BAB TECHNOLOGIE GmbH

LINKMODULE Documentation

Version 1.2.0.
Type: KNX/TP, EnOcean
Item no.: 10551, 13551

Manual version IV
As of 01/2016
Date: 8. February 2016

EN

BAB TECHNOLOGIE GmbH

Rosemeyerstr. 14
44139 Dortmund

info@bab-tec.de

Tel.: +49 (0) 231 – 476 425 - 30
Fax: +49 (0) 231 – 476 425 - 59
www.bab-tec.de

TABLE OF CONTENTS

List of figures

1 LINKMODULE

We are happy that you have purchased the **LINK**MODULE and thank you for your trust. The **LINK**MODULE provides a cost-effective and simple way to securely connect remote parts of the facility. Please read this description carefully in order to perform the best possible configuration.

BAB TECHNOLOGIE GmbH

Figure 1: LINKMODULE KNX/TP

Product name:	**LINK**MODULE
Intended use:	Modules for facility coupling via network
Type:	Modular device (Reiheneinbaugerät, REG)
Item number:	10551 (KNX) / 13551 (EnOcean)

1.1 FUNCTIONAL OVERVIEW

The **LINK**MODULE connects remote KNX or EnOcean systems via the network. If this is happening between the BAB devices **LINK**MODULE, EIB**PORT**, **FACILITY**MASTER, this kind of connection can be performed rapidly and securely across network domains. For this purpose, the BAB facility coupling report and BAB **SECURE**LINK have been implemented in addition to a KNXnet/IP Server.

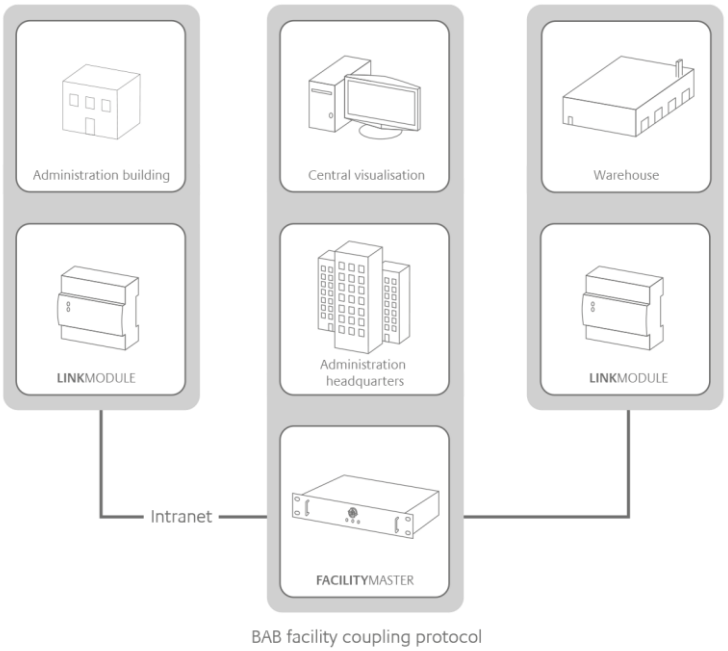


Figure 2: LINKMODULE – Facility coupling with FACILITY MASTER

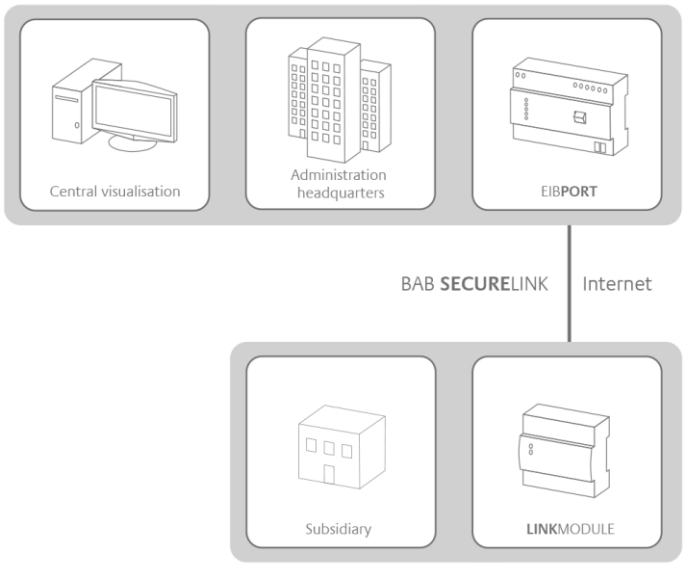


Figure 3: LINKMODULE – SECURELINK with EIBPORT

1.2 TECHNICAL DATA

Technical Data

- Operating voltage: 12-32V
- Typical power consumption 300mA at 12V
- Power consumption: <= 5 W
- Connection: Power supply via screw-type terminal
- Resistant to climate: EN 50090-2-2
- Ambient temperature: -5 to +35°C
- Storage temperature: -10 to +60 °C
- Rel. humidity (non-condensing): 5% - 80%

Mechanical Data

- Assembly: Modular device (REG) housing 4 TE
- Dimensions (W x H x D) in mm: 70 x 90 x 63
- Housing: Plastic
- Degree of protection: IP20 (according to EN 60529)
- Interfaces (depending on version):
  - Ethernet (all types) via RJ45 female connector
  - KNX/TP (type 10551) via pluggable screw terminal
  - EnOcean (type 13551) SMA male connector

Specific Features

- BAB facility coupling and BAB **SECURE**LINK

Software Requirements

- Communication: Network interface
- Browser: Current standard browsers

1.3 SCOPE OF DELIVERY AND INTERFACES

The scope of delivery of **LINK**MODULE includes the following content:

- 1 x **LINK**MODULE KNX/TP or **LINK**MODULE EnOcean
- 1 x enclosed CD

A power supply unit for the device is NOT included in the scope of delivery!

In addition to the terminal for the power supply (**12-32V DC**), the **LINKMODULE** provides the following interfaces:

- 1 x RJ 45; Ethernet 100Mbit/s Full Duplex
- KNX®/TP connection or SMA female connector for EnOcean

FACTORY SETTINGS ON DELIVERY:

IP address:	192.168.1.220
User name:	"admin"
Password:	"admin"

1.4 UPDATES

We reserve the right to offer firmware updates free of charge for the **LINK**MODULE. We will inform you about our new firmware via our newsletter or homepage. The update files are made available in the download section on our homepage.

www.bab-tec.de

1.5 IMPORTANT INFORMATION ON THE OPERATING INSTRUCTIONS

When using these instructions, it must be noted that the software described herein is constantly improved for the benefit of our customers so that the details might possibly not be up to date any more. Information on current **LINK**MODULE firmware and also on this description ("**LINK**MODULE documentation") can be found on www.bab-tec.de.

1.6 FUNCTIONAL SECURITY

If there are specific requirements to avoid risks for persons or property (functional security), additional measures must be taken which are to be considered during planning and executing. When utilising the **LINK**MODULE, there are interactions with other devices/connections which can lead to risks for the system. Failure of individual devices or functions or connections especially can result in the non-function of the system. There are several ways to reduce the risks, depending on the system and the customer requirements.
However, these measures must provide the necessary independence from the system operation (LINKMODULE **with facility coupling) and be constantly available.**

2 ASSEMBLY

The operating voltage of the LINKMODULE is 12-32V DC

The device presented here is the **LINK**MODULE KNX/TP, modular device (REG) housing 4 TE. Dimensions (width x height x depth): 70 x 90 x 63 mm

- In order to be able to connect the power supply comfortably, the pluggable screw terminals (see figure below) are removed.
- Now, the power supply cables are connected to the pluggable screw terminals (see figure below). In doing so, the **polarity** must be considered:

  (Left: plus (+), right: minus (-)).
- Now, the pluggable screw terminals can be reconnected to the **LINK**MODULE.
- The device can then be snapped onto the mounting rail according to DIN EN 60715.

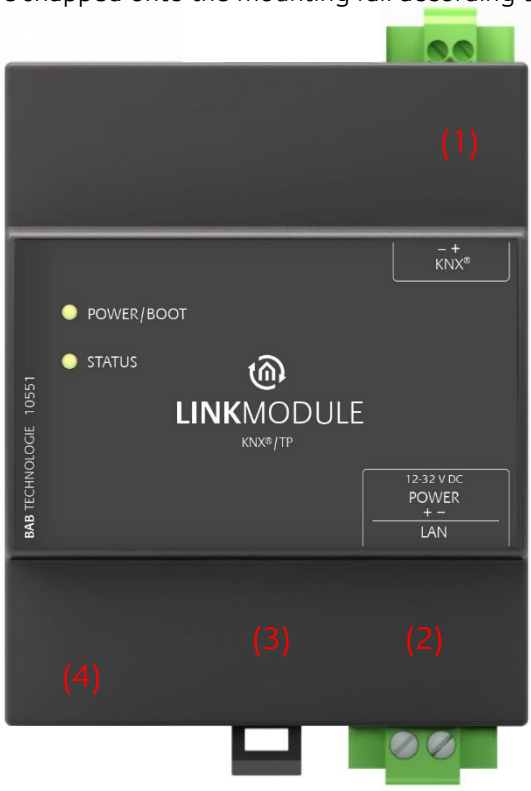


Figure 4: LINKMODULE terminal diagram

	LINKMODULE terminals
(1)	KNX/TP connection (type 10551) via pluggable screw terminal
(2)	Power supply via screw pluggable screw terminal 12-32V DC
(3)	USB terminal
(4)	RJ45 female connector for Ethernet LAN

2.1 LED STATUS

The **LINK**MODULE has two DUO LEDs ("Power/Boot" and "Status"). Each DUO LED provides a green and a red LED. The top LED is the Power/Boot LED, the bottom LED is the Status LED.

POWER / BOOT LED

LED display	Status
OFF	The device is not ready for operation. No operating voltage is supplied.
GREEN	The device is ready for operation.
FLASHING ORANGE	The device is booting.

STATUS LED

LED display	Status
OFF	The device is booting.
FLASHING GREEN	The device has started; the LED simulates a "heartbeat". The flashing interval increases depending on the device workload.
FLASHING RED	Communication takes place via KNX.

Explanation:
The green "Power/Boot" LED lights up as soon as the **LINK**MODULE is supplied with power. Two to three seconds after the power supply has been switched on, this LED also starts to flash red (flashing orange) until the booting process has been completed. Then, the LED is continuously illuminated green while the "Status" LED flashes green (simulating a "heartbeat"). The flashing frequency increases depending on the workload of the device.

It takes approx. **2 minutes** for the **LINK**MODULE to start.

2.2 INITIAL OPERATION

When the **LINK**MODULE has been assembled and started as described in chapter "Assembly", initial operation can now be performed as specified below.

Factory setting on delivery:

IP address	192.168.1.220
Subnet mask	255.255.255.0
User name	admin
Password	admin
Device Name	LinkModule

Note: The password must be changed immediately when logging in for the first time. If the password is lost, the device cannot be reset!

2.2.1 LANGUAGE

The language of the **LINK**MODULE interface depends on the language set in the browser. For the **LINK**MODULE, German and English are available.

2.2.2 SYSTEM REQUIREMENTS

In order to configure the device as requested, the following system requirements are necessary:

- A current browser (e.g. Firefox, Chrome, Safari etc.)
- Network and network cable
- Power supply via pluggable screw terminal
- A remote device with KNXnet/IP routing or BAB facility coupling enabled which is accessible via network
- Local connection to KNX or EnOcean system

2.2.3 ESTABLISHING CONNECTION

If the device is in delivery condition (see above), it can be accessed via the IP address mentioned above and the network settings must be adjusted to the address range if necessary. For this purpose, please refer to chapter "Adjusting the network settings of your computer". If you do not know the network settings of the device, the "DiscoveryTool" can help you to find out at which IP address the device is available (see below).

2.2.3.1 DISCOVERYTOOL

The "DiscoveryTool" software is platform-independent and can be run on any operating system. It can be found on the supplied CD or in the download section at www.bab-tec.de.

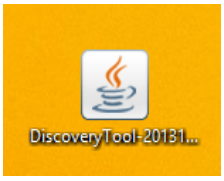


Figure 5: DiscoveryTool icon

Double-click the program icon to start the software. All devices available in the network are shown in the program window including device name and serial number. A **LINK**MODULE can be recognised by means of a serial number starting with "BT126*"(KNX/TP) and „BT136*“(EnOcean).

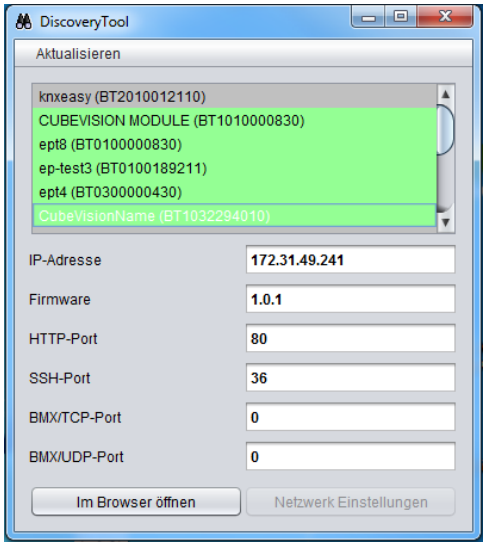


Figure 6: DiscoveryTool

The colour marking of the devices in the DiscoveryTool has the following meaning:

- Grey = Information is being retrieved
- Green = Device is within the same network area as the PC
- Yellow = Device is NOT in the same network area as the PC

Mark the required device in the list. The available device information is displayed in the fields below. If the device is marked green, you can immediately call up the start page of the device by pressing the "Open in browser" button. If the device is marked yellow, change the network settings of your PC correspondingly (see following chapter).

2.2.3.2 ADJUSTING THE NETWORK SETTINGS OF YOUR COMPUTER

In order to adjust the network settings of your computer and establish a connection to the device, please proceed as follows:

- Open the IP address settings (in Windows 7):
- Click "Start Button" --> "Control Panel" --> "Network"
- Select "Network Connection", then "LAN Connection" ("Intel PRO1000 GT" in the figure below).

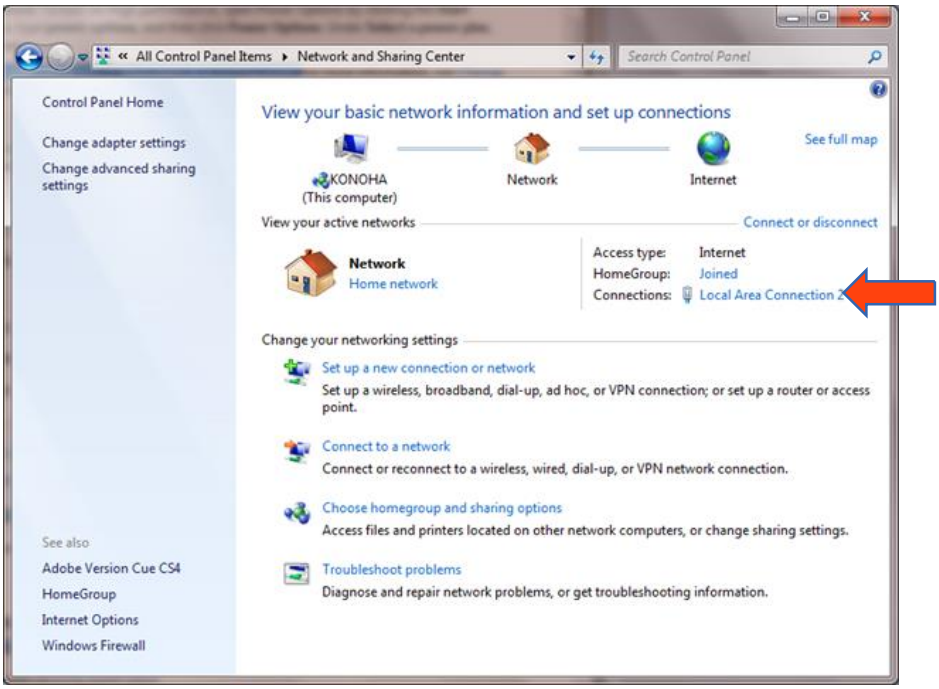


Figure 7: Windows - Network and Sharing Center

- Then click "Properties":

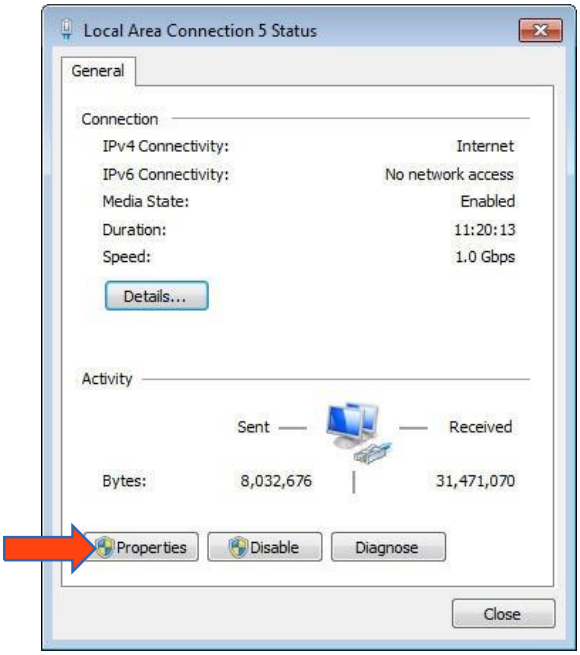


Figure 8: "LAN Connection" status

- Select "Internet protocol Version 4 (TCP/IPv4)" and click on "Properties" again:

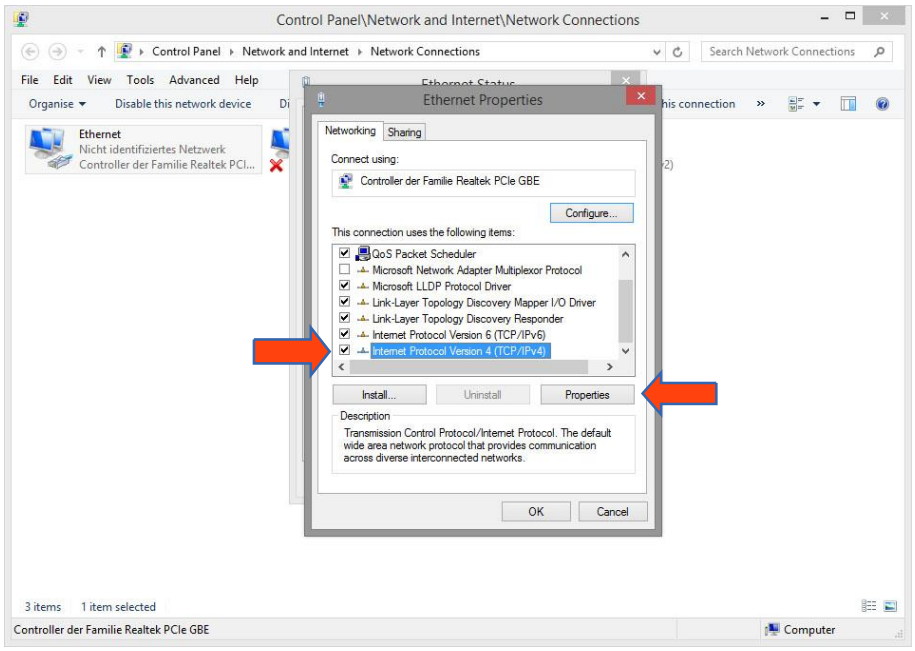


Figure 9: LAN Connection Properties

- Now note down the current IP address settings or take a screenshot in order to ensure that you can reset the IP address setting after configuring the **LINK**MODULE.
- Now change the IP address settings (IP address and subnet mask) as required:

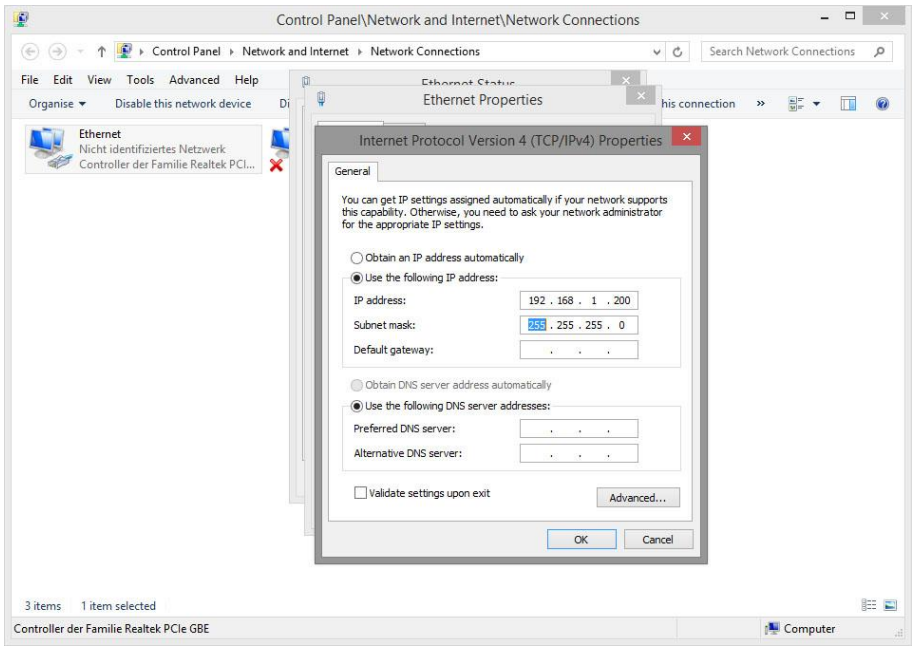


Figure 10: TCP/IPv4 Properties

Example of a valid configuration with factory settings of the **LINK**MODULE:

- Free IP address: 192.168.1.230
- Subnet mask: 255.255.255.0
- Now confirm your input with "OK".
- Close all windows until the "Windows Network and Sharing Centre Settings" window is shown.

Thus, you have adjusted the network settings of your PC to those of the **LINK**MODULE. The **LINK**MODULE web interface can be accessed via the browser. Restore the original network settings of your PC by following the steps described above as soon as you have configured the **LINK**MODULE correspondingly.

When the IP address of your PC and your **LINK**MODULE are placed in the same network mask, you can continue the configuration.

2.2.3.3 LOGIN

Now open your internet browser and enter the IP address into the address field (**on delivery 192.168.1.220**).

The web interface starts. In order to get full access, initially click "Login".

The login window opens, enter "**admin**" as the user name and "**admin**" as the password to log in.

Note: The password must be changed immediately when logging in for the first time. If the password is lost, the device cannot be reset!

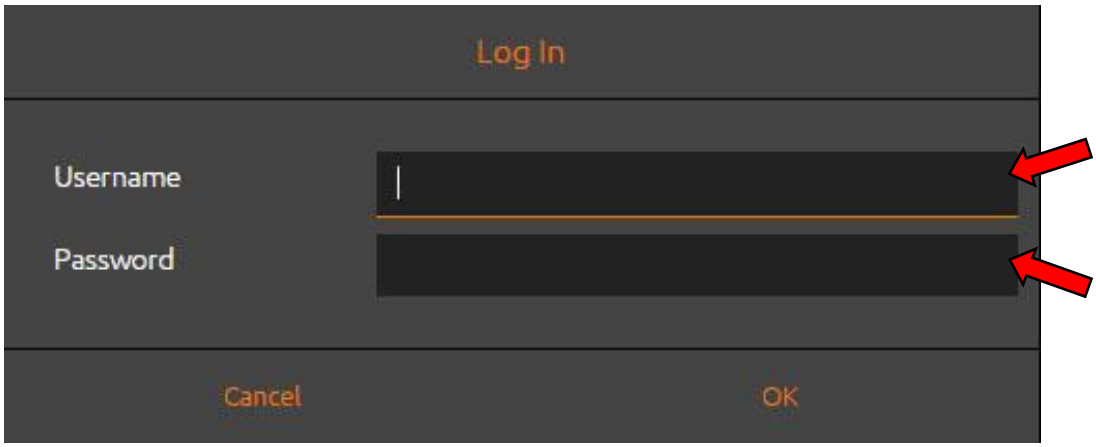


Figure 11: Login

The **LINK**MODULE menu with 6 configuration menus appears:

- VPN Server
- BAB **SECURE**LINK
- Facility coupling
- Configuration
- Information
- Logout

2.2.3.4 ADJUSTING THE NETWORK SETTINGS OF THE LINKMODULE

In order to modify the IP address of the **LINK**MODULE, click "Configuration"

Figure 12: LINKMODULE start menu

The configuration menu opens, the network settings are performed in the menu item "Network".

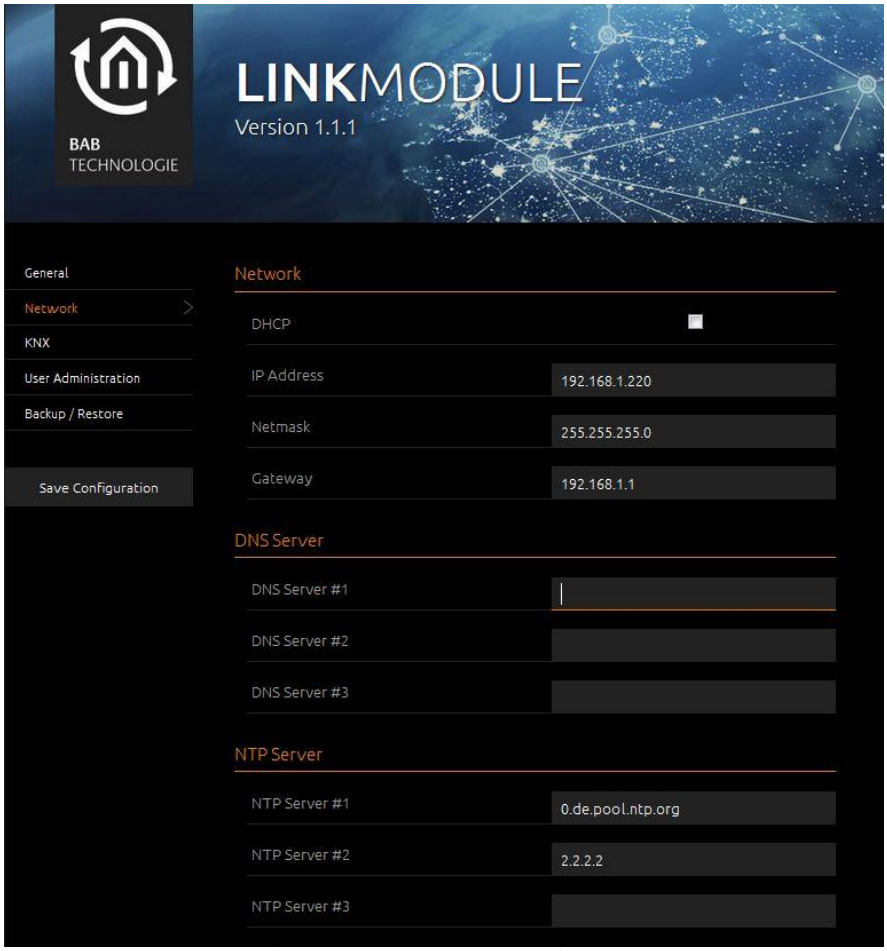


Figure 13: LINKMODULE Network menu

Now adjust the IP address to your network environment. When you have modified your IP address and you want it to be saved, click the "Save Configuration" field. In order to reconnect with the **LINK**MODULE web interface, your computer will again need the former IP address or the IP address corresponding to your current address space of the **LINK**MODULE (chapter "Adjusting the network settings of your computer").

Note: In order to browse the LINKMODULE now, you must enter your new IP address

DHCP: (Dynamic Host Configuration Protocol)
If DHCP is active, the device automatically obtains the network settings. For this purpose, the availability of a DHCP server in the local network is mandatory.

IP address / network mask / gateway:
If DHCP is not active, the network settings must be carried out statically. In case of doubt, contact your network administrator as to which settings are to be carried out. Please note that an IP address may never be assigned twice!

DNS server:
DNS is the abbreviation for Domain Name System. The DNS server converts Internet addresses, for example "www.bab-tec.de", into the IP address "85.214.89.170" and vice versa. Without a valid DNS entry, NTP, weather services from the Internet and UPnP do not work.

NTP server:
NTP is a free service for synchronising the system time of Internet-compatible devices. If time synchronisation is not possible, please check the system time from time to time in the "General" menu item.
NTP server list: e.g. http://www.pool.ntp.org/zone/europe

2.3 INITIALIZING VPN SERVER

In order to create a **SECURE**LINK connection between LINKMODULE; EIBPORT or **FACILITY**MASTER or to be able to access the device from a computer via VPN connection, a prior initialisation of the VPN server is required. In this regard, please note chapter "VPN Server / BAB **SECURELINK**".

2.4 LINKMODULE KNX/TP

For a **LINK**MODULE KNX/TP (item no. 10551) you open the menu "Configuration" – "KNX" in order to call up the KNX/TP configuration. In addition to the KNX configuration, the KNX interface of the device can also be tested here.

Note: Please check if KNX/TP is correctly connected to the device.

KNX INTERFACE (TYPE 10551)

Physical address:	Indicate the physical address of your **LINK**MODULE here.
KNXnet/IP tunnelling address:	Enter the address used for your KNXnet/IP tunnelling connection here. This address(es) are virtual addresses and may not be assigned a second time nor coincide with the physical (real) address of the LINKMODULE
KNXnet/IP routing:	Activates KNXnet/IP Routing in the **LINK**MODULE. **Note: This function can only be activated if the physical (real) address is a line or area linking address.**
KNXnet/IP tunnelling:	Activates KNXnet/IP tunnelling in the **LINK**MODULE

- Click on "Save Configuration" in order to accept the settings.

TEST INTERFACES

KNX address	Enter the group address you want to perform the test with here
Switching KNX address	By clicking "On/off", the address given above will be switched
Reading out address status	When clicking on "Status Query", a pop up window with the current status information about the group address given above will appear

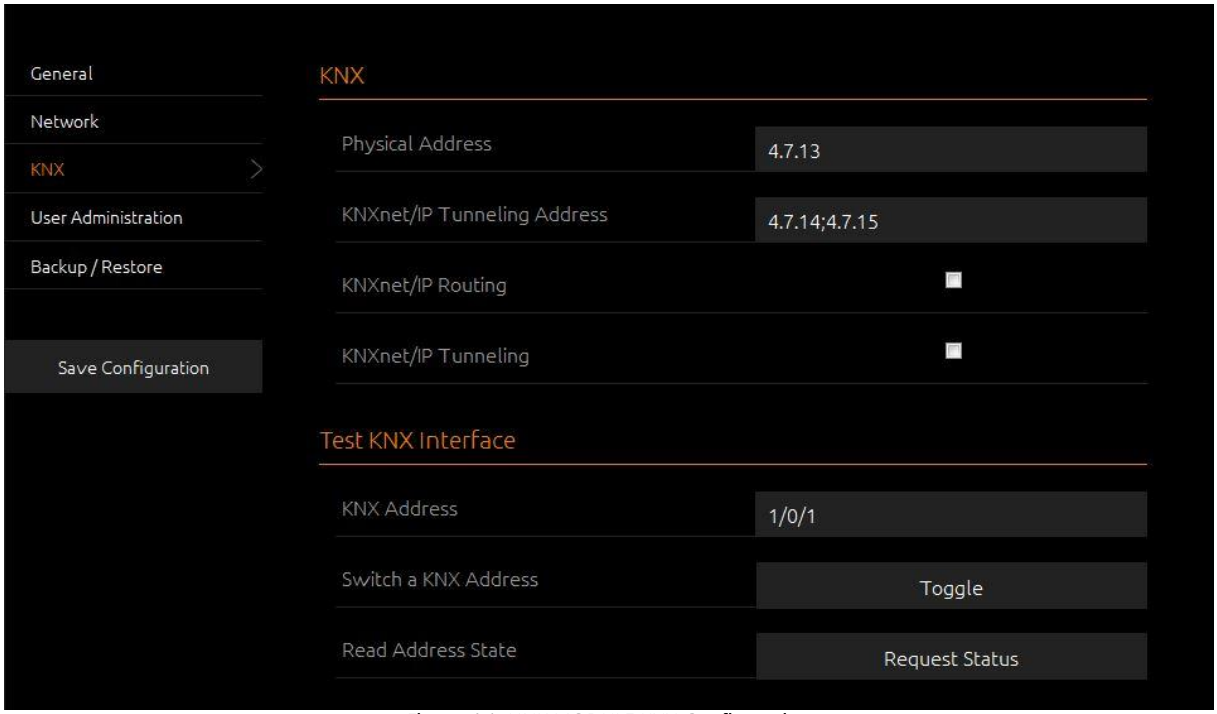


Figure 14: LINK MODULE KNX Configuration

2.5 LINK MODULE ENOCEAN

EnOcean is a radio system for buildings which, due to so-called "energy harvesting", doesn't require batteries and utilizes ambient energy, and is therefore low in maintenance and reliable. With this features, an EnOcean solution is very flexible and simultaneously cost-effective, which makes it the perfect solution for retrofitting.

Note: Please check if the magnet base antenna is correctly connected to the SMA female connector.

2.5.1 TECHNICAL DETAILS ENOCEAN INTERFACE

EnOcean (868 MHz):

Operational frequency:	868.3 MHz
Range: (depending on construction material)	300 m in open areas / 30 m in buildings
Input objects:	Any number
Output objects:	128
External antenna:	2.50 m cable, magnet base and SMA male connector.

2.5.2 OPERATING PRINCIPLE ENOCEAN

An EnOcean radio network consists of sensors and actuators. The sensors utilize your ambient energy to transmit the corresponding radio signal. So that an actuator can interpret and respond to the signals of a sensor, the actuator must be adapted to the sensor. The so-called EnOcean Profiles (EEP) determine how the data provided by the sensor are to be interpreted. Thus, it is important that sensor and actuator utilize the same EnOcean Profile (EEP).

Device categories / sensors
EnOcean distinguishes between three device categories in its sensor technology. The device category gives information about the kind of EnOcean signal involved and simultaneously about what the receiver can expect.

- Switch module: A module which sends out a corresponding radio signal via user interaction. That is switches, rockers, position and key card switches as well as window handles.
- 1 byte sensor: A sensor which sends out information of 1 byte size.
- 4 byte sensor: A sensor which sends out information of 4 byte size.

Actuators
Actuators will perform their controlling on the basis of sensor signals. Therefore, sensor and actuator have to be adapted to each other. Thus, it is important to know which EnOcean profile is to be emulated to address a LINKMOUDULE actuator correctly. The actuator manufacturer will inform you about which profile the actuator utilizes.

EnOcean Profiles (EEP)
The EnOcean profiles (EnOcean Equipment Profile - EEP) define the device category, the function and the device specification. During the **LINK**MODULE configuration, the KNX parameters automatically adapt to the selected profile. The profile consists of 3 number pairs separated by a hyphen:
XX-XX-XX

The different positions represent the following:
ORG-FUNC-TYPE

- ORG determines which messages form the communication base (see also 'Device categories/sensors').

- FUNC determines which device is involved, that is e.g. a switch or a temperature sensor.
- TYPE determines the exact specifications of the device functionality.

Transmitter ID (Trans. ID)
Is a definite device address which only exists once. This address allows the sending device to be identified.

Teaching Telegram / LRN Telegram
Is a special telegram used to "teach" the sensor to recognize the actuator, that is, to adapt the actuator to the sensor. It is important for the actuator to know from which hardware address it gets its sensor data. There are several kinds of adapting mechanisms. Please consider the respective descriptions.

2.5.3 ENOCEAN CONFIGURATION

The **LINK**MODULE internally works with the KNX group address system. In order to continue to use received EnOcean signals within the device or to trigger EnOcean telegrams, KNX group addresses must be used. You will find information about this in chapter "KNX Addressing".

2.5.3.1 ENOCEAN CONFIGURATION

In order to access the corresponding **LINK**MODULE configuration mask, open the menu "configuration" – "EnOcean Editor". Java Applets must be able to be started (please note also the indications in chapter "EnOcean Editor"). The window generally consists of 3 areas:

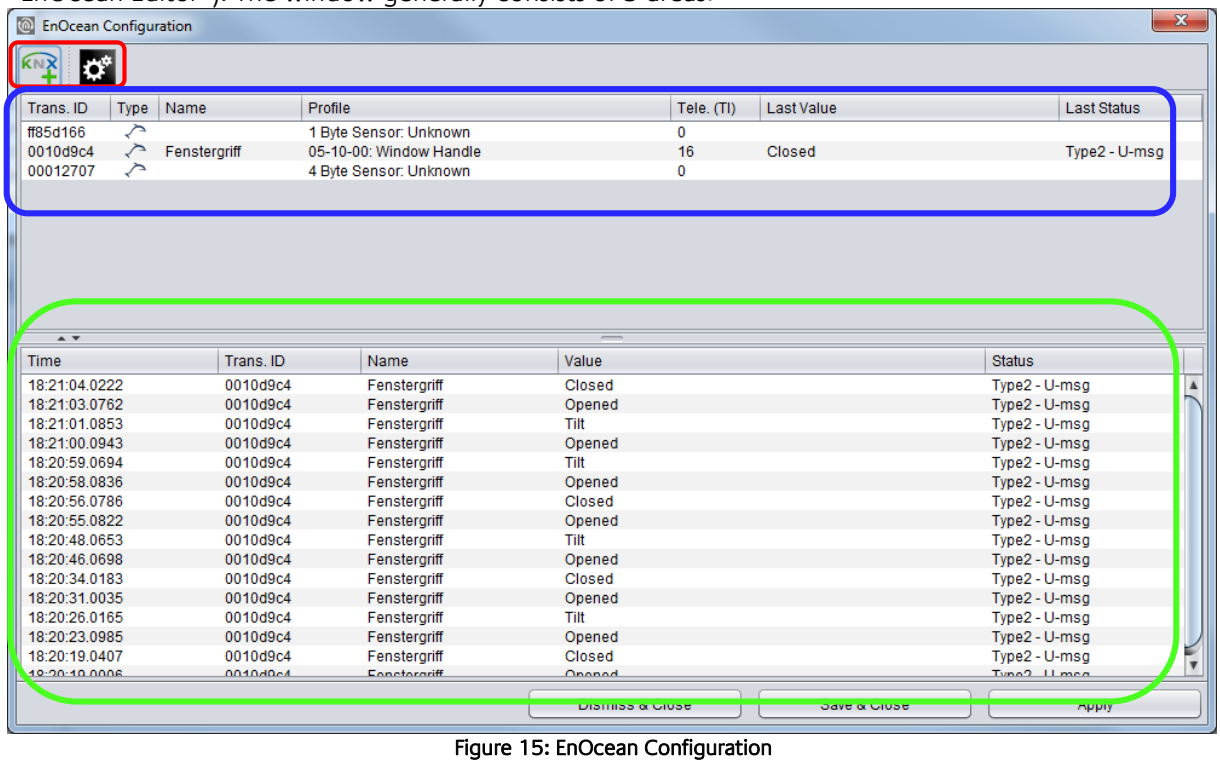


Figure 15: EnOcean Configuration

- (Red) *Configuration Menu*: Basic settings of the EnOcean module are adjusted here and the EnOcean devices are emulated.
- (Blue) *Device List:* All EnOcean devices are ordered and listed here in the order of their device ID (Trans. ID).
- (Green) *Telegram List:* All received EnOcean telegrams are listed here in the order of their arrival time.

Additionally, at the bottom of the window there are the action buttons available for securing or discarding the settings.

2.5.3.2 ENOCEAN SETTINGS

The EnOcean settings show the hardware parameters of the incorporated EnOcean module (TCM 300 Transceiver). The following settings can be performed:

Figure 16: EnOcean Settings

EnOcean active
Here, you can switch the module on or off.

Repeater
The repeater function is used to repeat a receiving signal in order to increase its range. The following settings are available:

- *Off:* Repeater function is turned off.
- *Level 1:* The telegram is repeated by one repeater only.
- *Level 2:* The telegram is repeated by two repeaters.

RX sensitivity
Determine the receiving sensitivity in which you want the EnOcean module to work. You can choose between "Low" and "High".

2.5.3.3 ADAPTING THE ENOCEAN DEVICE

All EnOcean devices within range are displayed both in the device list and in the telegram list as they are sending something. As already mentioned, the EnOcean telegram must be connected with a group address in order to make it usable for the LINKMODULE. This is done as follows:

1. Mark the device of interest in the device list.

Advice: If you are not sure which device has which Trans. ID, activate the device of interest and look up in the device list for which device the telegram counter increases (column "telegrams").

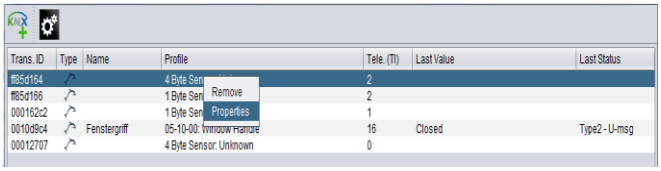


Figure 17: Calling up properties

2. When you have detected the device of interest, mark it with the mouse, press the right mouse button and click '*Properties*'. Alternatively, double-click on the device.

3. The window "*EnOcean Device Configuration*" will open. Via this dialogue, the EnOcean devices will be "adapted.

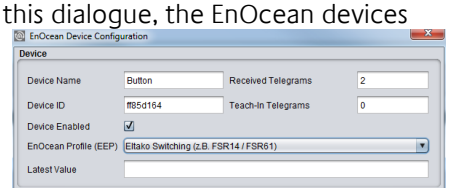


Figure 18: EnOcean Device Configuration

4. Initially, assign a definite "*Device Name*", referring to the device function. In the input screen, you will further find the following parameters:

- *Device ID:* This is the unique device address through which the device is identified.
- *Received Telegrams:* Here, the number of telegrams already received by the **LINK**MODULE from this device is counted.
- *Teach-in Telegrams:* If the device should send teach-in telegrams, their number is shown here.
- *Device Active:* If you would like to keep the device in the EnOcean configuration without using it, you can deactivate it for the **LINK**MODULE usage via this option.

- *EnOcean Profile (EEP):* The different EnOcean devices are defined via so-called profiles. Hereby, the device category involved is detected as early as at the signal input and a pre-selection is made. Then it is also possible to select from the profiles known from the LINKMODULE. As soon as a profile is selected, the corresponding KNX parameters are shown underneath.
- *Last Value:* This field interprets the payload of the last radio signal from this device ID according to the selected profile. If there is no profile selected, the crude data are shown.

5. Select the corresponding profile of your EnOcean device. If you are not sure about which profile your device 'speaks', please contact the manufacturer of the device. After the right profile has been selected, one or more input fields appear in the "*Parameters*" area:

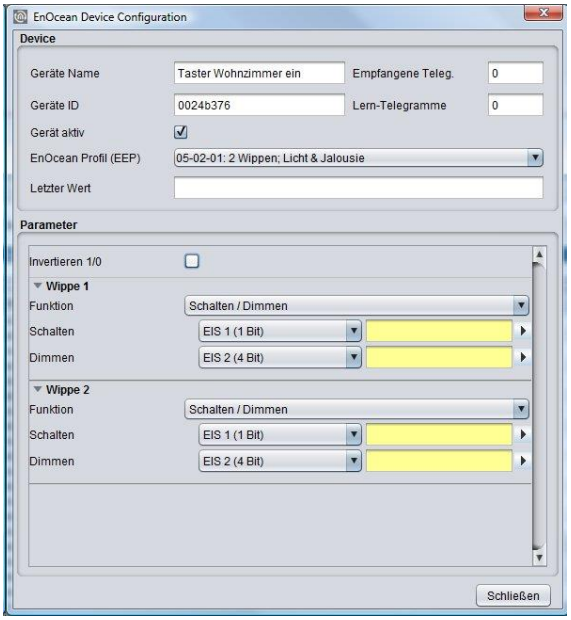


Figure 19: EnOcean Device Configuration

Different parameters appear depending on which profile has been selected. If one switch (rocker) has been selected, various additional functions can be carried out (see chapter "Configuration example for EnOcean button").

6. Now, enter the corresponding KNX group addresses in the address fields to obtain a connection to the selected EnOcean device. You will find detailed information about the KNX group addresses and their assignment in chapter "KNX Addressing".

7. When you have entered the addresses in the parameters as requested, close the *EnOcean Device Configuration* window.

8. Save the changes in the window "*EnOcean Configuration*" via the button „*Save & Close*“ or "*Assume*" (the window stays open).

As soon as this step is taken, the entered KNX telegrams are triggered via EnOcean signals. In order to be able to use the addresses more easily later, you should enter them into the ESF data with a definite designation (see Chapter "KNX Addressing")

2.5.3.4 EMULATING ENOCEAN DEVICES

The **LINK**MODULE provides a Transceiver Module which not only permits receiving but also sending EnOcean telegrams. In order to do this, the **LINK**MODULE emulates an EnOcean device. Via a configuration mask, you can determine which device is emulated with which KNX telegram by the **LINK**MODULE (the device internally works with KNX group addresses also during the EnOcean execution).

Assigning a new emulated device
In order to assign a new device, please click the KNX logo in the configuration menu ("*Editor*" > "*Extras*" > "*EnOcean Configuration*"). Thus, a window designated "*New Emulated Device*" will open.

In the upper half of the window, you will be asked to choose a hardware address. The address is unique and 128 different addresses can be assigned in total. If a device has already been assigned, the device name is highlighted in red on the ID list.

Selecting the device category
Depending on which actuator is to be controlled by EnOcean, the appropriate device category has to be selected. Additionally, the appropriate profile can be preselected directly beneath the corresponding category. By confirming with "*OK*", the settings will be confirmed and the "*EnOcean Device Configuration*" window will open.

Defining emulated device ("EnOcean Device Configuration")
The device assigned in this way is initially provided with a definite device name. Additionally, the following parameters are presented (see also chapter "Example: Emulate temperature sensor")

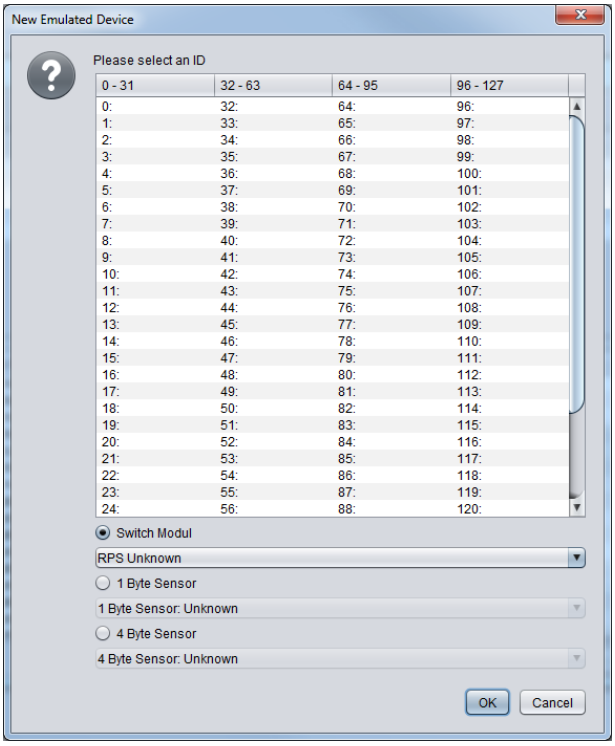


Figure 20: Emulating EnOcean device

- *Device ID:* Is the definite hardware address you have selected before. Can not be modified at this point.
- *Received Telegrams:* Shows the number of telegrams already received from this hardware address. In an emulated device, this number should generally be "0".
- *Teaching Telegrams:* Shows the number of "teaching telegrams" already sent from this hardware address.
- *Device Active:* If you would like to keep the device in the EnOcean configuration without using it, you can deactivate it for the **LINK**MODULE usage via this option.
- *EnOcean Profile (EEP):* Here, the profile the emulated device should use is selected. The profile settings depend on the actuator to be communicated with. If the profile is unknown, the manufacturer of the actuator can provide information.
- *Last Value:* This field interprets the user data from the last telegram according to the selected profile or simply displays it.

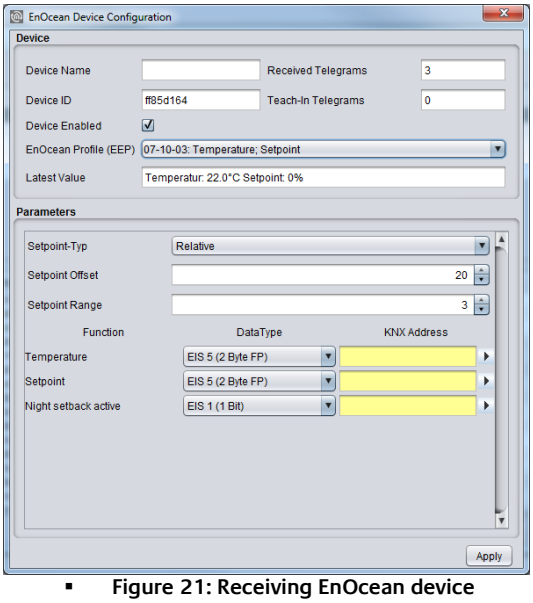
After all settings have been performed as requested, continue with the corresponding KNX parameters in the lower window section. These comply with the profile and are sent as KNX telegrams when there has been an EnOcean signal detected at receipt.

EXAMPLE: EMULATE TEMPERATURE SENSOR

Profile
"07-10-03 temperature, target value" is selected as the profile.

Parameters
According to this profile, the following parameters are available:

- *Basic Target Value:* Enter the basic target value for the actuator here. 20°C are preselected.
- *Maximum Target Value Modification:* Enter the maximum value in °C to modify the target value here. 3°C are preselected here.
- *Temperature:* Enter the group address transmitting the current temperature value (data type EIS 5) here.
- *Target Value:* Enter the group address to modify the absolute target value (data type EIS 5) here
- *Sending Teaching Telegram:* When the corresponding actuator is in the "learning" mode, the emulated sensor can be adapted via this trigger.



- **Figure 21: Receiving EnOcean device parameters**

When all parameters are set as required, close the window "EnOcean Device Configuration" and save your settings via the "Save & Close" or "Accept" button.

2.5.4 KNX ADDRESSING

The **LINK**MODULE addressing concept is based on the group addressing of the KNX system. Sending EnOcean Telegrams as well as transmitting received telegrams is performed based on KNX group addresses only. The KNX group address is a 16 bit address which is split in a so-called 'real' and a 'virtual' section. Additionally, there is a 2-digit as well as a 3-digit representation:

3-digit:
MG= Main Group / CG= Central Group / SG= Subgroup
MG / CG / SG

2-digit:
MG= Main Group / SG= Subgroup
MG / SG

Note: The LINKMODULE interface only supports the 3-digit representation.

Real / Virtual Address Space
The KNX address space ranges in total from 0/0/0 to 31/7/255 (in the 3-digit representation). Therein, the range from 15/7/255 is designated as real address space and the address space from 16/0/0 to 31/7/255 as virtual address space.

Note: For the communication between EnOcean and KNXnet/IP routing, only the real address space is used.

2.5.5 CONFIGURATION EXAMPLE FOR ENOCEAN BUTTON

In the following, an exemplary configuration for sending and receiving of an EnOcean button profile (profile "*05-02-01: 2Rockers, Light & Blind*") is shown.

2.5.5.1 LINKMODULE AS THE RECEIVER (ACTUATOR)

This switch provides either one or two rockers and transmits their status within a radio signal. In order to link these radio signals with KNX, various functions are available:

- *Switch / Dim:* The EnOcean push button can be used as a switch and as a dimmer. Thereby, a long keystroke is interpreted as a dim command.
- *Push Button:* When pushing the button, an EIS 1 telegram of the value 1 is triggered. When 'letting go', a telegram of the value 0 is triggered. One address can be assigned per position respectively (I and O).
- *Switch:* When pushing the button, the status is only changed once; either a 1 or a 0 is sent.
- *Blind:* For the "Move" and the "Step" commands, there is one address entered respectively (EIS 1).

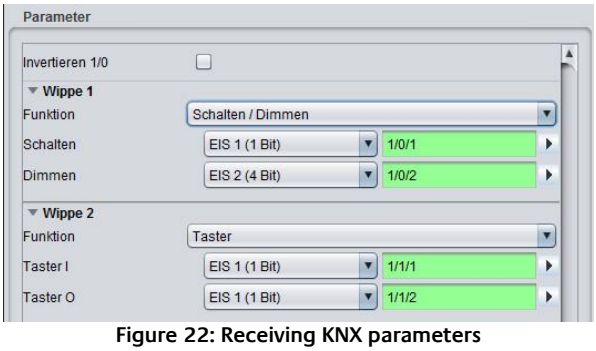


Figure 22: Receiving KNX parameters

Additionally, the output to the KNX addresses can be inverted. In this case, the actual output "1" becomes "0" and vice versa.

2.5.5.2 LINKMODULE EMULATES ENOCEAN PUSH BUTTON

When the profile mentioned above is emulated by the LINKMODULE, the parameter screen looks slightly different. The "switch" is missing as this function can not be carried out with EnOcean.

Functions

- *Switch / Dim:* There is one switch and one dim address for each rocker. The information on if it was switched or dimmed is sent in the KNX via different group addresses.
- *Push Button:* For the button, there is one address for the value "0" and one for the value "1". At reception on the respective input object, the corresponding EnOcean signal is transmitted.
- *Blinds:* The blind control also consists of two EIS 1 objects. One is for the 'Move' command ("1"), the other one for the 'Step' command ("0").

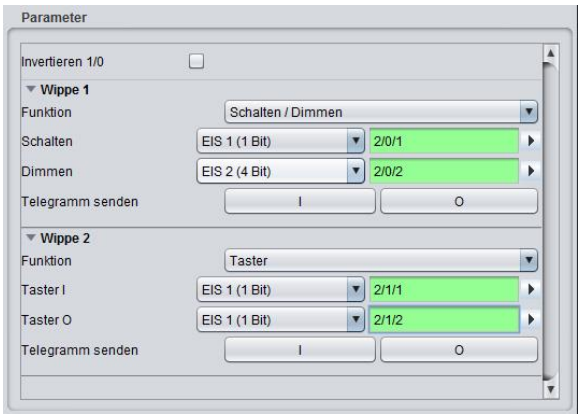


Figure 23: Sending KNX Parameters

Sending a Telegram
These buttons may be used to adapt the emulated device to the actuator of interest. These two buttons simulate the respective rocker directly from the EnOcean configuration.

Inverting
The respective EnOcean output values are inverted. The "1" becomes a "0" and vice versa.

3 VPN SERVER / BAB SECURELINK

The **LINK**MODULE provides an integrated VPN server, which may be used for two functions:

- Establishing a BAB **SECURE**LINK connection (device acts as VPN Client) to other BAB devices (LINKMODULE, EIB**PORT**, **FACILITY**MASTER)
- VPN server for a secured connection between PC and **LINK**MODULE via an OpenVPN client

In order to be able to use the functionalities, it is important for the integrated VPN server to be initialized after initial operation, see below:

3.1 INITIALIZING VPN SERVER

In order to use the VPN relevant services (BAB **SECURE**LINK, VPN server) in the **LINK**MODULE, the VPN server must be initialized once. In order to do this, click "Start Basic Configuration" in the "VPN Server" menu.

Figure 24: Initializing VPN Server

Note: The initialization takes approx. 10 minutes. During this time, the required certificates are produced. Please leave the browser window open until the configuration has been established successfully.

3.2 VPN SERVER

When the VPN server has been initialized successfully (see above), the VPN server settings will be displayed.

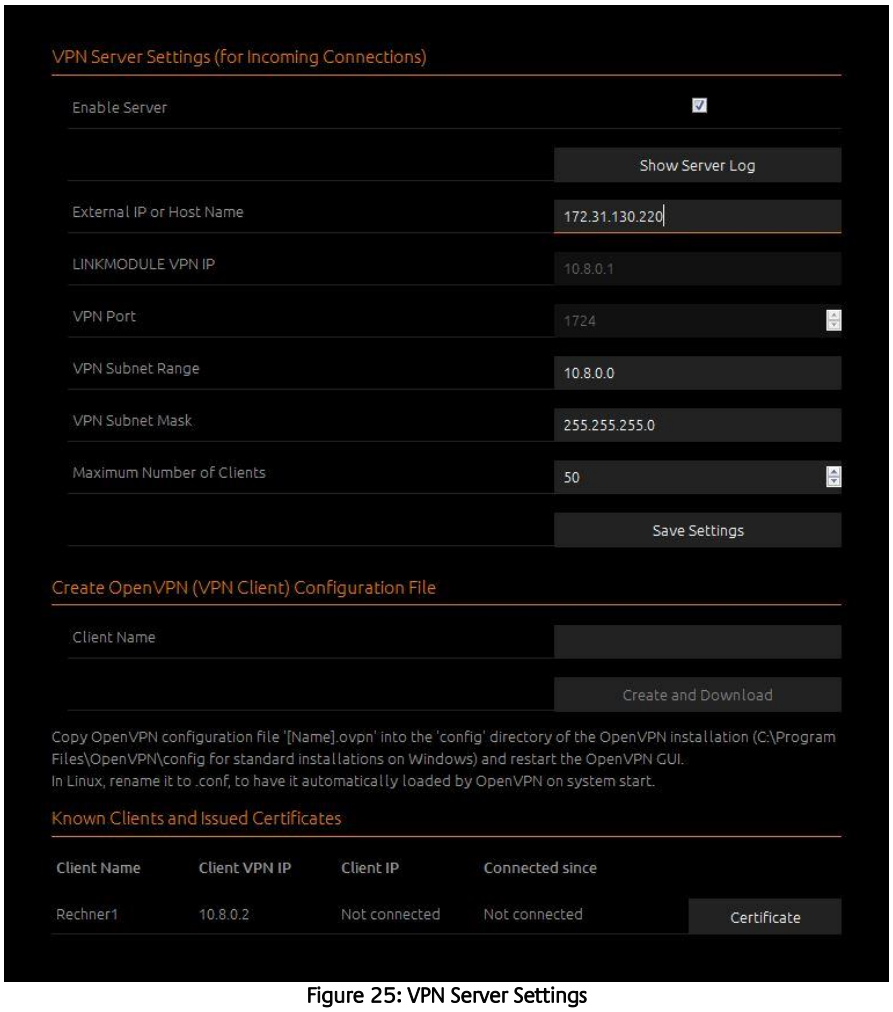


Figure 25: VPN Server Settings

VPN SERVER SETTING (FOR INCOMING CONNECTIONS)

In order to configure the VPN server for incoming connections, the following parameters are available:

- *Activating VPN Server:* VPN server is only activated by ticking the box.
- *Display Server Log:* "CLIENT LIST", "ROUTING TABLE" and "GLOBAL STATS" are displayed.
- *External IP Address / Host name:* Please enter the address under which the **LINK**MODULE is externally reachable here. If the incoming connection (a VPN client trying to connect to the server) is coming from the same network, the local IP address of the **LINK**MODULE has to be entered here. If the connection comes from outside the network, the external address of the respective network must be used (e.g. the external IP address of the DSL router).
- **LINK**MODULE *VPN IP:* Indicates the IP address the **LINK**MODULE has within the VPN network.
- *VPN Port:* Determines the port number on which the VPN service communicates.
- *VPN Subnet IP Section:* Determines the IP section in which the VPN network is established (10.8.0.0 is preset).
- *VPN Subnet Mask:* Determines the subnet section of the VPN IP section (255.255.255.0 preset).
- *Maximum Number of Clients:* This amount determines how many VPN clients can connect to the server.
- *Save Settings:* Saves the settings.

Note: The VPN server is only active when "Activate VPN server" is marked and the settings have been saved.

ESTABLISH OPENVPN (VPN CLIENT) CONFIGURATION FILE

Helps to create a VPN connection between computer and **LINK**MODULE. The VPN required connection settings are summed in an OpenVPN configuration file and saved on the local computer. OpenVPN is a free software for establishing VPN connections for almost all operating systems.

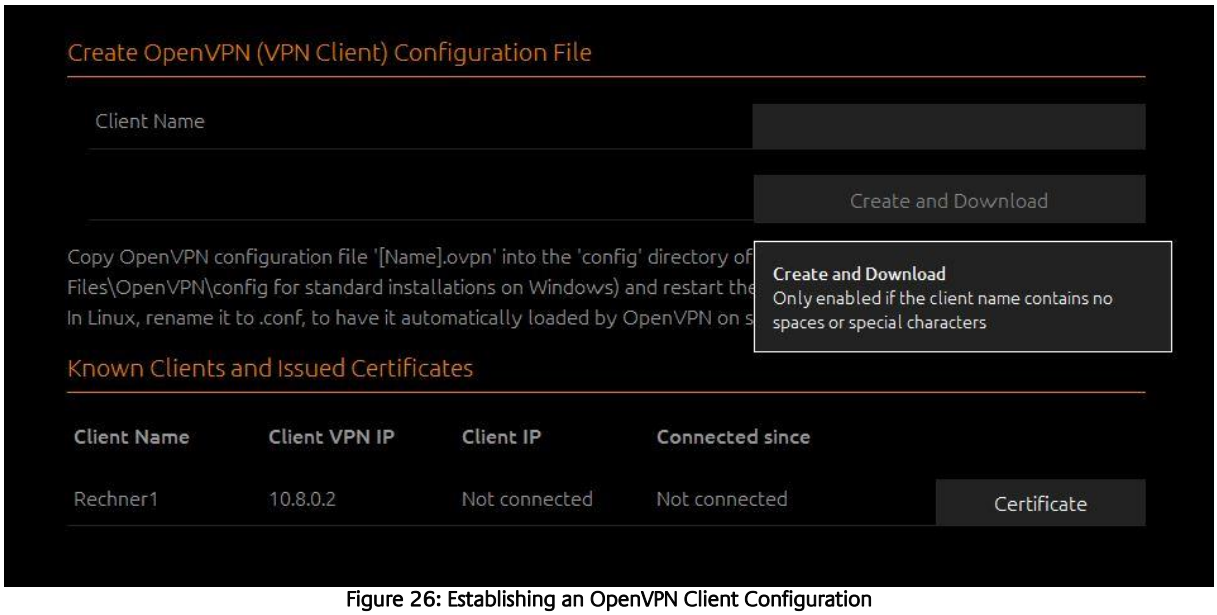


Figure 26: Establishing an OpenVPN Client Configuration

Please download the appropriate OpenVPN client software for your operating system.

- Windows: "OpenVPN GUI" (from www.openvpn.net)
- MAC OS: "Tunnelblick" (from www.tunnelblick.net)
- Android: "OpenVPN for Android" (from the Google PlayStore)
- iOS: currently no support ("inline mode" is not supported)

You will also find the current download links on our homepage: www.bab-tec.de.

- Enter the defined name for the configuration file under "Client Name". Via this name the respective computer will later be identified from the "Known Clients" list.
- Click "Establish and Download". A browser dialogue for downloading the "*.ovpn" configuration file will open. Save the configuration file on your computer. Simultaneously, the configuration file is displayed in the "Known Clients and Issued Certificates" list as a known client.
- Copy the OpenVPN configuration file '[Name].ovpn' in the 'config' register of the Open VPN installation (for Windows - "OpenVPN GUI". Standard path: "C:\Program Files\OpenVPN\config", in MAC OS simply open the file via "Tunnelblick") and restart OpenVPN GUI.
- Then, all loaded connection configuration files are displayed in the context menu of the OpenVPN clients. Click on the connection name of interest to connect.

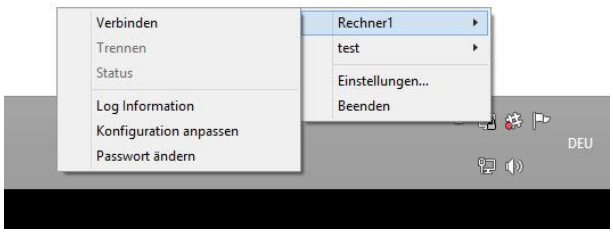


Figure 27: Establish OpenVPN GUI Connection

- A window with log messages will open and a connection attempt will be started. If the connection has been established successfully, the icon in the Windows system tray changes colour (green) and a corresponding message is shown.

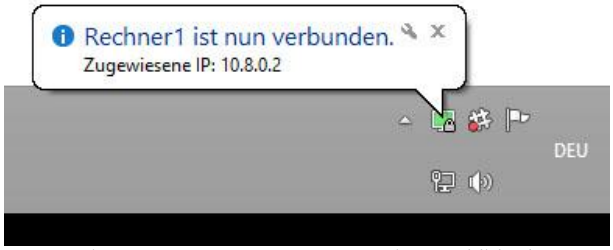


Figure 28: OpenVPN GUI Connection Established

KNOWN CLIENTS AND ISSUED CERTIFICATES

All established configuration data will be displayed in this list.

Figure 29: OpenVPN – Known Clients List

In an active connection, "Client IP" and "Connected since" are filled in with the corresponding values.

Certificate
Each connected client has received their own certificate via the configuration file. The certificate can be displayed, downloaded ("Download") or blocked ("Block") via the "Certificate" button.

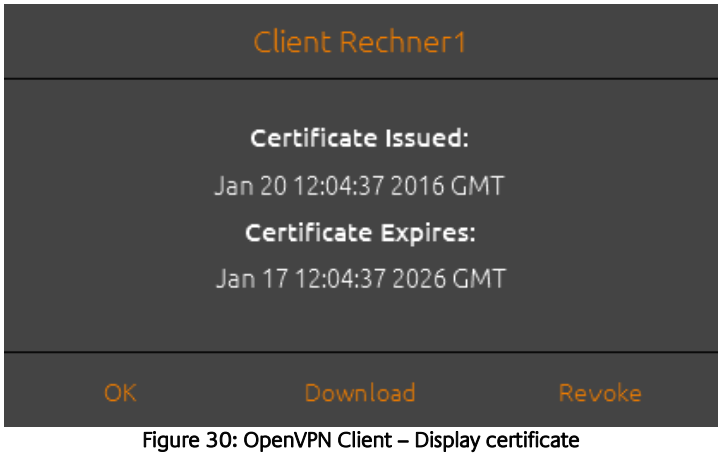


Figure 30: OpenVPN Client – Display certificate

Block client
In order to block a connected client, use the "Revoke" function in the "Certificate" menu. The client connection is cut off immediately. In order to reuse the client, the revoke has to be removed and a new configuration file has to be created.

- Open "Certificate" again. Click "Delete". Afterwards, you can again download a configuration file for the same client name.

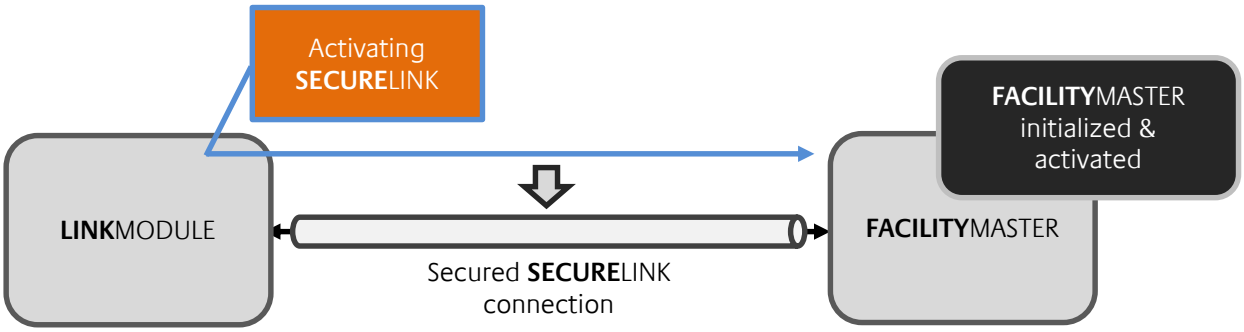
3.3 BAB SECURELINK

A **SECURE**LINK connection is a VPN connection specialized in BAB devices which allows a simple establishment of a secured linking of several system parts beyond network domains. Currently, **SECURE**LINK is available for the following devices:

- LINKMODULE
- EIB**PORT**
- **FACILITY**MASTER

3.3.1 CONNECTION PRINCIPLE

As an example, the **SECURE**LINK connection principle between **LINK**MODULE and **FACILITY**MASTER is displayed. The device (here: **LINK**MODULE) from which the **SECURE**LINK connection is established acts as VPN client, whereas the addressed device is the VPN server (here: **FACILITY**MASTER)



3.3.2 REQUIREMENTS

For a successful **SECURE**LINK connection, the following requirements occur:

- Complete network settings in both devices (Standard Gateway, DNS)
- The VPN server in the opposite device has to be initialized and activated (consider external IP address / host name)
- Communication on TCP port 1724 between both devices possible

3.3.3 ESTABLISH SECURELINK CONNECTION

In order to establish a **SECURE**LINK connection, please proceed as follows:

- Switch to the configuration window "BAB **SECURE**LINK ".
- Fill in the fields beneath BAB **SECURE**LINK.
  - *BAB VPN Server Address:* Enter the IP address or host name of the opposite BAB device which activated the VPN server.
  - *BAB VPN Server HTTP Port:* Enter the http port of the opposite BAB device here
  - *BAB Device Account / Password:* Enter the "admin" user data of the opposite BAB device.

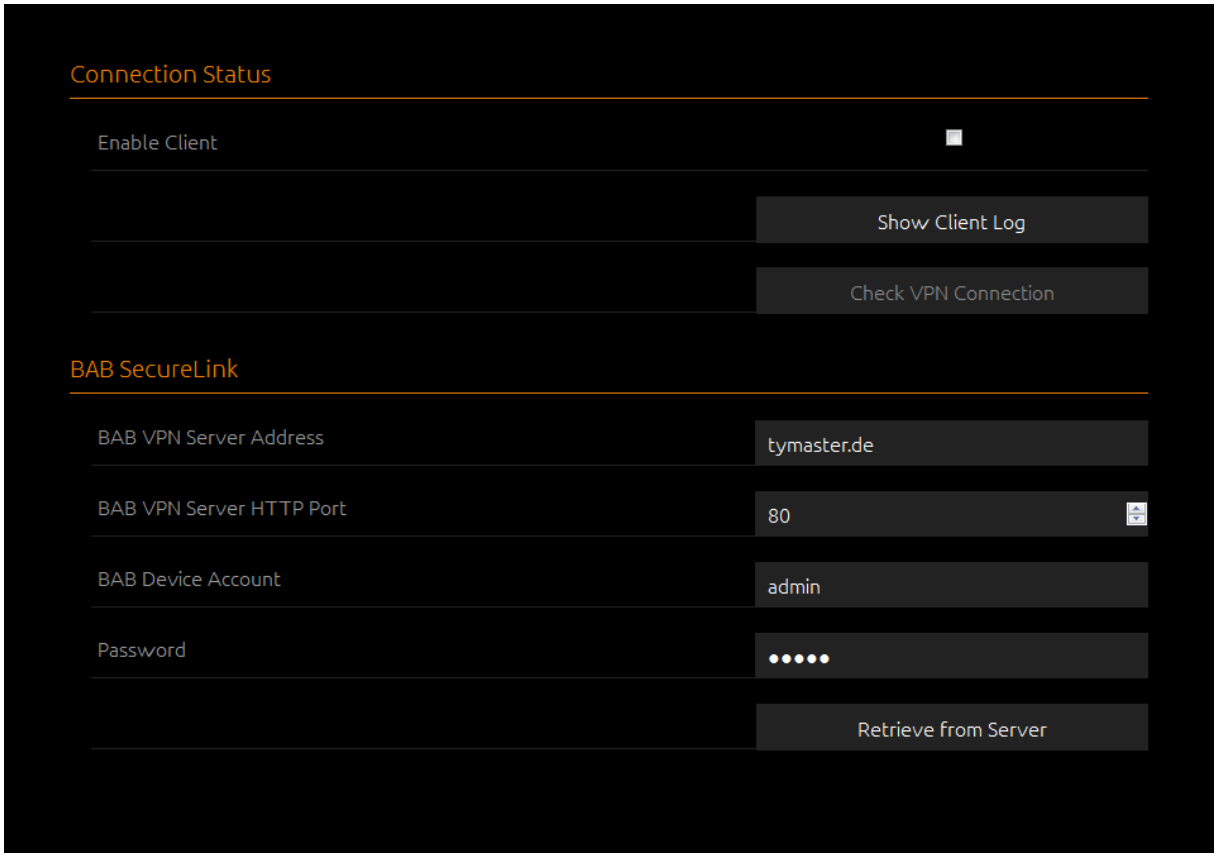


Figure 31: BAB SECURELINK Menu

- Click "Retrieve From Server". The required **SECURE**LINK user data will be loaded from the distant BAB device.
- Activate the control box "Enable client" beneath "Connection Status". Then, the connection is established.

Display Client Log
Log messages for monitoring the connection will be shown.

Testing VPN Connection
Here, the VPN connection can be tested in advance

3.4 FACILITY COUPLING

Via the "Facility coupling" service, group address telegrams are transmitted via a UDP Unicast connection from one BAB device to another. Due to the Unicast connection, the communication via network domains can be established with a lower effort than would be the case with a KNXnet/IP routing connection. The facility coupling are currently supported by the following BAB devices:

- EIB**PORT**
- **FACILITY**MASTER
- LINKMODULE
- **APP**MODULE Extension
- DUODMX GATEWAY Extension (only receiving)

Note: The facility coupling communication is a group address-based communication. Physically addressed telegrams will not be transmitted. Programming KNX devices by means of ETS is not possible via the facility coupling.

When using the facility coupling via BAB **SECURE**LINK, the connection is provided with additional protection. See chapter "Facility coupling via **BAB** SECURELINK".

3.4.1 REQUIREMENTS

For establishing a connection between BAB devices, the following conditions must be fulfilled.

- Complete network settings on both devices (Standard Gateway, DNS)
- Free communication to UDP Port 1735
- Fixed external target device address (fixed IP address / dynamic DNS address / VNP IP)
- Possibly established and activated **SECURE**LINK connection, if requested

Note: For receiving facility coupling telegrams, there is no need to perform any settings on the opposite device.

3.4.2 ESTABLISHING FACILITY COUPLING

Switch to the menu "Facility coupling" and click "Add Job". A new facility coupling job (service) will be added.

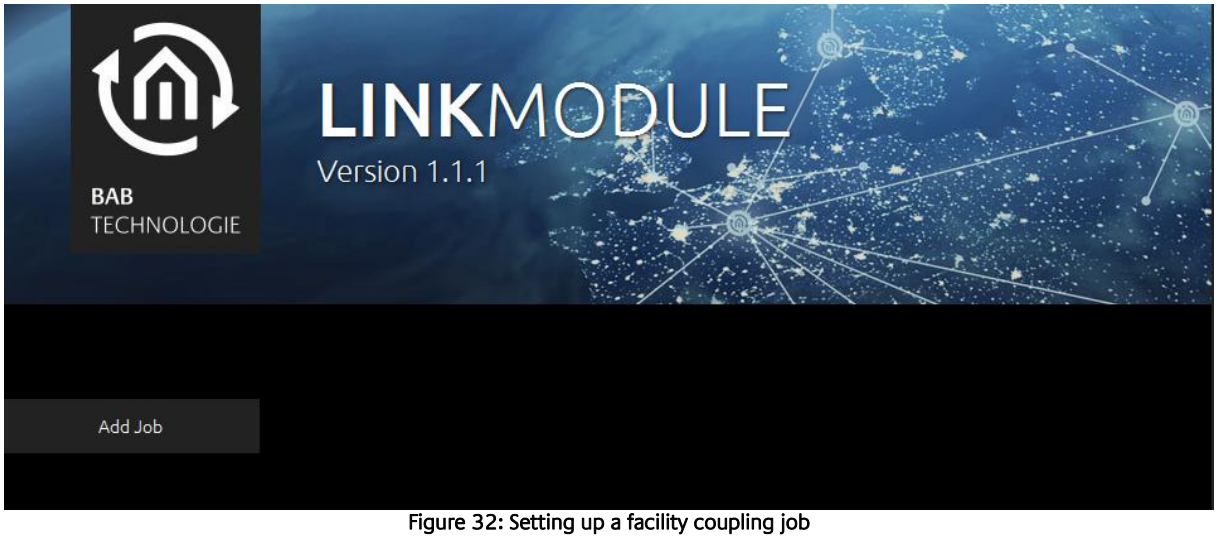


Figure 32: Setting up a facility coupling job

The facility coupling job configuration mask will appear. Fill in the requested fields. Per job (service) 10 filter rules may be assigned. Several services may be assigned simultaneously. The number of services is only limited by the system workload.

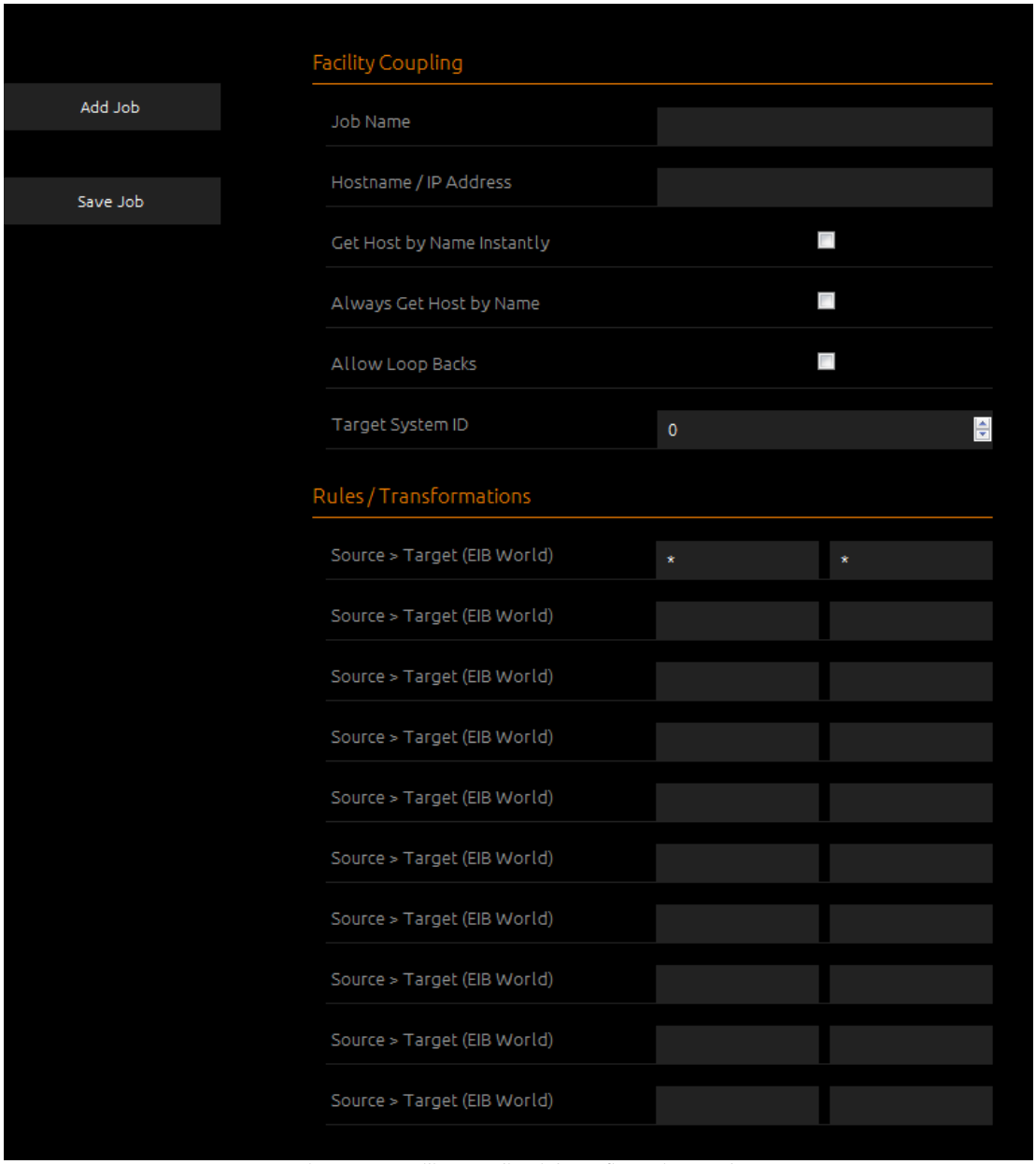


Figure 33: Facility coupling job configuration mask

The parameters are:

Job name
Assign a definite name for the job (service).

Host name or IP address
Host name or IP address of the distant BAB device with facility coupling support. For a connection via BAB **SECURE**LINK, indicate the VPN IP of the distant device here. (For **SECURE**LINK establishing, please consider chapter "BAB **SECURELINK**")

Resolving host name immediately

- *active*: the name resolution is performed immediately at initial operation
- *deactivated*: the name resolution is performed only when the facility coupling service is activated

Resolve host name every time
- *active*: the host name is resolved at every start of the facility coupling service. (only appropriate with dynamic name resolution)
- *deactivated*: the host name is only resolved at the first start of the facility coupling service

Feedback permitted
- *actively:* feedbacks via LAN are permitted
- *deactivated:* feedbacks via LAN are suppressed

Target system ID
Currently only usable for EIBPORT and **FACILITY**MASTER. Definite KNX system ID (0 - 255) (no entry: Target system ID = 0)

Rules / transformations
The transmitting rules allow the communication to the opposite device to be filtered and transformed. Therefore, e.g. real group addresses from the source world can be transcribed within virtual addresses (see below) in the target world in order to avoid unnecessary workload or group address overlapping. For rule input, wild cards can be used. The symbol "*" is used as a wild card. Depending on the position (before and after the "/"), the "*" represents the KNX main group or subgroup.

Rule	Meaning
//* -> */*/*	All KNX facility 1 main and subgroups are linked 1:1 into the KNX facility 2. **Caution:** In the target world, all incoming telegrams (from the real address space) are resent to the KNX!
6/*/* -> 6/*/*	All group addresses of the main group 6 of the KNX facility 1 are linked into the main group 6 of the KNX facility 2
7/*/* -> 17/*/*	All group addresses of main group 7 of the KNX facility 1 are linked into the virtual main group 17 of the KNX facility 2 ▪ Therefore, address overlapping can be avoided1
//1 -> */*/1	The addresses 0/0/1; 1/1/1; 2/2/1...32/7/1 are linked into the KNX facility 2

Virtual group addresses
The main groups 16-32 are the virtual group addresses. They are only available within the **LINK**MODULE and are not transmitted to the KNX interface. In facility coupling, virtual group addresses may apply to avoid address overlapping and unnecessary workload.

Example
E.g., if a lighting scene is to be started from facility 1 (**LINK**MODULE) to facility 2 (**FACILITY**MASTER), the lighting scene is provided with a virtual group address (e.g. 17/1) in facility 2. In the **LINK**MODULE of facility 1, the following rule might be parametered:
e.g. 2/3 -> 17/1. The real group address in facility 1 (e.g. assigned to a push button) is translated into the virtual group address in facility 2 (the lighting scene).

Note: For receiving facility coupling telegrams, there is no need to perform any settings in the opposite device.

BIDIRECTIONAL COMMUNICATION VIA FACILITY COUPLING

In order to establish a bidirectional communication between two BAB devices, it is required to set up one facility coupling job respectively in the correspondent opposite device. The facility coupling job always transmits to the devices indicated in the job mask in a unidirectional way only.

3.5 FACILITY COUPLING VIA BAB SECURELINK

If the facility coupling are established via the BAB **SECURE**LINK, the communication between the unit parts is tap-proof. To do this, please proceed as follows.

- Determine VPN server and VPN client.
- Initialize VPN server in both devices (see chapter "Initializing VPN Server")
- Establish **SECURE**LINK from client to server (see chapter "Establish **SECURELINK** connection")
- Establish facility coupling, indication VPN IP addresses (!) (see chapter "Establishing facility coupling")

By indicating the VPN IP address, the facility coupling communicate via the secured **SECURE**LINK tunnel.

4 CONFIGURATION

The configuration is for setting the following parameters:

- Device name, installation site, setting system time
- Performing network settings incl. NTP time server
- Physical addressing the KNX interface, KNXnet/IP settings
- Testing the KNX interface
- Linking EnOcean profile with KNX group addresses
- User Administration
- Save and Restore

4.1 SAVE CONFIGURATION

As soon as you have modified the configuration, please click on the "**Save configuration**" field.

4.2 GENERAL

In the "General" window, the following basic settings can be performed.

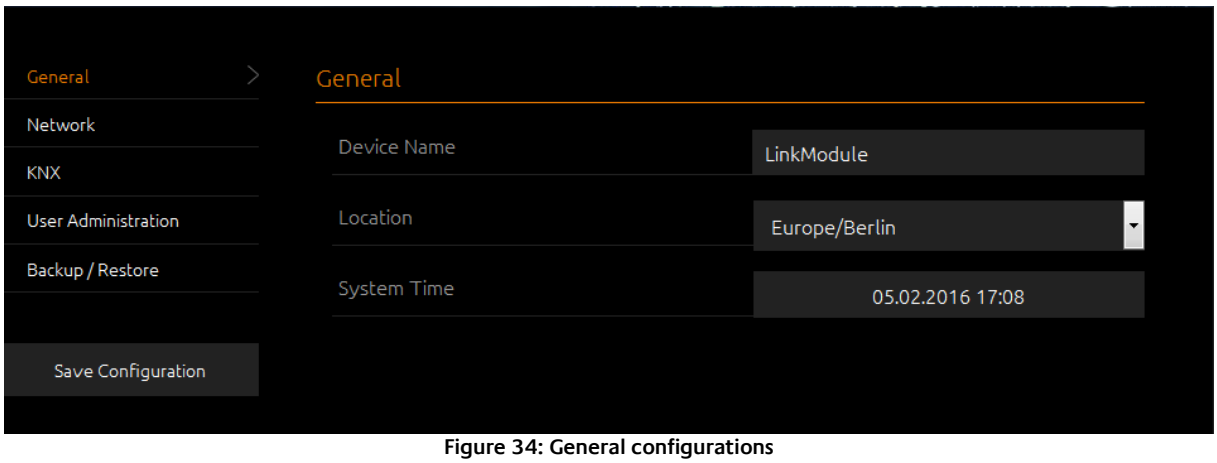


Figure 34: General configurations

Device name: Assign an individual name for the **LINK**MODULE, which name will be displayed in the "Discovery Tool" and the BAB STARTER.

Installation site: Adapt the installation site to the local time zone settings.

System time: Indicates the system time of the device. When clicking on the time indication, the system time is synchronized with the PC time.

Note: Please make sure that the system time of the device is up to date. A deviating system time can result into problems with the telegram handling! If possible, use an NTP time server for synchronization.

4.3 NETWORK

DHCP: If DHCP is active, the device automatically obtains the network settings. A DHCP server must be available in the local network.

IP address / network mask / gateway: If DHCP is not active, the network settings must be carried out statically. In case of doubt, contact your network administrator as to which settings are to be carried out. Please note that an IP address may never be assigned twice!

DNS Server: DNS is the abbreviation for Domain Name System. The DNS server converts Internet addresses, for example "www.bab-tec.de" into the IP address "85.214.89.170" and vice versa. Without a valid DNS entry, NTP, weather services from the Internet and UPnP do not work.

NTP Server: NTP is a free service for synchronising the system time of Internet-compatible devices. If time synchronisation is not possible, please check the system time from time to time in the "General" menu item.
NTP server list: e.g. http://www.pool.ntp.org/zone/europe

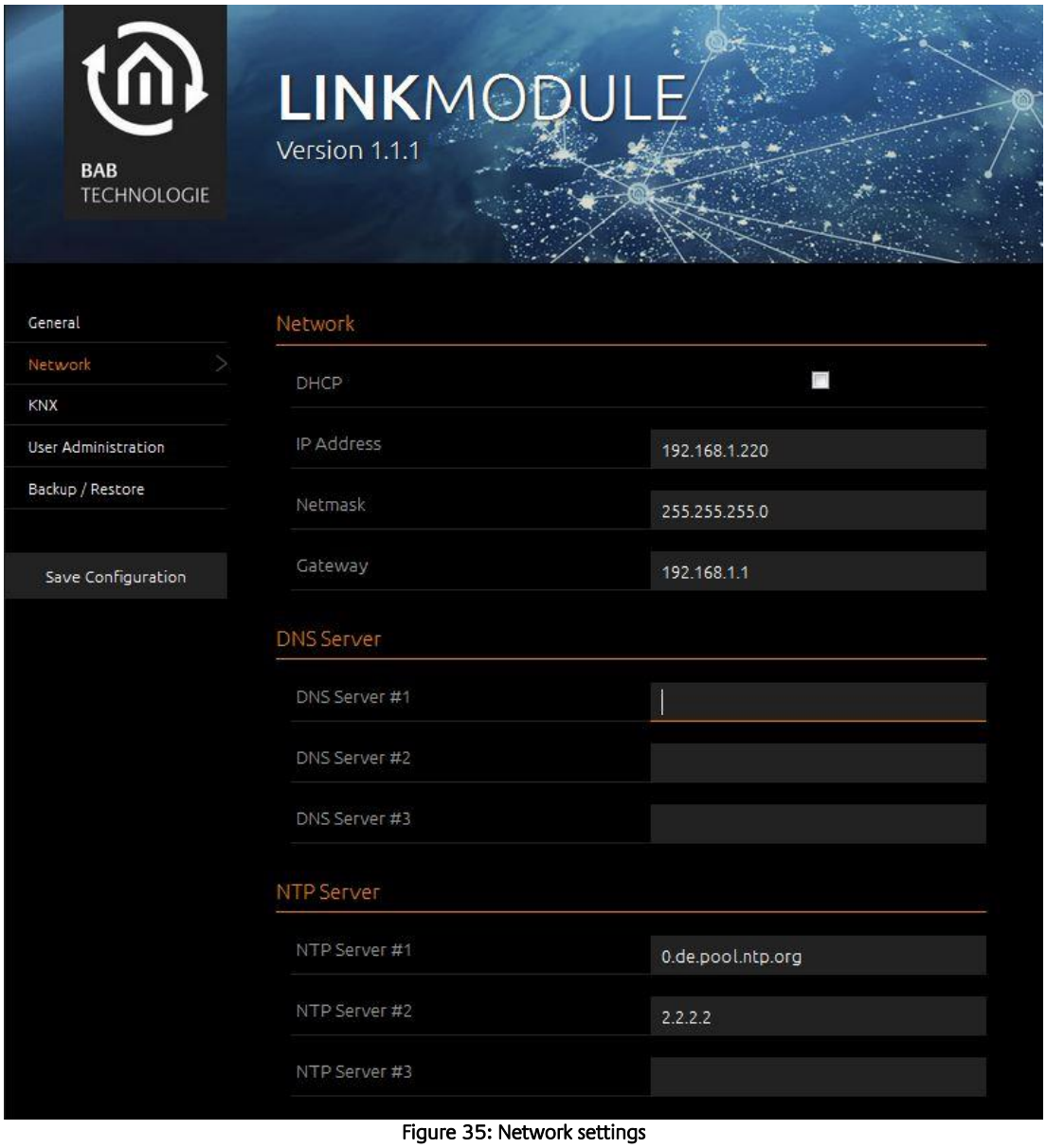


Figure 35: Network settings

4.4 KNX

The KNX-specific settings of the **LINK**MODULE are made in the "KNX" menu. Additionally, it is possible to test the KNX interface.

KNX

Physical address:
Here, you can determine the physical address to be used by the **LINK**MODULE in the KNX network. Please make sure that the physical address corresponds to the installation site and does not occur twice.

KNXnet/IP tunnelling address:
This addresses are used by the internal KNXnet/IP server for a KNXnet/IP tunnelling connection established to the device (using the **LINK**MODULE as a programming interface for the ETS). At least 2 free addresses must be entered. The addresses are separated via semicolon (Example: 4.7.14;4.7.15).

Note: Please note that this addresses must not be the same as the physical addresses (see above) and that they must not be used by any other participant in the line either.

KNXnet/IP routing:
Activates KNXnet/IP routing for the linking of lines and areas via KNXnet/IP. Can only be activated if the physical address (see above) corresponds to that of a line or area coupler.

Note: KNXnet/IP routing uses Multicast! Since multicast packages are usually not transferred by routers, "Routing" only works within a subnet. Use the facility coupling combined with SECURELINK if you want to link across network domains.

- Communication: Mulitcast 224.0.23.12, port 3671

KNXnet/IP tunnelling:
Activates the KNXnet/IP tunnelling access to the device. This connection can be used for programming KNX devices or for exchanging data. The **LINK**MODULE is the server.

Note: The number of the addresses indicated above determines the number of the connections simultaneously possible. The ETS requires 2 free addresses for a connection.

- Communication: Unicast, UDP Port 3671

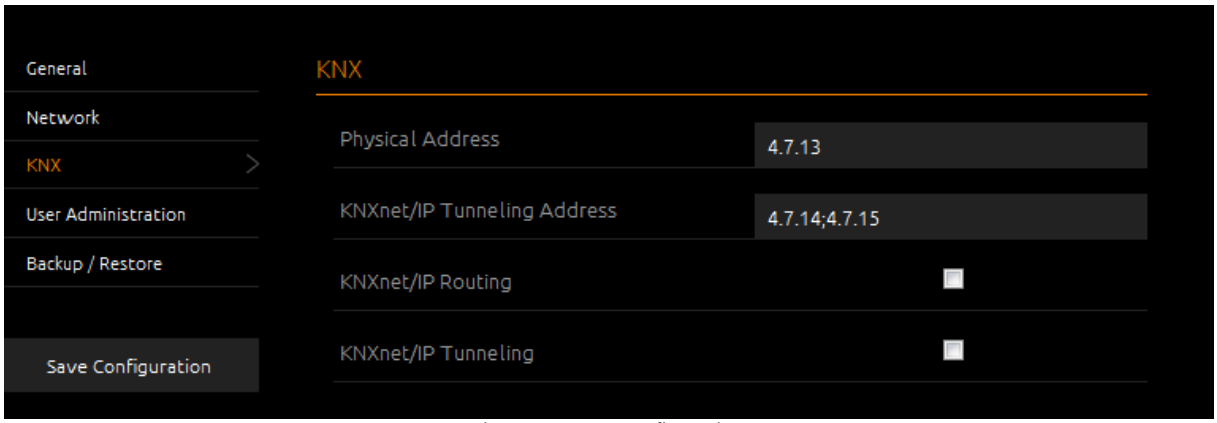


Figure 36: KNX Configuration

TESTING INTERFACE

KNX address
Enter the group address you want to test with here

Switching KNX Address
By clicking on "On/Off", a EIS 1 (1bit) switching command is triggered on the group address mentioned above.

Reading Out Address Status
When clicking on "Status Query", the status of the group address mentioned above is queried and displayed in a pop up window.

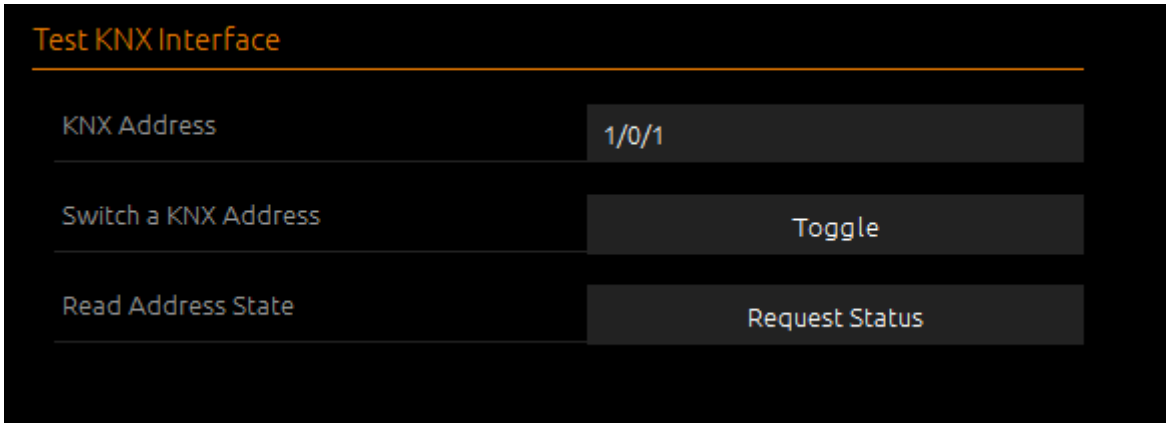


Figure 37: Testing KNX Interface

4.5 ENOCEAN EDITOR

When you use a **LINK**MODULE EnOcean, the link to the "EnOcean Editor" appears here instead of the KNX configuration. The EnOcean Editor is entirely described in the chapter "LINK MODULE EnOcean".

Note: The EnOcean Editor is a Java Applet application. Please use a browser allowing to start Java Applets or the program "BAB STARTER" to start the editor.

- Usage in BAB STARTER: You will find the software and the corresponding documentation on the CD enclosed or in the download section of our homepage, www.bab-tec.de.
- Starting in the browser: Please consider the following chapter.

4.5.1 JAVA SETTINGS / PREPARATIONS ON THE CLIENT PC

Note: When working with the EnOcean Editor, the following JAVA settings are mandatory to be considered priorly.

PC Requirements
In order to be able to use the EnOcean Editor, you need Java and a browser. Thus, the editor is independent of the operating system.

Java and browser version
We recommend using a current version of Apple Safari or Mozilla Firefox as a browser. Please note that a current Java version has been installed and that the Java browser plug-in is up-to-date. If Java has not been installed yet, you will find a current version at www.java.com. Please check the following settings on your computer before you start working in the EnOcean Editor.

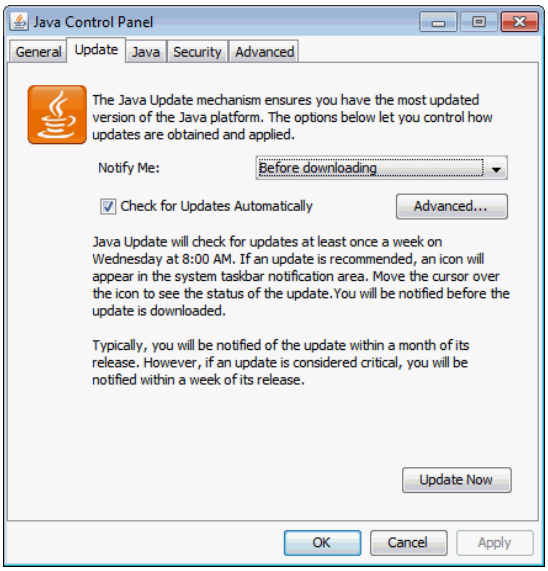


Figure 38: Updating Java

Deleting and deactivating temporary files
Please close all browser windows (also download windows etc.) and switch to the Java Control Panel via "*Start*" > "*System Control*" > "*Java*". On the first tab, "*General*", there are the "*Settings*" of the "*Temporary Internet Files*". Please remove the tick at "*Leave Temporary Files on Computer*" and delete all files using the "*Delete Files*" button.

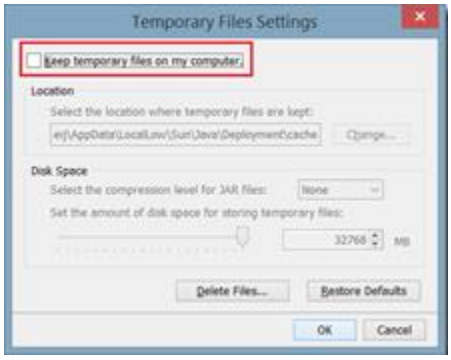


Figure 39: Deactivate Temporary Files

Expand main memory for Java / deactivate old Java versions
Switch from the "General" tab to the "*Java*" tab. Please open the settings for the Java Runtime Environment via "*Displays*". The window shows you all Java versions installed on this computers. If several versions are installed, please de-install all versions except the current version. Then, double-click into the "*Java Runtime Parameters*" field and enter "*-Xmx256M*"(pay attention to the minus sign). Then press "*Enter*" and leave the window using "*OK*".
In the "*Java Control Panel*" window below, it is important that you click "*Apply*" before closing the window with "*OK*".

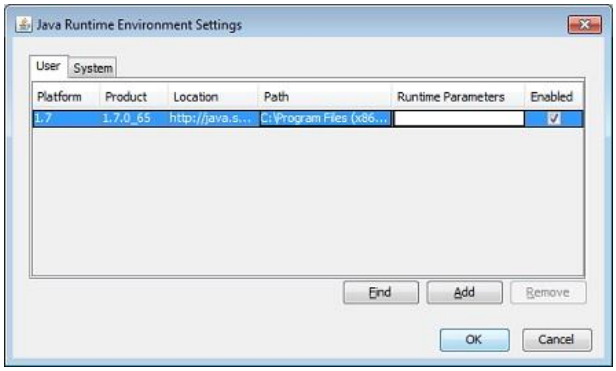


Figure 40: Expanding Java Main Memory

Afterwards, please also empty the cache data of your browser. Instructions on how to do this can be found on the Internet or in the help file of the browser. After all steps have been carried out and completed, the browser must be restarted.

4.5.2 BAB STARTER

In more recent browsers problems may occur when Java applets as they are used in the EnOcean Editor are to be started. To avoid the problem, you can use the new software "BAB STARTER". You will find the software and the corresponding documentation on the CD enclosed or in the download section of our homepage, www.bab-tec.de.

4.6 USER ADMINISTRATION

The menu item "User Administration" is to be able to modify or add user data.

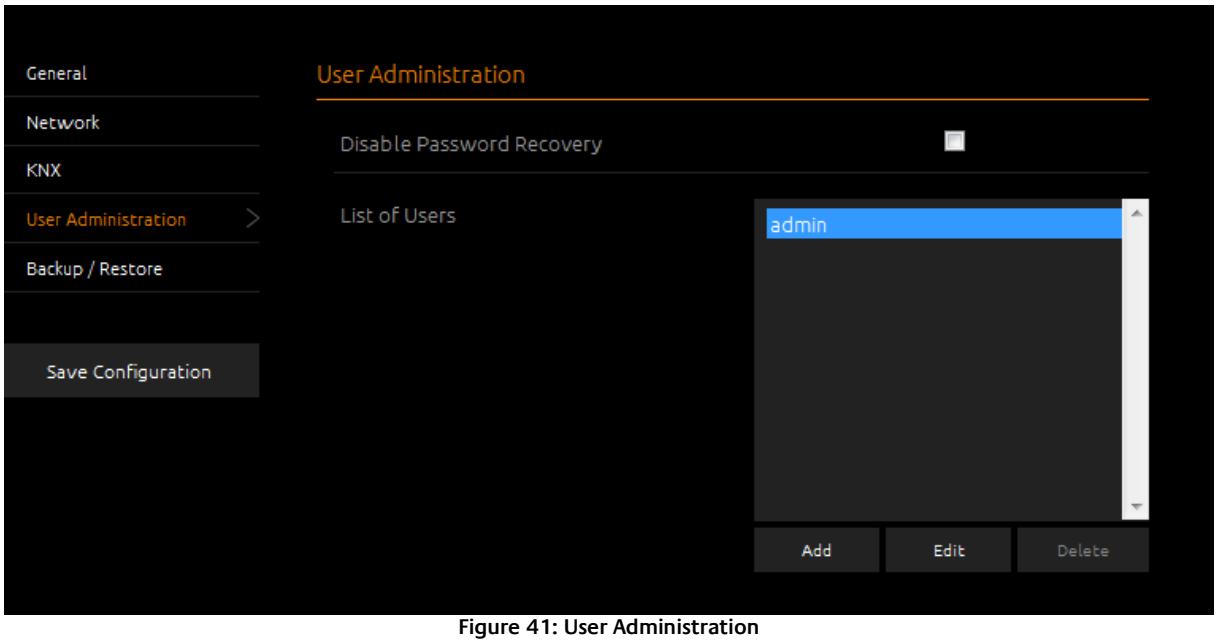


Figure 41: User Administration

4.7 BACKUP / RESTORE

In the menu item "Backup / Restore", you can create security backups and restore these backups, if necessary. By clicking on "Create a Backup", you can download and save a backup from the LINKMODULE. Then, you can upload these by activating the "Select Backup File" button beneath "Restore Settings".

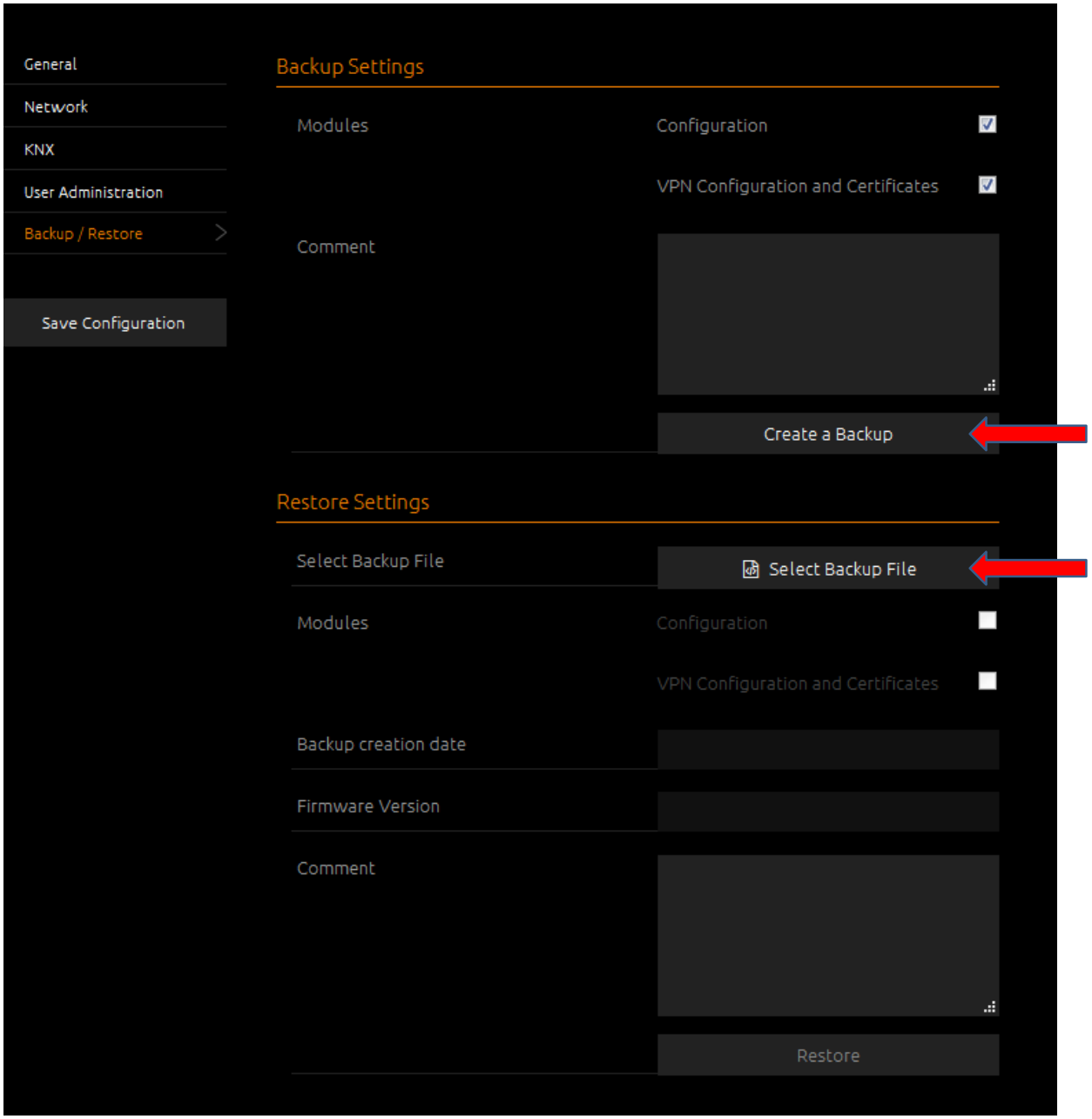


Figure 42: Save

4.8 SYSTEM

In the menu item System, you will find the functions "Reboot Device" and "Firmware Update". In order to perform the function "Reboot Device", please click the "Perform Reboot" button.

FIRMWARE UPDATE

In the menu item Firmware update you can manually select and upload the update files.

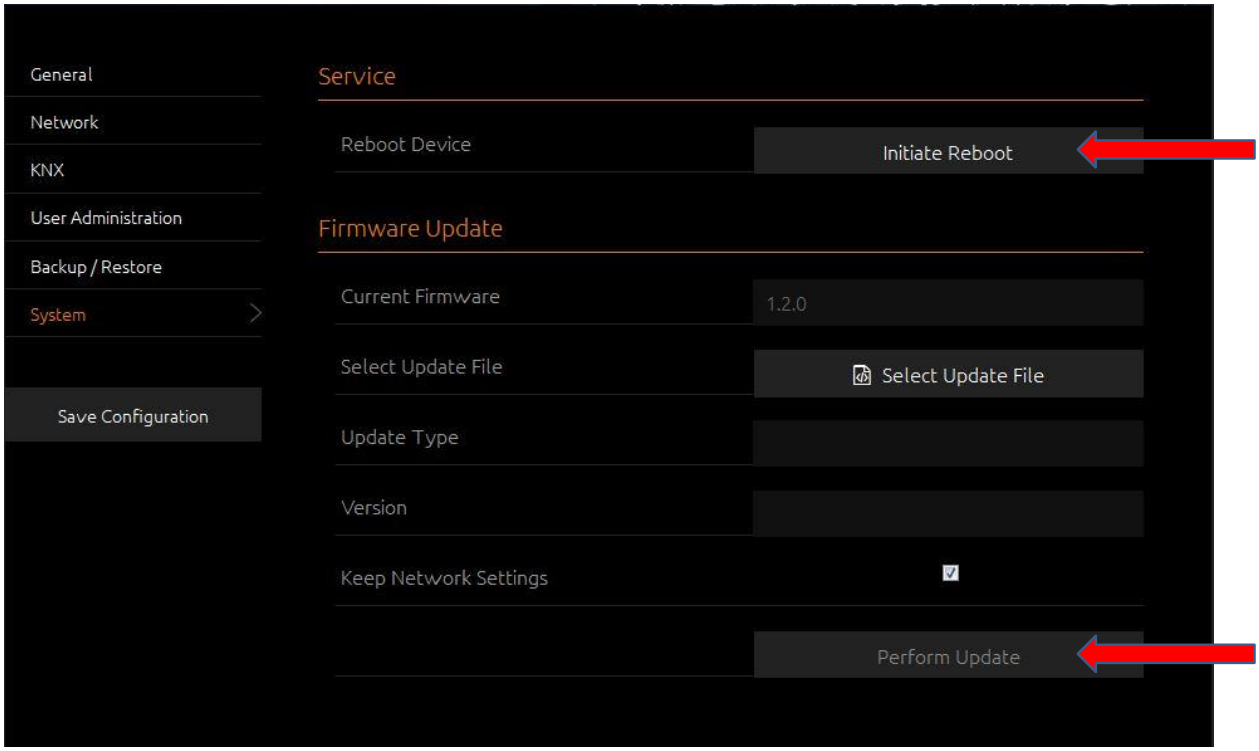


Figure 43: System

4.9 LEAVE CONFIGURATION

In order to leave the menu or to go back to the start page, please use the "Back" function of the browser or click the BAB TECHNOLOGIE "Home button" (complete header diagram of the LINK MODULE web interface).

Figure 44: Home Button

5 INFORMATION

Beneath the menu item Information you will find all the relevant information about your **LINK**MODULE such as system information, processor workload, Java storage workload and software licenses.

If support is required, please have this information ready.

In order to leave the menu or to go back to the start page, please use the Back function of the browser or click the BAB TECHNOLOGIE Home button.

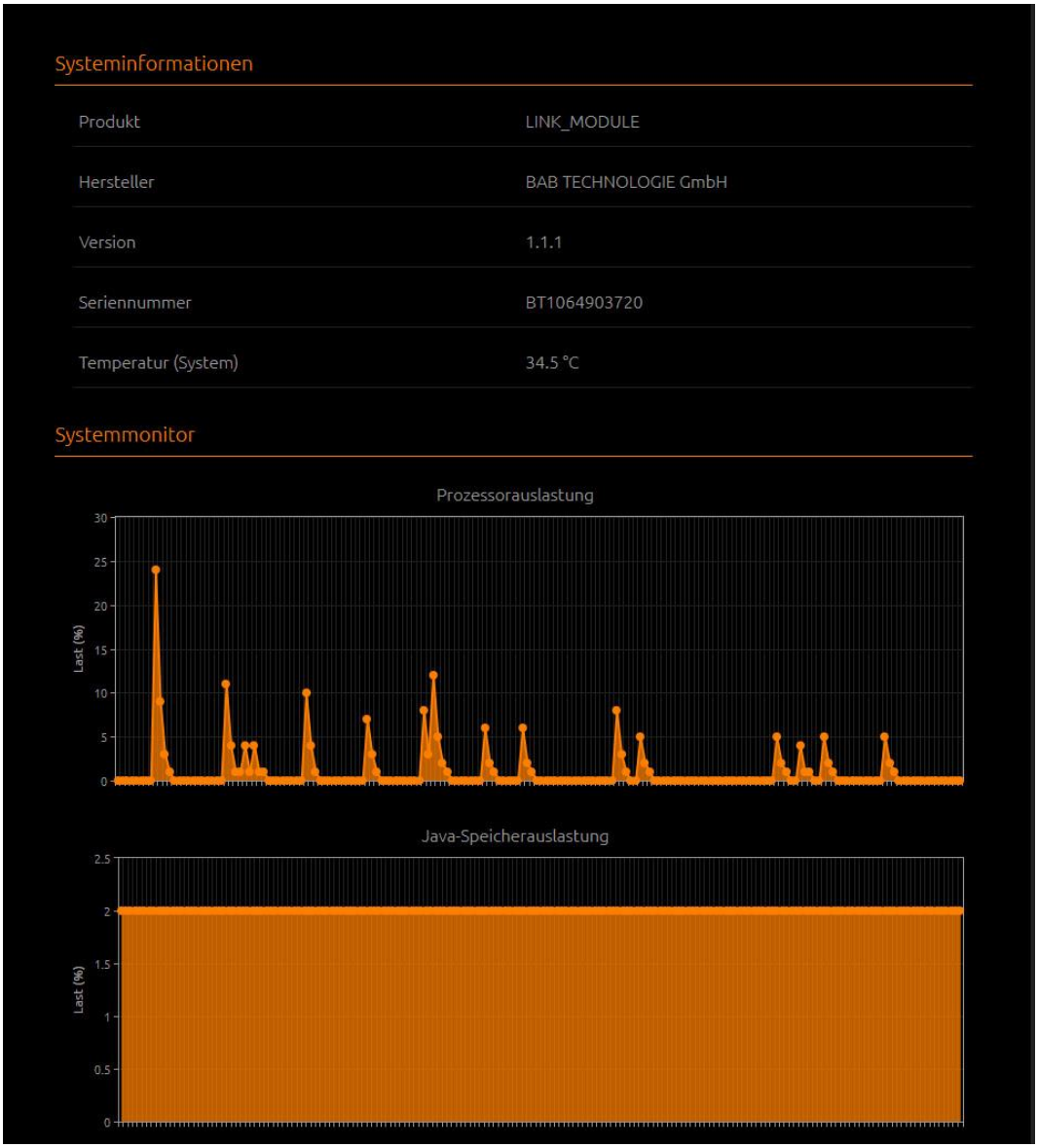


Figure 45: Information

6 LOGOUT

When you have performed all modifications, you can log out by clicking on the "Logout" field.