfonie basic and Toplink.

For the providers Sipgate Basic/Plus, 1&1 and Deutsche Telekom, an additional SIP connection with separate SIP account data must be created for each additional number provided by the SIP provider. In order to enable outgoing calls to be made via other numbers or SIP connections, additional authorisation classes should be configured under **Numbering**->**User Settings**->**Class of Services**.

(7) The **Class of Service** leave behind `Default CoS`.

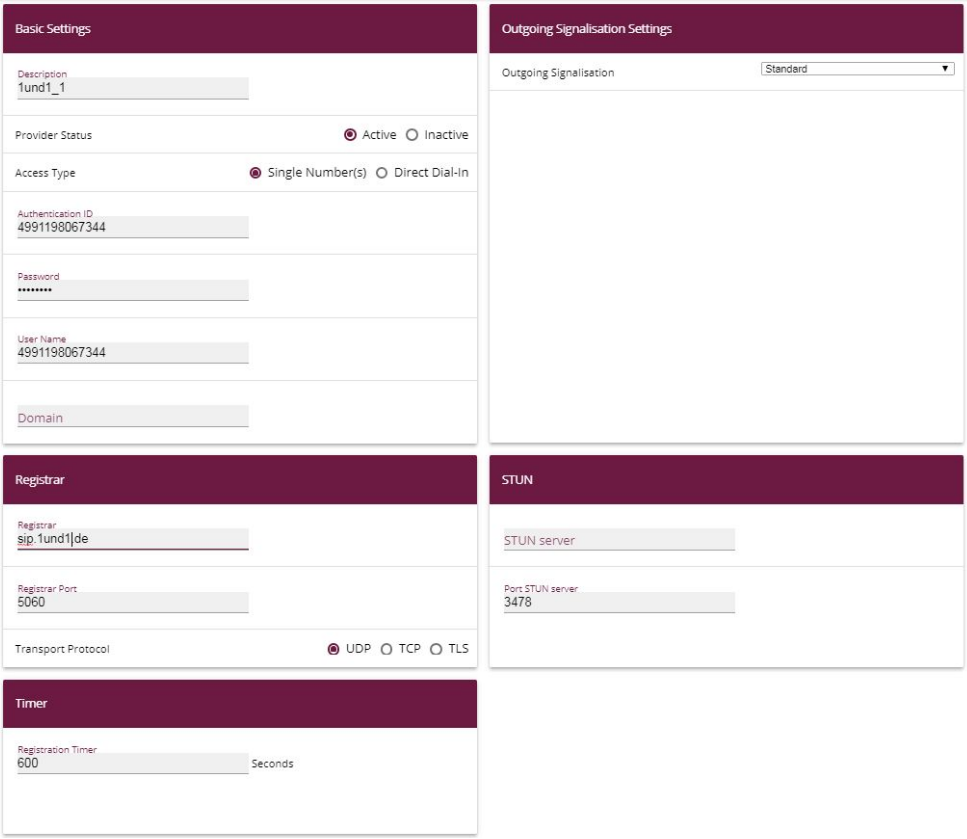
(8) Enable **Generate international phone number** and **Generate national subscriber number**.

(9) Leave the remaining settings unchanged and confirm them with **OK**.
After the system is successfully registered with the SIP provider, the status display of the respective SIP connection changes to ✓.

9.3.1.1 1&1

For the SIP provider 1&1, the prefix `49` must be replaced by `0` for the incoming number. By doing this, this ensures the numbers and names from the system telephone book are correctly displayed for any incoming calls.

(1) Go to **VoIP**->**Settings**->**SIP Provider**-> **<1und1>** ->✎.



Basic Settings

Description: 1und1_1

Provider Status: ● Active ○ Inactive

Access Type: ● Single Number(s) ○ Direct Dial-In

Authentication ID: 4991198067344

Password: ••••••••

User Name: 4991198067344

Domain

Outgoing Signalisation Settings

Outgoing Signalisation: Standard

Registrar

Registrar: sip.1und1.de

Registrar Port: 5060

Transport Protocol: ● UDP ○ TCP ○ TLS

STUN

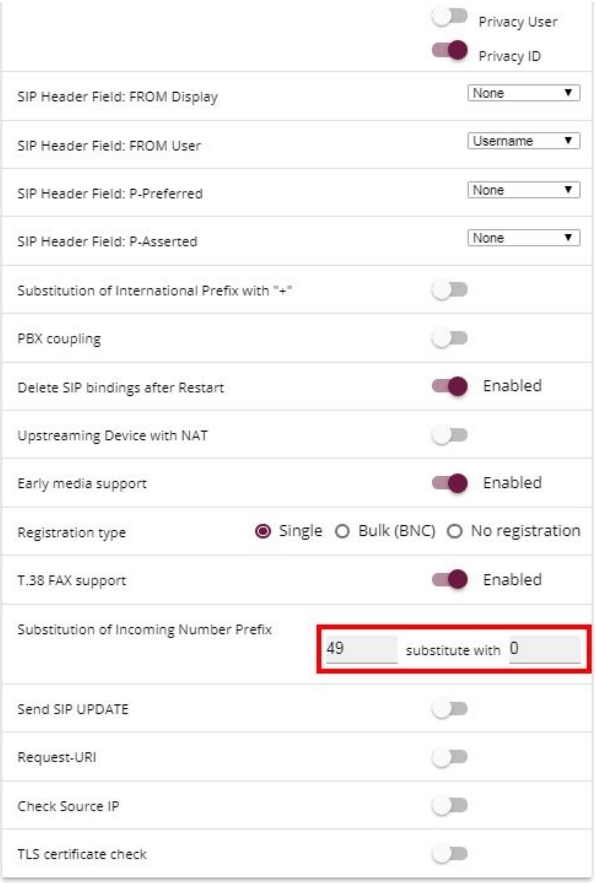
STUN server

Port STUN server: 3478

Timer

Registration Timer: 600 Seconds

Fig. 88: **VoIP**->**Settings**->**SIP Provider**-> **<1und1>** ->✎



Privacy User

Privacy ID

SIP Header Field: FROM Display	None
SIP Header Field: FROM User	Username
SIP Header Field: P-Preferred	None
SIP Header Field: P-Asserted	None
Substitution of International Prefix with "+"	
PBX coupling	
Delete SIP bindings after Restart	Enabled
Upstreaming Device with NAT	
Early media support	Enabled
Registration type	● Single ○ Bulk (BNC) ○ No registration
T.38 FAX support	Enabled
Substitution of Incoming Number Prefix	49 substitute with 0
Send SIP UPDATE	
Request-URI	
Check Source IP	
TLS certificate check	

Fig. 89: **VoIP**->**Settings**->**SIP Provider**-> **<1und1>** -> ✎ ->**Advanced Settings**

Proceed as follows:

(1) Enter *49* under **Substitution of Incoming Number Prefix**.

(2) Enter *0* under **substitute with**.

(3) Leave the remaining settings unchanged and confirm them with **OK**.

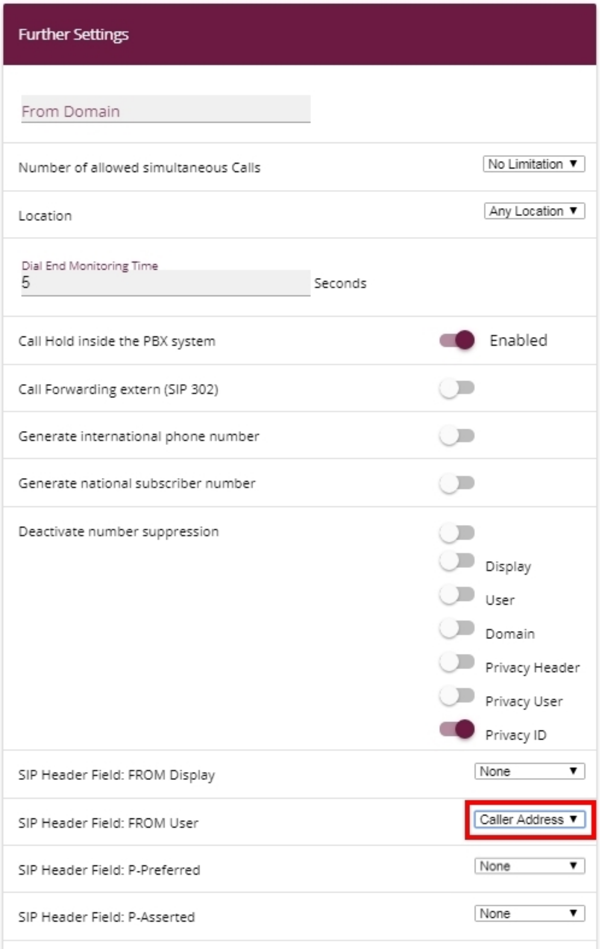
Note

If the PBX Wizard is used again for this connection, then all settings are reset in the **VoIP** -> **Settings** -> **SIP Provider** menu.

9.3.1.2 QSC-IPfonie basic

The option `Caller Address` must be enabled for the **SIP Header Field: FROM User** for the SIP provider QSC-IPfonie basic. By doing so, this then makes it possible to use different numbers for outgoing calls.

(1) Go to **VoIP**->**Settings**->**SIP Provider**-> **<qsc_ipfonie_ basic>** -> ✎ ->**Advanced Settings**.



Further Settings

From Domain

Number of allowed simultaneous Calls: No Limitation

Location: Any Location

Dial End Monitoring Time: 5 Seconds

Call Hold inside the PBX system: Enabled

Call Forwarding extern (SIP 302)

Generate international phone number

Generate national subscriber number

Deactivate number suppression

Display

User

Domain

Privacy Header

Privacy User

Privacy ID

SIP Header Field: FROM Display: None

SIP Header Field: FROM User: Caller Address

SIP Header Field: P-Preferred: None

SIP Header Field: P-Asserted: None

Fig. 90: **VoIP**->**Settings**->**SIP Provider**-> **<qsc_ipfonie_ basic>** -> ✎ ->**Advanced Settings**

Proceed as follows to extend the SIP header:

(1) Enable the option `Caller Address` under **SIP Header Field: FROM User**.

(2) Leave the remaining settings unchanged and confirm them with **OK**.

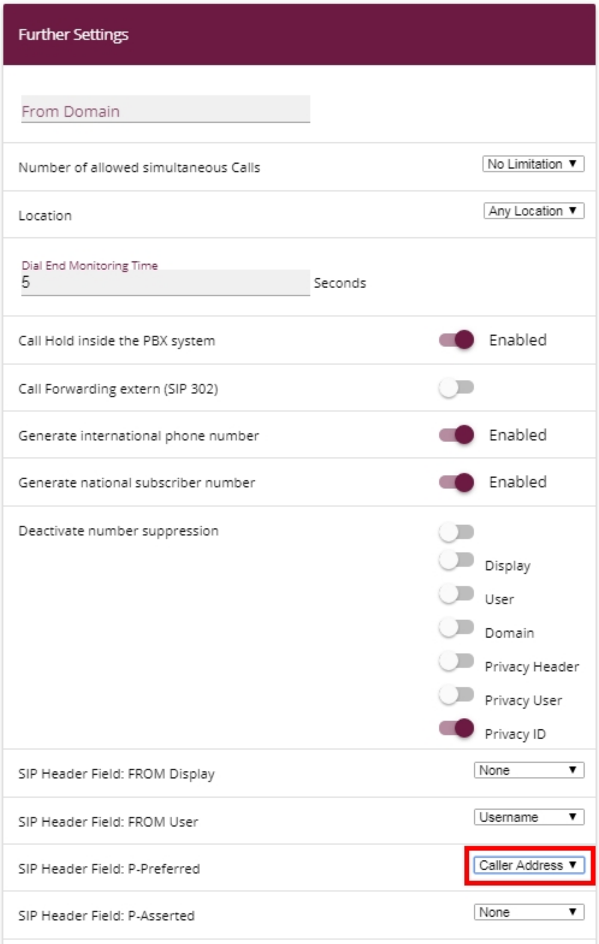
Note

If the PBX Wizard is used again for this connection, then all settings are reset in the **VoIP**->**Settings**->**SIP Provider** menu.

9.3.1.3 Toplink

The option *Caller Address* must be enabled for the **SIP Header Field: P-Preferred** for the SIP provider Toplink.

(1) Go to **VoIP**->**Settings**->**SIP Provider**-> **<toplink>**->✎ ->**Advanced Settings**.



Further Settings

From Domain

Number of allowed simultaneous Calls: No Limitation ▼

Location: Any Location ▼

Dial End Monitoring Time: 5 Seconds

Call Hold inside the PBX system: ● Enabled

Call Forwarding extern (SIP 302): ○

Generate international phone number: ● Enabled

Generate national subscriber number: ● Enabled

Deactivate number suppression: ○
- ○ Display
- ○ User
- ○ Domain
- ○ Privacy Header
- ○ Privacy User
- ● Privacy ID

SIP Header Field: FROM Display: None ▼

SIP Header Field: FROM User: Username ▼

SIP Header Field: P-Preferred: Caller Address ▼

SIP Header Field: P-Asserted: None ▼

Fig. 91: **VoIP**->**Settings**->**SIP Provider**-> **<toplink>**-> ✎ ->**Advanced Settings**

Proceed as follows to extend the SIP header:

(1) Enable the option `Caller Address` under **SIP Header Field: P-Preferred**.

(2) Leave the remaining settings unchanged and confirm them with **OK**.

Note

If the PBX Wizard is used again for this connection, then all settings are reset in the **VoIP**->**Settings**->**SIP Provider** menu.

9.3.2 SIP provider (extension)

Prerequisite

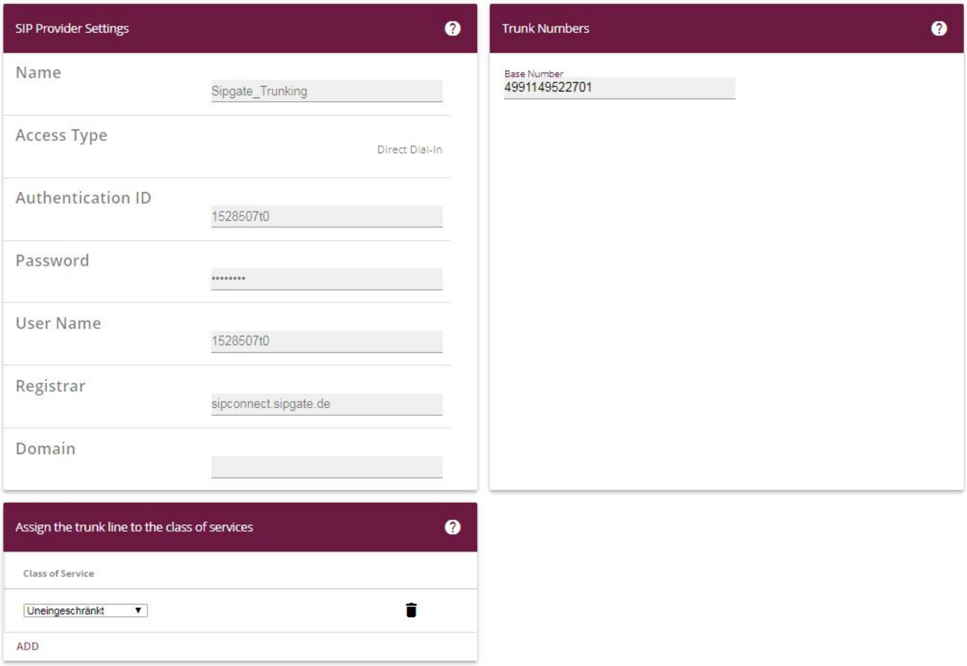
The following describes how to set up a SIP provider when using an extension connection.

(1) Go to **Assistants**->**Telephony**->**Trunks**->**New**.

(2) Select *SIP - Direct dial-in* under **Connection Type**.

(3) Under **Type** select *User-defined*.

(4) Click **Next**.



SIP Provider Settings

Name: Sipgate_Trunking

Access Type: Direct Dial-In

Authentication ID: 1528507t0

Password: ••••••••

User Name: 1528507t0

Registrar: sipconnect.sipgate.de

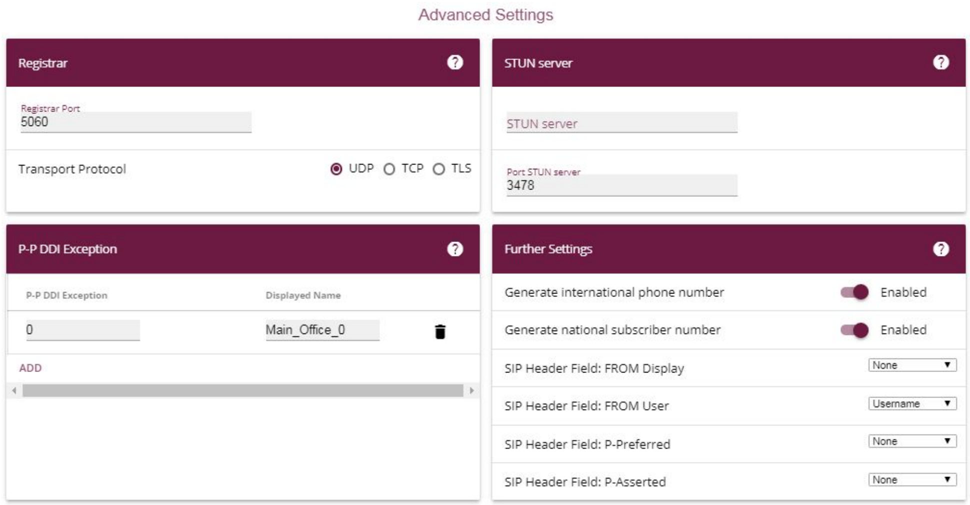
Domain:

Trunk Numbers

Base Number: 4991149522701

Assign the trunk line to the class of services

Class of Service: Uneingeschränkt



Advanced Settings

Registrar

Registrar Port: 5060

Transport Protocol: ● UDP ○ TCP ○ TLS

STUN server

STUN server

Port STUN server: 3478

P-P DDI Exception

P-P DDI Exception	Displayed Name
0	Main_Office_0

ADD

Further Settings

Generate international phone number	Enabled
Generate national subscriber number	Enabled
SIP Header Field: FROM Display	None
SIP Header Field: FROM User	Username
SIP Header Field: P-Preferred	None
SIP Header Field: P-Asserted	None

Fig. 93: **Assistants**->**Telephony**->**Trunks**->**New**-> **<SIP Provider (Extension)>**

Proceed as follows to save the login information of the SIP provider:

> **Note**
>
> For certain SIP providers, a **STUN server** must be configured for gateways with established VoIP PBX in LAN assistant.

(1) Enter a name for the SIP provider under **Name**, e.g. `Sipgate_Trunking`.

(2) Enter your provider's **Authentication ID** (SIP-ID), e. g. `1528507t0`.

(3) Enter the **Password** you received from your VoIP provider.

(4) For **Login Name**, enter the name that your VoIP provider has sent you, e. g. `1528507t0`. This is the SIP-ID for the providers Sipgate and QSC.

(5) Enter an IP address or a domain name as the SIP **Registrar**.

- For Sipgate Trunking: `sipconnect.sipgate.de`
- Für QSC-IPfonie extended: `sip.qsc.de`

(6) Enter a **Base Number**, e.g. `4911149522701`.

(7) Use **Add** under **Authorisation Class** to create a new entry and select an authorisation class, e.g. `Default CoS`.

(8) Use **Add** under **Class of Service** to create a new entry.
Enter the extension number that your VoIP provider has given you under **Direct Dial Exception (P-P)**, e. g. `0`.
Enter a name for the connection under **Displayed Name**, e.g. `Zentrale-0`. This is

displayed on the system telephone for incoming calls.

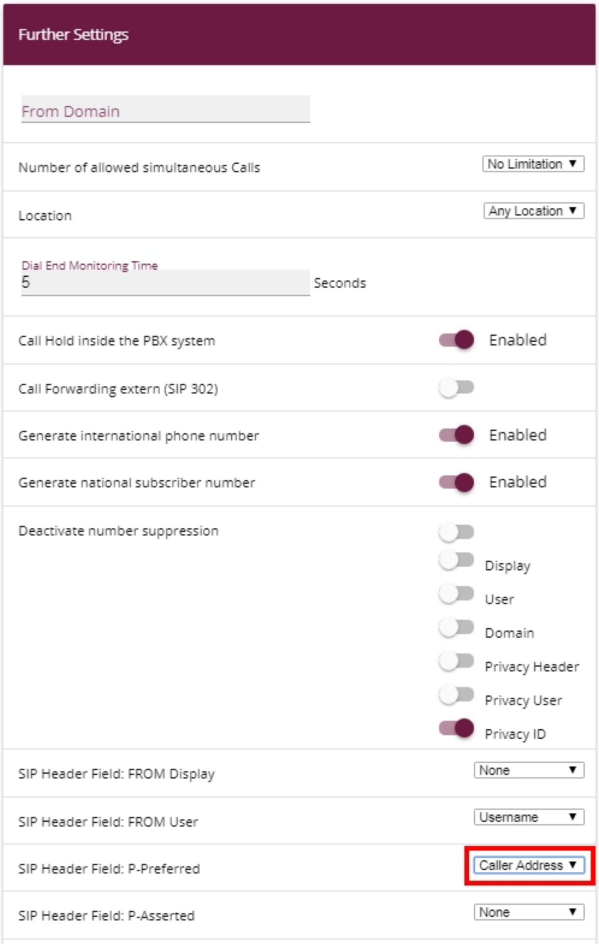
(9) Enable **Generate international phone number** and **Generate national subscriber number**.

(10) Leave the remaining settings unchanged and confirm them with **OK**.
After the system is successfully registered with the SIP provider, the status display of the respective SIP connection changes to ✔.

9.3.2.1 Sipgate Trunking

The option `Caller Address` under **SIP Header Field: P-Preferred** must be enabled for the SIP provider Sipgate Trunking.

(1) Go to **VoIP**->**Settings**->**SIP Provider**-> **<sipgate_trunking>** ✎ ->**Advanced Settings**.



Further Settings

From Domain

Number of allowed simultaneous Calls: No Limitation ▼

Location: Any Location ▼

Dial End Monitoring Time: 5 Seconds

Call Hold inside the PBX system: ● Enabled

Call Forwarding extern (SIP 302): ○

Generate international phone number: ● Enabled

Generate national subscriber number: ● Enabled

Deactivate number suppression: ○
- ○ Display
- ○ User
- ○ Domain
- ○ Privacy Header
- ○ Privacy User
- ● Privacy ID

SIP Header Field: FROM Display: None ▼

SIP Header Field: FROM User: Username ▼

SIP Header Field: P-Preferred: Caller Address ▼

SIP Header Field: P-Asserted: None ▼

Fig. 94: **VoIP**->**Settings**->**SIP Provider**-> **<sipgate_trunking>** ✎ ->**Advanced Settings**

Proceed as follows to extend the SIP header:

(1) Enable the option `Caller Address` under **SIP Header Field: P-Preferred**.

(2) Leave the remaining settings unchanged and confirm them with **OK**.

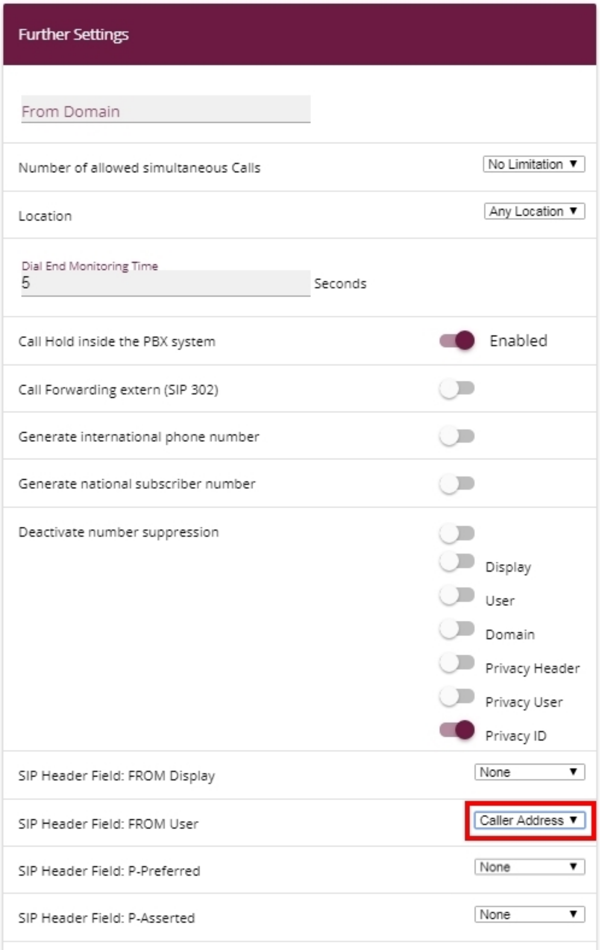
Note

If the PBX Wizard is used again for this connection, then all settings are reset in the **VoIP**->**Settings**->**SIP Provider** menu.

9.3.2.2 QSC-IPfonie extended

The option `Caller Address` must be enabled for the **SIP Header Field: FROM User** for the SIP provider QSC-IPfonie extended.

(1) Go to **VoIP**->**Settings**->**SIP Provider**-> **<qsc_ipfonie_extended>** ✎ ->**Advanced Settings**.



Further Settings

From Domain

Number of allowed simultaneous Calls: No Limitation ▼

Location: Any Location ▼

Dial End Monitoring Time: 5 Seconds

Call Hold inside the PBX system: ● Enabled

Call Forwarding extern (SIP 302): ○

Generate international phone number: ○

Generate national subscriber number: ○

Deactivate number suppression: ○

○ Display

○ User

○ Domain

○ Privacy Header

○ Privacy User

● Privacy ID

SIP Header Field: FROM Display: None ▼

SIP Header Field: FROM User: Caller Address ▼

SIP Header Field: P-Preferred: None ▼

SIP Header Field: P-Asserted: None ▼

Fig. 95: **VoIP**->**Settings**->**SIP Provider**-> **<qsc_ipfonie_extended>** ✎ ->**Advanced Settings**

Proceed as follows to extend the SIP header:

(1) Enable the option `Caller Address` under **SIP Header Field: FROM User**.

(2) Leave the remaining settings unchanged and confirm them with **OK**.

Note

If the PBX Wizard is used again for this connection, then all settings are reset in the **VoIP**->**Settings**->**SIP Provider** menu.

9.4 Variants 1 + 2: Configuration of authorisation class (optional)

A suitable authorisation class must be assigned to the user for outgoing calls via a SIP provider.

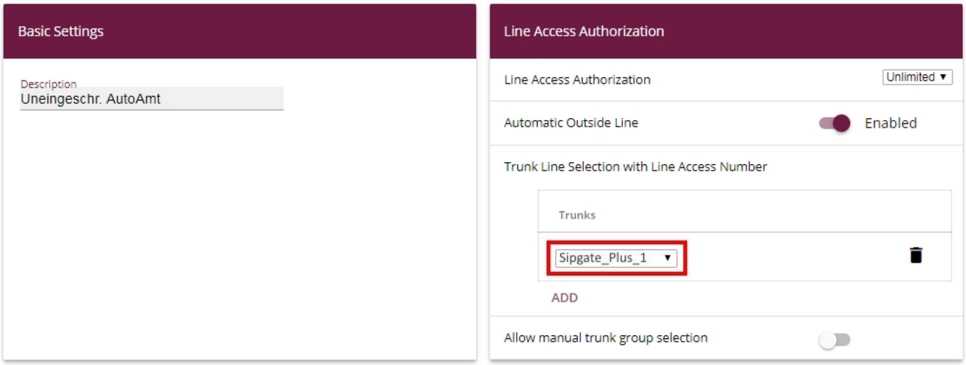
Note

Create a user under **Numbering**->**User Settings**->**Users**.

You can use the same authorisation class for the user as is used for the configuration of the SIP provider, e.g. `Unlimited`.

In all other cases, the authorisation class assigned to the user must be amended as follows:

(1) Go to **Numbering**->**User Settings**->**Class of Services**-> **<User Authorisation Class>** ✎ ->**Basic Settings**.



Basic Settings

Description: Uneingeschr. AutoAmt

Line Access Authorization

Line Access Authorization: Unlimited

Automatic Outside Line: Enabled

Trunk Line Selection with Line Access Number

Trunks: Sipgate_Plus_1

Allow manual trunk group selection

Fig. 96: **Numbering**->**User Settings**->**Class of Services**-> **<User Authorisation Class>** ✎ ->**Basic Settings**

Proceed as follows to amend the authorisation class:

(1) Use **Add** under **Trunk Line Selection with Line Access Number** to create a new entry and select your VoIP connection, e.g. `Sipgate_Plus_1`.

(2) Confirm with **Apply**.

9.5 Variants 1 + 2: Configuration of numbers in the be.IP plus

9.5.1 Assignment of incoming calls

The following part stipulates which internal subscribers or teams can be reached via the external number of the SIP provider.

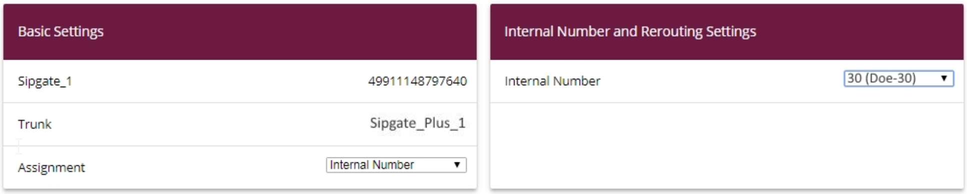
Note

A user must already have been created for the following step.

Create a user under **Numbering**->**User Settings**->**Users**. Assign an appropriate authorisation class to the user (see *Variants 1 + 2: Configuration of authorisation class (optional)* on page 105).

Assign a telephone to the user in the **Terminals** menu.

(1) Go to **Numbering**->**Call Distribution**->**Incoming Distribution**->**<49911148797640>** ✎.



Basic Settings

Sipgate_1	49911148797640
Trunk	Sipgate_Plus_1
Assignment	Internal Number

Internal Number and Rerouting Settings

Internal Number	30 (Doe-30)

Fig. 97: **Numbering**->**Call Distribution**->**Incoming Distribution**->**<49911148797640>** ✎

Proceed as follows to assign the external number to an internal number:

(1) Select `Internal Number` under **Assignment**.

(2) Select the internal number of the corresponding user under **Internal Number**, e.g. `30 (Doe-30)`.

(3) Confirm with **OK**.

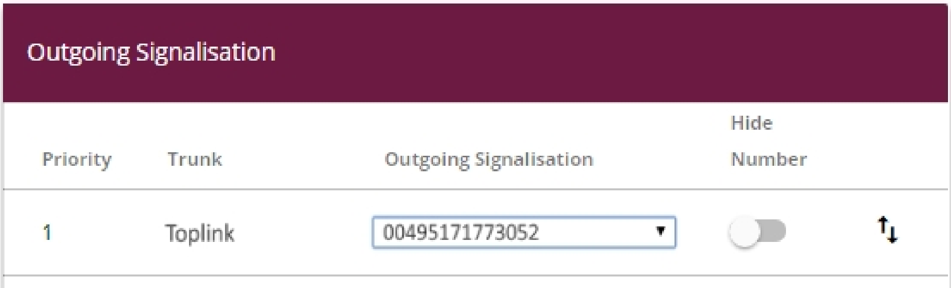
(4) Repeat the procedure for all other SIP provider numbers.

9.5.2 Configuring of outgoing calls

9.5.2.1 SIP provider (individual number) QSC-IPfonie basic and Toplink

If several numbers are configured for a SIP provider, then the number which is sent with outgoing calls can be set for the participants.

(1) Go to **Numbering**->**User Settings**->**Users**-> **<Doe-30>** ✎ ->**Outgoing Signalisation**-> **<30>** ✎.



Outgoing Signalisation

Priority	Trunk	Outgoing Signalisation	Hide Number	
1	Toplink	00495171773052 ▾	○	↑↓

Fig. 98: **Numbering**->**User Settings**->**Users**-> **<Doe-30>** ✎ ->**Outgoing Signalisation**-> **<30>** ✎.

Proceed as follows to assign an outgoing number to an internal number:

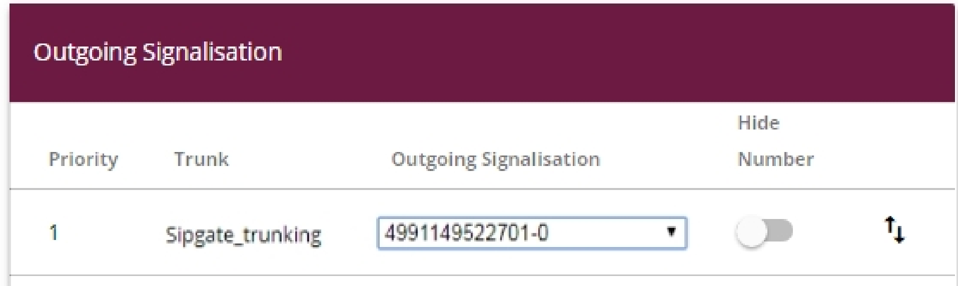
(1) Select a number, e.g. `00495171773052`, under SIP Provider Name, e.g. **Toplink**.

(2) Confirm with **Apply**.

9.5.2.2 SIP Provider (Extension) Sipgate Trunking and QSC-IPfonie extended

For outgoing calls, the main number along with the user's extension number are sent by default. This is in line with the setting *Standard, Own DDI Signals*. However, outgoing calls by the creating subscriber can also be sent using other configured numbers in the extension number range.

(1) Go to **Numbering**->**User Settings**->**Users**-> **<Doe-30>** ✎ ->**Outgoing Signalisation**-> **<30>** ✎.



Outgoing Signalisation

Priority	Trunk	Outgoing Signalisation	Hide Number	
1	Sipgate_trunking	4991149522701-0 ▾	○	⇅

Fig. 99: **Numbering**->**User Settings**->**Users**-> **<Doe-30>** ✎ ->**Outgoing Signalisation**-> **<30>** ✎.

Proceed as follows to select the outgoing number:

(1) Select a configured number, e.g. `004991149522701-0`, under SIP Provider Name, e.g. **Sipgate_trunking**, which is then transmitted to the other subscriber.
If you select `Standard, Own DDI Signals`, the main number is transmitted along with the separate extension number.

(2) Confirm with **Apply**.

9.6 Overview of Configuration Steps

Variant 2: Configuration of the gateway (e.g. bintec RS353jw)

Field	Menu	Value
WAN interface for VoIP priorisation	**VoIP** ->**VoIP PBX in LAN** ->**New**	`Internet-PPPoE`
Maximum Upload Speed	**VoIP** ->**VoIP PBX im LAN** ->**Neu** ->**Next**	e.g. `2000` kbps
IP Address of VoIP PBX within your LAN		e.g. `192.168.0.251`
Port SIP server	**VoIP** ->**VoIP PBX im LAN** ->**Neu** ->**Next**	`5060`

Variant 2: Configuration of be.IP plus

Field	Menu	Value
Default Gateway IP Address	**Assistants**+**First steps**+**Basic Setup**	e. g. `192.168.0.254`
Fixed DNS Server Address	**Assistants**+**First steps**+**Basic Setup**	`Enabled`
DNS Server 1	**Assistants**+**First steps**+**Ba-**	e. g. `192.168.0.254`

Field	Menu	Value
	sic Setup	

Variants 1 + 2: Configuration of country settings

Field	Menu	Value
International Prefix / Country Code	**System Management->Global Settings->System**	e.g. *49*
National Prefix / City Code	**System Management->Global Settings->System**	e.g. *911*

SIP provider (individual number)

Field	Menu	Value
Name	**Tr** **u** **n**	e.g. *Sipgate_Plus_1*

Field	Menu	Value
	->**New**-> **<SIP-Provider>**	
Authentication ID	**Tr** **u** **n**	e.g. *1527861e0*

Field	Menu	Value
	->**New**-> **<SIP-Provider>**	
Password	**Tr** **u** **n**	e.g. *Supersecret*

Field	Menu	Value
	->**New**-> **<SIP-Provider>**	
Login Name	**Tr** **u** **n**	e.g. *1527861e0*

Field	Menu	Value
	->New-> <SIP-Provider>	
Registrar	**Tr** **u** **n**	e.g. *sipgate.de*

Field	Menu	Value
	->**New**-> **<SIP-Provider>**	
Single Number	**Tr** **u** **n**	e.g. *4911148797640*

Field	Menu	Value
	->New-> <SIP-Provider>	
Displayed Name	**Tr** **u** **n**	e.g. *Sipgate_1*

Field	Menu	Value
	->**New**-> **<SIP-Provider>**	
Class of Service	**Tr** **u** **n**	e. g. *Unlimited*

Field	Menu	Value
	->**New**-> **<SIP-Provider>**	
Generate international phone number	**Tr** **u** **n**	*Enabled*

Field	Menu	Value
	->New-> <SIP-Provider>	
Generate national subscriber number	**Tr** **u** **n**	*Enabled*

Field	Menu	Value
	->New-> <SIP-Provider>	

1&1

Field	Menu	Value
Substitution of Incoming Number Prefix	**VoIP->Settings->SIP Provider-> <1und1> -> ✎ ->Advanced Settings**	*49*
substitute with	**VoIP->Settings->SIP Provider-> <1und1> -> ✎ ->Advanced Settings**	*0*

QSC-IPfonie basic

Field	Menu	Value
SIP-Header-Field: FROM User	**VoIP->Settings->SIP Provider-> <qsc_ipfonie_basic> -> ✎->Advanced Settings**	*Caller Address*

Toplink

Field	Menu	Value
SIP-Header-Field: P-Preferred	**VoIP->Settings->SIP Provider-> <toplink> -> ✎ ->Advanced Settings**	*Caller Address*

SIP provider (extension)

Field	Menu	Value
Name	**N e Assistants->Telephony->w-> <SIP-Provider (Extensions)>**	e.g. *Sipgate_Trunking*
Authentication ID	**N e Assistants->Telephony->w-> <SIP-Provider (Extensions)>**	e.g. *1528507t0*
Password	**N e Assistants->Telephony->w-**	e.g. *Supersecret*

Field	Menu	Value
	> **<SIP-Provider (Extensions)>**	
Login Name	**N e Assistants**->**Telephony**->**w-** > **<SIP-Provider (Extensions)>**	e.g. *1528507t0*
Registrar	**N e Assistants**->**Telephony**->**w-** > **<SIP-Provider (Extensions)>**	e.g. *sipconnect.sipgate.de*
Base Number	**N e Assistants**->**Telephony**->**w-** > **<SIP-Provider (Extensions)>**	e.g. *4911149522701*
Class of Service	**N e Assistants**->**Telephony**->**w-** > **<SIP-Provider (Extensions)>**	e. g. *Unlimited*
P-P DDI Exception	**N e Assistants**->**Telephony**->**w-** > **<SIP-Provider (Extensions)>**	e.g. *0*
Displayed Name	**N e Assistants**->**Telephony**->**w-** > **<SIP-Provider (Extensions)>**	e.g. *Zentrale-0*
Generate international phone number	**N e Assistants**->**Telephony**->**w-** > **<SIP-Provider (Extensions)>**	*Enabled*
Generate national subscriber number	**N e Assistants**->**Telephony**->**w-**	*Enabled*

Field	Menu	Value
	> **<SIP-Provider (Extensions)>**	

Sipgate Trunking

Field	Menu	Value
SIP-Header-Field: P-Preferred	**VoIP**->**Settings**->**SIP Provider**-> **<sipgate_trunking>** -> ✎ ->**Advanced Settings**	*Caller Address*

QSC-IPfonie extended

Field	Menu	Value
SIP-Header-Field: FROM User	**VoIP**->**Settings**->**SIP Provider**-> **<qsc_ipfonie_extended>** -> ✎ ->**Advanced Settings**	*Caller Address*

Variants 1 + 2: Configuration of authorisation class (optional)

Field	Menu	Value
Trunk Line Selection with Line Access Number	**Numbering**->**User Settings**->**Class of Services**-> **<Benutzerberechtigungsklasse>** ✎ ->**Basic Settings**	e.g. *Sipgate_Plus_1*

Assignment of incoming calls

Field	Menu	Value
Assignment	**Numbering**->**Call Distribution**->**Incoming Distribution**-> **<49911148797640>** -> ✎	*Internal Number*
Internal Number	**Numbering**->**Call Distribution**->**Incoming Distribution**-> **<49911148797640>** -> ✎	e.g. *30 (Doe-30)*

Configuration of outgoing numbers - SIP provider (individual number) QSC-IPfonie basic and Toplink

Field	Menu	Value
e.g. Toplink	**Numbering**->**User Settings** ->**Users**-> **<Doe-30>** ✎	e.g. *00495171773052*

Field	Menu	Value
	Outgoing Signalisation-> **<30>** ✎	

Configuration of outgoing numbers - SIP Provider (Extension) Sipgate Trunking and QSC-IPfonie extended

Field	Menu	Value
e.g. Sipgate_Trunking	**Numbering** ->**User Settings** ->**Users**-> **<Doe-30>** ✎ ->**Outgoing Signalisation** -> **<30>** ✎	e.g. *004991149522401-0*

Chapter 10 bintec 4Ge-LE as WAN path to a be.IP

10.1 Introduction

After login the **be.IP** starts in the view **Initial operation**.

After running through the assistant, the **be.IP** starts in the view **Users**. To access all menu points, switch to the view **Full Access**.

The following section describes the connection of a **bintec 4Ge-LE** as a backup WAN path to a **be.IP**.

The **GUI** (Graphical User Interface) is used for configuring.

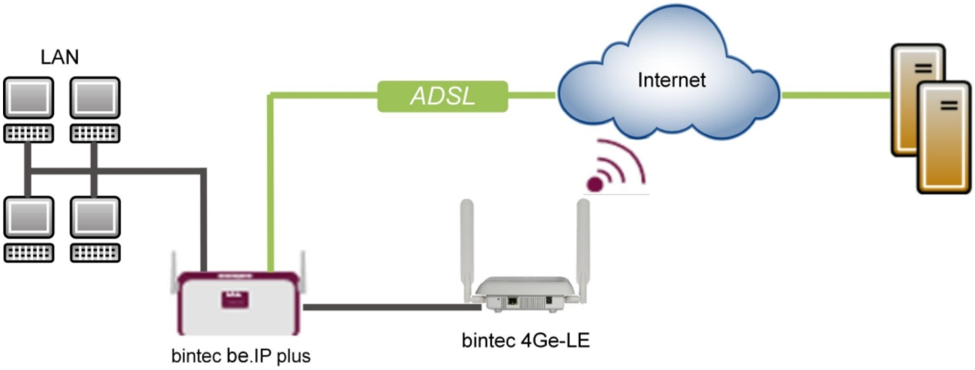


Fig. 100: Example scenario

Requirements

- A **bintec 4Ge-LE**
- A bintec **be.IP** or a **be.IP plus** with current firmware. You can check the BOSS version of your **be.IP** in the menu **System Management**->**Status**.
- An existing configuration as set up by a completed **Quick Start assistant**.

10.2 Configuration

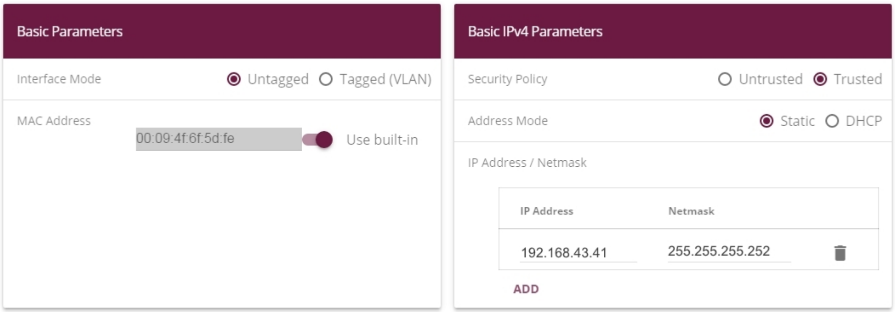
Connection of bintec 4Ge-LE

In principle the **bintec 4Ge-LE** runs as a DHCP Client and receives from the gateway the names and the PIN for the SIM card via the option 43 (Vendor specific). The device uses this data to establish a LTE (UMTS/GPRS) connection and provides the received IP address, the gateway and the DNS server as DHCP server on an Ethernet connection of **be.IP** tagged with VLAN 463. This means that the **be.IP** is on the actual interface DHCP server on a virtual port with VLAN 463 against DHCP client!

In the example, en1-4 (the blue DMZ/WAN Port) is used, although this can be configured in the same way on any separate port.

The interfaces are now adjusted/created in the first step.

(1) Enter in the menu **LAN**->**IP Configuration**->**Interfaces**-> **en1-4** ✎.



Basic Parameters

Interface Mode ● Untagged ○ Tagged (VLAN)

MAC Address 00:09:4f:6f:5d:fe Use built-in

Basic IPv4 Parameters

Security Policy ○ Untrusted ● Trusted

Address Mode ● Static ○ DHCP

IP Address / Netmask

IP Address	Netmask
192.168.43.41	255.255.255.252

ADD

Fig. 101: **LAN**->**IP Configuration**->**Interfaces**-> **en1-4** ✎

Proceed as follows:

(2) Leave the **Interface Mode** settings as `Untagged`. The interface is not assigned for a specific purpose.

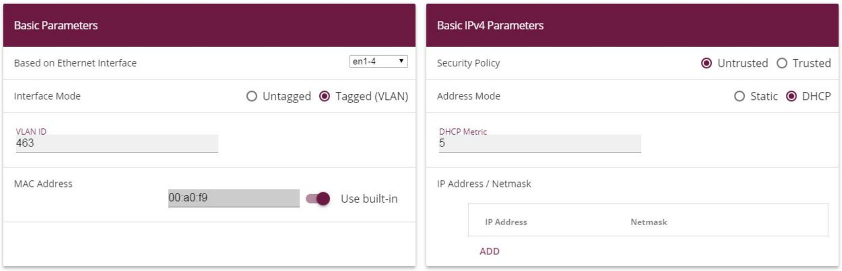
(3) Leave the **Security Policy** settings as `Trusted`. All IP packets are allowed through except for those which are explicitly prohibited.

(4) Enter the **IP Address / Netmask** of the virtual interface, here e.g. `192.168.43.41` und `255.255.255.252`.

(5) Click **OK** to confirm your entries.

In the next step, create a new interface.

(1) Go to **LAN**->**IP Configuration**->**Interfaces**->**New**.



Basic Parameters

Based on Ethernet Interface: en1-4

Interface Mode: ○ Untagged ● Tagged (VLAN)

VLAN ID: 463

MAC Address: 00:a0:f9 ● Use built-in

Basic IPv4 Parameters

Security Policy: ● Untrusted ○ Trusted

Address Mode: ○ Static ● DHCP

DHCP Metric: 5

IP Address / Netmask

IP Address	Netmask

Fig. 102: **LAN**->**IP Configuration**->**Interfaces**->**New**

Proceed as follows:

(2) Under **Based on Ethernet Interface** select the virtual interface *en1-4*.

(3) Set the **Interface Mode** to *Tagged (VLAN)*.

(4) Assign a VLAN to the interface. To do this, enter the **VLAN ID** *463*.

(5) For **Security Policy**, select *Untrusted*.

(6) Select the **Address Mode** *DHCP*. An IP address is assigned to the interface dynamically via DHCP.

(7) Under **DHCP Metric** select the priority of the route, which is *5* in our example.

(8) Click **OK** to confirm your entries.

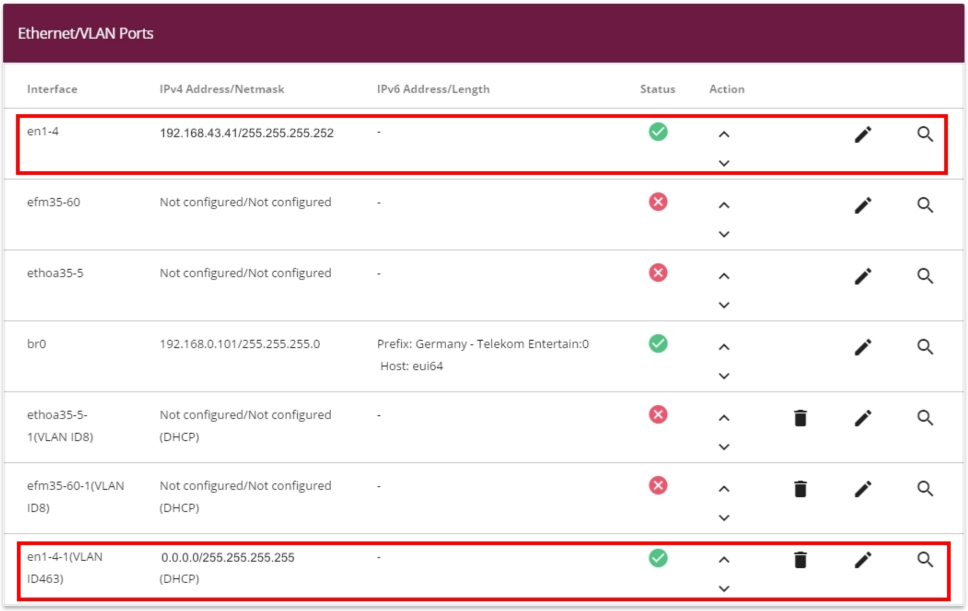
The netmask for en1-4 was selected with /30 so that only one IP range of 2 addresses is needed:

- **be.IP** (192.168.43.41)

- **bintec 4Ge-LE** (192.168.43.42)

Network address is therefore 192.168.43.40, broadcast address is 192.168.43.43.

The complete configuration now looks like this:



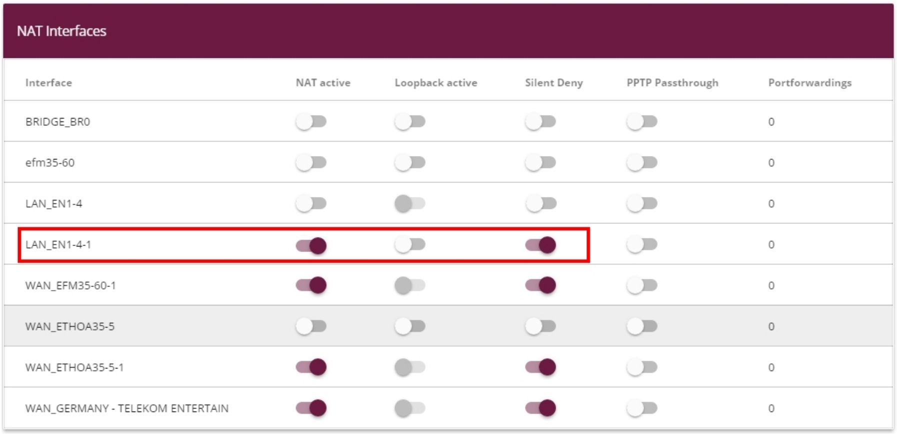
Ethernet/VLAN Ports

Interface	IPv4 Address/Netmask	IPv6 Address/Length	Status	Action
en1-4	192.168.43.41/255.255.255.252	-	✓	
efm35-60	Not configured/Not configured	-	✗	
ethoa35-5	Not configured/Not configured	-	✗	
br0	192.168.0.101/255.255.255.0	Prefix: Germany - Telekom Entertain:0 Host: eui64	✓	
ethoa35-5-1(VLAN ID8)	Not configured/Not configured (DHCP)	-	✗	
efm35-60-1(VLAN ID8)	Not configured/Not configured (DHCP)	-	✗	
en1-4-1(VLAN ID463)	0.0.0.0/255.255.255.255 (DHCP)	-	✓	

Fig. 103: **LAN->IP Configuration->Interfaces**

Now for the virtual interface `en1-4-1` must be enabled as IPv4 WAN interface **NAT**.

(1) Go to **Network->NAT->NAT Interfaces**.



NAT Interfaces

Interface	NAT active	Loopback active	Silent Deny	PPTP Passthrough	Portforwardings
BRIDGE_BR0	○	○	○	○	0
efm35-60	○	○	○	○	0
LAN_EN1-4	○	○	○	○	0
LAN_EN1-4-1	●	○	●	○	0
WAN_EFM35-60-1	●	○	●	○	0
WAN_ETHOA35-5	○	○	○	○	0
WAN_ETHOA35-5-1	●	○	●	○	0
WAN_GERMANY - TELEKOM ENTERTAIN	●	○	●	○	0

Fig. 104: **Network->NAT->NAT Interfaces**

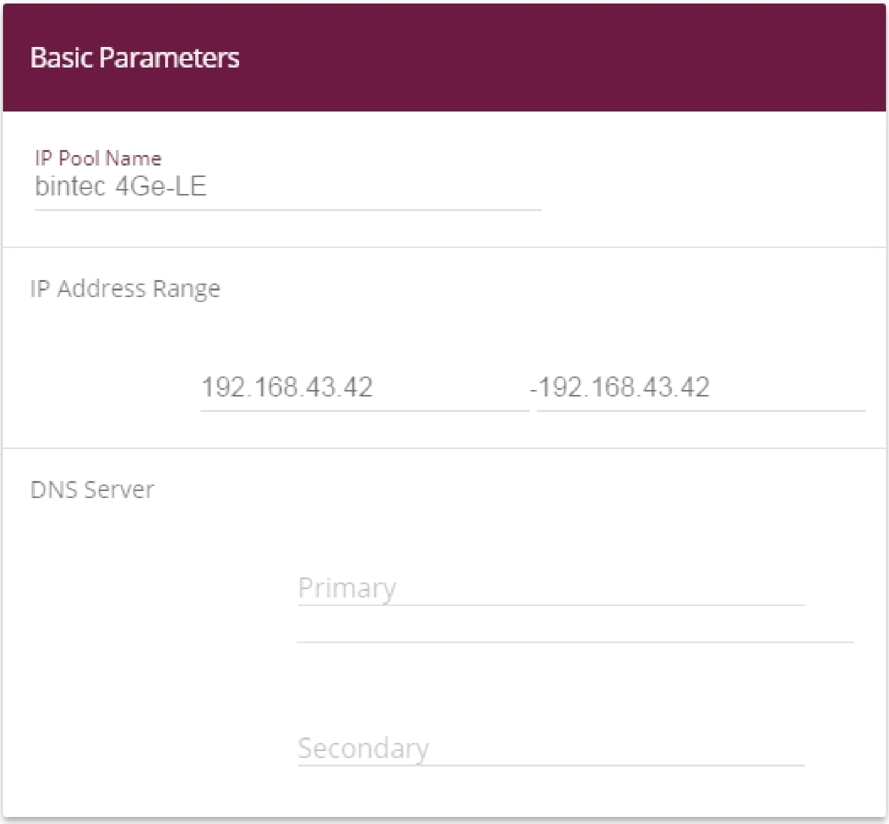
(2) For the **Interface** `LAN_EN1-4-1` enable the options `NAT active` and `Silent Deny`.

(3) Click **OK** to confirm your entries.

The last configuration step is setting up the DHCP server with the corresponding DHCP option *43* on the interface *en1-4*. For security reasons, a static connection of the IP address to the MAC address of the **bintec 4Ge-LE** is carried out so that only this received an IP address (and only this is sent the option 43 with the PIN included).

To activate the device as DHCP server, the IP address pool must first be defined.

(1) To do so, go to the **Local Services**->**DHCP Server**->**IP Pool Configuration**->**New** menu.



Basic Parameters

IP Pool Name: bintec 4Ge-LE

IP Address Range: 192.168.43.42 -192.168.43.42

DNS Server

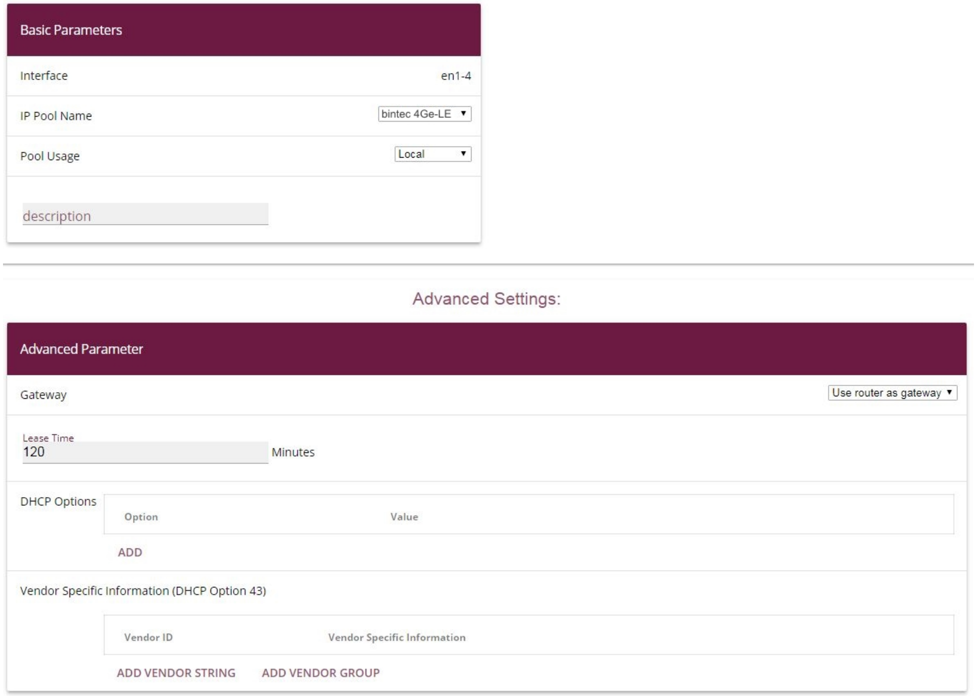
Fig. 105: **Local Services**->**DHCP Server**->**IP Pool Configuration**->**New**

(2) Under **IP Pool Name** enter any description, here e.g. *bintec 4Ge-LE* .

(3) Under **IP Address Range** enter the IP address of the IP address pool, here *192.168.43.42 - 192.168.43.42* .

(4) Confirm with **OK**.

Under **Local Services**->**DHCP Server**->**DHCP Configuration**->**New** you can now set up the DHCP pool.



Basic Parameters

Interface en1-4

IP Pool Name bintec 4Ge-LE

Pool Usage Local

description

Advanced Settings:

Advanced Parameter

Gateway Use router as gateway

Lease Time 120 Minutes

DHCP Options

Option	Value

Vendor Specific Information (DHCP Option 43)

Vendor ID	Vendor Specific Information

Fig. 106: **Local Services**->**DHCP Server**->**DHCP Configuration**->**New**

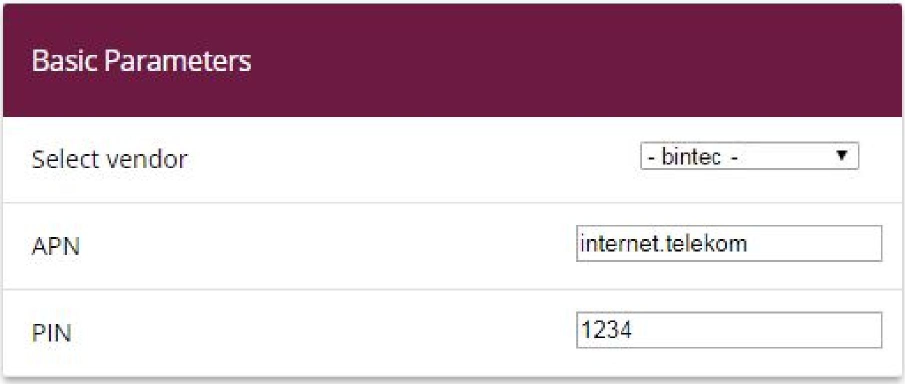
Proceed as follows:

(1) Select **Interface** *en1-4*.

(2) Under **IP Pool Name** select the configured IP pool name *bintec 4Ge-LE*.

(3) Click **Advanced Settings**.

(4) In the **Vendor Specific Information (DHCP Option 43)** field, click on the **Add Vendor String** button.



Basic Parameters

Select vendor	- bintec -
APN	internet.telekom
PIN	1234

Fig. 107: **Local Services**->**DHCP Server**->**DHCP Configuration**->**New**->**Advanced Settings**

(5) Under **Select vendor** select *-bintec-* .

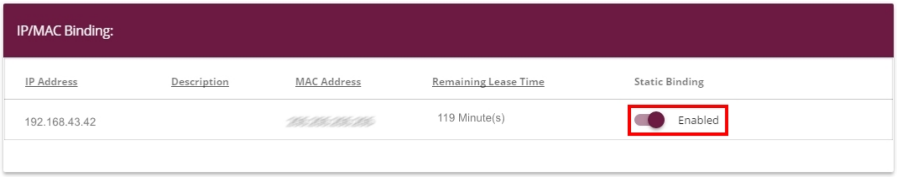
(6) Enter the **APN** (Access Point Name) of the provider of your SIM card, here e.g. *internet.telekom*.

(7) Enter the **PIN** of the SIM card, e.g. *1234*.

(8) Click **Apply**.

The last step involves establishing the static connection of the IP Address to the MAC address.

(1) Go to the **Local Services**->**DHCP Server**->**IP/MAC Binding** menu.



IP/MAC Binding:

IP Address	Description	MAC Address	Remaining Lease Time	Static Binding
192.168.43.42		[redacted]	119 Minute(s)	● Enabled

Fig. 108: **Local Services**->**DHCP Server**->**IP/MAC Binding**

(2) Enable the **Static Binding** option.

(3) Confirm with **OK**.

With this configuration only the **bintec 4Ge-LE** on the interface *en1-4* receives an IP address with the SIM card PIN included in option 43.

This concludes the configuration. Store the configuration using **Save configuration** above the menu bar

10.3 Overview of Configuration Steps

Adjusting the metric

Field	Menu	Value
Metric	**Network->Routes->IPv4 Route Configuration->** ✎	*0*

Adjusting the interface

Field	Menu	Value
Interface Mode	**LAN->IP Configuration->Interfaces-> en1-4** ✎	*Untagged*
Security Policy	**LAN->IP Configuration->Interfaces-> en1-4** ✎	*Trusted*
IP Address / Netmask	**LAN->IP Configuration->Interfaces-> en1-4** ✎	e. g. *192,168.43.41* / *255.255.255.252*

Configuring a new interface

Field	Menu	Value
Based on Ethernet Interface	**LAN->IP Configuration->Interfaces->New**	*en1-4*
Interface Mode	**LAN->IP Configuration->Interfaces->New**	*Tagged (VLAN)*
VLAN ID	**LAN->IP Configuration->Interfaces->New**	*463*
Security Policy	**LAN->IP Configuration->Interfaces->New**	*Untrusted*
Address Mode	**LAN->IP Configuration->Interfaces->New**	*DHCP*
DHCP Metric	**LAN->IP Configuration->Interfaces->New**	e. g. *5*

Activating NAT

Field	Menu	Value
NAT active	**Network->NAT->NAT Interfaces**	*Enabled*
Silent Deny	**Network->NAT->NAT Interfaces**	*Enabled*

Configuring the IP pool

Field	Menu	Value
IP Pool Name	**Local Services**->**DHCP Server**->**IP Pool Configuration**->**New**	e.g. *bintec 4Ge-LE*
IP Address Range	**Local Services**->**DHCP Server**->**IP Pool Configuration**->**New**	e.g. *192.168.43.42* - *192.168.43.42*

DHCP configuration

Field	Menu	Value
Interface	**Local Services**->**DHCP Server**->**DHCP Configuration**->**New**	*en1-4*
IP Pool Name	**Local Services**->**DHCP Server**->**DHCP Configuration**->**New**	*bintec 4Ge-LE*
Vendor Specific Information (DHCP Option 43)	**Local Services**->**DHCP Server**->**DHCP Configuration**->**New** ->**Advanced Settings**	*Add Vendor String*
Select vendor	**Local Services**->**DHCP Server**->**DHCP Configuration**->**New** ->**Advanced Settings** ->**Add Vendor String**	*-bintec-*
APN	**Local Services**->**DHCP Server**->**DHCP Configuration**->**New** ->**Advanced Settings** ->**Add Vendor String**	e.g. *internet.telekom*
PIN	**Local Services**->**DHCP Server**->**DHCP Configuration**->**New** ->**Advanced Settings** ->**Add Vendor String**	e. g. *1234*

IP/MAC Binding

Field	Menu	Value
Static Binding	**Local Services**->**DHCP Server**->**IP/MAC Binding**	*Enabled*

Chapter 11 Configuration help

11.1 Change the startup view

The **be.IP** starts after login until completion of the wizard **Initial operation**, always in the **Initial operation** view. The **be.IP** starts after completion of the wizard, always in the **Users** view.

Requirements

A **be.IP plus**

Configuration destination

After login as *admin* your **be.IP plus** should show a different view from the one described above.

You can choose from the following views:

- **Quick start**
- **User**
- **Full access**.

11.1.1 Configuration

You can change the start view of the **be.IP plus**.

(1) Initiate a SSH connection to your device, e.g. with Putty.
You are now in the SNMP shell of your gateway. The login prompt will appear.

(2) Log in to your device as **admin**.

(3) Enter `biboextadminitialguiview?` to display the different view options.
(readwrite) full_access (1), user (2), initial_operation (3) will appear.

(4) If you want to change the start view to **full access**, enter `biboextadminitialguiview=full_access`.

(5) If you want to change the start view to **user**, enter `biboextadminitialguiview=user`.

(6) If you want to change the start view to **quick start**, enter `biboextadmininitial-`

`guiview=initial_operation`.

(7) If you want to keep the chosen setting after a reboot, save the current configuration.

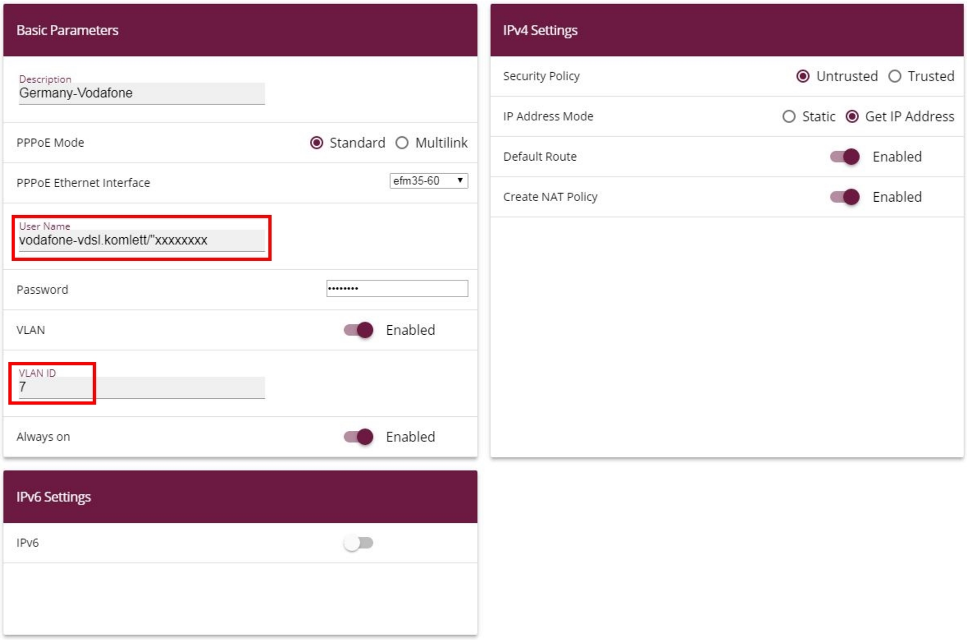
11.2 Setting up for a Vodafone VDSL connection

Setting up the Internet and voice connection will be described below. These settings are important for configuration to a Vodafone VDSL connection.

11.2.1 Setting up the Internet connection

A connection to the Internet service provider must be set up in order to create an Internet connection.

To do so, go to the **WAN**->**Internet + Dialup**->**PPPoE**->**New** menu.



Basic Parameters

Description: Germany-Vodafone

PPPoE Mode: ● Standard ○ Multilink

PPPoE Ethernet Interface: efm35-60

User Name: vodafone-vdsl.komlett/"xxxxxxxx

Password: ••••••••

VLAN: Enabled

VLAN ID: 7

Always on: Enabled

IPv4 Settings

Security Policy: ● Untrusted ○ Trusted

IP Address Mode: ○ Static ● Get IP Address

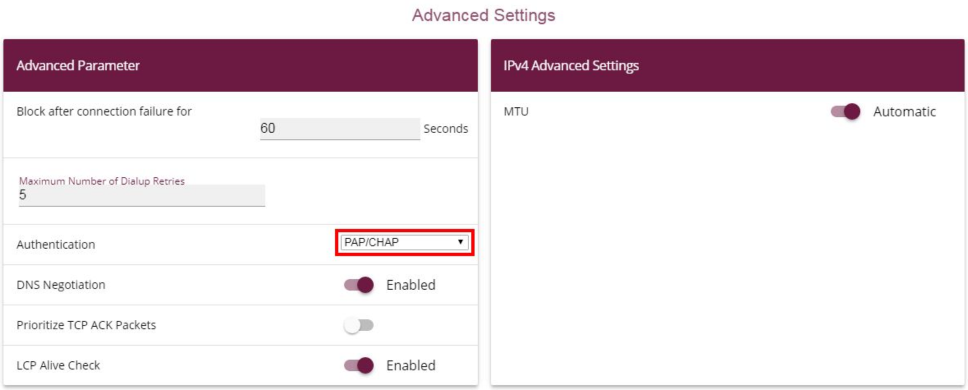
Default Route: Enabled

Create NAT Policy: Enabled

IPv6 Settings

IPv6

Fig. 109: **WAN**->**Internet + Dialup**->**PPPoE**->**New**



Advanced Settings

Advanced Parameter

Block after connection failure for 60 Seconds

Maximum Number of Dialup Retries 5

Authentication PAP/CHAP

DNS Negotiation Enabled

Prioritize TCP ACK Packets

LCP Alive Check Enabled

IPv4 Advanced Settings

MTU Automatic

Fig. 110: **WAN**->**Internet + Dialup**->**PPPoE**->**New**->**Advanced Settings**

Proceed as follows:

(1) Select **Description** then enter a name to uniquely identify the PPPoE partner. The first character in this field must not be a number No special characters or umlauts must be used.

(2) Select the **PPPoE Ethernet Interface** for the connection.

(3) Under **Login Name** it is necessary to use `vodafone-vdsl.komplett/"` as a prefix. Enter the login details after it.

(4) Enable the **VLAN** function.

(5) The **VLAN ID** is set to `7` by default. It is possible to change the VLAN ID (e.g. 132) or enter the VLAN ID that you obtained from your provider.

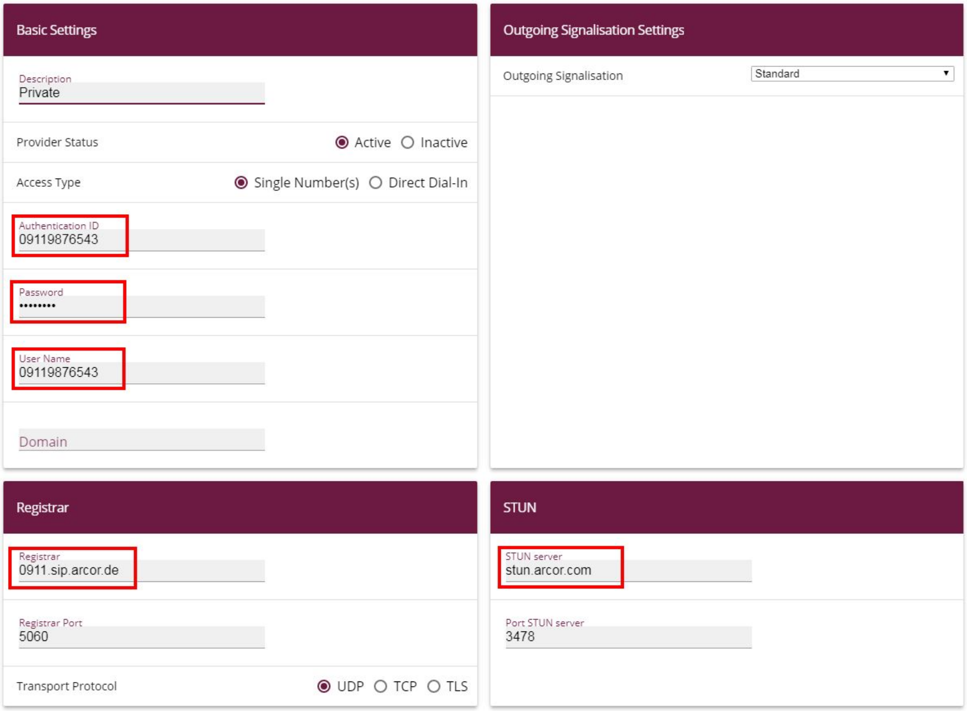
(6) Click **Advanced Settings**.

(7) Select the **Authentication** `PAP/CHAP`.

(8) Click **OK** to confirm your entries.

11.2.2 Setting up the voice connection

Configure the voice connection in the **VoIP**->**Settings**->**SIP provider**->**New** menu.



Basic Settings

Description: Private

Provider Status ● Active ○ Inactive

Access Type ● Single Number(s) ○ Direct Dial-In

Authentication ID: 09119876543

Password: ••••••••

User Name: 09119876543

Domain

Outgoing Signalisation Settings

Outgoing Signalisation: Standard ▾

Registrar

Registrar: 0911.sip.arcor.de

Registrar Port: 5060

Transport Protocol ● UDP ○ TCP ○ TLS

STUN

STUN server: stun.arcor.com

Port STUN server: 3478

Fig. 111: **VoIP**->**Settings**->**SIP provider**->**New**

Proceed as follows:

(1) Enter a **Description** for the connection, e.g. `Private`.

(2) Under **Authentication ID** and under **Login Name** enter the telephone number including the dialling code, such as `09119876543`.

(3) Enter the **Password** that you received from your provider.

(4) Under **Registrar** enter the dialling code of the connection and the ending too, e.g. `0911.sip.arcor.de`.

(5) You can enter a **STUN server** here, such as `stun.arcor.com`.

(6) Click **OK** to confirm your entries.

This means that the settings required for a Vodafone VDSL connection are complete. All other settings remain the same as with another provider.

11.3 Configuration of a DynDNS account

Configuration of a DynDNS account on a **be.IP plus** or a bintec VPN router is described below.

Requirements

(1) A **be.IP plus** or a bintec VPN router with 10.1.Rev system software. 5.

(2) An active Internet connection with a dynamic IP address

(3) A DynDNS account with a DynDNS provider

The graphical user interface (GUI) is used for configuration.

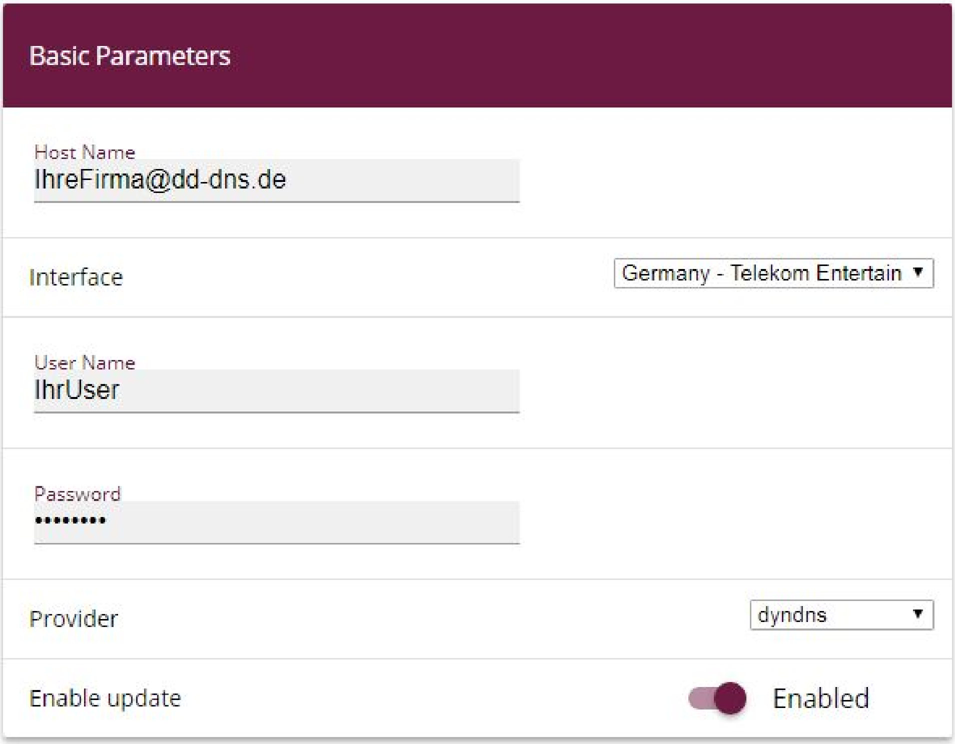
Note

There are many German and international DynDNS providers that can be used to set up a DynDNS account. There are providers who charge a fee and others are free-of-charge. Examples include DynDNS.com, selfHOST.de or SPDNS.de. An account from TwoDNS.de is used in this example.

11.3.1 Configuration

Open a web browser and enter the IP address of your router into the address field. Use your login information to log into the router.

Go to the **Local Services**->**DynDNS Client**->**DynDNS Update**->**New** menu.



Basic Parameters

Host Name: IhreFirma@dd-dns.de

Interface: Germany - Telekom Entertain

User Name: IhrUser

Password: •••••••••

Provider: dyndns

Enable update: Enabled

Fig. 112: **Local Services**->**DynDNS Client**->**DynDNS Update**->**New**

Proceed as follows:

(1) Enter the **Host Name** as registered with the DynDNS provider e.g. `IhreFirma@dd-dns.de`.

(2) Select the **WAN-Interface**, the IP address of which should be transferred to the DynDNS provider, e.g. `Telekom`.

(3) Under **Username** enter the name of the account as it is registered with the DynDNS provider, in this case `IhrUser`.

(4) Enter the **Password** as registered with the DynDNS provider e.g. `SuperSecret`.

(5) Select the DynDNS **provider** with which the above data is registered; here it is `TwoDNS`.

(6) Enable the **Enable update** option.

(7) Click **OK** to confirm your entries.

You can access help on available configuration options via the online help system.

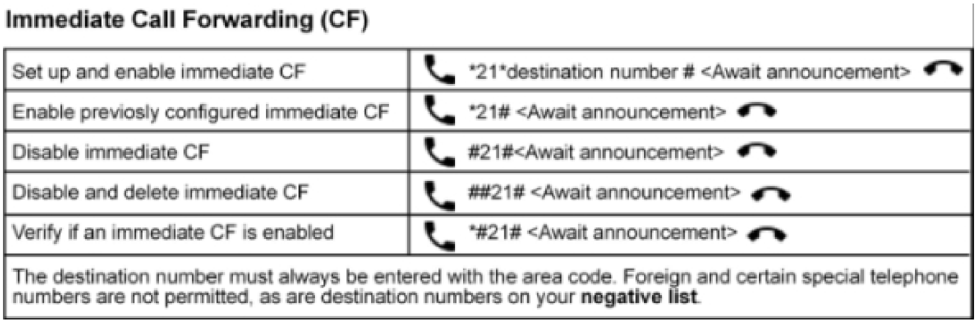
11.4 Use of agency features and functions with the IP-

based connection

IP-based telephone connections provide various agency features that are similar to ISDN connections, in this case an example of "Deutschland LAN IP Voice&Data" from Deutsche Telekom.

A list of all possible functions can be found at *https://hilfe.telekom.de/hsp/cms/content/HSP/de/3378/FAQ/theme-133631783/Auftrag/theme-82239611/IP-basierter-Anschluss/faq-445419652*

Immediate call forwarding (AWS-sofort) is used as an example in the following explanations:



Immediate Call Forwarding (CF)

Set up and enable immediate CF	📞 *21*destination number # <Await announcement> ☎
Enable previosly configured immediate CF	📞 *21# <Await announcement> ☎
Disable immediate CF	📞 #21#<Await announcement> ☎
Disable and delete immediate CF	📞 ##21# <Await announcement> ☎
Verify if an immediate CF is enabled	📞 *#21# <Await announcement> ☎
The destination number must always be entered with the area code. Foreign and certain special telephone numbers are not permitted, as are destination numbers on your **negative list**.	

11.4.1 be.IP and be.IP plus as the media gateway

These devices forward the strings that were received from ISDN via SIP to the "agency" so that when entering it on the end device only the features of a downstream ISDN telephone system have to be taken into account if necessary, and that enquiries regarding the telephone system should be directed to the relevant manufacturer.

11.4.2 be.IP plus as PBX

It is necessary to distinguish between two cases, depending on settings in the authorisation class

- Outside line with the exchange code
- Automatic outside line

11.4.2.1 Outside line with the exchange code

If an outside line is set, then this exchange code (normally "0") should be added as a prefix to the actual sequence so that, for our example, setting up and activation of "AWS-sofort" for the telephone number 0228-123456789 yields the string **0*21*0228123456789#**. The exchange code must, clearly, be selected depending on the setting.

11.4.2.2 Automatic outside line

It must be taken into account regarding the automatic outside line that a prefixed "*" character triggers the selection of an internal extension.

Example: If the automatic outside line is set and extension 10 wishes to have an internal call with extension 30, then the dialling sequence would be: ***30**

However, this feature of **be.IP plus** as PBX which was described earlier can lead to the idea that dialling "*21" will reach the internal extension 21. The dialling sequence for the telephone system must make it clear that this string must be transferred to the agency with "*" as a prefixed character.

This happens by consciously dialling an "internal number" then obtaining an outside line via the exchange code (usually "0"), so prefixing with "*0"!

The following dialling sequence is the result of the example for setting up and activating a "AWS-sofort" for the telephone number 0228-123456789: ***0*21*0228123456789#**

The exchange code must, clearly, be selected depending on the setting.

11.5 Setting up the function key for controlling the integrated access point

11.5.1 Note

The following description only covers configuration of the function key for activating / deactivating the access point integrated in the **be.IP**. This does not cover the settings of the wireless module and creation of a wireless network.

The `Full Access` view is required for accessibility of the relevant menus.

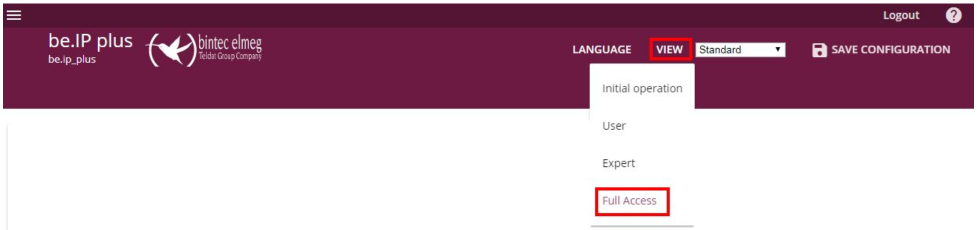


Fig. 113: Configuration interface header bar

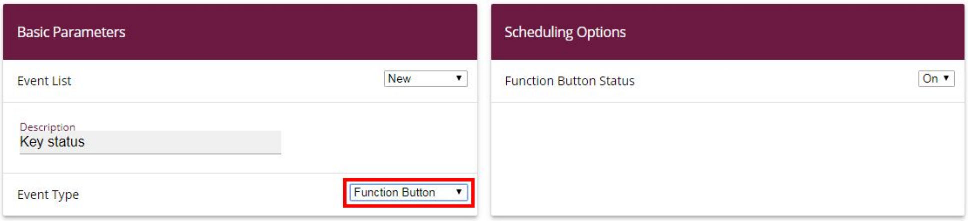
On the plan view, the function key can be found on the Ethernet interfaces on the left-hand side next to the RSMA connection (screw-in connection for the WLAN antenna).

The task of monitoring a state - in this case, whether the key is active or inactive - is done by the **scheduler**. Depending on whether this applies to one or several initiators, specific actions can be carried out, in this example the action would be `activating/deactivating the access-point`. The initiators are cyclically monitored in an adjustable interval so that there is a time delay between actuating the key and the action of the access point.

11.5.2 Configuration

11.5.2.1 Setting the initiator

The status of the function key as `on` or `off` must be configured as an **Trigger**. Go to the **Local Services**->**Scheduling**->**Trigger**->**New** menu.


Basic Parameters

Event List: New

Description: Key status

Event Type: Function Button

Scheduling Options

Function Button Status: On

Fig. 114: **Local Services**->**Scheduling**->**Trigger**->**New**

Proceed as follows:

(1) Enter any **Description** for the event list, in this case `Key status`.

(2) Under **Event Type** select the `Function Button` option.

(3) Set the **Function Button Status** to `On`.

(4) Press **OK** to confirm your entries.

Note

The function key does not change the status between `on` and `off` every time it is actuated, but also changes the status depending on the time difference between presses!

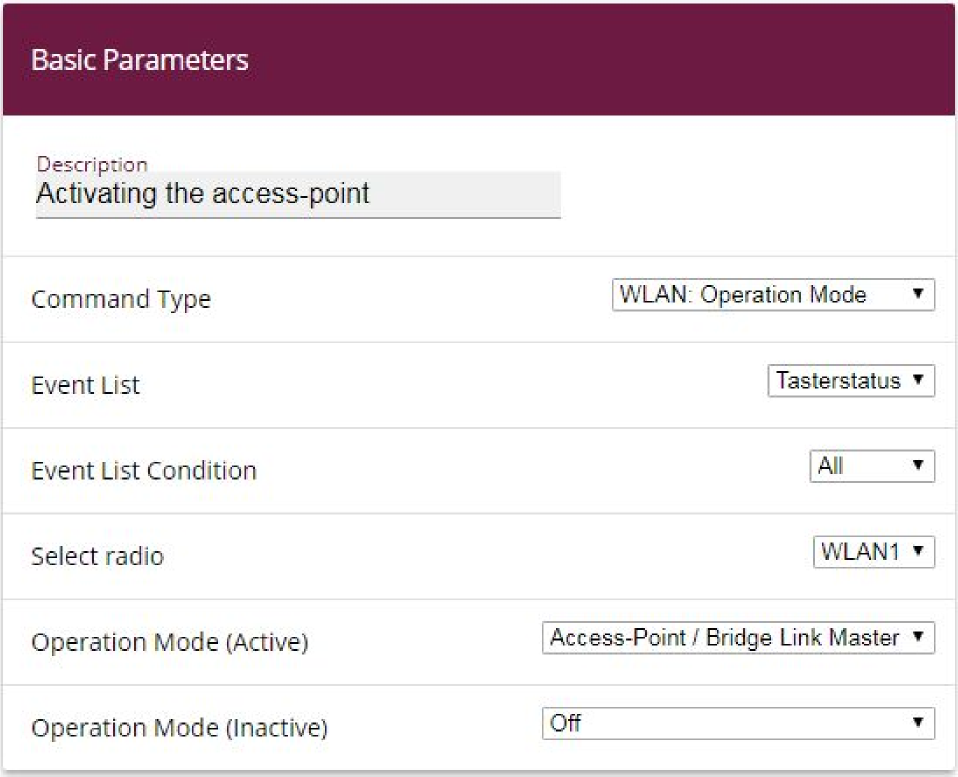
If actuated for more than one second, but less than three, then the status is `on`. Actuation longer than three seconds sets the key status to `off`.

Unintended actuation or so-called "toggling" between statuses is therefore avoided.

11.5.2.2 Configuring the action

In the next step, the action is now defined depending on the state of the initiator.

Go to the **Local Services**->**Scheduling**->**Actions**->**New** menu.



Basic Parameters

Description: Activating the access-point

Command Type	WLAN: Operation Mode
Event List	Tasterstatus
Event List Condition	All
Select radio	WLAN1
Operation Mode (Active)	Access-Point / Bridge Link Master
Operation Mode (Inactive)	Off

Fig. 115: **Local Services**->**Scheduling**->**Actions**->**New**

Proceed as follows:

(1) Enter any **Description** for the action, in this case *Activating the access-point*.

(2) Under **Command Type** select the *WLAN: Operation Mode* option in the drop-down menu.

(3) Select the **Event List** that you defined in the **Trigger** menu as an initiating event list, in this case *Key status*.

(4) Under **Event List Condition** leave the settings on *All*.

(5) Regarding the integrated **WLAN1**, set the **operation mode (active)** to *Access-Point / Bridge Link Master*.

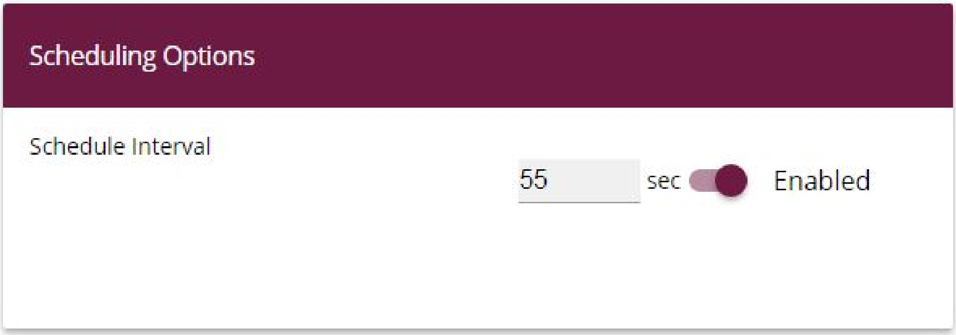
(6) Set the **operation mode (inactive)** to *Off*.

(7) Press **OK** to confirm your entries.

11.5.2.3 Enable scheduling

At the end, configure the schedule interval.

Go to the **Local Services**->**Scheduling**->**Options** menu.


Scheduling Options

Schedule Interval 55 sec ● Enabled

Fig. 116: **Local Services**->**Scheduling**->**Options**

Proceed as follows:

(1) Enable the **Schedule Interval** option.

(2) Keep the default value at *55 seconds*. If the value has to be adjusted, do not select a value below 10 seconds.

(3) Press **OK** to confirm your entries.

At this point, configuration is completed.

After a test, the performed configuration should be saved with the button

SAVE CONFIGURATION above the menu bar.

11.5.3 Overview of Configuration Steps

Setting the initiator

Field	Menu	Value
Description	**Local Services->Scheduling->Trigger->New**	e.g. *Key status*
Event Type	**Local Services->Scheduling->Trigger->New**	*Function Button*
Function Button Status	**Local Services->Scheduling->Trigger->New**	*On*

Configuring the action

Field	Menu	Value
Description	**Local Services->Scheduling->Actions->New**	e.g. *Activating the access-point*
Command Type	**Local Services->Scheduling->Actions->New**	*WLAN: Operation Mode*
Event List	**Local Services->Scheduling->Actions->New**	*Key status*
Event List Condition	**Local Services->Scheduling->Actions->New**	*All*
Select radio	**Local Services->Scheduling->Actions->New**	*WLAN1*
Operation mode (active)	**Local Services->Scheduling->Actions->New**	*Access-Point / Bridge Link Master*
Operation mode (inactive)	**Local Services->Scheduling->Actions->New**	*Off*

Enable scheduling

Field	Menu	Value
Schedule Interval	**Local Services->Scheduling->Options**	*Enabled* and *55 sec*