

**be.SD***x*

# User Manual

Copyright© bintec elmeg GmbH V. 1.2.3 2020-10-13

# Table of contents

1	Introduction .....	4
2	Logging on to the be.SDx platform .....	5
3	Start page .....	6
3.1	Adding a new customer .....	7
3.2	Setting up a customer network .....	9
3.2.1	Locations .....	9
3.2.2	Status .....	13
3.2.3	Applications .....	15
3.2.4	LAN .....	17
3.2.5	WLAN .....	23
3.2.6	Notifications .....	33
3.2.7	Devices .....	35
3.2.8	Internet .....	40
3.2.9	Customer administration .....	46
4	User .....	48
4.1	Adding a new user .....	49
5	On-site installation .....	53
5.1	Cabling .....	54
5.1.1	SDx1020 Series .....	54
5.1.2	SDx3020 Series .....	54
5.1.3	SDx5020 Series .....	55
5.2	Importing a Configuration File .....	56
5.2.1	Calling the installation interface .....	56
5.2.2	Uploading a configuration file .....	58

5.3	Manually setting up Internet access.....	59
5.3.1	Selecting the connection type.....	60
5.3.2	Authorization at the platform.....	64
5.3.3	Retrieving the final configuration.....	65
5.4	Potential errors and troubleshooting.....	66
5.5	Reverting to factory settings.....	70

# 1 Introduction

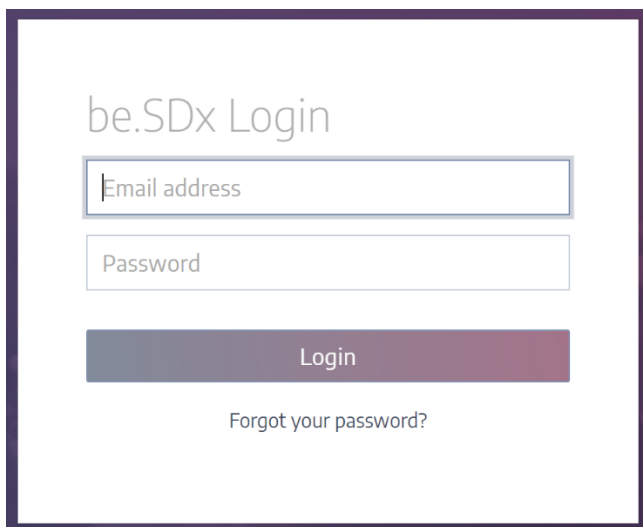
The be.SDx solution allows you to deploy, manage and monitor customer data networks using the cloud. With be.SDx, you first lay out the whole customer's infrastructure (including subsidiaries) and then connect devices on-site. If you want to change something after the initial configuration of the devices has been completed, transmitting a new configuration to all locations, or only those selected, is a couple of clicks away.

The be.SDx multi-client system ensures that those logged into the system can view and (when necessary) change any relevant data. The following roles are provided:

The **Administrator** can perform all actions allowed by the system. In addition, by way of example, **Users** can be set up to look after certain customers and manage and modify their data (where necessary). Furthermore, **read only** access can be granted. This makes viewing and monitoring certain data records possible but bans any modifications.

## 2 Logging on to the be.SDx platform

1. Click on the link you received by e-mail (<https://portal.besdx.com>). The **be.SDx Login** window opens in your standard browser.
2. Enter your e-mail address and password. Click on **Login**.

A screenshot of the be.SDx Login page. The page has a white background with a dark purple border. At the top, the text "be.SDx Login" is displayed in a light grey font. Below this, there are two input fields: the first is labeled "Email address" and the second is labeled "Password". Below the input fields is a dark purple button with the text "Login" in white. At the bottom of the page, there is a link that says "Forgot your password?".

The **Home** page opens.

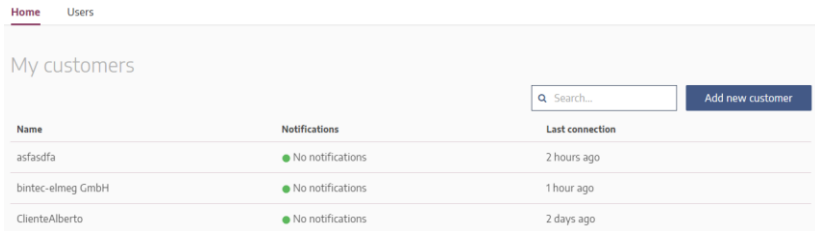
If you have already entered your password during a previous login but have forgotten it, you can reset it by clicking on **Forgot your password?** You will need to enter your e-mail address and click on **Reset Password**.

### 3 Start page

**Note:**

All be.SDx features are described below. However, not all functions are accessible to all users for editing (making and saving changes), since access is permission-dependent. If you lack permissions to carry out your daily work, please contact your system administrator.


On the start page, the **My customers** summary table shows all customers managed by the current user. You can search for a specific customer, edit an entry, or **Add a new customer**.



The screenshot shows a web interface with a navigation bar containing 'Home' and 'Users'. Below the navigation bar is a section titled 'My customers'. On the right side of this section, there is a search input field with a magnifying glass icon and the text 'Search...', and a blue button labeled 'Add new customer'. Below the search and button is a table with three columns: 'Name', 'Notifications', and 'Last connection'. The table contains three rows of data:

Name	Notifications	Last connection
asfasdfa	● No notifications	2 hours ago
bintec-elmeg GmbH	● No notifications	1 hour ago
ClienteAlberto	● No notifications	2 days ago

When you log in for the first time, the list is empty. If customers have already been created, you can see the last connection established for each customer and whether any notifications have been created.

Click on the  icon to return to the **My Customers** homepage from other pages.

## 3.1 Adding a new customer

When creating a new customer, a wizard guides you through the most important settings. After successfully running the wizard, you can adapt the configuration to your customer's specific needs.

### New network assistant

This wizard will guide you through the creation and basic configuration of a new customer. You can adjust the configuration in Advance Settings after wizard completion.

Please enter the name of your new customer.

Please set a password for customer device deployment.

### 1 Configure applications

Add applications for your new customer and prioritize them. If you enable VPN for one of the applications, we automatically create a VPN Network for you.

Type	Name	Traffic Priority	VPN
Any	Any other application	Low	<input type="checkbox"/>

When creating a new customer, you need to:

- enter a **name** to identify them.
- set a **password** so that the so-called **Installer User** can authenticate devices when they are integrated into the network.
- **add applications** to define services that can be accessed on the network and prioritize traffic.
- configure one or more network **Locations**.

- define the type of **Internet** connection available at the locations.
- add **Devices** for network access.
- set **WLAN** parameters
- if necessary, modify the IP address configuration for such locations.
- specify the **number of devices** with static and dynamic IP addresses for each location.

**Add next location** lets you create additional locations. You can copy the settings made for previous locations or manually configure the new location.

When setting up a location, you can enable the **Deny Local Breakout** option. This forces the location's Internet traffic to access the Internet via the VPN connection to the main office rather than directly via the local access (see [Edit Location](#)).

**Finish configuration** completes wizard configuration and stores the settings in the cloud. The global status page of the newly created customer is displayed (the **Global Network** tab above the menu bar). You can switch the view to a specific location and, if necessary, adjust the configuration.

Once you have made all changes, the devices can be connected and put into operation at the various locations (see [On-site installation](#)).

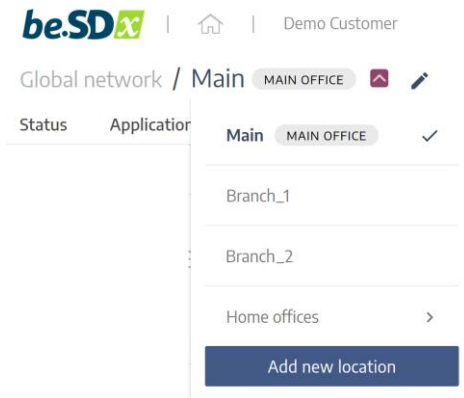


## 3.2 Setting up a customer network

Click on a customer from the **My customers** summary section found on the start page.

### 3.2.1 Locations

You can add additional locations for your customer at any time using the **Add New Location** option:



#### 3.2.1.1 Location Type Home Office

To enable employees to access the customer's company network from a stationary home office, you can select **Home Office** in the wizard when selecting the location type. The wizard then creates a simplified configuration that can be imported into the device on site.

Manual on-site setup as described in [Manually setting up Internet access](#) is also possible.

### New Location ✕

Please enter a name for this location.

**Type**

Company location

Home office

**Internet**

Please specify all Internet lines for this location.

**Devices**

Please add all network devices that will be used in this location.

**WLAN**

Enable WLAN

**LAN**

Select the interoffice network that the location needs to access.

**Note:**

*The setup of the access for a mobile employee (Mobile Office) is done in the menu [Internet > Remote Access](#) of the main office.*

When setting up a home office, the following restrictions apply due to the simplified configuration:

- When setting up the home office for the first time, only the **SDx1020** series devices without a DSL modem are available. Internet access must be provided via an upstream gateway or via an LTE connection. You can later add access points or additional Internet access, e.g. an LTE connection for backup.
- In the home office, only one wireless network is supported.

### 3.2.1.2 Edit Location

When you select an existing location for editing, the menus you can access from the status page display only the settings and devices that are relevant for that location.







When editing the basic data of a location using the pencil icon, the **Deny Local Breakout** option is of particular interest:









The screenshot shows a dialog box titled "Edit Location" with a close button in the top right corner. The dialog contains a "Name" label followed by a text input field containing "Branch\_1". To the right of the input field are two checkboxes: "This is the main office." and "Deny local breakout", each with a small information icon to its right. At the bottom of the dialog, there are three buttons: a red "Delete" button on the left, a white "Cancel" button in the middle, and a blue "Edit" button on the right.

With this option, you can force the location's traffic to access the Internet via the VPN connection to the main office rather than directly via the local access. This does not apply to data traffic from a private network set up at the location: This traffic which is, e.g., generated by a guest network still does not reach the company VPN, but is routed locally to the Internet. Voice data sent to a Cloud PBX is also excluded.

In the applications overview of the location, the difference is indicated by the VPN icon: without a ban on local breakout, only few applications are using the VPN connection:

Type	Name	Traffic Priority	VPN
Corporate	Webserver	Normal	
Corporate	Backup	Low	
SaaS	Office365 Microsoft365 Common and Office Online	Normal	
SaaS	Atlassian	Normal	
SaaS	Office365 Skype for Business Online and Microso...	Real-time	
Any	Any other application	Low	

After activating the option, however, all company data traffic is routed through the VPN:

Type	Name	Traffic Priority	VPN
Corporate	Webserver	Normal	
Corporate	Backup	Low	
SaaS	Office365 Microsoft365 Common and Office Online	Normal	
SaaS	Atlassian	Normal	
SaaS	Office365 Skype for Business Online and Microso...	Real-time	
Any	Any other application	Low	

## 3.2.2 Status

If you have successfully completed the initial configuration of a new customer, the status page of this customer is displayed.

The screenshot shows the 'Global network' status page. At the top, there are navigation tabs: 'Status' (selected), 'Applications', 'Notifications', 'Devices', and 'Customer admin'. The main content is divided into several sections:

- Network status:** A row of five cards: 'Locations' (2 Undeployed), 'Network traffic' (empty line), 'Device status' (2 Unprovisioned), 'VPN status' (empty circle), and 'No notifications' (green checkmark).
- Deployment:** Three columns of controls:
  - Download/Send configurations:** Radio buttons for 'Download configurations' (selected) and 'Send configurations'. A dropdown menu is set to 'All locations'. A 'Download' button is at the bottom.
  - Installer user:** Username 'bintecelmeggmbh', a password field with dots, and a 'Change installer password' button.
  - Device deployment mode:** Radio buttons for 'Automatic authorization' (selected) and 'Authorization through email'. A 'Change deployment mode' button is at the bottom.
- Network analyzer:** A section with the instruction 'Select a dataset, location and timespan to analyze the network.' Below are three dropdown menus: 'Bandwidth / Traffic', 'Select location (1)', and 'Last hour'.

### Note:

*If a configuration has already been transferred to the devices on-site, a warning message may appear at the top of the page to inform that the configuration needs to be updated after changes have been committed. If you click on **Apply Configuration**, the configuration is applied to all devices (regardless of the location). You can perform this transfer immediately, or you can set a specific time for it. Depending on the type of configuration change, the affected devices may perform a restart and are therefore unavailable for a short time.*

On the status page, you can see the **Network status** of the selected customer. You can verify that all devices have been deployed and provisioned at all locations. The VPN status is displayed, and you can see if there are any notifications. Clicking on a notification takes you to the **Notifications** menu, or to the **Network Analyzer** below.

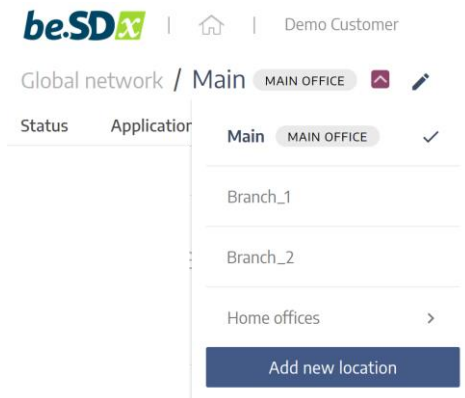
The latter will apply a set of filters to give you a better understanding of the notification itself.

Under **Deployment**, all details for device deployment at the respective locations are defined. You can use the **Download configuration** or **Send configuration** options to download the configuration of one or all devices as a file, or send it to an e-mail address. Configuration files can be loaded into a device on-site (meaning no additional settings are necessary).

On site, it is also possible to put a device into operation by manually setting up the Internet connection by means of a wizard and then integrating it into the platform using the login data of the so-called "installer user". The device synchronizes its settings with those stored on the platform, and the on-site installation is complete.

Under **Network Analyzer**, you can scan the whole customer network (or a subnetwork thereof) from various perspectives and within a specific period. Results are displayed in a graphic overview.

Under **Global Network**, found at the top of the page, you can either select an existing location or add new locations. The menus displayed vary depending on whether the **Global Network** tab (instead of a specific location) has been selected.



When selecting a location, the **LAN**, **WLAN**, and **Internet** menus appear.

The screenshot shows the 'Global network / MAD' interface with the 'MAIN OFFICE' location selected. The top navigation bar includes 'Status', 'Applications', 'LAN', 'WLAN', 'Notifications', 'Devices', and 'Internet'. The 'Network status' section displays five cards: 'Location' (Undeployed), 'Network traffic' (empty line), 'Device status' (3 Unprovisioned), 'VPN status' (empty circle), and 'No notifications' (green checkmark). The 'Deployment' section has three sub-sections: 'Download/Send configurations' with radio buttons for 'Download configurations' (selected) and 'Send configurations', a 'Download' button, and a 'Change installer password' button; 'Installer user' with a text field containing 'matthiasclient' and a 'Change installer password' button; and 'Device deployment mode' with radio buttons for 'Automatic authorization' (selected) and 'Authorization through email', and a 'Change deployment mode' button. The 'Network analyzer' section has a dropdown menu for 'Bandwidth / Traffic', 'All devices', and 'Last hour'.

### 3.2.3 Applications

In the **Applications** menu, you assign a priority for the data traffic created by the services available across the network with the help of predefined categories.

The screenshot shows the 'Global network / MAD' interface with the 'MAIN OFFICE' location selected. The top navigation bar includes 'Status', 'Applications', 'LAN', 'WLAN', 'Notifications', 'Devices', and 'Internet'. The 'Applications' section has a search bar and an 'Add new application' button. Below is a table with columns: Type, Name, Traffic Priority, VPN, and Actions.

Type	Name	Traffic Priority	VPN	Actions
Corporate	SAP	High	<input checked="" type="checkbox"/>	<a href="#">✎</a> <a href="#">☰</a>
SaaS	Office365 Exchange Online	Normal	<input checked="" type="checkbox"/>	<a href="#">✎</a> <a href="#">☰</a>

You can configure an application for the entire network (*All locations*), for a single location, or for multiple locations.

### Note:

An application that is configured for a specific location overwrites an identical application that was assigned to that location by the “All Locations” setting.

Data traffic is configured using three types of application:

- *Voice* (voice data), i.e. PBX or Cloud
- *Corporate* (company-internal data traffic), e.g. SAP
- *SaaS* (Software as a Service), e.g. Office365 Exchange Online.

**Traffic priority** determines which applications are given priority, i.e. how the available bandwidth is distributed. For voice applications, priority is automatically set to *real-time* so that, for example, there are no delays when making voice calls.

In the **Applications** menu, you can edit existing entries, search for entries, and add new ones.

### 3.2.3.1 Add a new application

The screenshot shows the 'Add new application' form in a network management interface. The breadcrumb path is 'Global network / MAD MAIN OFFICE'. The navigation menu includes 'Status', 'Applications' (highlighted), 'LAN', 'WLAN', 'Notifications', 'Devices', and 'Internet'. The form title is 'Applications / Add new application'. It contains the following fields:

Application type	Application name	Traffic Priority	VPN
Corporate		Select...	<input type="checkbox"/>
IP	Ports (TCP)	Ports (UDP)	
0.0.0.0	0, 0:0	0, 0:0	

Buttons: Cancel, Add

To configure a new application, you must:

- select an **Application type**, namely *Voice* (voice data), *Corporate* (company-internal data traffic) or *SaaS* (Software as a Service).
- for **Application type** = *Corporate*, enter the **name of the application, e.g. Intranet**.



- for **Application type** = *SaaS*, select the **application** from the drop-down menu, e.g. *Office365 Exchange Online*.
- for the application types *Corporate* or *SaaS*, select the **Traffic priority**, e.g. *Normal*.
- enter the **IP address** or **Hostname** of the server in the network on which the application is hosted if selecting **Application type** = *Corporate*.
- specify the **Ports** for data traffic over TCP and UDP.
- leave **All Locations** at its default setting if you want the service to be available throughout the global network or select the **Locations** where you want the service to be available.

The system determines for which services traffic is routed through a VPN. For example, a VPN is automatically used when selecting the **Voice Application type** and **PBX Service type** (data traffic of a telephone system) or the **Corporate Application type** (internal data traffic within the company).

### 3.2.4 LAN

The **LAN** menu is displayed when a location is selected in the drop-down menu above the menu bar (if **Global Network** is selected, the menu is not displayed). Here, you can edit existing entries, search for entries, and add a new network.

The screenshot shows the 'LAN' configuration page in a web interface. At the top, there is a breadcrumb 'Global network / MAD' and a 'MAIN OFFICE' indicator. Below this is a navigation bar with tabs for 'Status', 'Applications', 'LAN' (selected), 'WLAN', 'Notifications', 'Devices', and 'Internet'. Under the 'LAN' tab, there are sub-tabs for 'Networks', 'Ports', and 'VLAN'. The main content area is titled 'Networks' and contains a search bar, an 'Add new network' button, and a table of existing networks. The table has columns for Name, IP address, Netmask, DHCP range, Fixed range, DNS server, and VLAN ID. An 'Actions' dropdown menu is visible at the end of each row.

Name	IP address	Netmask	DHCP range	Fixed range	DNS server	VLAN ID	Actions
Macronet	192.168.0.1	255.255.255.2...	192.168.0.7 - 11	192.168.0.2 - 6	192.168.0.1		[edit] [checkbox]

### 3.2.4.1 Add new network

The screenshot shows a web-based configuration interface for adding a new network. The breadcrumb path is 'Global network / MAD MAIN OFFICE'. The navigation menu includes 'Status', 'Applications', 'LAN' (selected), 'WLAN', 'Notifications', 'Devices', and 'Internet'. The sub-menu for 'Networks' is open, showing 'Ports' and 'VLAN'. The main heading is 'Networks / Add new network'. The form is divided into three sections: 'General information' with a 'Visibility' section (radio buttons for 'Private addressing' and 'Interoffice network'), a 'Name' field, and 'Network configuration' with fields for 'IP address', 'Netmask', 'DNS server', and 'VLAN'. The 'Static IP addressing' section has a 'Fixed IP range' field and a 'Dynamic IP addressing (DHCP)' checkbox. 'Cancel' and 'Add' buttons are at the bottom right.

To configure a new network, you must:

- decide whether you want to create a **Private** or an **Interoffice network**.  
An interoffice network is routed between locations via IPsec while a private network is only available at the respective location.
- assign a **name** and an **IP address** to the network.
- select or set up a **VLAN**; VLANs divide your network into individual logical subnets, if necessary.
- define address ranges for **Static** and **Dynamic IP address assignment** in your network.

*Note:*

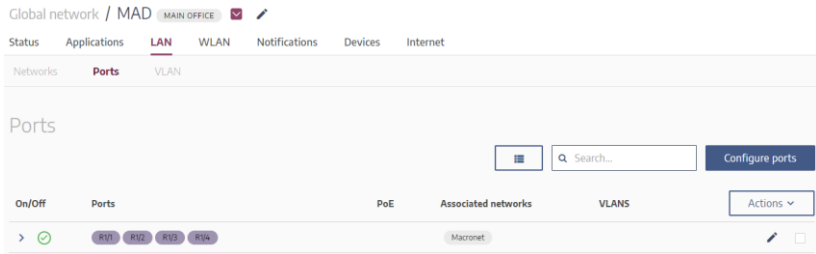
*These two address ranges must not overlap.*


*Newly created networks must be assigned a port to become active.*

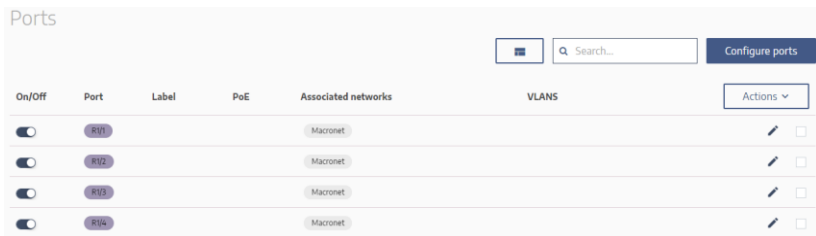
- activate **DHCP options** and set the parameters for a DHCP relay agent, if necessary.

### 3.2.4.2 Configuring Ports

A list of configured port groups is displayed in the **LAN > Ports** menu.



By clicking on the  icon, or the arrow at the left of the entry, ports are individually displayed in a list:



In the **Configure Ports** menu, you can select ports and assign them to a network individually or in groups.

Global network / MAD MAIN OFFICE

Status Applications LAN WLAN Notifications Devices Internet

Ports / Configure ports

Device  
MAD\_ROUTER...

Ports  
1 2 3 4 ETH SFP  
Configured Selected

Selected ports  
Select...

Label

Associated networks  
Macronet (Untagged)

Options  
 Use 802.1x for LAN authentication  
Server address: [edit icon]

Cancel Save

- The **Label** is used to label a port.  
*Note:*  
*Only one untagged network can be assigned to a port.*
- Under **Associated networks** you can define to which of the existing networks ports are going to be assigned to.
- If you enable *Use 802.1x for LAN authentication*, you can edit the **Server address**.

Edit server address

Server address  
000.000.000.000

Username  
[masked] @teldat.com

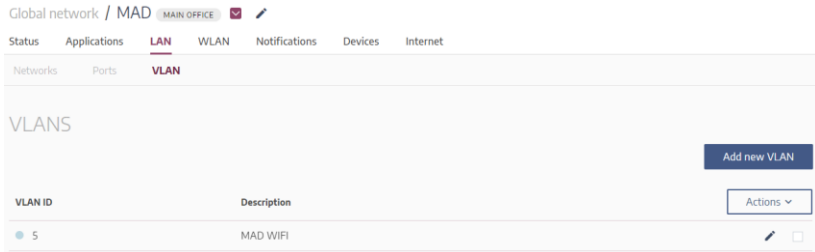
Password  
[masked]

Cancel Save

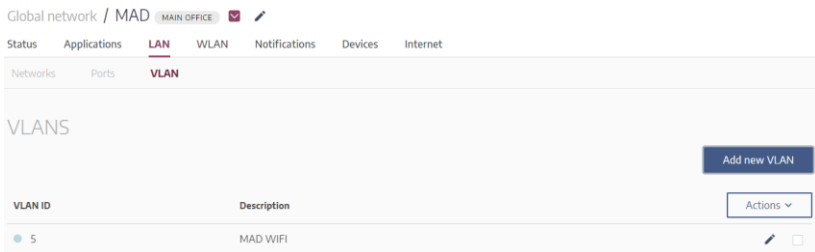
Enter the address of the authentication server and the access data for this port or group of ports here.

### 3.2.4.3 Add new VLAN

Existing VLANs are displayed in the **LAN > VLAN** menu.



VLANs divide your network into logical groups.



To create a new VLAN, you must

- assign a **VLAN ID**.
- enter a **Description**.
- select a **Tag color** for a better overview.

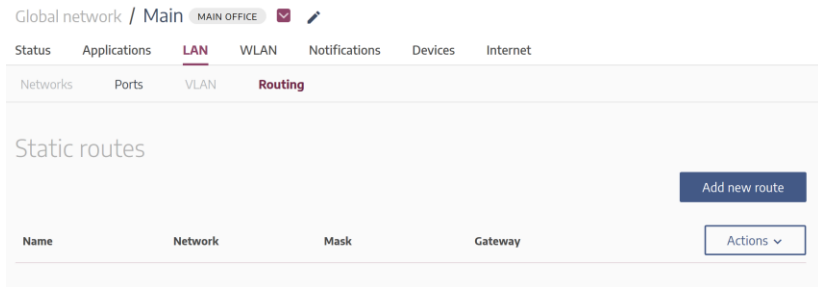
*Note:*

*Each VLAN must be assigned to exactly one network.*

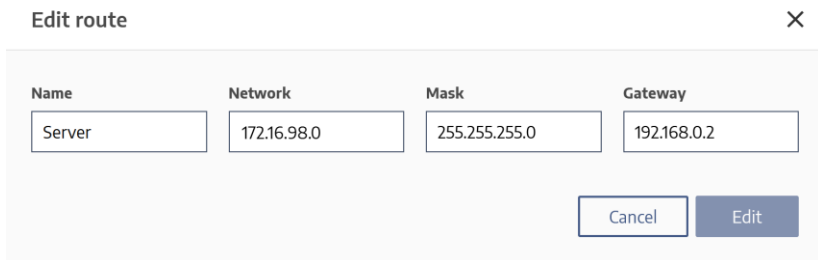
### 3.2.4.4 Routing

When setting up the main office, you can create static routes in the **Routing** menu so that devices or services in a remote network that is not directly connected to the be.SDx router can be made accessible.

The menu first displays a list of already created routes:



Use the **Add new route** button to create new routes:



To create a route, you must

- give the route or the connected network a name.
- enter the IP address at which the network can be reached.
- specify the netmask of the target network.
- specify the IP address of the gateway through which the target network can be reached.

*Note that this gateway must perform Network Address Translation between the destination and source networks.*

In a second step, you create an entry in the [Applications](#) menu which specifies the IP address of the service or server in the remote network and provides corresponding QoS functions for connections to this network.

## Note

To give an IPSec client access to a network accessible via routing, this network must be added to the IPSec client setup in the **Internet > Remote Access** menu. You may need to make the IPSec profile available to the employee once again.



## 3.2.5 WLAN

The **WLAN** menu sets up and edits a wireless network. It is displayed when a **location** is selected in the menu bar (if **Global Network** is selected, the menu is not displayed).

### 3.2.5.1 Wireless networks

Select the location for which you want to set up a WLAN. Go to the **WLAN > Wireless Networks** menu.

Wireless networks that already exist are displayed in the summary. You can edit the existing entries and add new ones.


Global network / Zweigt1  

Status Applications LAN **WLAN** Notifications Devices Internet

**Wireless networks** Radio profiles Access points

### Wireless networks

[Add new network](#)

SSID	Description	Security mode	WPA mode	Network	Actions
Firma	Corporate_WLAN_Network	WPA PSK	WPA2	Macronet	 <input type="checkbox"/>

Click on the **Add New Network** button.

The screenshot shows a web interface for configuring a new wireless network. At the top, there is a breadcrumb trail: 'Global network / Zweig1'. Below this is a navigation bar with tabs for 'Status', 'Applications', 'LAN', 'WLAN' (which is active), 'Notifications', 'Devices', and 'Internet'. Under the 'WLAN' tab, there are sub-tabs for 'Wireless networks', 'Radio profiles', and 'Access points'. The main content area is titled 'Networks / New wireless network'. It is divided into three sections: 'General information', 'Security', and 'Mac Control'. In the 'General information' section, there are three input fields: 'Network name (SSID)', 'Description (Optional)' (with a placeholder 'Type description'), and 'Network' (a dropdown menu currently showing 'Macronet'). To the right of these fields are three checkboxes: 'Hidden network', 'Intra-cell repeating', and 'Guest network'. The 'Security' section has a 'Mode' dropdown menu currently set to 'None'. The 'Mac Control' section has a checkbox for 'Whitelist Mode' which is currently unchecked.

The following options to add a new network are available:

### General Information

- The **Network name (SSID)** of the wireless network. This is visible to WLAN clients.
- A **Description** for this SSID - this only serves internal administration purposes and is hidden from other devices.
- You can select one of the networks created in the **LAN** menu. If you create a VLAN configuration there, you can separate WLAN traffic from other network traffic.

### Options

- *Hidden network*: This option ensures that this network is not open to WLAN clients for selection.
- *Intra-cell repeating*: This option allows clients connected to this SSID to exchange data with each other.
- *Guest Network*: Here you can define this wireless network as a separate guest network. To do this, you must create a



separate network for this purpose in the LAN menu and assign it to the wireless network using the **Network** option.

## Security

- The following mechanisms can be selected as **Mode** to secure WLAN data traffic
  - *None*
  - *WPA-PSK*
  - *WPA Enterprise*.
- WPA can be applied in different versions, available as **WPA modes**:
  - *WPA*
  - *WPA2*
  - *WPA/WPA2*.
- **The WPA cipher / WPA2 cipher** option specifies the encryption you want to use for WPA:
  - *TKIP*
  - *AES*
  - *TKIP/AES*.

*The use of TKIP is not recommended as this encryption method must be considered insecure and is only available for compatibility reasons.*

- **WPA password**: You must set a password! Otherwise, data transfer within this SSID takes place without encryption.
- When using *WPA Enterprise*, access to the wireless network is controlled via a RADIUS server. Enter the **IP address** and **Password** of the RADIUS server (only for *WPA Enterprise*).

## MAC control

- **Whitelist mode** - Entries in the white list are not blocked.

### Note:

*If you activate the whitelist mode, but the list is empty, access to the network is impossible.*

Activate the **Whitelist Mode** option. Click on **Edit MAC Filter List** to add a MAC address.

MAC filter list: Whitelist

MAC Address	Description
00-12-34-56-ac-cd	MAC-Address

Buttons: Add, Cancel, Save

- Enter the **MAC address** and **description** of the client you want to grant access to.
- Click on **Save**.

## Client management

Client Management

Max clients (soft, hard) ⓘ

Band Steering ⓘ

○ Deactivated

● 5GHz preferred

Traffic Management

SNR (Sticky client avoidance) ⓘ

Enable SNR Management

Threshold (dBm) Grace time (seconds)

0 5

Data rate trimming ⓘ

2.4GHz band 5GHz band

All (Min. 1MBit/s) All (Min. 6MBit/s)

Buttons: Cancel, Add

- In the **Max. Clients (soft/hard limit)** fields, enter the number of clients that can connect to this wireless network. The **Soft limit** specifies the number of clients whose login attempts are initially prevented. If a client repeats its request, it is still

admitted. As soon as the **Hard limit** is reached, no more clients are allowed.

- Under **Band Steering**, you can move clients from the band originally selected to one that is less busy. You can disable the function or select one of the two frequency bands available (2.4 GHz or 5 GHz). Clients will then be moved to this band, where possible.

## Traffic management

In this section, you set up the distribution of the available bandwidth in this WLAN:



- Activate SNR Management to specify the **Threshold** and **Grace time** parameters.  
Since clients with bad connections may slow the wireless network down for all clients, you can use the **Threshold (dbm)** parameter to define a threshold value for a client's signal level:
  - Specify the lower RSSI threshold in dBm. If this value is undershot for longer than the specified grace time, the access point stops the communication with the affected client.
  - Enter the timeout in seconds during which the data transfer rate may fall below the RSSI threshold without the client being excluded from communications.
- The **Data Rate Trimming** option allows you to enhance WLAN performance as needed. You can block low data transfer rates to enforce the use of higher rates. Similarly, to what happens when an **RSSI Threshold** is applied, this may help increase the network's overall performance.
  - 2.4GHz band: *(All (min. 1Mbit/s), min. 6Mbit/s, min. 12Mbit/s, min. 24Mbit/s)*
  - 5GHz band: *(All (Min. 6Mbit/s), 12Mbit/s, Min. 24Mbit/s)*

Note:

If you use **Data rate trimming**, older clients may not be able to connect to the network because they may not support the selected data rates.

### 3.2.5.2 Radio profiles

A summary of all radio profiles created is displayed in the **WLAN > Radio profiles** menu. You can edit the existing entries and add a new radio profile.



Global network / Zweig1  

Status Applications LAN **WLAN** Notifications Devices Internet



Wireless networks **Radio profiles** Access points

## Radio profiles

[Add new radio profile](#)

Description	Operation band	Wireless mode	Bandwidth	Actions
2.4 GHz Radio Profile	2_4GHz	gn	20MHz	 <input type="checkbox"/>
5 GHz Radio Profile	5GHz	anac	80MHz	 <input type="checkbox"/>

Click on the **New radio profile** button.

Global network / Zweig1  

Status Applications LAN **WLAN** Notifications Devices Internet

Wireless networks **Radio profiles** Access points

## Radio profiles / New

**Description**

**Operation band**

2.4GHz  
 5GHz


**Wireless mode**


**Bandwidth**


**Advanced options**

**Channel Plan**

**Beacon period**

Background scanning 

Airtime fairness 

Short guard interval 

[Cancel](#) [Add](#)

To add a new **Radio profile**, you must:


- enter a **description** for the radio profile.
- select a **Frequency band**, *2.4 GHz* or *5 GHz*.
- in **Wireless mode**, select the wireless standard to be used.
- select whether the data traffic is to be transmitted with a **Bandwidth** of 20, 40 or 80 MHz

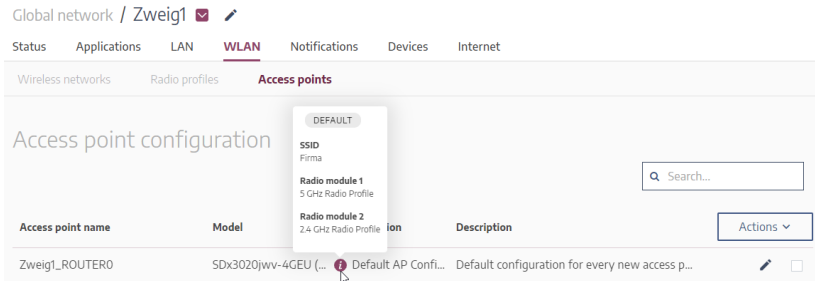
Moreover, you have the following options:



- **Channel Plan**  
In the 2.4 GHz frequency band: *Global Mode, ETSI Mode, User defined*  
In the 5 GHz frequency band: *Indoor (without weather channels), Indoor – No DFS/TPC, Outdoor (without weather channels), User defined*  
When selecting *User defined*, it is necessary to select one or more channels (in the 2.4 GHz band: 1 - 13; in the 5 GHz band: 36 - 140).
- **Beacon period**: Enter the time in milliseconds between the sending of two beacons.
- **DTIM period**: Enter the interval for the Delivery Traffic Indication Message (DTIM).
- To automatically search for neighboring or rogue access points on the network at regular intervals, activate the **Background Scan** function.
- The **Airtime Fairness** function ensures that sender resources belonging to the access point are distributed wisely among connected clients.
- Activate the **Short Guard Interval** function to shorten the Guard Interval from 800 ns to 400 ns to increase the maximum data rate. In less than optimal conditions, this may, however, lead to an increase in packet errors.

### 3.2.5.3 *Access points*

The **WLAN > Access Points** menu displays the list of configured access points (or routers with WLAN support). Access points are

added in the **Devices** menu. Hover your cursor over the  to display the current configuration of an access point.





Global network / Zweig1  

Status Applications LAN **WLAN** Notifications Devices Internet

Wireless networks Radio profiles **Access points**


### Access point configuration


Search...



Access point name	Model	Radio module 1	Radio module 2	Description	Actions
ZweigL-ROUTER0	SDx3020jwv-4GEU (...)	5 GHz Radio Profile	2.4 GHz Radio Profile	Default AP Config...	 

Click on the **Actions** button to *copy* an existing configuration, to *paste* it (i.e. to assign it to at least one device) or *remove* the configuration from a device. These options allow a fast management of existing configurations and devices.

If you want to assign a configuration to several devices, you must:

- Select a device.
- If no configuration has been assigned to the device, click on the  icon and assign a configuration.
- Under **Actions**, copy the configuration of the device.
- Select the devices to which you want to assign this configuration.
- Assign (*paste*) this configuration under **Actions**.

You can edit an access point by clicking on the  symbol:

Global network / Zweig1  

Status Applications LAN **WLAN** Notifications Devices Internet

⏪ Access point configuration / Zweig1\_ROUTER0



**Configuration**

Default AP Configuration DEFAULT ▾

Edit configuration

**Name**  **Description (Optional)**

**LED mode**  ▾

**SSID**   

Radio module 1	<input checked="" type="checkbox"/> Radio module 2
<b>Radio profile</b> <input type="text" value="Select..."/> ▾	<b>Radio profile</b> <input type="text" value="Select..."/> ▾
<b>TX power (dBm)</b> <input type="text" value="20 dBm"/> ▾	<b>TX power (dBm)</b> <input type="text" value="Select..."/> ▾

WLAN access point configuration looks as follows:

- The access point configuration is displayed. Using the **Actions** button, you can create a new configuration by selecting **New Configuration**.
- You can change the **Name** of the configuration template as well as its **Description**.
- You can select the **LED mode**: *normal*, *minimum*, or *off*. For information on the status indicators, refer to the manual of the device in use.
- **SSID** allows for all wireless networks set up in the **WLAN > Wireless Networks** menu to be selected. Assign one of them to the access point.



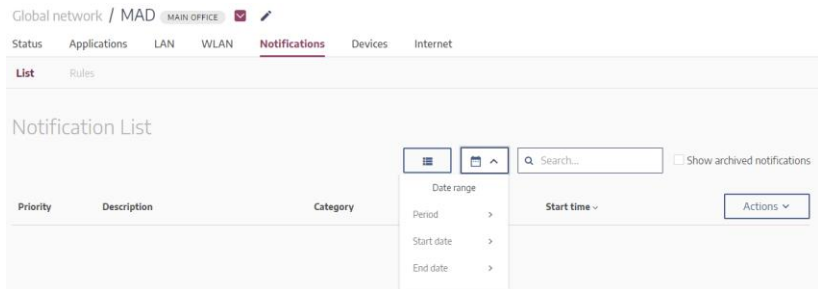
- With **Radio module 1/2**, you assign one or more radio profiles to the configuration template. This depends on the number of radio modules provided by the specific access point.
- **TX Power (dBm)** shows the current transmit power. You can select a different transmission power: *5 dBm to 23 dBm*.

### 3.2.6 Notifications

The **Notifications** menu allows you to specify the events that will generate a notification on a given priority level. The number of current notifications is also displayed on the **Status** page.

#### 3.2.6.1 List

The **Notifications > List** menu displays all messages pertaining to the selected customer that involve the entire network (**Global Network**) or specific locations (depending on the option selected in the dropdown list).

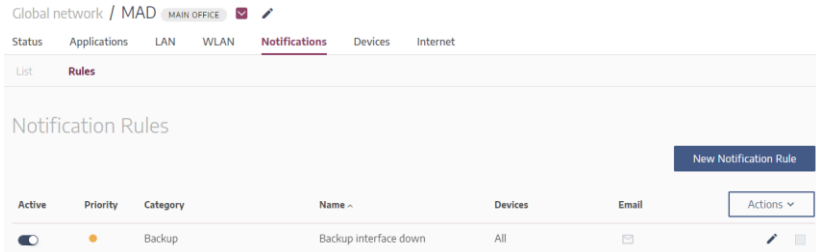


You can filter the **Notifications** list by choosing a predefined *period* (*Last hour, Today, Last 24 hours, Last week and Last month*) or by entering the *start date* and *end date*. Moreover, you can search for a specific notification. If you activate **Display Archived Notifications**, older notifications also become available.

By clicking on a message, detailed information appears, and you have the option of adding a comment (if necessary).

### 3.2.6.2 Rules

In the **Notifications > Rules** menu, the rules according to which notifications are generated are displayed.



You can edit existing rules and add new ones. The summary allows you to individually activate or deactivate the rules displayed.

To offer a better summary, rules are divided into categories. After selecting a **Category**, you can select the desired **Rule**.

The screenshot shows a 'New Notification' dialog box with a close button (X) in the top right corner. It contains two dropdown menus: 'Category' with 'Backup' selected and 'Rule' with 'Select...' selected. At the bottom right, there are two buttons: 'Cancel' and 'Add'.

To create a new **Notification rule**, you must

- select a **Category**.
- select a **Rule**.
- select a **Trigger** that determines the conditions under which the rule matches, if necessary. Usually, a threshold value is used in combination with a period during which this value may not be exceeded or undercut.
- specify the **Locations** and **Devices** the rule will apply to.

### Note:

If a rule is applied to all locations, it must also be applied to all devices. If a rule is applied to a specific device, the device location must be selected first under **Locations**.

- select a **Priority**.
- specify whether an **E-mail notification** is to be sent when the event occurs and, if so, to which e-mail address(es).

## 3.2.7 Devices

The **Devices** of the selected customer are displayed in the summary.

Global network / MAD MAIN OFFICE ✖ ✎

Status Applications LAN WLAN Notifications **Devices** Internet

### Devices

Search... Add new device

Name	Status	Type	Model	Firmware	Actions
MAD_Router	● Unprovisioned	ROUTER	SDx1020jwv-4GEU		Reboot Update firmware
MAD AP	● Unprovisioned	ACCESS_POINT	W2003ac		Replacement Block Unblock Remove Select none Select all (2)

Under **Actions**, you can perform different operations on the selected devices:

- restart device(s)
- update the firmware
- replace device(s) - You replace a device on-site with one of the same type, the configuration on the platform remains the same.
- Block or unblock a device.
- remove device(s) – You remove the device from the customer’s network and reset the configuration.
- select nothing
- select all.

The above actions allow you to configure and manage many devices in one step, simplifying and speeding up your work.

**Note:**

*You can perform a firmware upgrade on multiple devices in one step if these devices use the same firmware image.*

To update the firmware, you must

- Select one device or select multiple devices with the same firmware image.
- Click on **Actions > Update Firmware**
- Under **Update Firmware**, select the firmware for the update.
- Under **Scheduling**, select whether the firmware should be updated **as soon as possible** or **at a specific time**.
- If necessary, set the date and time for the update.

Click on the desired entry to display details about this device.



in addition to the other **Actions**, you can renew the pre-shared key for establishing the VPN connection of this device.

The **Block** function is useful for troubleshooting and quick firmware updates. When a device is locked, it only accepts requests from the controller. This ensures that you can unlock it again.

Use the **Enable SSH connection** button to allow a temporary SSH connection by a temporary user (with read permissions) and a password for an internet interface. This connection can be used for support and troubleshooting. You can specify the time frame for the

connection and, if necessary, also set the source IP address and port to further restrict access. The connection is terminated either manually or by the timer expiring. In both cases, the temporarily created user is deleted.

The screenshot shows the beSD web interface. At the top, there is a navigation bar with the beSD logo, a home icon, the text 'Max\_WLAN\_Test', and a user profile 'maximilian.nuss@bintec-elmeg.com'. Below this is a breadcrumb trail: 'Global network / WLAN\_Main / MAIN OFFICE'. A secondary navigation bar includes 'Status', 'Applications', 'LAN', 'WLAN', 'Notifications', 'Devices' (highlighted), and 'Internet'. The main content area is titled 'Devices /SDx1020/ Enable SSH connection'. It contains a form with the following fields: 'Line' (a dropdown menu showing 'WANT (Ethernet)'), 'Username' (text input with 'admin'), 'Password' (password input with masked characters), 'Allowed source IP' (text input with '192.168.0.1'), 'SSH Port' (text input with '22'), and 'Session time (min)' (text input with '30'). At the bottom right of the form are two buttons: 'Cancel' and 'Enable SSH connection' (with a checkmark icon).

After the time set for the connection has elapsed, it is unconditionally disconnected. This prevents security issues that could arise, for example, from incompletely terminated sessions.

By selecting **Edit device**, you can change the device or type name, add notes and an image for identification.

### 3.2.7.1 Adding a new device

Click on **Add new device** to create a new device.

The screenshot shows the 'Add new device' form in the Global Network management interface. The breadcrumb path is 'Global network / MAD MAIN OFFICE'. The navigation menu includes 'Status', 'Applications', 'LAN', 'WLAN', 'Notifications', 'Devices' (highlighted), and 'Internet'. The form title is 'Devices / Add new device'. The form contains the following fields and options:

- Name:** A text input field.
- Authorization:** A section with a help icon and two radio buttons: 'Automatic authorization' (selected) and 'Authorization through email'.
- Type:** A dropdown menu with 'Select...' as the placeholder.
- Model:** A dropdown menu with 'Select...' as the placeholder.
- Notes:** A large text area for adding notes.
- Photo:** A placeholder for a device photo, indicated by a camera icon.
- Buttons:** 'Cancel' and 'Add' buttons at the bottom right.

To add a new device, you need to:

- assign a **Name**
- select a **Location** - this option is available when you add a device in the **Global Network** view. Since there can only be one router per location, this **Type** of device may not be available
- select **Automatic authorization** or **Authorization by e-mail** (see [Authorization at the platform](#))
- select the **Type** of device, e.g., router
- select a device **Model**.

If you choose **Authorization by email**, an authorization link will be sent to the email address you provide.

You can also add notes and an image.

#### Note:

*If the new device is a router, you must configure its ports in the **LAN** >*

*Ports menu. Otherwise, you will receive a corresponding message on the status page.*

### 3.2.7.2 Exceptions

The **Exceptions** button allows you to view and edit a list of devices that are currently blocked for deployment.

Exceptions from provisioning are required if you want to replace or remove a device that is set up for automatic authorization and provisioning. In this case, the controller will not provision the corresponding device, even if it requests a configuration.

All devices that are removed at a site (whether through replacement or permanent removal) are initially added to the list of exceptions for automatic provisioning. If a new device is then provisioned at a site, it is ensured that it is correctly managed by the platform.

Depending on the **Device** menu in which you call the function, only the devices that are locked for the current location or - in the **Global Network** menu - all locked devices with the associated location information are displayed. Similarly, in the menu of a specific location, you can lock devices only for that location, and in the **Global Network** menu, you can select one or more locations.

Auto-provisioning exceptions ×

MAC Address	Description	Locations
<input type="text" value="F2:C0:D9:75:80:D0"/>	<input type="text" value="Blocked 1"/>	<input style="border: none;" type="text" value="All locations"/>

#### Note

*Devices that are removed from a location using the **Replace** or **Remove** action are automatically added to the list for the*

corresponding location. If you want to deploy such a device again, you must first remove it from the list.

## 3.2.8 Internet

The **Internet** menu is displayed when a location is selected at the upper menu bar (if **Global Network** is selected, the menu is not displayed). In the **Internet** menu, configure the Internet access for the location selected.

### 3.2.8.1 Lines

In the **Internet > Lines** menu, you can add new connections and edit existing ones.

The type of Internet connection is determined by the **Type** parameter:

- *xDSL* (DSL Digital Subscriber Line; xDSL is a collective term for the various DSL standards)
- *SFP* (Small Form-factor Pluggable, i.e. transmission via optical fiber)
- *Ethernet*
- *3G/LTE* (mobile radio standard).

Global network / MAD MAIN OFFICE 🔍 ✎

Status Applications LAN WLAN Notifications Devices **Internet**

**Lines** Backup Rules

Lines Add new line

On/Off	Name	Type	Status	Carrier	Bandwidth up / down	Actions
<input type="checkbox"/>	WAN1	Ethernet	Off	Generic (DHCP)	300 / 300 Mbps	<span>✎</span> <span>🗑️</span>

Backup Lines

On/Off	Name	Type	Status	Carrier	Bandwidth up / down	Actions
--------	------	------	--------	---------	---------------------	---------

To configure a new connection, you must



- select the **Type** of line, namely *xDSL*, *SFP*, *Ethernet* or *3G/LTE*.
- select the **Country**, e.g. *Germany*.
- select the **Carrier**, e.g. *Deutsche Telekom*.

Global network / MAD MAIN OFFICE

Status Applications LAN WLAN Notifications Devices **Internet**

Lines Backup Rules

Internet Settings / Add new line

Line information

Type	Country	Carrier
Ethernet	Germany	Generic (DHCP)
		Other (User-defined)

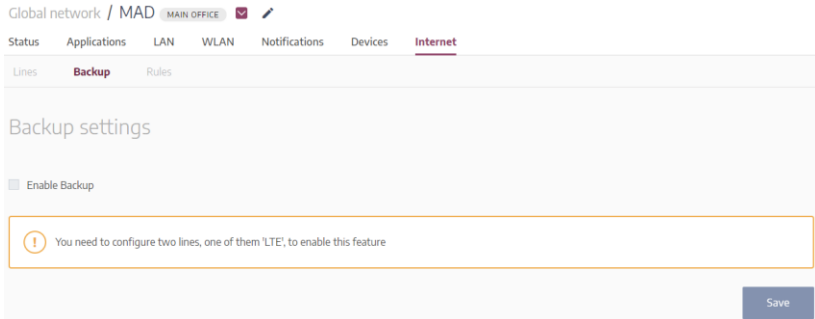
SAVE CANCEL

A predefined profile is displayed for the selected carrier. Normally, you can leave these settings at their default values.

If you have received a **Username** and **Password** from your carrier, you must enter these parameters here.

The **Expected bandwidth in MBit/s** option is also preset according to the type of Internet connection selected. The uploading and downloading values are required for QoS (Quality of Service), i.e. for the distribution of the available bandwidth among the services used (see [Applications](#)). These values need to be adjusted according to the performance of your internet connection.

In the **Internet > Backup** menu, you can specify settings for a backup connection. This connection is used when the primary Internet connection fails.



If you have created at least two connections under **Internet > Lines** and one of them is a 3G/LTE connection, you can configure a backup connection.

Under **Internet > Backup**, you must activate the **Enable backup** option and select the desired line.

*Note:*

*Only 3G/LTE connections can be used as backup lines.*

### **Load balancing for multiple Internet connections**

If you have created more than one Internet access, data to be transferred are automatically distributed among the active connections. If the connection assigned to a data stream is interrupted, the assignment changes to an available connection. Load balancing does not require configuration.

*Note*

*Connections that are set up as backups are not included in this load distribution. They are only used if no standard connection is available.*

### 3.2.8.2 Rules

In the **Internet > Rules** menu, you can configure additional Internet access parameters.

The screenshot shows the 'Rules' configuration page for a network device. At the top, it displays 'Global network / MAD' with a 'MAIN OFFICE' status indicator. Below this are navigation tabs for 'Status', 'Applications', 'LAN', 'WLAN', 'Notifications', 'Devices', and 'Internet'. The 'Rules' tab is active, showing sub-tabs for 'Lines', 'Backup', and 'Rules'. The main content area is titled 'Rules' and includes a 'Main Office Access' section with an 'Add public IP / hostname' button. Below this is a 'DNS servers' section with 'Primary DNS' (8.8.8.8) and 'Secondary DNS' (000.000.000.000) input fields. A 'DynDNS' section contains three input fields: 'Server IP / Hostname', 'Username' (e.g. "john91"), and 'Password' (e.g. "123456"). At the bottom, there is a 'Port forwarding rules' section with an 'Add a port forwarding rule' button and a 'Save' button in the bottom right corner.

The following areas are available:

- **Main Office Access:** Add public IP / Hostname (only for main office locations)
- **DNS server**  
You can set up two individual DNS servers, one primary and one secondary.
- **DynDNS**  
With DynDNS, a service ensures that a network can always be reached via the same domain name. You can configure this service here.

We recommend using the “Free dynamic DSN service” of no-ip.com.

- **Port Forwarding**

Here, you can configure port forwarding rules by choosing **Add Port Forwarding Rule**. These rules verify that connections arriving at a certain router port are directed to a specific port belonging to a specific host inside your network.

*Note about DynDNS*

*For the main office you enter the host name of the public IP address accessible via DynDNS under **Main Office Access**, for the branch offices you can enter the host name directly during the configuration of the DynDNS provider.*

*The following DynDNS services have been successfully tested:*

- *"Free dynamic DNS" from no-ip.com*
- *dyndnsfree.de.*

*The platform supports one DynDNS account per router.*

A branch office must be able to connect to the main office in order to establish the VPN between the locations. If the Internet access of the main office is made directly without an upstream gateway, it is sufficient to enter the IP address or the host name of the main office under **Main Office Access**.

If Internet access is provided via an upstream gateway, you must ensure that connections on UDP ports 500 and 4500 are forwarded to the be.SDx device of the main office. If the branch office also accesses the Internet through an upstream gateway, port forwarding does not need to be configured there because the branch office initiates the IPSec connection.

*Note*

*If the be.SDx devices are behind a strictly configured firewall or web filter, make sure that the following addresses can be reached:*

- *portal.besdx.com*
- *discover1.cloudnetmanager.com.*

### 3.2.8.3 Remote Access

In the **Remote Access** menu, you can give employees access to the company network via an IPsec client installed on a mobile device or PC. The setup is done in two sections.

#### 1. Global Settings

In the **Global Settings** you define the interface at which incoming IPsec connections are accepted, which IP addresses are internally assigned to the clients and which key is used to secure the connection.

The screenshot shows the 'Remote access' configuration page. Under 'Global settings', there are four fields: 'Interface' (a dropdown menu showing 'WAN1 (xDSL) - main.democustomer.n...'), 'IPsec client pool (Starting IP)' (a text box with '172.16.0.100'), 'Number of IPsec clients' (a spinner box with '10'), and 'Pre-shared key' (a text box with masked characters). At the bottom right, there are 'Clear' and 'Save' buttons.

#### 2. Add new IPsec client

Then, for each employee who is to have access to the company network, you define the settings with which they must authenticate themselves and to which network they are allowed to access.

The screenshot shows the 'Add new IPsec client' dialog box. It has a title bar with a close button (X). The form contains four input fields: 'Name' (with placeholder 'Type name'), 'Email' (with placeholder 'Type email'), 'Username' (with placeholder 'Type username'), and 'Password' (with placeholder 'Type password'). Below these is a 'Network access' dropdown menu with 'Select' as the current selection. At the bottom right, there are 'Cancel' and 'Add' buttons.

Use the **Actions** button above the list of configured IPSec clients to perform the following actions:

- *Delete*
- *Disconnect* - the connection of a client currently connected to the corporate network is disconnected.
- *Download VPN profile file* - you can download a configuration file for the bintec elmeg Secure Client, which the employee can import. This eliminates the need for a time-consuming setup of the IPSec client.
- *Send VPN profile file* - You can send the configuration file to the stored e-mail address of the employee.

#### *Note*

*Employees can only create one active IPSec connection with one configuration entry. To maintain several connections at the same time, a corresponding number of entries is required. Otherwise, when a second connection is established, the already existing one becomes inactive.*

### 3.2.9 Customer administration




The following information about the currently selected customer is displayed in the **Customer Management > Info** menu:

- **Company**
- **Email**
- **Notes.**

**Info**

---

### Customer information

Company	Demo Customer	
Email		
Notes		

[Delete customer](#) [Renew Pre-shared Keys](#)

You can change this information or delete the selected customer. Furthermore, you can renew the pre-shared keys of all VPN connections of this customer in this menu. In doing so, all existing VPN tunnels will be temporarily interrupted, the configurations of the routers will be adjusted and then distributed to them again so that the connections can be re-established.

*Note:*

*To delete a customer, you first have to remove all active and inactive devices of this customer from the database. All cloud configurations are deleted, and no backup is possible.*

## 4 User

All currently configured users are displayed in the **Manage Users** summary. You can search for, edit, or delete existing users, as well as add new ones.

Home Users

### Manage users

Search... [Add new user](#)

Name	Email	Permissions	Customer access	Last activity	
Documentation Admin2	██████████@teldat.com	admin	All customers	● 21 days ago	<a href="#">✎</a> <a href="#">✖</a>
SA_Admin1 SA_Admin1	██████████@teldat.com	admin	All customers	● 1 hour ago	<a href="#">✎</a> <a href="#">✖</a>



## 4.1 Adding a new user

**Add user** ✕

**Name**  **Surname**

**Email**

What can they do?

Admin Can manage everything    User Can't manage users, can manage network configurations    Read Only Can only read configurations

**Access these customers**

▾

Enable two-factor authentication. ⓘ

To create a new user, you must

- enter the new user's **Name**, **Surname** and **E-mail address**.
- define the user's permissions:

- A user with *Admin* rights can perform all actions supported by the system.

*Note:*

*Take special care when assigning admin rights, because a user with admin rights can create or delete other administrators, among other things.*

*Please note that admin rights always apply to all customers and cannot be restricted to individual customers.*

- A user with *User* privileges can change network configurations but cannot manage other users.

- *Read only* means that a user can view, but not change, network configurations.
- specify the customers the user can manage.
- if necessary, select the option **Enable two-factor authentication** (see below for further explanation)

**Add** creates the new user and displays it in the **Manage Users** summary.

### **Two-Factor Authentication**

If you activate two-factor authentication for a user, the user must synchronize an application for generating an additional one-time

password (e.g. Google or Microsoft Authenticator) with the be.SDx platform before the first or the next login:

## Configure two-factor authentication

Please, scan this QR code with your favorite authentication application



Is there any problem scanning the QR code?  
Enter this text in the mobile application to  
configure it manually

**FOZBE2V7HLTWFRKE**

### Verification

Login

Cancel

If the application has been successfully synchronized with the platform, this will be indicated accordingly in the user administration. Here you can also enforce a renewal of the synchronization:

### Edit user ✕

**Name**  **Surname**

**Email**

What can they do? ⓘ

Admin Can manage everything  User Can't manage users, can manage network configurations  Read Only Can only read configurations

Enable two-factor authentication. ⓘ

● **Synchronized**

### Note

*After synchronization of the Authenticator app, the user must enter a one-time password created by the app each time he or she logs in.*

## 5 On-site installation

There are two methods to install a router at a location: via an easy-to-use web interface, you (or a customer employee) can either load a configuration file previously exported from the be.SDx platform into the router or configure Internet access by means of a wizard. Once connected to be.SDx, all that remains to be done is to authorize the router on the platform using the "Installer User" credentials and load the final configuration.

*Note:*

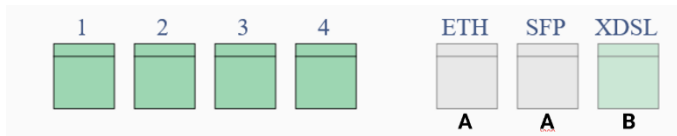
*An access point or switch can be put into operation on-site without this procedure. These devices automatically gain access to the be.SDx platform via the router.*

## 5.1 Cabling

The correct cabling depends on the router model to be installed and on the Internet connection available on site. For more information, refer to the manual of the respective router.

### 5.1.1 SDx1020 Series

Depending on the model, devices of this series can establish an Internet connection via xDSL, Ethernet (RJ45 or SFP) or LTE (**SDx1020x-4G..**):

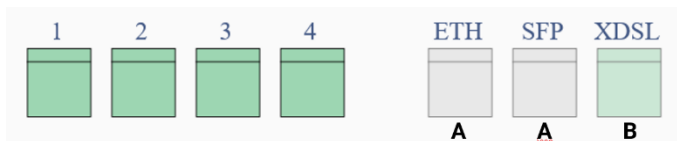


- A - Internet access via Ethernet for connection to an existing access router or modem.
- B - xDSL- direct access via DSL connection.

For Internet access via LTE, a SIM card must be installed. Refer to the router manual for information.

### 5.1.2 SDx3020 Series

Depending on the model, devices of this series can establish an Internet connection via xDSL, Ethernet (RJ45 or SFP) or LTE (**SDx3020x-4G..**):



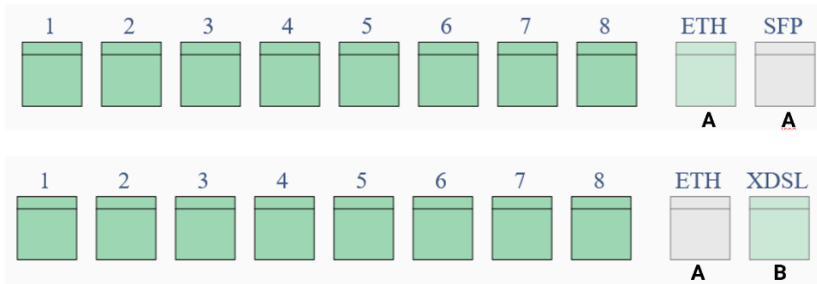
- A - Internet access via Ethernet for connection to an existing access router or modem.

- B - xDSL- direct access via DSL connection.

For Internet access via LTE, a SIM card must be installed. Refer to the router manual for information.

### 5.1.3 SDx5020 Series

Depending on the model, devices of this series can establish an Internet connection via xDSL or Ethernet (RJ45 or SFP):



- A - Internet access via Ethernet for connection to an existing access router or modem.
- B - xDSL- direct access via DSL connection.

## 5.2 Importing a Configuration File

On each customer's be.SDx home page, you can download configuration files for their locations once the cloud setup is complete. If you make these files available to the customer or his local employee, they only need to import the file associated with the location in order to take the router into operation. Once the device is authenticated on the platform, it synchronizes its configuration and is then displayed as *Active*.

On-site, the following procedure must be observed:

### 5.2.1 Calling the installation interface

Since the local router is not yet integrated into the network, connect a PC to one of the LAN ports so that the PC receives an IP address via DHCP. If you then open a web browser, you will automatically be redirected to the Installation Wizard home page.

*Do not connect a router in an ex-works state to an existing network. Since a DHCP server is active on the device at this time, this can lead to network problems.*



Logging in is not necessary, as you immediately see a summary of the available connections:



## Welcome


Welcome! We will now guide you through the process of installing your Bintec router.


### Available Internet access interfaces

DSL (Annex B/J)	ETH5	SFP	LTE
			
			


 Not Available

 Available

 Not Available

 Available

 SIM Card Not Detected

 SIM Card Detected

[Start deployment by uploading a file](#)

[Start manual deployment](#)

Green ports are available for connecting to the internet, white ones are not.

## 5.2.2 Uploading a configuration file

Selecting the **Start deployment by uploading a file** option takes you to the next step:



### Upload a configuration file

**Upload a file:**  No file has been selected

Choose rollback mode:

**Manual**     **Auto**

In manual rollback mode, if there is no Internet connectivity when the device restarts after the configuration file (selected above) is uploaded, factory settings need to be restored manually. To do this, please follow the instructions set forth in the installation manual.

**Upload**

**Back**

Select the appropriate configuration file. To be able to load the file into the router, it must be available as a TXT file. If you have a ZIP file, unpack it before uploading.

If the imported configuration does not allow for an Internet connection, you can choose whether to automatically reset the router to its factory settings or perform this step manually (see [Resetting to factory settings](#)). Activate the **Manual** option to avoid an undesired reset if the router into which the file is imported has not reached its final location yet.

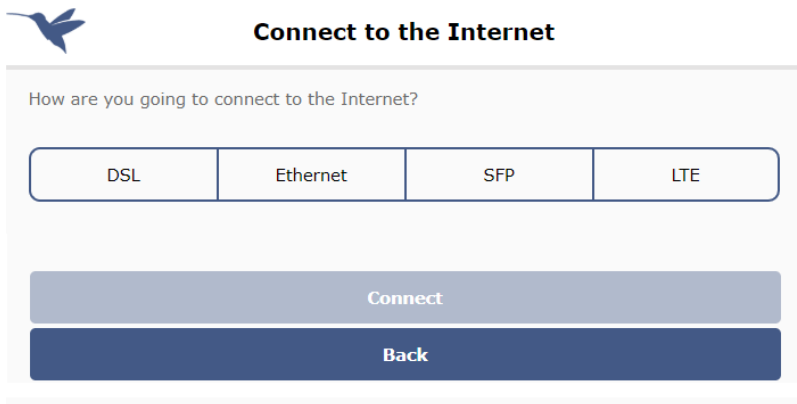
Click on **Upload** - the configuration file is now transferred. If the transfer completes correctly, click on **Save & Restart**. The router restarts in order to activate the configuration and to connect to the platform.

### 5.3 Manually setting up Internet access

Instead of importing a configuration file, you can also establish the Internet connection manually by means of the installation wizard. Select the **Start manual deployment** option found on the start page.

### 5.3.1 Selecting the connection type

Depending on the hardware configuration of the router you are installing, you can connect to the Internet in different ways:



**Connect to the Internet**

How are you going to connect to the Internet?

DSL	Ethernet	SFP	LTE
-----	----------	-----	-----

Connect

Back

Select the type of connection that applies to the location and click on **Connect**.

#### 5.3.1.1 *Internet access via DSL*

If you want to access the Internet over a DSL connection, you only need to enter a few pieces of information:



## Connect to the Internet

How are you going to connect to the Internet?

DSL	Ethernet	SFP	LTE
-----	----------	-----	-----

Please ensure that the DSL cable is plugged.

Choose configuration:

Quick settings     Advanced settings

Country:

Carrier:

Username:

Password:

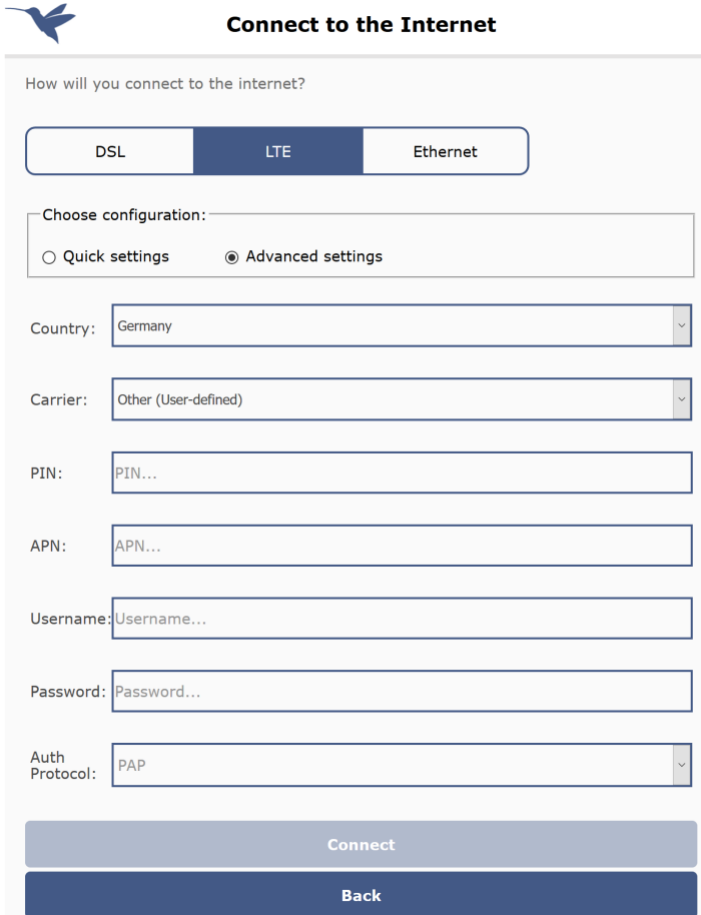
Connect
Back

Select one of the predefined providers here and enter their **login data**.

*If you want to define a custom provider, the wizard switches to advanced setup mode. In this case, you should provide additional information for installation purposes.*

### 5.3.1.2 Internet access via LTE

If the router to be installed has an LTE modem and a SIM card in place, you can also connect to the Internet using LTE:



**Connect to the Internet**

How will you connect to the internet?

DSL   **LTE**   Ethernet

Choose configuration:

Quick settings    Advanced settings

Country: Germany

Carrier: Other (User-defined)

PIN: PIN...

APN: APN...

Username: Username...

Password: Password...

Auth Protocol: PAP

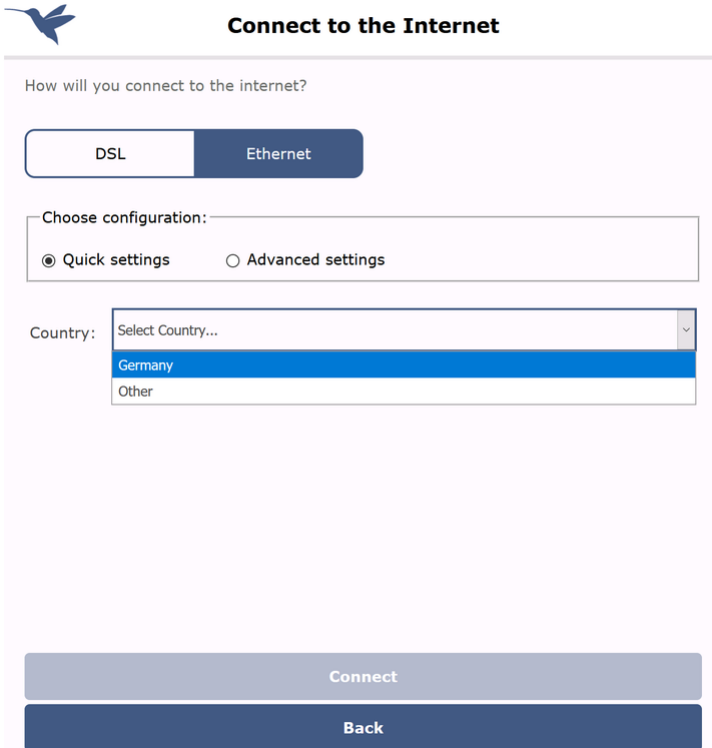
Connect


Back

Here, you must enter the **connection data** belonging to your LTE provider. You will find the relevant information in your mobile data contract.

### 5.3.1.3 Internet access via Ethernet

Finally, you can also connect to the Internet using an upstream modem or router that already exists on-site. In most cases, the configuration of the router to be installed is carried out via DHCP:



 **Connect to the Internet**

How will you connect to the internet?

DSL  Ethernet

Choose configuration:

Quick settings  Advanced settings

Country:

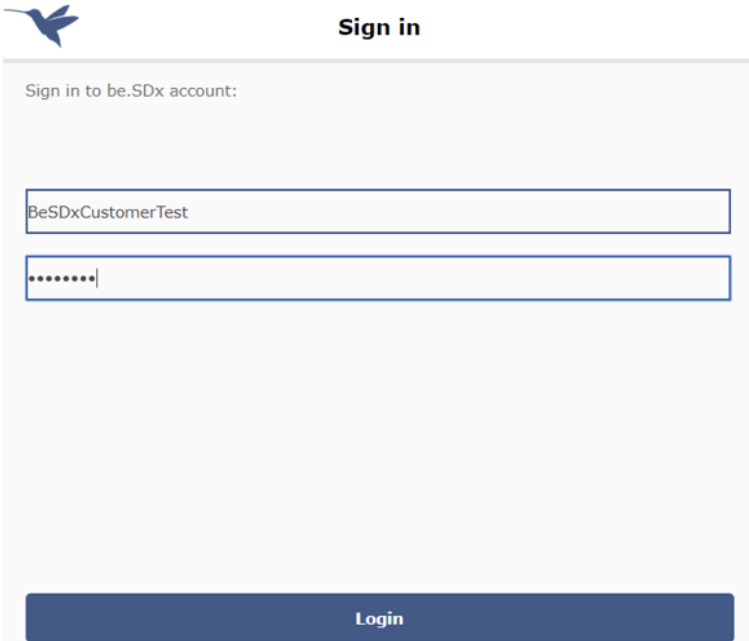
- Germany
- Other

Simply select the **country** of installation and then the *Generic (DHCP)* value under **Carrier**. The router immediately attempts to obtain a configuration via DHCP.

*If a more complex configuration is required, you can switch to advanced setup mode. In this case, you should provide more information for installation purposes.*

### 5.3.2 Authorization at the platform

As soon as the router has successfully connected to the Internet, it also connects to the **be.SDx** platform. Click on **Continue** and you can authorize it by entering the login details of the installer user and clicking on **Login**.



The image shows a 'Sign in' form for a be.SDx account. At the top left is a blue bird icon. The title 'Sign in' is centered. Below the title, the text 'Sign in to be.SDx account:' is displayed. There are two input fields: the first contains the text 'BeSDxCustomerTest', and the second contains seven dots followed by a vertical cursor. At the bottom of the form is a dark blue button with the text 'Login' in white.

Now select the location where you are currently performing the installation. Only those locations are available for which the current router model has been configured.

If the platform provides for automatic authorization, no further action is required. If you have selected authorization by e-mail, an



authorization link will be sent to the e-mail address you have specified.

### 5.3.3 Retrieving the final configuration

Once the router has successfully logged on to the platform, the configuration is synchronized to ensure that it is operating with the latest settings. Click on **Install configuration**. The router downloads the configuration and any available software updates from the platform; then it restarts again and activates the new configuration:



#### Provisioning finalized



Congratulations! Your router has been successfully configured.

The router will now restart and connect to the Internet with your new configuration.

You can close this window.

The router is now displayed as managed on the be.SDx platform.

## 5.4 Potential errors and troubleshooting

### Internet connection not available



#### Connect to the Internet



Oops! Your CNM connection is not available.

#### NETWORK STATUS:

IP Address:	192.168.212.201/22
Unicast Pkts Rcv:	6341
Multicast Pkts Rcv:	899453
Bytes Received:	79559262
Packets Transmitted:	4600
Bytes Transmitted:	609667

Retry

Back

Click on **Retry** to launch a new connection attempt. Click on **Back** to change any necessary parameters and then launch a new connection attempt.

## Deployment Process Failed



### Provisioning failed



Oops! The connection to the server timed out [error 15]

Check your network connection and click the "Retry" button to try provisioning again. If the problem persists, please contact your dealer for further assistance.



Check your network connection status. If you click on **Retry**, the deployment process is restarted. If the error persists, contact your dealer.

## Incomplete Configuration after a rollback (Manual Deployment)



### Configuration not completed



Oops! Something went wrong.

Click the "Retry" button to connect to the Internet. Please check your configuration in CNM or contact your support team before trying zero touch provisioning again.



When you click on **Retry**, the **Check Connectivity** page opens. As soon as an Internet connection is available, the **be.SDx** platform URL is opened in a new tab in order to review and manually fix the configuration problems. If necessary, contact our support team before restarting the deployment process.

## Incomplete configuration after a rollback (when importing a file)



### Configuration not completed



Oops! Something went wrong.

Please click the "Retry" button to use the manual method or to try uploading the configuration file again.



If you click on **Retry**, the **Welcome** page opens. You can either reload a configuration file or configure it manually.

## 5.5 Reverting to factory settings

Sometimes, restoring factory settings may be necessary. To do this, turn off the router and keep the **RESET** button pressed while switching it back on. Release the **RESET** button before the **STATUS LED** stops flashing (after approx. three seconds).

### Please note

If a device is reset to factory settings on site, you may have to make a change to the settings on the be.SDx platform.

Each device authenticates itself on the platform using a certificate which is created when the device is first put into operation and then stored on the router and the platform. The reset deletes this certificate on the router so that it can no longer log on to the platform to synchronize with the settings made there. Depending on how you put the router back into operation on site after the reset, this state will be corrected in different ways:

- You can put the router back into operation by manually setting up Internet access: In this case, the certificate is recreated and synchronized with the platform so that the router can be operated as before and is correctly displayed on the platform.
- You import a previously saved configuration file: In this case, the certificate will not be restored, and the router will be displayed as "not provisioned" on the platform. If the configuration matches the local environment, the router will function, but will not be able to synchronize with the platform.

In the second case, you can heal the situation by calling up the **Devices** menu on the platform and performing the **Replacement** action for the affected router. This causes the router and the platform to exchange certificates again, and the device can be managed as expected.

### Note

You can also completely re-provision a device that has been reset on site using the **Remove** action on the platform. However, you will need to reconfigure it on the platform, which is not necessary when using the **Replace** option.