eNet SMART HOME

# eNet SMART HOME connect

## Table of Contents

# 1 eNet SMART HOME system

The eNet server is the heart of every eNet SMART HOME system and offers end customers the basis for an easy-to-use and secure Smart Home and installation engineers easily understandable and professional commissioning of the system.

The commissioning interface **eNet SMART HOME connect**, which is accessed via a web browser, offers functions such as:

- Device search for adding devices
- Device localisation for clear identification
- Resetting the device to the default setting
- Configuring the device
- Programming connections between devices
- Measurement of the signal quality for error diagnosis
- Recording of telegrams for error diagnosis
- Device and server update

In everyday operation, the eNet server provides the end customer with functions such as:

- Smartphone operation via the **eNet SMART HOME app**
- Secure remote access via the app
- Automatic execution of If-Then rules
- Activation of device groups via scenes using the app or wall/hand-held transmitter
- Automatic time-based control of devices
- Provision of measurement data, such as energy consumption and actuator states, such as light and Venetian blind, for the app

An eNet SMART HOME system consists of the following devices:

- eNet actuators for the execution of actions, such as switching or dimming of loads
- eNet sensors for operation on the device or recording environmental data
- eNet server as the central unit
- RMD power supply

The following devices are required for commissioning and operation of the eNet system using the app:

- Smartphone or tablet for operation via the  **eNet SMART HOME app**
- WiFi-compatible router for operation via the **eNet SMART HOME app**
- Computer for commissioning via **eNet SMART HOME connect**

## 1.1 System requirements

**eNet SMART HOME app**

For app installation, a smartphone with the operating system Android (Version 5.0 or higher) or iOS (Version 9.3 or higher is required).

**eNet SMART HOME connect**

At least the following requirements must be fulfilled to use the commissioning interface:

- Min. screen resolution 1366x768 (web browser in full-screen mode)
- WLAN router (only when using WLAN)
-  The computer and eNet server belong to the same network (network component of the IP addresses is identical)
- Allow cookies in the web browser (this is preset in the web browser by default)
- Activate the cache in the web browser (this is preset in the web browser by default)
- Web browser with JavaScript and HTML5 support (Internet Explorer, Firefox, Google Chrome or EDGE)

ⓘ  We recommend using the current web browser version.

## 1.2 Commissioning via eNet SMART HOME connect

Commissioning of an eNet system takes place in a few steps.

| | |
|---|---|
| **1. Setting up a network connection**<br>Set up the network connection between the<br>eNet server and the computer via a router. | Addressing is preset via DHCP. |
| **2. Entering the IP address**<br>Open the web browser and enter the<br>IP address of the eNet server in the address<br>line of the web browser. | The IP address of the eNet server can be<br>read off in the app or in the router. |
| **3. Logging into the eNet server**<br>Enter your user name and password in the<br>log-in screen. | Username: **admin**<br>Password: **admin** |
| **4. Creating a project**<br>Creating a project and basic settings | During first commissioning, the window<br>is opened directly after log-in. |
| **5. Create the building structuren**<br>Adding areas and rooms | Implementation in the **Rooms** view |
| **6. Adding and configuring devices**<br>From device search or catalogue | Implementation in the **Devices** view |
| **7. Creating the connections**<br>Connecting sensor channels with actuator<br>channels | Implementation in the **Connections** view |
| **8. Programming connections** | Implementation in the **Connections** view<br>or in the **System overview** |

Figure 1: Commissioning with the eNet server - At a glance

ⓘ As soon as a connection is programmed, the connection in the eNet system is active and the eNet devices connected via radio can be operated.

ⓘ **eNet SMART HOME app**: As soon as a building structure has been created, a device downloaded, a room added and its channels named, use in the app is possible.

ⓘ The commissioning of an eNet system with the eNet server is described in detail in the following chapters. There is a chapter for each view describing the commissioning steps and the functions of the appropriate view.

**Desktop commissioning with catalogue devices**

The first step of the planning and commissioning of an eNet system can also be carried out at the desk using catalogue devices, without actual devices from the system. In a later workstep, the catalogue devices can be replaced with the real devices from the system via a device search. Any previously made settings are applied.

**Additional parameters**

In addition to the settings made on the device, other parameters can be set on all eNet devices via the eNet server, e.g. actuator behaviour after voltage return. The parameters to be set are dependent on the type of device. In the commissioning interface, descriptions of the individual parameters can be recalled using the ⬚i button.

**Energy sensors**

Energy sensors can be integrated into the project for determining voltage, current and energy values. These values can be viewed via the app or can be used as an input condition for automated controllers in If-Then rules.

**Troubleshooting**

During commissioning, it is possible to measure the signal strength of transmitters. The signal arriving at the receiver is evaluated. Signal quality measurements can be performed for all eNet devices connected via the eNet Server. The quality of the signal is shown using colour coding according to the traffic light principle. In this way, for example, the mounting location can be checked directly and, if necessary, changed, or a repeater can be deployed.
If faults occur during operation of an eNet system, telegrams can be recorded for a specific period of time and exported for evaluation. The troubleshooting tools are located in the **Diagnostics** view.

**Subsequent changes in the project**

Even after a project has been completed, the commissioning interface can be used to make changes to the eNet system at any time, such as adding new devices, supplementing connections or changing device settings.

**Update of the device software**

Updates to the devices can be performed via the eNet server. Updates for device, catalogue and server software are supplied bundled in an update file, which can be loaded into the system settings of the eNet server and then installed  (see chapter 5.1. Carry out update). Should the file also contain device updates, then these can be programmed into the devices via the eNet server after execution of the update.

# 1.3 Operation via eNet SMART HOME app

Using the  **eNet SMART HOME app**, operation of the eNet system is possible with a smartphone.

⬚i    Scene creation in the app is not possible for as long as a user is logged into the commissioning interface. All the other functions can still be used in the app and eNet devices operated.

The following information from the commissioning interface is displayed in the app:
-    Building structure (see chapter 7. Rooms view)
-    Channel location and name (Figure 11)
-    Display of the icon of the selected device class for switch actuators for light control ⬚ or switching loads ☺
     (Figure 12)
-    Buttons configured for the app  (Figure 11)
-    Channel settings (see chapter 8.3.3. Channel settings)

The following automation functions can only be implemented via the **eNet SMART HOME app**:
-    Creating, modifying and deleting scenes
-    Creating, modifying and deleting time controllers
-    Creating, modifying and deleting If-Then rules

ⓘ To implement time controllers in conjunction with astro functions, the location and date and time must be set in the system settings  (see chapter 6. First steps in the commissioning of an eNet system)

# 2 Commissioning the eNet server

## 2.1 Setting up the connection to the eNet server

A wired network connection (LAN) via a router is required for the first commissioning of the eNet Server. Addressing takes place automatically via DHCP. In the as-delivered state, the eNet Server is appropriately preconfigured. The network configuration can be modified using the buttons of the eNet Server to LAN with fixed IP address and LAN with DHCP, see the operating manual of the eNet Server.

There are various options for connecting the commissioning interface of the eNet server, which are described below.

Precondition: The eNet Server is mounted, the power supply is connected and any external antennas are connected - see the operating manual of the eNet server.

ⓘ   If, as when delivered, the setting "DHCP" is selected in the network settings, it is essential to ensure that the eNet server is connected to a router with DHCP server. If the eNet server is connected to a computer directly, then both devices will obtain an auto IP, which is not then known to the user. As a consequence of this, it might not be possible to access the start page of the eNet server.

### Connection via IP address, obtained from the eNet SMART HOME app

Precondition: The app is installed on the smartphone, the eNet server and smartphone are connected in the same network via a WiFi router.

- Open the app.
ⓘ   The IP address of the eNet server can be found on the Home page and in the System menu of the app.
- Set up the network connection between the eNet Server and the computer via a WiFi router.
- Open the web browser.
- Enter the IP address of the eNet Server in the address line of the web browser.
  The log-in screen of the eNet Server is opened in the web browser.

### Connection via IP address, obtained from the router

- Set up the network connection between the eNet Server and the computer via a router.
- Open the web browser.
ⓘ   The IP address of the eNet server is assigned by the router (DHCP setting) and can also be read off in the user interface of the router, e.g. with a Fritzbox, via the IP address "fritz.box" and then "Home network/Home network overview".
- Enter the IP address of the eNet Server in the address line of the web browser.
  The log-in screen of the eNet Server is opened in the web browser.

### Connection via domain name of the eNet Server

Precondition: The router has an integrated DNS server  (see chapter 5.6.3. Basic principles).
- Set up the network connection between the eNet Server and the computer via a router.
- Open the web browser.
- Enter the **eNet server** in the address bar of the web browser.
ⓘ   With some routers, the host name of the router must also be entered, e.g. **eNetServer.fritz.box**.
  The log-in screen of the eNet Server is opened in the web browser.

### Set up the connection via network settings (UPnP)

Precondition: The computer supports UPnP. Only applicable for the Windows operating system.
- Set up the network connection between the eNet Server and the computer via a router.
- Start the computer and open Windows Explorer.

- Open the network.
  The eNet server is listed there.
- Double-click the entry.
  The log-in screen of the eNet Server is opened in the web browser.

## 2.2 Secure connection

Encrypted communication via an https protocol can be used for the secure connection between eNet server and computer within a home network. The connection is set up using a security certificate. The security certificate can be viewed via the web browser.
When the connection is established for the first time, a warning message appears, is generated by the web browser. In some web browsers, this warning message must be confirmed once in order to set up the connection. Some web browsers have been set so that the warning message appears and has to be confirmed during each access.

[i] This setting can be made in the system settings of the eNet server in the **Network**.

[i] A connection via an https protocol is sensible, for example, if the eNet server is integrated in an open WiFi network or in a WiFi network with poor protection (e.g. WEP) or in a public WiFi/LAN network.

## 2.3 Logging on and deleting users

If the connection between the eNet Server and computer has been established, the log-on screen of the eNet Server will appear.
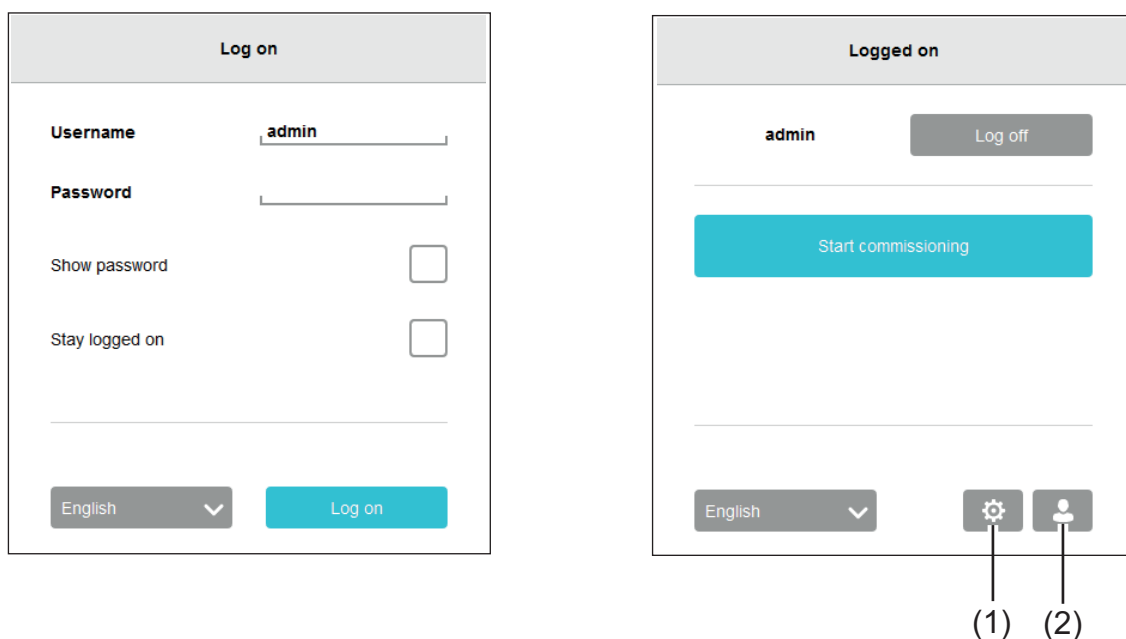
Figure 2: Log-on screen before (left image) and after log-in (right image)

(1)  Recalling the system settings
(2)  Recalling the user administration

[i] If the commissioning interface, system settings or the user administration is open, then no further user can log on. Only the user **admin** can log onto the commissioning interface.

[i] A maximum of eight users can log onto the eNet server via the **eNet SMART HOME app**.

[i] For as long as the user **admin** is logged onto the commissioning interface, no scenes can be created in the **eNet SMART HOME app** and none can be saved after editing. All the other functions can still be used in the app and eNet devices operated.

**Log-on as user**

During first log-on of the administrator, "admin" must be entered both as the username and password. For security reasons, the password should then be changed. The administrator has authorisations to access the commissioning interface, the user administration, the **eNet SMART HOME app** and the system settings of the eNet server.

If a user logs on, then access to the user administration, the **eNet SMART HOME app** and, depending on authorisation, the system settings is possible (see chapter 4. The user administration).

&#9432; If the **Stay logged on** option is enabled, then the user does not need to log on again when accessing again. If the last access is seven or more days in the past, then a new log-on will be required, even if the checkmark is set.

&#9432; The user is also logged out on the log-on screen.

## 2.4 Select language

For the commissioning interface, system settings and user administration, it is possible to choose between the languages German, English and Dutch in the logon screen (Figure 2).

&#9432; The language switchover has no effect on the language of the **eNet SMART HOME app**. The language of the app is set automatically via the system language of the smartphone. If a language is not yet available in the app, English will be used automatically for the app.

## 2.5 Usernames and passwords in the eNet SMART HOME

For security reasons, different users are given different rights in the eNet SMART HOME. A distinction is generally made between the installation engineer (admin), the users of the eNet system, the optional online service (remote access) and the separate project password, which is only required on importing and exporting the project file of an encrypted eNet system. In detail, these are:

- An administrator with the fixed user name "admin" and a password to log onto the **eNet SMART HOME app**, user administration, the system settings and the commissioning interface
- Multiple users with individual user names and passwords for logging onto the **eNet SMART HOME app**, the user administration and the system settings
- A **my.enet-smarthome.de** user account with e-mail address as a user name and password to enable optional remote access
- A project password to export/import the project file of an eNet system with activated encryption

&#9432; If there is a factory reset of the eNet Server, all the created users are deleted. The passwords of the administrator and default user are reset to the default settings (see chapter 4. The user administration) and (see chapter 5.3. Perform a factory reset of the eNet server). The user data for remote access is not reset. This is only possible at **my.enet-smarthome.de**. An exported project file with active encryption can also be reimported after a factory reset. The password individually issued during the export is required for this.

&#9432; The passwords of the users and the administrator can be reset to the default setting using the buttons of the eNet Server, see the operating manual of the eNet Server.

# 3 The commissioning interface

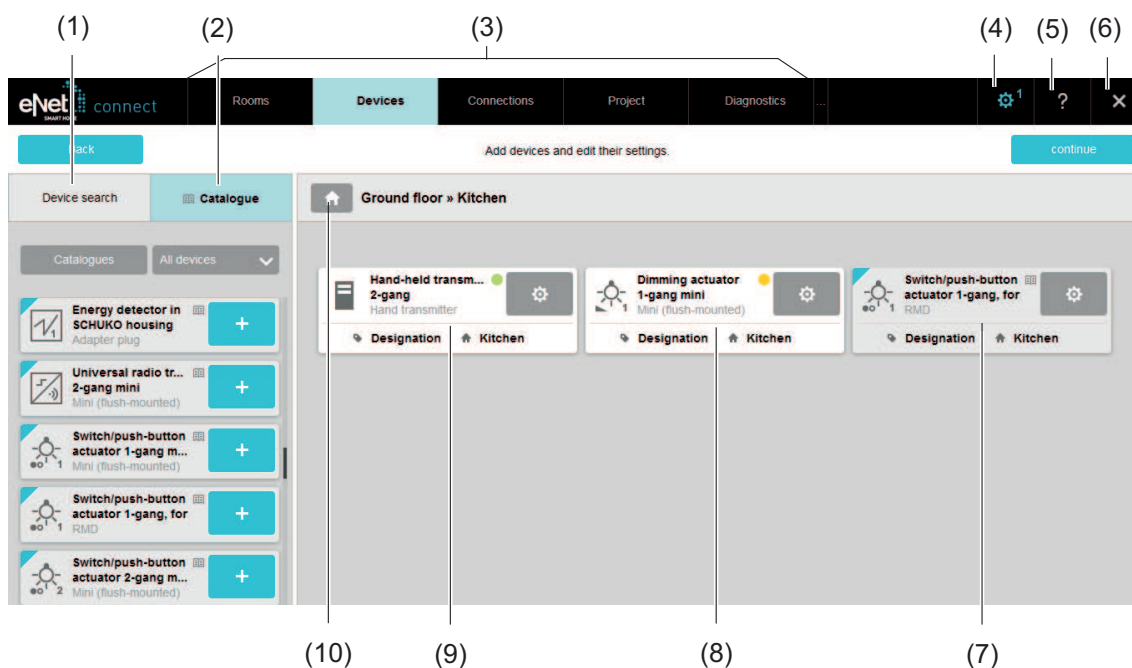The structure of the commissioning interface is shown using the example of the **Devices** view.



Figure 3: The commissioning interface - example of the Devices view

(1) Devices from the device search
(2) Devices from the catalogue
(3) The views
(4) Switch to the system overview, the system settings or the user administration
(5) Open language-dependent product documentation, manufacturer's website or licence information
(6) Close commissioning and switch to the log-on screen
(7) Search for device in the project using serial number (device information window), device name, channel name and device designation  (Figure 11)
(8) Device from the catalogue in the Kitchen room (catalogue device codes: Catalogue icon, blue corner, grey illustration)
(9) Device from the device search in the Kitchen room, not yet programmed (yellow code)
(10) Device from the device search in the Kitchen room, programmed (green code)
(11) Open created building structure for room selection

## 3.1 Illustration of the devices

In the device display, information on the device, such as the device status, can be seen. The status of the devices is illustrated using colour coding.
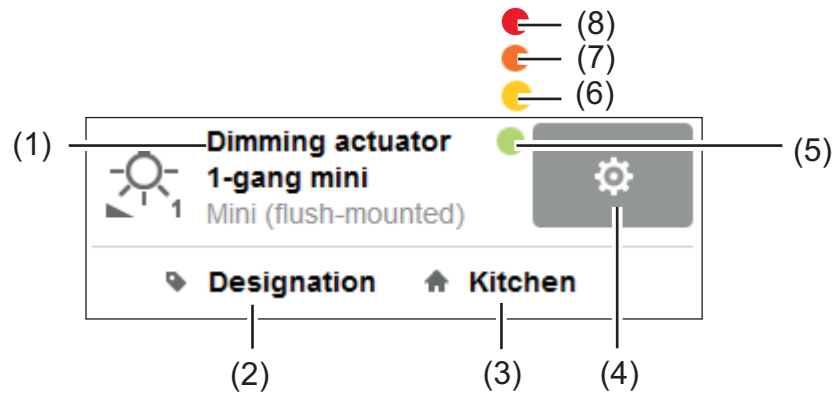
Figure 4: Display of the devices from the installation

(1) Device name
(2) More detailed description of the device location
(3) Device location
(4) Device settings
(5) Green coding: Device is programmed, no changes are available
(6) Yellow coding: Device not programmed, or changes are available
(7) Orange coding: Device cannot be contacted or in an invalid state
    Measure: Restore device (see chapter 8.10. Restore device)
(8) Red coding: No access to the device
    Measure: Check power supply and program the device as necessary

ℹ️  If a device is added to a room, the **device location** (room in which the device is installed, e.g. kitchen) is automatically entered in the device display. The exact description of the device location, e.g. ceiling, can be changed in the device settings (see chapter 8.3. Device settings).
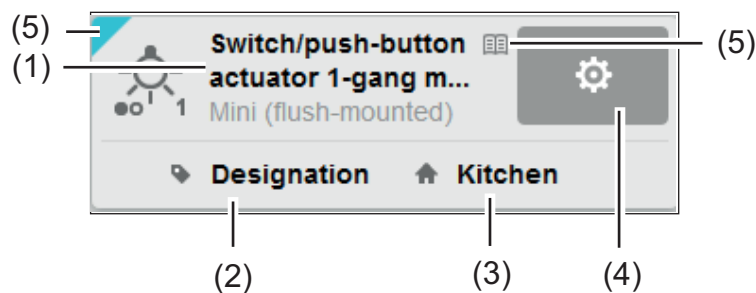


Figure 5: Display of the catalogue devices

(1) Device name
(2) More detailed description of the device location
(3) Device location
(4) Device settings
(5) Codes as catalogue device

## 3.2 Display of the device channels
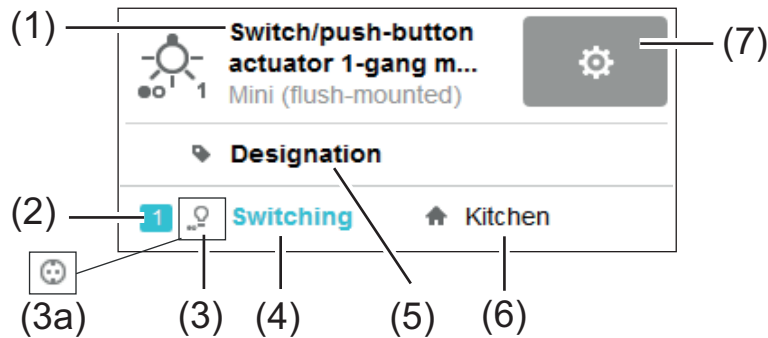
Device channels are shown in the **Connections** view.

Figure 6: Illustration of a device channel

(1) Device name
(2) Channel number
(3) Actuator switches a luminaire or (3a): Actuator switches another load
The icon is displayed in the **eNet SMART HOME app** and is used for targeted operation of the actuators. Channels set to the "Light bulb" icon are also used for the central function "Lighting". This setting can be made in the device settings of a switching actuator.
(4) Channel name, display in the **eNet SMART HOME app**
(5) More detailed description of the device location
(6) Channel location
(7) Device settings

# 4 The user administration

New profiles can be created and existing profiles managed in the user administration. A distinction is made between the roles "Administrator", "User with authorisation for settings of the eNet server" and "App user".

Rights of the "Administrator":
- Access to the commissioning interface incl. system settings and user administration
- Access authorisation to the app for the operation and configuration of the eNet system
- Create and delete user profiles
- Assign and remove authorisation for settings of the eNet server
- Change passwords of users and their own password
- Can obtain remote access for the app, commissioning interface, system settings and user administration

ⓘ    No further administrator can be created. The name cannot be changed. On first log-on, the password is **admin** and should be changed immediately.

Authorisations of the "Users with authorisation for settings of the eNet server":
- Access authorisation for the system settings and user administration
- Access authorisation to the app for the operation and configuration of the eNet system
- Assign and remove authorisation for settings of the eNet server
- Create and delete user profiles
- Change passwords of users and their own password
- Can obtain remote access for the app, system settings and user administration

ⓘ    A user with authorisation for settings of the eNet server has already been created (username: **user**, password:  **user**). Additional users can be created. We recommend not creating more than ten users. There must be at least one user with this authorisation.

Rights of "App users":
- Access authorisation to the app for the operation of the eNet system
- Changing your own password in the user administration
- Can obtain remote access for the app and user administration

ⓘ    Multiple users can be created. We recommend not creating more than ten users.

## 4.1 Creating, changing or deleting a user profile

**Procedure:**

▪    Start the user administration by pressing the 🔲 button in the log-on screen.

ⓘ    The user administration can also be opened via the menu 🔲 or in the first commissioning window  (see chapter 6. First steps in the commissioning of an eNet system).

▪    Select **New user**.

The **Create new user** window is opened.

▪    Enter your user name and password twice.

▪    If necessary, select **User may change settings** for access authorisation to the configuration via the app and the system settings.

     The user profile is created with **Confirm**.

ⓘ    Select the 🔲 button to change a profile. Depending on the authorisation, passwords and the **User may change settings** setting may be changed.

ⓘ    Select the 🔲 button to delete a profile.

# 5 System settings of the eNet server

The window for the system settings of the eNet server is opened using the [⚙] button in the log-on screen.

ℹ️ It is also possible to switch to the system settings via the [⚙] in the menu bar of the commissioning interface.

The following actions can be performed on the tabs of the system settings:
- Perform an update of the eNet server
- Disabling buttons on the eNet server
- Reset eNet server
- Set date and time
- Select the installation location
- Perform network settings
- Set up a connection via https  (see chapter 2.2. Secure connection )
- Configuring remote access to the eNet Server via the Internet

ℹ️ The version of the eNet server can be seen on the **General** tab.

## 5.1 Carry out update

In the **General** tab, an update of the eNet server can be loaded and performed. Updates of the eNet Server, commissioning interface, the device software and the catalogues can be contained in the update.

The current software version of the eNet server can be downloaded from our website as a zip archive. The file for the update of the eNet server with the file ending *.iuf is available in the zip archive.

ℹ️ During a device update, the connection between the computer and eNet Server must be maintained and the web browser must remain open with the commissioning interface during the complete update operation. This is particularly important for an update of battery-powered eNet devices and to display messages which can appear during the operation. For this reason, ensure that the computer does not switch off automatically during the period of the update or switches to the standby state and that that the computer is supplied with power via a power supply unit.

ℹ️ The power supply must not be interrupted during a server update since this could then result in faults of the eNet server.

ℹ️ If there are updates for the device software after a server update, they are displayed in the **system overview** and can be performed there.

ℹ️ Device updates can be performed for a maximum of eight identical devices simultaneously.

ℹ️ Before performing a server update, the project should always be backed up using the **Export project** function.

The actual update must always be performed manually. The loading of an update file can be performed manually or partly automatically. The settings for this can be made in the **Update procedure** list:

**Manual download**

An update must be searched for and the update file uploaded to the eNet server with the **Manual download** setting.

Upload update file manually

- ▪ To select the update file (e.g. from a USB stick), select the [...] button.
- ▪ Select the **Start** button to upload the update file to the eNet Server and to start the update.

Uploading the update file from the Internet

- ▪ Select the **Search** button to search for an update on our website.

  If an update file is available, this is displayed behind **Online update**.
- ▪ If an update is available, select the **Start** button to upload the update file to the eNet Server and to start the update.

**Automatic search**

With the **Automatic search** setting, an update is searched for on our website automatically at regular intervals. If an update is available, then it is displayed in the system settings in the **General** tab behind **Online update** and in the **System overview**.

▪ If an update is available, select the **Start** button to upload the update file to the eNet Server and to start the update.

**Automatic download**

With the **Automatic download** setting, an update is searched for on our website automatically at regular intervals. If an update is available, the update file is uploaded automatically to the eNet Server and displayed in the **General** tab behind **Online update**.

▪ If an update is available, select the **Start** button to start the update.

### 5.1.1 Migrating project after a server update

The update of an eNet Server can potentially support a new device type or enable new performance features for existing devices. These performance features must be transferred to the project. This is done by the migration of the project to the new server version.

After an update, the project is loaded and migrated automatically.

ℹ️ The migration of a project cannot be undone. For this reason, before performing a server update and the subsequent automatic project migration, a project backup should always be performed. The **Export project** function is used for this.

## 5.2 Disabling local operation on the eNet server

Operation via the buttons of the eNet server can be prevented using the **Lock local operation** function in the **General** tab.

ℹ️ It is still possible to restart the eNet Server by pressing the button for a longer period of time (press **RESTART** button longer than 10 seconds).

## 5.3 Perform a factory reset of the eNet server

The eNet server can be reset to the default setting using the **Reset eNet server** function on the **General** tab. At the same time, all project-related data, users and passwords are deleted. The network configuration is reset to the wired connection via LAN with addressing via DHCP. The software state of the eNet Server incl. catalogue remains intact. After a successful reset, the log-on screen appears.

ℹ️ Alternatively, only the network configuration, all users incl. passwords can selectively be reset or the project can be deleted in a targeted fashion using the buttons on the eNet server (see eNet server operating manual).

## 5.4 Set date and time

The system time of the eNet server, consisting of the date and time, can be entered manually or synchronised internally at a defined time using a time server, the so-called NTP server (NTP: Network Time Protocol).

ℹ️ The system time of the eNet server is necessary for telegram recording and for time control using the **eNet SMART HOME app**.

The following options are available for setting the system time of the eNet server:

- Manually enter time: Enter the time and date in the appropriate text boxes and select the time zone
- Apply system time from computer: Select the **Transfer current time** button
- Use time server: Select the **Automatic time (Internet)** function and, if necessary, specify two time servers. Two time servers are preset, which can be used. A time is set for the time of daily synchronisation.
- Take summer time into account: Summer time can be activated manually (**Summer time** function) or automatically (**Summer time automatic** function). If automatic activation is selected and summer time is currently being used, then the **Summer time** function is set automatically, meaning that the two functions are selected.

ⓘ The **Summer time automatic** function only takes summer and winter times within the EU into account.

ⓘ When using the time server, a time zone must be selected, in order to adjust the time according to the time zone.

## 5.5 Enter the installation location

On the **Location** tab, the Installation location can be selected from a list or the coordinates can be entered manually. Specifying the location takes seasonal sunrise and sunset times into account.

ⓘ The specification of the installation location is necessary for time controllers via the **eNet SMART HOME app** in conjunction with the astro function.

## 5.6 Network settings

A wired network connection (LAN) via a router is required for the first commissioning of the eNet Server. Addressing takes place automatically via DHCP. In the as-delivered state, the eNet Server is appropriately preconfigured.(see chapter 2.1. Setting up the connection to the eNet server).

If first commissioning of the eNet server has taken place, various settings such as addressing via the fixed IP address and wireless connection via WiFi can be be made in the system settings on the **Network** tab.

### 5.6.1 Addressing

The connection to the eNet server can also be made using a fixed IP address. The corresponding IP address, subnet mask and standard gateway of the eNet Server are stored in the system settings (see table), where they can be changed and activated.
If the fixed IP address is set as addressing, a DNS server must be stated, so that all the services of the eNet Server function. When using a router with an integrated DNS address, the router address is stated as the DNS server. If the router used has no integrated DNS server, then the address of the DNS server of the Internet provider must be entered.

ⓘ The eNet server can be set to "Addressing via fixed IP address with LAN" using the buttons on the eNet server (see operating manual of the eNet server).

| IP parameters | |
|---|---|
| IP address | 192.168.0.22 |
| Subnet mask | 255.255.255.0 |
| Standard gateway | 192.168.0.1 |

### 5.6.2 WiFi settings

After first commissioning of the eNet server, the network connection can also be wireless. The WiFi parameters of the eNet server must be set accordingly in the system settings on the **Network** tab.

**Procedure:**
- Select **WiFi active**.
- Enter the **SSID name** of your network.
- Select the encryption type.
- Enter the WiFi network key.

ⓘ When the **Show key** checkbox is checked, the WLAN network key is only shown if the key is changed. Switching tabs within system settings does not save the new key. The key is only saved when you leave system settings or by clicking the **Apply** button.

ⓘ This unique key must be used in every device equipped with a WiFi router in the selected radio network.

ⅈ   The LAN cable must be removed for the wireless connection via WiFi.

ⅈ   The connection to the eNet Server can also be made using the fixed IP address of the eNet Server, if the addressing has been configured correctly (see chapter 5.6.1. Addressing). Addressing can be selected via a router with DHCP (see chapter 2.1. Setting up the connection to the eNet server).

### 5.6.3 Basic principles

IP address
Each subscriber must have a unique IP address in order to be accessible in a network.

Subnet mask
To distinguish between the individual networks, the IP address is divided into the network component and the device component. The network component addresses the network and the device component addresses the network subscribers (e.g. PC or eNet server). Which part of the IP address belongs to the network component and which to the device component is determined by the subnet mask.

DHCP
The eNet server can be addressed using a fixed IP address or, if a router with an integrated DHCP server is connected, using a DHCP (Dynamic Host Configuration Protocol).
With DHCP, network settings of the individual terminals, such as the IP addresses, can be coordinated automatically and configured centrally by the DHCP server (e.g. router in a home network). When DHCP is activated, each time the power supply is switched on, the eNet server requests its IP address of the DHCP server, along with the corresponding parameters such as subnet mask, standard gateway and, if necessary, DNS address.

DNS Server
If the router has a DNS server, the IP address of the eNet server is not always required. The eNet server can be accessed via its domain name. The DNS server, which stored the assignment of domain name and IP address, ensures the connection between the eNet server and the computer.

## 5.7 Remote access to the eNet server

Remote access to the eNet server via the Internet is possible using remote access. Remote access allows access to the commissioning interface, the system settings and the user administration. In addition, remote access to the eNet system is possible via the **eNet SMART HOME app**.
For this, once-only user registration at **my.enet-smarthome.de** is required. Then, remote access must be activated either via the system settings of the eNet server or using the **eNet SMART HOME app**. If activation takes place via the app, then remote access for the smartphone used is also activated.

ⅈ   Port 8443 in the network is used for remote access. Thus, this port must be enabled in the WiFi router (or in an additional firewall) for outgoing connections. This is usually set by default on WiFi routers, meaning that no changes need be made. However, if remote access does not work, check this setting in the network.

ⅈ   The first activation of remote access for an eNet server is free of charge for a test period. A paid-for extension is available at **my.enet-smarthome.de**. If no extension has taken place by the end of the free test period, then remote access is deactivated automatically and no further costs are incurred.
To activate the free test period, it is sufficient to create a user account at **my.enet-smarthome.de** and activating remote access, using the user data in the app or in the system settings.

ⅈ   The use of remote access beyond the test period can be extended for a fee at **my.enet-smarthome.de**. Activated remote access can be deactivated again there at any time.

ⅈ   Depending on the distance to the eNet server and Internet bandwidth, long response times must be expected when operating the eNet system via remote access.

ⅰ   After activating remote access, remote access to the commissioning interface can take place from directly **my.enet-smarthome.de**. Click the corresponding link to the eNet Server. If the web browser used supports a popup blocker, this must first be deactivated.

**Register remote access at my.enet-smarthome.de**

The once-only registration by the user to create a user account for remote access takes place at **my.enet-smarthome.de**.
The activated eNet servers can be seen on **my.enet-smarthome.de** and remote access can be deactivated for the eNet Server and the apps here. Deactivation deletes the server data and disconnects all connected apps. Remote access is then no longer possible.

**Activation of remote access via eNet SMART HOME app**

ⅰ   Precondition: The user has set up an account at **my.enet-smarthome.de** and the free test period for the eNet server has not yet expired or an extension was paid for.

ⅰ   Precondition: The user is connected to the eNet server via the home network.

▪   Select **Remote access** in the System menu of the app.

▪   Enter and activate the personal user data at **my.enet-smarthome.de** (e-mail address and password).

   Remote access for the eNet system and the smartphone used is activated and the eNet server is registered under **my.enet-smarthome.de**. The registration can be seen in the system settings of the eNet server and at **my.enet-smarthome.de**. The **Allow remote access** setting is activated automatically in the system setting. Remote access to the eNet system is possible.

ⅰ   With activated remote access, the **eNet SMART HOME app** connects automatically with the home network via WiFi as soon as the app is located within the range of the home network.

ⅰ   This operation must be performed for every user to receive remote access to the eNet system with the same user data on their smartphone.

ⅰ   Deactivation of remote access in the app only deactivates remote access for the smartphone used. Other users of the eNet system with activated remote access are not affected by this.

**Activation of remote access via the eNet server**

Activation of remote access is performed in the system settings on the **Remote access** tab.

ⅰ   Precondition: The user has set up an account at **my.enet-smarthome.de** and the free test period for the eNet server has not yet expired or an extension was paid for.

ⅰ   Precondition: The user is connected to the eNet server via the home network.

▪   Enter the personal user data at **my.enet-smarthome.de** (e-mail address and password).

▪   Select **Activate remote access**.

   The eNet Server is now registered at  **my.enet-smarthome.de**.

▪   Activate **Allow remote access** to allow remote access to the eNet server.

   Remote access to the eNet system is now possible.

ⅰ   If remote access is also to be possible via the e**Net SMART HOME app**, then this function must also be activated again there.

ⅰ   Remote access cannot be fully deactivated in the system settings of the eNet Server. However, the **Allow remote access** function can be used here to block an activated remote access to the eNet system for all app users and for access to the eNet server via **my.enet-smarthome.de**.

# 6 First steps in the commissioning of an eNet system

The first step for the commissioning of an eNet system via the eNet server is the creation of the project.

After the first start of the commissioning interface, a window opens, in which a new project can be created or an existing project imported (10) and the first basic settings made.
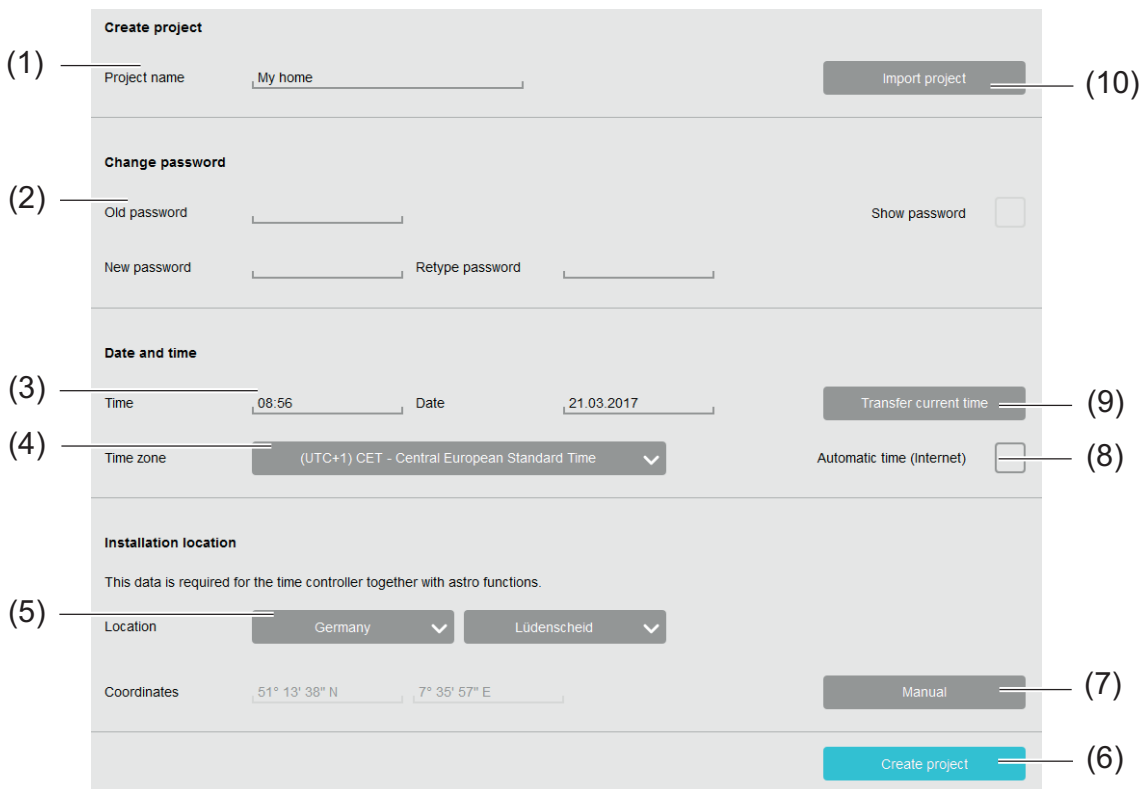
Figure 7: Create project and basic settings window

**Procedure:**
- Enter a project name (1).
- Change the password for access to the eNet Server (2).
- ℹ For security reasons, the password should be changed the first time the eNet server is used. The user name for commissioning is always **admin** and cannot be changed.
- Enter the date and time manually (3) or apply the current system time of the computer (9) or select **Automatic time (Internet)** (8)  (see chapter 5.4. Set date and time).
- ℹ If, on starting, the eNet server finds a time server, then it used as the default setting.
- ℹ  The date and time are necessary for the display during telegram recording and for time controllers using the app.
- Select the time zone from the list (4).
- Specify the installation location (5) or enter the coordinates manually (7).
- ℹ **eNet SMART HOME app:** The specification of the location is necessary for time controllers in combination with the astro function of the app.
- Select **Create project** (6).

# 7 Rooms view

After project creation, the system automatically switches to the **Rooms** view for the creation of the building structure.

The building structure consists of so-called areas and floors, in which rooms are created. The names of the areas, floors and rooms can be chosen freely and can consist of a maximum of 15 characters. Rooms without an area assignment could be a garage or a summerhouse, which cannot be assigned to a floor or an area.

ⓘ **eNet SMART HOME app**: The created building structure with its areas, floors and rooms is used for display and orientation in the app. Device channels assigned to the room of of their action, so that targeted access to the consumers is possible via the app.

## 7.1 Create and change the building structure

The building structure is created through the creation of areas and floors (1) and the rooms (8) (Figure 8).

The building structure can be changed later on. Areas, floors and rooms can be renamed or deleted. The functions become visible when the cursor is moved over a graphical element, e.g. room, (5) and (6). Areas, floors and rooms can also be moved by drag & drop  (Figure 8) (7).
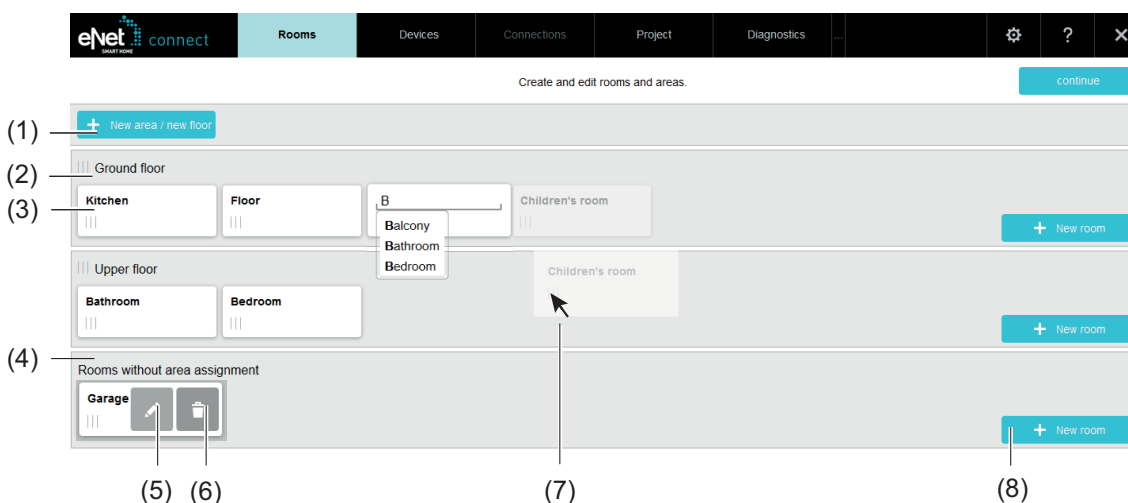


Figure 8: Rooms view - Example

(1)   Add area/floor

(2)   Floor in the building structure, e.g. ground floor

(3)   Room in the building structure, e.g. kitchen

(4)   Area for rooms without an assignment to an area, e.g. garage

(5)   Rename room

(6)   Delete room

(7)   Move room

(8)   Add room to an area or a floor

ⓘ   When a room is deleted, the devices contained in the room are deleted. A room cannot be deleted if it contains devices from a programmed connection. The connection must be deactivated in advance.

ⓘ   When moving a room to another area or another floor, the devices remain in the room and are moved with the room into the other area or other floor.

ⓘ   Areas are moved, renamed and deleted in the same way as rooms are.

ⓘ   In the next step, the assignment of the devices to the rooms in the building structure is formed. The **Next** button is used to switch to the **Devices** view.

ⓘ With touch operation, e.g. on an iPad, the mouse-over functions (5) and (6) appear when the element is pressed for a longer period of time.

# 8 Devices view

After creating the building structure in the **Rooms** view, the devices can be configured in the next step and the rooms added in which they are installed.
Devices of the installation or catalogue devices can be used for this commissioning step. Installation devices are read into the eNet server via a device search. Catalogue devices must later be replaced with installation devices via a device search.

ⓘ **eNet SMART HOME app**: The app displays the channel name and channel location for operation or further use, e.g. for creating scenes. The channel name and channel location are specified in the **Devices** view of the commissioning interface in the device settings when adding the devices.
As soon as an actuator channel is assigned to a room and a channel has been assigned, it can be used in the app.

## 8.1 Add devices to the eNet system

For commissioning with devices of the eNet system, the devices are read into the eNet server using the device search in the commissioning interface.
When adding a device to a room, it is possible to configure devices and their device channels directly  (see chapter 8.3.1. Configuring the device).

Devices from the device search can

- be added to the project as a new device
- Replacing catalogue devices in the project
- Replace the installation devices in the project, e.g. a defective device

ⓘ When replacing the catalogue devices with system devices, the device and channel settings and connections are transferred.

ⓘ The connection data and settings of a device can be transferred or rejected when inserting the device via a device search.

ⓘ The settings on the operating mode switch of a device are applied during the device search. If the operating mode switch on the device is set to the **PC** position, the setting of the operating mode and channel settings of the actuators (e.g. switching or Venetian blind for the switching/Venetian blind actuator) can then take place in the commissioning interface. If the operating mode switch is in another position than **PC**, then these settings can no longer be changed in the commissioning interface.

ⓘ If a defective device is to be replaced, the new device must be read in using the device search and replaced in the project.

ⓘ If a device to be replaced with a new device remains in the system, this can lead to malfunctions. The device must be disconnected from the mains or reset  (see chapter 8.9. Reset device).


Information on the device search

- The device search finds the devices which have been switched directly to programming mode or in which the supply voltage was interrupted and restored within the last 3 minutes. In the case of RMD devices, it may be necessary to interrupt the voltage for several minutes, since the power supply unit stores energy. In the case of devices that are not directly accessible, the voltage interruption and restoration is a wise idea.
- Only those devices that do not already exist in the current project are found in the device search.
- However, the device search is terminated automatically by the eNet Server when switching to another view or the commissioning interface is closed. To avoid unnecessary telegram traffic, the device search should be terminated after all the devices have been read in, using the **Stop search** function.
- The list of found devices not yet added to the project is deleted when the device search is restarted.

- During a device search, the devices cannot be reset to the default setting using the buttons of the eNet Server.
- With an encrypted project, during the period of a device search, the project is deactivated for the project export, meaning that all the functions executed via the eNet Server, such as time controls, are not available during this period. After the end of the device search, the project is reactivated automatically and functions started as appropriate.
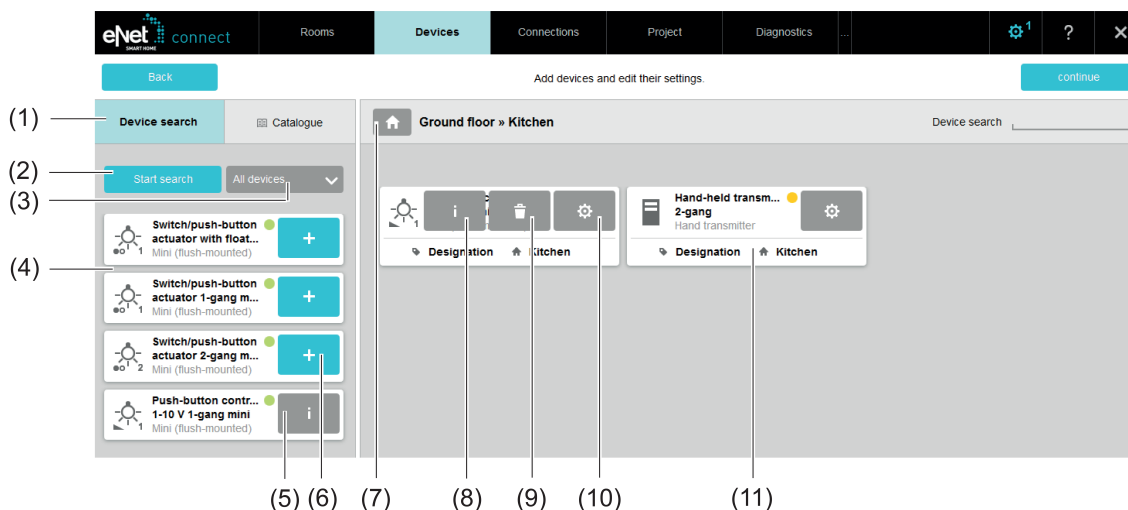


Figure 9: Add a device from a device search - Example

(1) **Device search** tab
(2) Start/stop device search
(3) Filter list according to sensors, actuators or repeaters
(4) List of found devices from the device search
(5) Device cannot be added to the project, e.g. because it is contained in another eNet project
(6) Add the device to the selected room or add via drag & drop
(7) Select the room from the building structure, in which the device to be added is installed (installation or device location)
(8) Recall device information
(9) Remove devices from the project
(10) Recall device settings
(11) Device in the project (from device search), already programmed (green code)

**Procedure:**
- Select a room from the building structure (7).
- ⓘ If no room has been selected before this, the building structure is shown automatically for room selection on switching to the **Devices** view.
- Select the **Device search** tab (1).
- Select **Start search** (2).
- Switch the devices to programming mode or interrupt the power supply for at least 10 seconds.
  The list of the devices found is displayed (4).
- If necessary, filter the device selection according to sensors, actuators or repeaters (3).
- Add the devices to the selected room using the ⊞ button or via drag & drop.
  The device settings window opens  (Figure 11) and (Figure 12).

ⓘ A device is replaced in the project by a device from the current device search by dragging the new device onto the device to be replaced (drag & drop method). If the ⊞ button was selected, then the device to be replaced can be selected from a list.

■ Make the settings and apply them with **Save** or **Close** (Figure 11).

The device is added to the selected room and the as yet unprogrammed device is shown in yellow.

ⓘ During the next programming operation, the device data is saved to the devices. The code in the device display changes from yellow to green.

ⓘ On adding a previously used device as a new device, device data, such as the parameters and connections to other devices, can be transferred with the **Import device data** function or rejected with the **Reset device data** function.

ⓘ If a device of the same type already exists in the room, then the device can be added as a new device or be exchanged with a device from the installation or can replace a catalogue device. When replacing catalogue devices with devices of the installation, device data, such as the parameter settings and connections, is transferred automatically. The devices must then be programmed.

ⓘ With touch operation, e.g. on an iPad, the mouse-over functions (8) and (9) appear when the element is pressed for a longer period of time.

### 8.1.1 Troubleshooting in the device search

**Why are eNet devices not found during the device search?**

Cause 1: Devices are out of radio range.

Measure: Reduce the distance or insert an additional repeater.

Cause 2: Devices are not in programming mode or the supply voltage has not been restored within the last 3 minutes.

Measure: Switch the device to programming mode.

Cause 3: The eNet server is connected together with a RMD reception module.

Measure: Disconnect the cable connection to the RMD reception module and remove the device from the system.

Cause 4: The device already exists in the project.

**Why can a device found using the device search not be inserted into the project?**

Cause 1: The device was already a part of another project and was not removed correctly from the project or the device is part of another system.

Measure: End the device search and carry out a reset to the default setting on the device (see device operating manual).

Cause 2: No room was selected.

Measure: Select room.

## 8.2 Adding catalogue devices

Commissioning of the eNet system can take place partially or entirely with catalogue devices. The catalogue devices can be replaced with devices from the system in a later workstep, meaning that parameters and connections are applied automatically. For this, the devices of the system must be read in via a device search.

ⓘ Catalogues of various manufacturers of the eNet Alliance are stored in the eNet server and can be shown in a targeted manner.
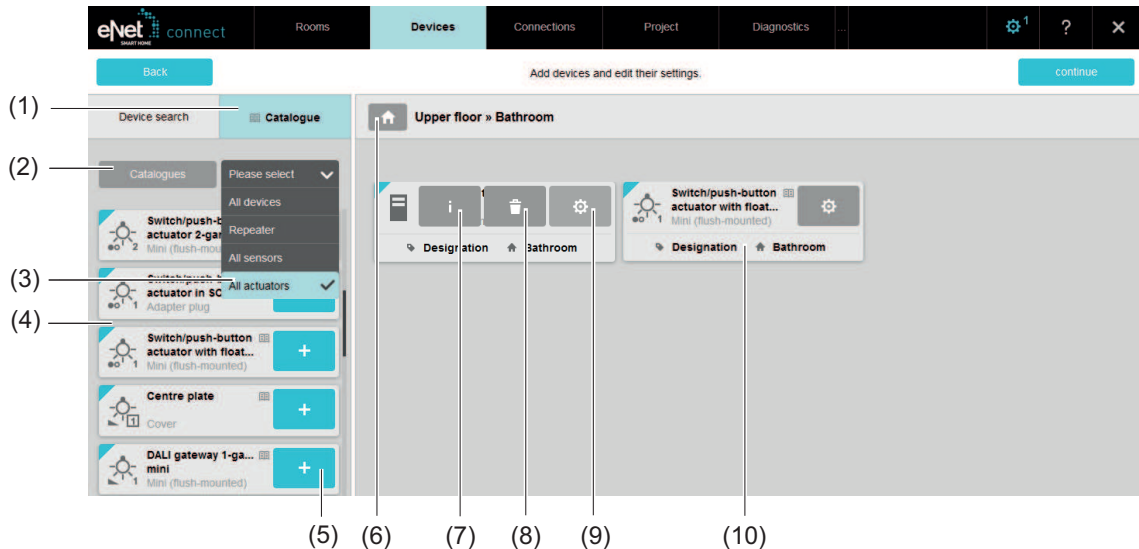
Figure 10: Adding catalogue devices - Example

(1) **Catalogue** tab
(2) Select catalogues of different manufacturers
(3) Filter list according to sensors, actuators or repeaters
(4) List of the catalogue devices
(5) Add catalogue device to the selected room
(6) Select the room from the building structure, in which the device to be added is installed (installation or device location)
(7) Recall device information (restricted for catalogue devices)
(8) Catalogue device in the project
(9) Open device settings
(10) Catalogue device added to the room

**Procedure:**
- Select the room from the building structure, in which the device to be added is to be installed (6).
- ℹ️ If no room has been selected before this, the building structure is shown automatically for room selection on switching to the **Devices** view.
- Select the **Catalogue** tab (1).
- If necessary, select the required manufacturer catalogue using the **Catalogue selection** button (2).
- If necessary, filter the device selection according to sensors, actuators or repeaters (3).
  The devices of the catalogue are displayed (4).
- Add the device using the ⊞ button (5) or via drag & drop.
  The device settings window opens  (Figure 11) and (Figure 12).
- Make the settings and apply them with **Save** or **Close** ..(Figure 11) and (Figure 12).
  The device is added to the selected room.
- ℹ️ Before the eNet system is handed over, catalogue devices should be replaced with devices of the installation (see chapter 8.1. Add devices to the eNet system).
- ℹ️ Catalogue devices are not displayed in the **eNet SMART HOME app** and can only be replaced with devices of the eNet system.

## 8.3 Device settings

On adding a device, device settings can be made in the **Devices** view and are dependent on the device type.

For later changes, the window for device settings can be opened using the ⬚⚙ button in the device display  (Figure 10) (9).

The following settings are possible:

- Name device channels, e.g. channel location "Kitchen", channel name "Venetian blind"
- Configure device channels, e.g. switch to "Switching" on the switching/Venetian blind actuator
- Set the parameters of the devices and device channels, e.g. disable manual commissioning on the device, disable local operation by channel
- Set multi-device parameters, e.g. activate repeater mode
- Configure the buttons for use in the **eNet SMART HOME app**

ⓘ Descriptions of the individual device parameters can be recalled in the device settings via the ⬚ⓘ button.

ⓘ The device must be accessible via radio in order for the eNet server to access devices. If necessary, battery-operated devices must be "woken up" through on-site actuation.

### 8.3.1 Configuring the device

The window for the device settings is opened on adding a device or via the ⬚⚙ button and is explained using an example for a transmitter  (Figure 11) and an actuator  (Figure 12)
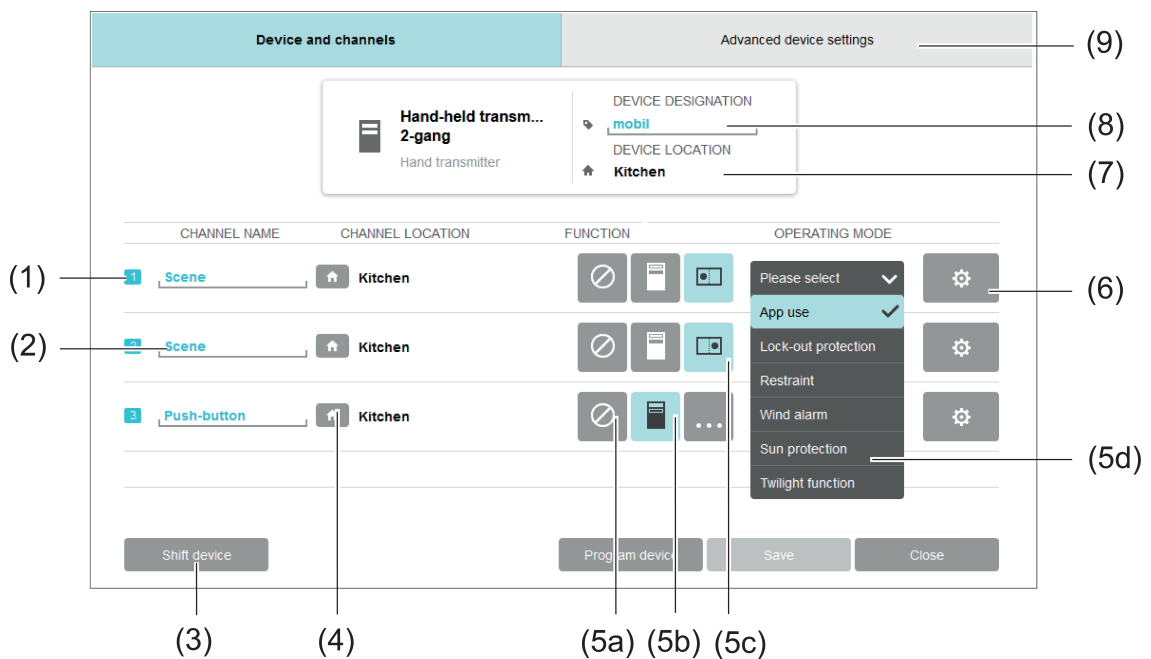


Figure 11: Device settings window - Example of 2x hand-held transmitter

(1)   Channel number

(2)   Assign or change the **channel name**. **eNet SMART HOME app**: The channel name is displayed in the app for the use of the device channels.

(3)   Move the device to another device location. **eNet SMART HOME app**: The app displays the channel locations and the device channels assigned to the channel location.

(4)   Select the **channel location**.

(5a) Select Do not use channel. On activation, the channel is not displayed in the **eNet SMART HOME app** and is disabled for use in the commissioning interface.

(5b) Configure the button as a rocker (for use in connections). Buttons are preconfigured as rockers and are required for direct operation of actuator channels.

(5c) Configure the button for the use of disabling and threshold value functions or for use in the app. Disabling and threshold value functions are created in the **Connections** view.

(5d) Configure the button to one of the disabling and threshold value functions or for use in the app. **eNet SMART HOME app**: **App use** must be selected here for use in the app.

(6) Recall channel settings (see chapter 8.3.3. Channel settings).

(7) Display of the device location (automatically entered on adding the device to a room)

(8) More detailed description of the device for identification in the project.

(9) **Advanced device settings** tab, set to the device parameter and functions such as **Reset device** and **Localise device** can be activated.

[i] The **channel location** specifies the room, where the sensor or actuator channel is active. Example: An actuator in the cellar switches the luminaire in the living room. Here, the device location is the cellar and the channel location is the living room.

[i] The **device location** specifies the room in which the device is installed.
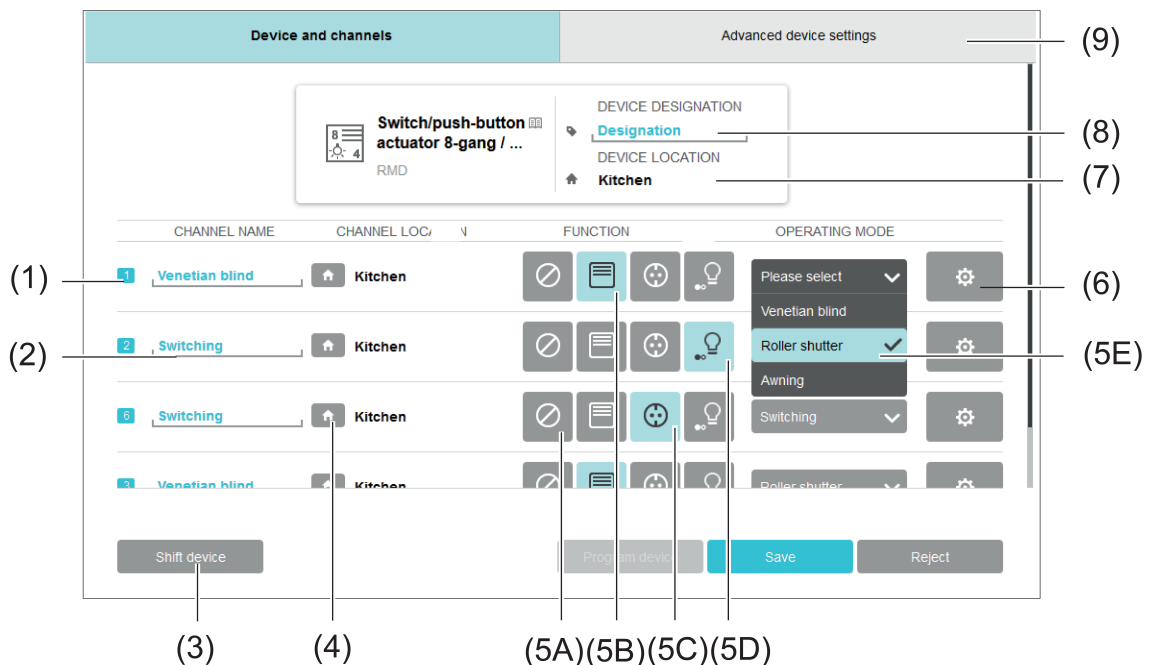


Figure 12: Device settings window - Example of switching/Venetian blind actuator

(1) Channel number

(2) Assign or change the **channel name**. **eNet SMART HOME app**: The channel name is displayed in the app for the use of the device channels.

(3) Move the device to another device location.

(4) Select the **channel location**. **eNet SMART HOME app**: The app displays the channel locations and the device channels assigned to the channel location.

(5A) Select Do not use channel. On activation, the channel is not displayed in the **eNet SMART HOME app** and is disabled for use in the commissioning interface.

(5B) Set the channel type to Venetian blind.

(5C) Set the channel type to Light. **eNet SMART HOME app**: Channel is used for the Lighting central function in the app. The [icon] icon is displayed in the app.

(5D) Set the channel type to Switching. If switching over the channel type from Venetian blind to switching when there is a connected load, disconnect the load from the circuit. Otherwise, the Venetian blind motor can be damaged. **eNet SMART HOME app**: The ⊚ icon is displayed in the app for the switching of loads. No use for Lighting central function.

(5E) Select the operating mode of the channel.

(6)  Recall channel settings  (see chapter 8.3.3. Channel settings).

(7)  Device location (automatically entered on adding the device to a room)

(8)  More detailed description of the device for identification in the project.

(9)  **Advanced device settings** tab, set to the device parameter and functions such as **Reset device** and **Localise device** can be activated.

ⓘ  **eNet SMART HOME app**: All the actuator channels added to rooms and assigned for the Light and Venetian blind units are automatically integrated into central functions of the app. This means that, in one operating step, actuator channels, to which a unit belongs, e.g. light, can be operated. Central functions are created for the entire project, for each area and for each individual room.

ⓘ  The **channel location** specifies the room, where the sensor or actuator channel is active. Example: An actuator installed in the cellar switches the luminaire in the living room. Here, the device location is the cellar and the channel location is the living room.

ⓘ  The **device location** specifies the room in which the device is installed.

## 8.3.2 Setting device parameters

Parameters affecting the entire unit can be set in the **Advanced device settings** (e.g. disabling local operation).

ⓘ  Descriptions of the individual device parameters can be recalled in the device settings via the ⓘ button.

ⓘ  The **Advanced device settings** tab also contains supplementary functions for the devices, e.g. **Reset device**, **Localise device**, which are described in special chapters.

## 8.3.3 Channel settings

The channel settings for each device channel can be reached via the ⚙ button  (Figure 12) (6). Basic parameters can be set, for example, in the **Channel settings** tab, operating hours read off and reset. Additional settings, such as the parameters of the device channels, are possible in the **Advanced channel settings** tab.

ⓘ  Descriptions of the individual device parameters can be recalled in the device settings via the ⓘ button.

ⓘ  With energy sensors, the measured values (voltage, current, active/reactive power, etc.) can be read off.

# 8.4 Device information

The use of device channels in connections is displayed in the device information and channels can be controlled. Additional information on the device, such as the article number, serial number and device location can also be seen there.

ⓘ  The device information can be recalled via the ⓘ button.

The amount of information displayed in the information window is dependent on the device type. The information windows are described below using the example of a 1-10 V control unit.
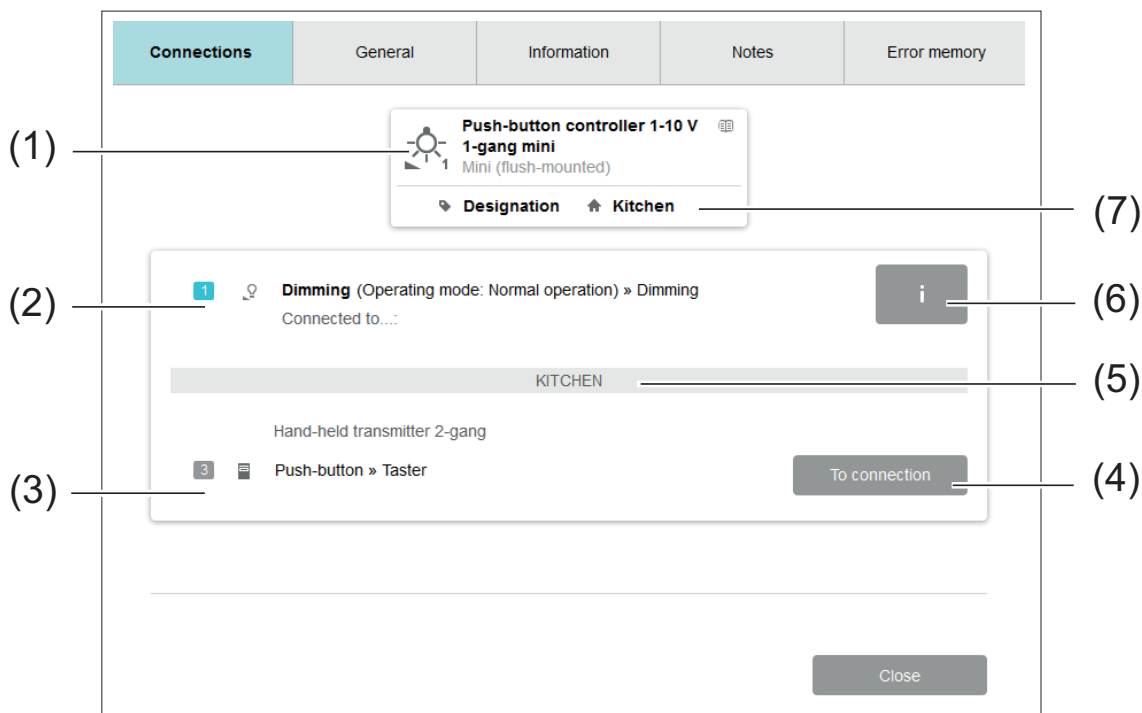
**Connection tab**



Figure 13: Device information - Connections tab

(1) Display of the selected device
(2) Device channel of the actuator with channel name (dimming)
(3) Connected device channel of a sensor with channel name (dining table light)
(4) Switch to the connection the channels in the **Connections** view
(5) Channel location of the subsequent device channels
(6) Information on the device channel
(7) Device location of the selected device

**General tab**

Control of the channels is possible via the **General** tab. In addition, the item number and device name are shown.

**Information tab**

The **Information** tab contains device information, such as the device location, item number, product group code, design, phase-out code, battery and parameter status.

**Notes tab**

In the **Notes** tab, it is possible to enter notes, e.g. the connected load. The notes on the device are output in the project report  (see chapter 10.2. Create project report).

**Error memory tab**

Switching to the **Error memory** tab reads out and then displays the error memory of the device. If there is an error, the displayed text is required for Support.

## 8.4.1 Channel information

Using the ⓘ button, the channel information in the **Connections** tab can be recalled in the device information (Figure 13) (5).
In the **Channel control** tab of the actuator channels, it is possible to control the channels and

read off the status of the forced operation.

In the **Channel information** tab, the operating hourscounter can be reset and information on channel use is visible.

ⓘ  With dimming actuators, the set dimming principle can be read off.

ⓘ  With energy sensors, the measured values (voltage, current, active power, reactive power and apparent power and absolute active energy) can be read off.

## 8.5 Search for a device in the project

In the Devices view, the following search criteria can be used to search for devices in the project:

- Serial number (see device information)
- Device name (see device settings or device information)
- Channel name (see device settings)
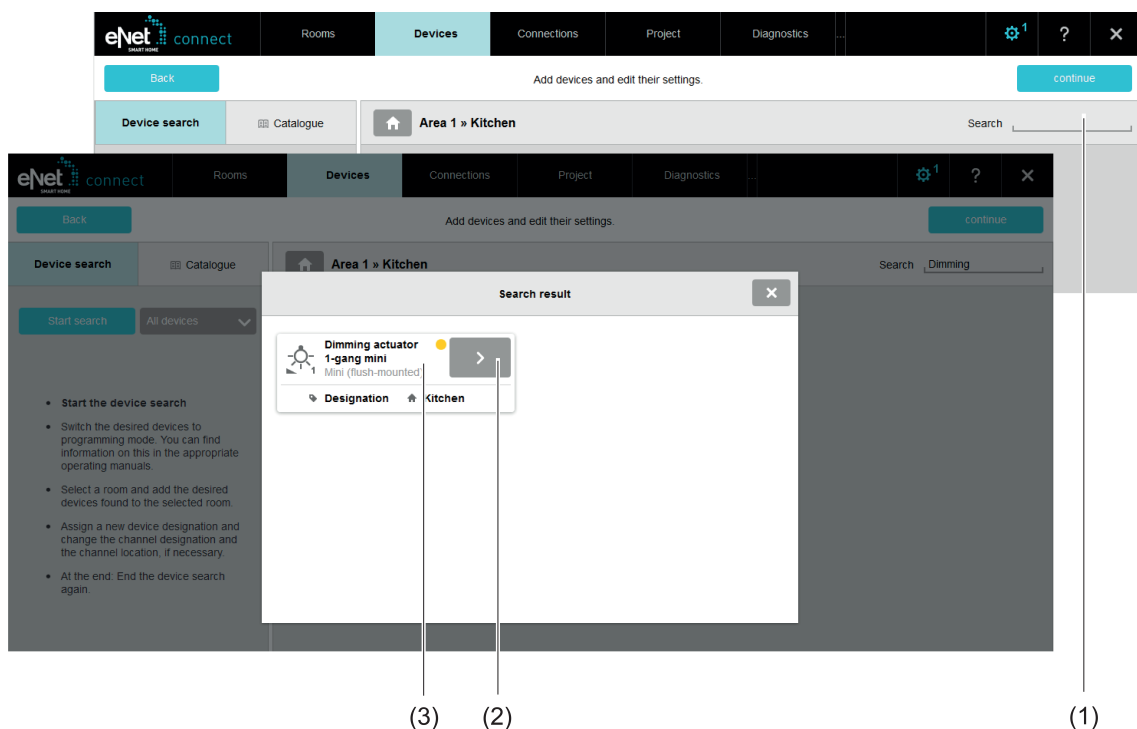- Device designation (see device settings)



Figure 14: Search for devices in the project

(1)  Enter search criterion

(2)  Switch to the device that was found

(3)  Device that was found

**Procedure:**

■  Enter search criterion (1)  (Figure 14).

   When entering the initial letters, project-specific search criteria will be offered as a list.

■  Start the search using the ENTER key or select a criterion from the list.

   A window with the devices that were found is opened  (Figure 14).

■  Use the arrow key (2) to switch to the device that was found.

   The device that was found is outlined in blue. If the device is located in another device location, a switch is made to this device location.

ⓘ Use the **Back** button to switch back to the original device location. The blue outline and the **Back** button are removed using the **X** button.

## 8.6 Deleting a device from the project

Devices can be removed from the project using the **Delete device** button  (Figure 10) (8). In so doing, device data, such as device and channel settings, is reset and connections to other devices are deleted.

ⓘ To avoid miscommunication of the previously connected devices, the devices remaining in the project must be reprogrammed. The devices that must be reprogrammed are listed in the system overview  (see chapter 12.1. System overview).

ⓘ If a device is removed from the project to which the eNet server has no access at this time, the information and parameters remain in the device. To add the device to the same or another project via a device search, a factory reset of the device must be performed first - see the operating manual of the device.

## 8.7 Shift device

Devices can be moved to another device location in the device settings using the **Shift device** function  (Figure 12) (3). The device location is updated in the device display  (Figure 4) (3).

## 8.8 Localise device

A device in the installation downloaded via the device search and added to the project can be added using the **Localise device** function.

**Procedure:**

- Select the ⌗ button in the device display.
- Select the **Advanced device settings** tab  (Figure 12) (9).
- Select **Localise device**.

  A window opens with the device display.
  To localise an actuator, the connected load is switched on and off periodically (approx. every 4 seconds), depending on the type of the actuator. Venetian blind drives move alternately up and down approximately every 4 seconds. To localise a sensor, the LED on the sensor flashes red every second. If necessary, battery-operated devices, such as hand-held and wall transmitters, must be "woken up" through on-site actuation. This should be repeated with other hand-held and wall transmitters until the transmitter to be localised is found using the flashing signal.

## 8.9 Reset device

The parameters are reset to the factory setting and connections to other device channels are deleted using the **Reset device** function. However, the device is not deleted from the project. The function can be recalled via the **Advanced device settings** tab  (Figure 12).

**Procedure:**

ⓘ If the device is linked to other devices in one or more connections, then the connections must be deactivated in the first step (see chapter 9.4. Deactivating connections).

- Select the ⌗ button in the device display  (Figure 10) (9).
- Select the **Advanced device settings** tab  (Figure 12) (9).
- Select **Reset device**.

  Connections to other devices are deleted. The parameters of the device are set to default values. The settings on the operating mode switch of the device are transferred again after the device is reset.

## 8.10 Restore device

If a device from a project is reset, the eNet Server can no longer reach the device. The device is coded red in the commissioning interface. The device can be restored from the project with its

device data using the **Restore device** function. In addition, devices in an invalid state and coded orange can be restored using this function.

**Procedure:**
- Select the [⚙] button in the device display  (Figure 10) (9).
- Select the **Advanced device settings** tab  (Figure 12) (9).
- Select **Restore device**.
- Switch the device to programming mode.
- ⓘ The device may only be switched to programming mode if the **Restore device** function was recalled in advance.

  The device can again be reached by the eNet Server and writes the device data from the project to the device.

## 8.11 Adding a repeater

To extend the range of the eNet system, an eNet repeater can be used or the repeater mode of a mains-powered eNet device activated. Whilst the repeater mode of mains-powered devices receives all the unfiltered eNet radio telegrams and transmits them onwards, the eNet repeater used as an adapter can alternatively only repeat the telegrams of selected devices, leading to considerably lower telegram traffic.
Repeaters should only be used in a very targeted manner, as their use can result in an increased radio load, a lengthening of the reaction times and a shortened battery lifespan for battery-powered devices.
- ⓘ We recommend using a maximum of two repeaters in an eNet system in order to prevent a high level of telegram traffic.

**Procedure for activating repeater mode on a mains-powered eNet device:**
- Add device to the room (see chapter 8.1. Add devices to the eNet system).

  The **Device settings** window opens.
- ⓘ The [⚙] button in the device display of the device can be used to reopen the **Device settings** window (Figure 10) (9).
- Select the **Advanced device settings** tab  (Figure 12) (9).
- Switch repeater mode to **On**.

**Procedure for using the eNet repeater ZS:**
- Add device to the room  (see chapter 8.1. Add devices to the eNet system).

  The **Device settings** window opens.
- ⓘ The [⚙] button in the device display of the repeater can be used to reopen the **Device settings** window (Figure 10) (9).
- ⓘ To ensure that bidirectional communication between the connected actuators and sensors is not interfered with, all the actuators and sensors of a connection must always be added to the repeater.
- Select the **Add device** function and select the appropriate devices from the selection menu.
- The devices are added to the repeater using the **Use devices** button. The received eNet radio telegrams are repeated for the selected devices.
- ⓘ If no devices are added to the repeater, then the repeater will repeat all the eNet radio telegrams.

## 8.12 Delete connections

Devices which were previously used in an eNet system or in the same project of the eNet Server in the past and which were read in via a device search may contain connections to devices not in the project. The **Delete connection** function allows the deletion of connections to unknown devices.

ⓘ All the connections to unknown devices can be deleted simultaneously in the **system overview** (see chapter 12.1. System overview).

**Procedure:**

- Select the ⟨ ☼ ⟩ button in the device display (Figure 10) (9).
- Select the **Advanced device settings** tab (Figure 12) (9).
- Select **Delete connection**.

# 9 Connections view

Actuator and sensor channels are interconnected in the **Connections** view  (Figure 15). A connection between devices creates a particularly fail-safe direct sensor-actuator link, whose configuration is reserved for the specialist carrying out the commissioning. Connections do not need an eNet server to be used and can even be used fully if there is a fault in the eNet server. Connections are not visualised in the **eNet SMART HOME app** nor can they be changed via the app. Sensor channels used in a connection are also not available in the app (e.g. for If-Then rules). This is because the basic installation of the eNet system performed by the specialist should be protected against outside intervention.

The disabling functions **Lock-out protection** and **Restraint** and the threshold value functions **Sun protection** and **Twilight** are also created in the **Connections** view.

In this view, the connections can be programmed individually for direct use. Changes to the programmed connections are possible later on.

The following rules apply to connections:

- Device channels can be used in multiple connections.
- In a connection, all the sensor channels control all the actuator channels.
- To aid structuring, each connection is assigned to a room from the building structure.

A connection can have the following states  (Figure 15) (5):

- Connection is inactive (grey coding): Connection is not yet programmed. Changes are possible. Connection can be programmed.
- Connection is active (green coding): Connection is programmed and active in the eNet system. The connection is disabled for changes. The connection be deactivated or switched to Edit mode.
- Connection in Edit mode (yellow coding): The connection remains active in the devices and can be changed. Changes can be programmed to the devices or rejected.

ⓘ Changes to the device settings of the devices are possible can be programmed directly into the device.
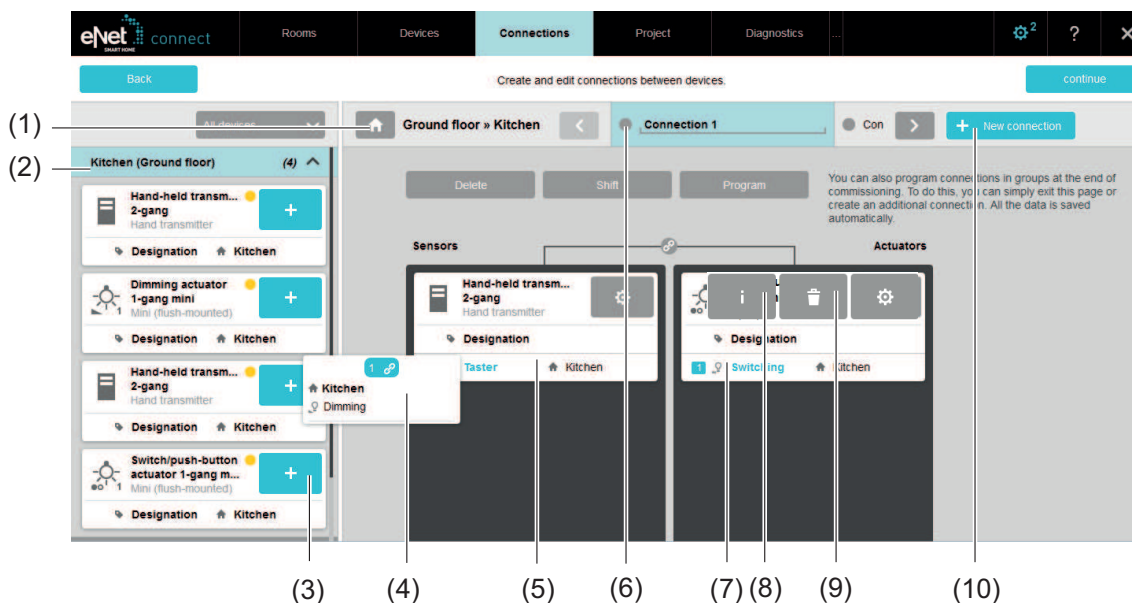
## 9.1 Create connection



Figure 15: Connections view

(1) Select a room for the assignment of the connection
No effect on the app but is used for structuring in the commissioning interface.
(2) Select a room from the building structure for device selection

(3) Add or delete sensor or actuator channels from this device to the channel
   If the button is blue, the device has at least one channel in the selected room
   If the button is grey, the device has no channel in the selected room

(4) Display additional connections of the channel

(5) Sensor channel

(6) Coding of the state of the connection

(7) Actuator channel

(8) Recall device information

(9) Remove device from the connection

(10) Create new connection for further editing

**Procedure:**

- Select the room to which the connection should be assigned (1).
- Select **New connection** to create a new connection (11).
- Enter the name of the connection in the text field.
- Select the room in which the device is installed, whose channel(s) are to be added to the connection (2).
- Add the sensor and actuator channels to the connection using the ⊞ button or via drag & drop (5). Already used channels can be removed again here.

  The **Select channel** window opens, in which the channel settings can be made and the channels selected for the connection. The function and the operation mode of the channel cannot be changed here. This is performed in the device settings.

  **Apply** adds the selected channels and unselected channels are removed.

ⓘ The connection has been created but is not active and must be programmed (see chapter 9.2. Program connection).

ⓘ A channel can be contained in multiple connections. The number of additional connections is displayed on the channel (4). It is possible to switch to a further connection via this display.

ⓘ With touch operation, e.g. on an iPad, the mouse-over functions such as (8) appear when the element is pressed for a longer period of time.

## 9.1.1 Disabling functions

The disabling function **Lock-out protection** and **Restraint** can be created as a connection. Disabling functions are given priority and can override functions without priority. In a connection, one sensor channel for activating 🔒 and one sensor channel for deactivating the disabling function 🔓 are connected to the actuator channels.
If a disabling function with set priority is active, the operation of the appropriate actuator channels is disabled until the disabling function is deactivated. The exception to this is the activation of another function with the same or higher priority. The priority can be set in 4 levels in the channel settings.

The following rules apply to the disabling functions:
- In a connection with disabling functions, additional sensor channels of the same type and actuator channels can be added at a later time
- It is possible to set the behaviour of the actuators when a disabling function is recalled and deactivated in the channel settings of the actuator channel
- The priority of a disabling function can be set on each actuator channel in the channel settings. There are the following priorities: 1 (Highest) to 3 (Lowest) and 0 (No priority).
- Lock-out protection: Priority 1 preset (highest priority)
- Restraint: Priority 2 preset

**Procedure:**

Precondition: The sensor channels are configured for the disabling function (see chapter 8.3.1. Configuring the device).

- Creation connection for the disabling function (see chapter 9.1. Create connection).

- ℹ️ Only one connection must be created for the recall and deactivation of a disabling function.
- ■ Add sensor channels for activating and deactivating the disabling function to the connection using the ⊞ button or via drag & drop.
  The **Select channels** window opens.
- ■ Select the ⚙ button behind the appropriate channel to make channel settings.
- ■ Select the channels and add to the connection with **Apply**.
- ■ Add the actuator channels to the connection using the ⊞ button or via drag & drop.
  The **Select channels** window opens.
- ■ Select the ⚙ button behind the appropriate channel to make channel settings.
- ■ On the **Advanced channel settings** tab, set the parameters for the behaviour of the actuator channel on activating the disabling function, e.g. **Activate Venetian blind position lock-out protection**.
- ■ Set the parameters for the behaviour of the actuator channel on deactivating the disabling function **Behaviour after the end of the disabling function**.
- ■ If necessary, assign a different priority for the disabling function.
- ■ Select the channels and add to the connection with **Apply**.
- ℹ️ The connection has been created but is not active and must be programmed (see chapter 9.2. Program connection).

## 9.1.2 Threshold value function

In a connection, the threshold value functions **Sun protection** and **Twilight** can be created. Threshold value scenes are triggered by falling below or exceeding a threshold value set in the sun sensor and control connected actuator channels. The behaviour of the actuator to take place when the threshold value is exceeded or fallen below is set in the channel settings of the appropriate actuator channel.

The following rules apply to the threshold value functions:
- In a connection with threshold value functions, additional sensor channels of the same type and actuator channels can be added at a later time
- A connection is required for both the **Sun protection** and **Twilight** functions of a sun sensor
- It is possible to set the behaviour of the actuator channels when the threshold value function is activated and deactivated
- The priority of the threshold function is set on each actuator channel
- Sun protection: Priority 0 preset (no priority)
- Twilight: Priority 0 preset (no priority)
- ℹ️ A priority can be assigned to a threshold value function, in order to disable the connected actuator channels until the threshold value function is deactivated. The exception to this is the activation of another function with the same or higher priority. The priority can be set in 4 levels (0 for no priority, 1 for the highest priority, running down to 3).

Below, the creation of a threshold value is illustrated, using the example of sun protection:

**Creating sun protection with a sun sensor**
- ■ Create a connection for the threshold value function (see chapter 9.1. Create connection).
- ■ Add the sun sensor to the connection using the ⊞ button or via drag & drop.
  The **Select channels** window opens.
- ■ Select the ⚙ button behind the appropriate channel to make channel settings.
- ■ Select the **Sun protection** channel and add to the connection with **Apply**.
- ■ Add the actuator channels to the connection using the ⊞ button or via drag & drop.
  The **Select channels** window opens.
- ■ Select the ⚙ button behind the appropriate channel to make channel settings.

- On the **Advanced channel settings** tab, set the parameters for the behaviour of the actuator channel on activating the threshold value function, e.g. **Activate sun protection brightness value**.
- Set the parameters for the behaviour of the actuator channel on deactivating the threshold value function, e.g. **Deactivate sun protection brightness value**.
- If necessary, assign a different priority for the **Sun protection** function.
- Select the channels and add the channel to the connection with **Apply**.

ℹ️ The connection has been created but is not active and must be programmed (see chapter 9.2. Program connection).

### 9.1.3 Wind alarm

Using the **Wind alarm** function, an actuator can be controlled according to a wind speed threshold value. To implement the **Wind alarm** function, a standard wind sensor with relay output, an eNet universal transmitter and the eNet actuator to be activated are necessary. The universal transmitter must be configured for the **Wind alarm** function and then connected to the actuator.
The **Wind alarm** function possesses a priority and can thus not be overridden by functions or commands of a lower priority.

**Procedure:**

The universal transmitter must first be configured for the wind alarm in the device settings.

- To do this, in the **Devices** view, open the device settings of the universal transmitter using the ⚙ button.
- Select the **Scenes for signal contact** function.
- Select the **Wind alarm** operating mode.
- Close the device settings.
- Create a connection for the wind alarm (see chapter 9.1. Create connection).
- Add the universal transmitter to the connection using the ⊞ button or via drag & drop.
  The **Select channels** window opens.
- Select the ⚙ button behind the appropriate channel to make channel settings.
- Select the channels and add to the connection with **Apply**.
- Add the actuator channels to the connection using the ⊞ button or via drag & drop.
  The **Select channels** window opens.
- Select the ⚙ button behind the appropriate channel to make channel settings.
- The parameters of the channel can be set on the **Advanced channel settings** tab, e.g. a different priority can be assigned for the **Wind alarm** function.
- Select the channels and add the channel to the connection with **Apply**.

ℹ️ The connection has been created but is not active and must be programmed (see chapter 9.2. Program connection).

ℹ️ Further information on the **Scenes for signal contact** function of the universal transmitter can be found in the operating manual of the universal transmitter.

## 9.2 Program connection

In the **Connections** view, the connections can be programmed individually.

ℹ️ All the created connections can be programmed in a single step in the **system overview** or in the **Project** view (see chapter 12.1. System overview) and (see chapter 10. Project view) .

**Procedure:**

- Select **Program**.
- If necessary, actuate battery-operated devices.

The connections and device settings are transmitted to the devices of the eNet system. The applications can be used immediately. The connection is disabled for further changes - but can be set back to Edit mode for changes using the **Edit** button.

## 9.3 Edit connection

A connection can be changed, e.g. device channels can be added or removed from the connection. During editing, the connections remain in the devices, meaning that actuator operation is still possible in Edit mode. Changes can then be transmitted to the devices of the system or rejected again.

**Procedure:**

- Select **Edit**.

  The connection changes to Edit mode and can be changed. The connection remains active in the eNet system.

- If necessary, select **Shift** to assign the connection to another room (only for structuring).
- ⓘ Simultaneous changing of multiple connections is possible in Edit mode.
- To reject the changes and exit Edit mode, select **Reject**.
- To apply the changes to the devices, select **Program**.

  Changes are transmitted to the devices of the installation. The connection is active and can no longer be changed.

- ⓘ A connection cannot be programmed without a sensor channel or without an actuator channel.
- ⓘ Should a connection be deleted completely, then the connection data must first be removed from the devices using the **Deactivate** button (see chapter 9.4. Deactivating connections) and then deleted using the **Delete** button.

## 9.4 Deactivating connections

The connection must be deactivated to remove a connection from the eNet system. When a connection is deactivated, the connection data is removed from the devices.

**Procedure:**

- Select **Deactivate**.

  The connection is no longer active in the eNet system. The connection data is removed from the devices.

- ⓘ After the deactivation of a connection, it is possible to delete the connection fully from the project using the **Delete** button.

# 10 Project view

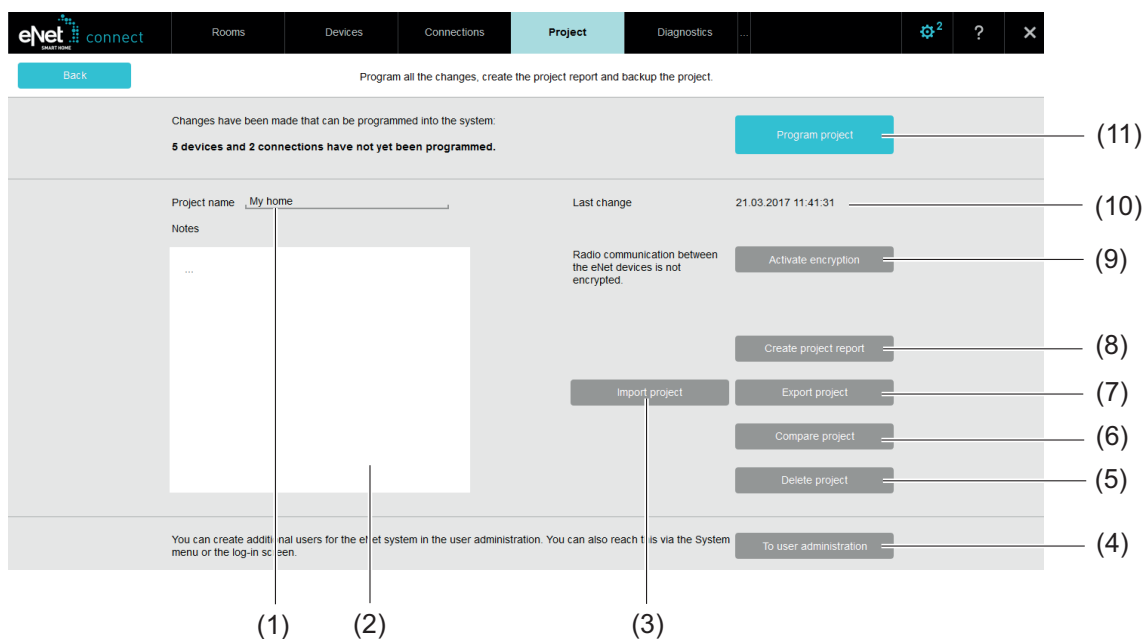In the **Project** view, functions affecting the entire project can be applied.



Figure 16: Project view

(1)   Project name (entered on first commissioning  (see chapter 6. First steps in the commissioning of an eNet system))

(2)    Enter notes on the project

(3)    Perform the import of a project

(4)   Switch to user administration

(5)   Permanently delete a project

(6)   Compare the devices of the eNet system with the project in the commissioning interface

(7)   Perform an export of the project, e.g. to create a backup copy

(8)   Compile project documentation as a PDF file

(9)   Activate or deactivate encrypted radio transmission

(10) Time stamp of the last change of the project (incl. changes via the eNet SMART HOME app)

(11)  Program all the changes in the project into the devices of the eNet system

## 10.1 Activate or deactivate encryption

With activated **encryption**, all the eNet devices in the system communication via fully-encrypted radio telegrams. The encryption of the radio telegrams prevents access to the eNet system by third parties and eavesdropping on the transmitted data. At the time of activation, a one-time connection of the eNet Server to the Internet is required to activate **encryption**.

[i]   Manual commissioning is not possible when **encryption** is activated.

[i]   To activate or deactivate a project's encryption, it must be possible to contact all devices in the project. If devices cannot be contacted, check the radio range and the devices' power supply/battery before repeating the process.

[i]   With an encrypted project, during the period of a device search, the project is deactivated for the project export, meaning that all the functions executed via the eNet Server, such as time controls, are not available during this period. After the end of the device search, the project is reactivated automatically and functions started as appropriate.

ⓘ A project cannot be encrypted for security reasons if the project contains devices which do not support encryption. This could be devices that do not generally support encryption or devices with an old software version. Encryption of the projection can be performed after a device update of the devices with old software versions. The current operating manuals of the eNet devices contain information as to whether the eNet devices support this function.

ⓘ If encryption is activated in a project, in which devices exist with unknown connections to devices outside the project, then these connections become unusable. This is the case if, for example, a connection to a device from the project was set up via manual commissioning.

ⓘ If encryption is active, the function **Reassign key** appears in the **Project** view, with which a new network key can be issued. This function can be performed if the current key no longer seems secure. In so doing, note that, after changing the key, a new export of the project must take place, as this makes the previously exported project unusable.

## 10.2 Create project report

Using the **Create project report** button, it is possible to create project documentation in PDF format.

The content of the project documentation can be selected in a targeted manner:
- Building structure (only rooms to which devices have been added)
- Overview of the building with devices and connections
- Parameter list of the individual devices
- Information on connections (number of connections, device location and name, channel location and name of the connected channels)
- Parts list of the devices with article numbers
- Result of the signal quality measurement, if a measurement was performed over the entire project in the system overview  (see chapter 12.1. System overview)
- System settings of the eNet server

**Procedure:**

▪ Select **Create project report**.

The documentation generated is provided as a PDF file for opening or downloading.

ⓘ If the web browser used supports a popup blocker, this must first be deactivated.

## 10.3 Import and export project

To archive a project, the entire project can be exported with all the data. If necessary, for example to reset a project to the project export status, the archived project can be imported into an eNet Server and restored for use and editing.

When is a project export advisable?
- To backup an executable intermediary status during commissioning
- To backup the project after commissioning has been completed
- After changes to the project, for example if the encryption was deactivated and later reactivated
- When the network key changes

ⓘ We recommend handing over the archived project and the project report to the customer as documentation. The password for decrypting the project and the user data of the administrator can be handed over to the customer, for example, in a sealed envelope.

### 10.3.1 Export project

If encryption is active, an individual password must be issued when a exporting a project, which is required again to import the project. This is necessary for secure encryption use.

**Procedure:**

▪ Select **Export project**.

▪ If encryption is active, enter an individual password.

A dialog for saving the project appears. The project data is saved on the computer as an iex file.

ⓘ Keep the encryption password safe, as the exported project cannot be restored to full functionality without the right password. The project can only be viewed after being imported.

## 10.3.2 Import project

An archived project can be imported into an eNet Server to restore the archived project status.

Important notes about importing projects:

- When a project is imported, all the data of the current project is lost. To back up the data, the current project must be exported before another project is imported.
- If the active project is unencrypted, only an unencrypted project can be imported.
- If the active project is encrypted, only an encrypted project can be imported. The network keys must be identical. If the network key is changed for an active project, and the project is not archived with the new network key, a project import cannot be performed.
- An encrypted project can be viewed by importing it without entering the password via the **Analyse project** button. However, activating and editing the project is not possible. The password is polled again on each new log-on to the commissioning interface, until it has been entered once to activate the project.
- If tado devices are part of the project to be imported and the project will be imported into a new eNet Server, the tado account access data must be entered again in the **eNet SMART HOME app**.
- If an archived project is to be imported into a new eNet Server, all steps for the initial commissioning of an eNet Server must be performed, e.g. configure the network settings (see chapter 5. System settings of the eNet server) and creating users (see chapter 4. The user administration). The project can be imported when creating the project (see chapter 6. First steps in the commissioning of an eNet system).
- When importing a project created with an eNet Server of version V1.x, the system changes in the **eNet SMART HOME System** and the resulting necessary project migration mean that all the data such as timer modules, logic modules, action modules, scenes, presence simulations and metering recordings is lost. Please refer to the information on migrating a V1.x project to a V2.x project on the update.enet-smarthome.com website!
- The version of the eNet Server to which a project is to be imported must be at least the same version (or a more recent version) than the eNet Server with which the project was exported. For this reason, an update of the eNet server may have to be performed in advance.

**Import completed project**

Application 1: The eNet Server is defective and the archived project is to be read into a new eNet Server.

Application 2: The project is to be read into a new eNet Server, on which a project already exists.

ⓘ If the project in the eNet system is encrypted and an unencrypted project is to be imported (or vice versa), the eNet Server can no longer communicate with the devices in the eNet system!

- Select **Import project**.

  A selection dialog opens.

- Select project file for the import and choose **Import**.

- If encryption is active, the password must be entered to decrypt the project (see chapter 10.3. Import and export project).

  If a project exists on the eNet Server, it is automatically deleted. The computer imports the new project into the eNet Server and activates it.

- Perform a system comparison to compare the devices in the eNet system with the devices in the project  (see chapter 10.4. Compare project)by selecting the **Write data** function, to transfer the device data from the project to the devices in the eNet system.

**Import the intermediate status of a project**

Application: The intermediate status was saved during commissioning and is now to be reimported. Changes were made between archiving the intermediate status and the project import, and more devices were read into the project.

- Select **Import project**.

  A selection dialog opens.

- Select project file for the import and choose **Import**.

- If encryption is active, the password must be entered to decrypt the project (see chapter 10.3. Import and export project).

  If a project exists on the eNet Server, it is automatically deleted. The computer imports the new project into the eNet Server and activates it.

- Perform a system comparison to compare the devices in the eNet system with the devices in the project  (see chapter 10.4. Compare project)by selecting the **Write data** function, to transfer the device data from the project to the devices in the eNet system.

- ⓘ Devices that were added to the project after archiving the intermediate status are not detected during the project comparison, and must first be reset (see chapter 8.9. Reset device) and then read in again  (see chapter 8.1. Add devices to the eNet system).

## 10.4 Compare project

Changes made to the devices of the eNet system can be applied to the project of the commissioning interface via a project comparison. A project comparison can also undo changes to the devices of the eNet system by writing the project data to the devices of the eNet system.

ⓘ Some devices (e.g. tado devices) can only be synchronised via the eNet SMART HOME app!

The following changes are taken into account during a project comparison:

- New connections of recognised devices, created in the eNet system through manual commissioning
- New devices linked in the eNet system through manual commissioning to existing devices of the eNet system
- Devices removed manually to the eNet system, e.g by factory reset
- Changes to parameters and operating mode on devices of the eNet system

**Procedure:**

- Select **Compare project**. If necessary, actuate battery-operated devices.

  The devices, parameters and connection data are compared. If there are differences between the project and the devices of the eNet system, then it is possible to choose between the **Write data** and **Read-in data** functions.

- Select **Write data** to transmit the device data from the project to the devices of the eNet system.

  Changes performed manually on the devices on the eNet system are undone and overwritten with the data from the project.

- Select **Read-in data** to transmit the changed device data from the eNet system to the project.

  If connections between devices in the project were recreated through manual commissioning, a new connection is created.

  If connections between a new device and a device from the project were recreated through manual commissioning, then the new device is detected as an unknown device and can be read in via a device search. After the device has been read into the project via a device search, a new connection is created with the new device.

  If a connection between devices in the project was deleted manually directly on the device, the connection is then adapted or deleted.

## 10.5 Delete project

The project can be deleted permanently with all the data using **Delete project**. However, the devices of the eNet system remain untouched, meaning that direct device connections remain functional after deletion. By contrast, during a factory reset, all the users and settings, such as network settings or data for remote access of the eNet Server, are deleted, meaning that the eNet Server is in the same state as when delivery from the factory.

- ⓘ   If the devices in the project are not removed beforehand, then they cannot be added with a new project. The devices must first be reset manually through a factory reset, see device operation manual.

- ⓘ   Before deleting a project, it is wise to back up the current project using the **Export project** function.

- ⓘ   Before deleting a project, always remove the devices from the project on which local operation was disabled. This is necessary because these devices can otherwise no longer be reset to the factory settings after the project is deleted and can thus not be added to a project again!

# 11 Diagnostics view

In the **Diagnostics** view, the signal quality measurement and telegram recording for diagnostic purposes can be recalled.

## 11.1 Measuring the signal quality

The signal quality measurement can be used to measure the quality of the radio signals between the sensor channels and connected actuator channels. For the measurement, a device (actuator or sensor) is selected from which the signal quality of all the connected channels is measured.

With this signal quality measurement, the logic links between devices, which were created via scenes or If-Then rules in the **eNet SMART HOME app** are taken into account. The logic links are created via the eNet Server, which is taken into account in this signal quality measurement.

ⓘ   A signal quality measurement can be performed for all the connections of all the devices of the eNet system in a single step in the **system overview**. However, in so doing, the eNet Server and thus also the logic links created via the **eNet SMART HOME app**, are not taken into account (see chapter 12.1. System overview).

The result of the measurement is shown using colour coding according to the traffic light principle:
- Green: Good reception
- Yellow: Sufficient reception (observe as necessary to see if interference occurs)
- Red: No reception (check device and power supply, use repeater as necessary)
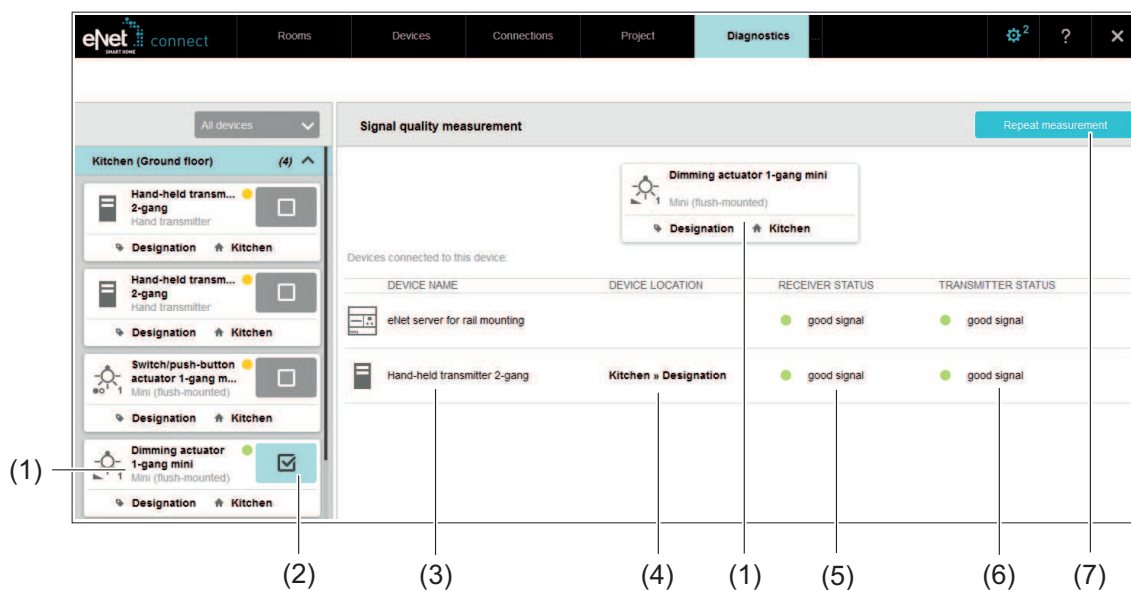


Figure 17: Signal quality measurement - example of dimming actuator

(1)   Selected device

(2)   Add or remove device

(3)   Connected device

(4)   Device location and designation of the connected devices

(5)   Reception quality of the connected device when it receives a telegram from the selected device - e.g. hand-held transmitter as receiver: The signal from the dimming actuator is received by the hand-held transmitter at a good quality level

(6)   Reception quality of the selected device when it receives a telegram from the connected device - e.g. hand-held transmitter as transmitter: The signal from the hand-held transmitter is received by the dimming actuator at a good quality level

(7)  Repeat, start or stop measurement

**Procedure  (Figure 17):**

ℹ️  For signal quality measurement, the connections which contain the device channels must be active. If a connection is in Edit mode or it is deactivated, then the signal quality measurement can only be performed for the eNet Server.

▪  Select the desired device which should start the measurement (2).

ℹ️  If a device has already been added, then reselecting it allows it to be removed.

ℹ️  If a device has already been added, then it can be replaced by selecting another device.

The device (1) and all connected devices are added to the work area (3).

ℹ️  The eNet server is taken into account as a connected device during each measurement.

▪  Select **Start measurement** (7).

The measurement is carried out and the results then illustrated (5) and (6).

ℹ️  An insufficient connection can be improved by adding a repeater. In the selection in the **Connections** view, the Repeater filter can be used to display the devices with a repeater function. The repeater function can be activated in the **Device settings/Advanced device settings**. Since the use of repeaters may lead to higher telegram traffic and, in consequence, faults in telegram transmission, a maximum of only two repeaters should be used. The eNet Repeater ZS, which is designed as an adapter, is to be favoured here, if a configuration is desired, in which only the telegrams of selected devices are repeated.

▪  The measurement can be repeated (7) to check directly the impact of changes made to the system.

ℹ️  In a signal quality measurement, a repeater is only taken into account when no reception would be available without the repeater.

# 11.2 Record telegrams

Telegrams can be recorded in the background for several hours. The computer does not have to be connected to the eNet server for this. However, before the computer is removed, the commissioning interface must always be closed  (Figure 3) (6). The telegram recordings can be exported for an evaluation of the telegram traffic.

ℹ️  During telegram recording, it is possible to continue working in the other views of the commissioning interface.

ℹ️  Up to 2,000 telegrams can be recorded; after that the oldest entries are overwritten.

ℹ️  The diagnostic function displays what a channel is transmitting but not what it is receiving. The recipient of a particular telegram and its contents can thus not be analysed with this diagnostic function.

ℹ️  It is possible to use the telegram recording to show the telegram traffic which does not originate in devices of the eNet system. Here, the recording should be started directly without a device having previously been selected.

Applications for telegram recording:
-  Test for whether a channel is transmitting
-  Evaluate telegram exchange between the sensor and actuator channel
-  Quantitative evaluation of telegram traffic, e.g. proportion of third-party telegrams
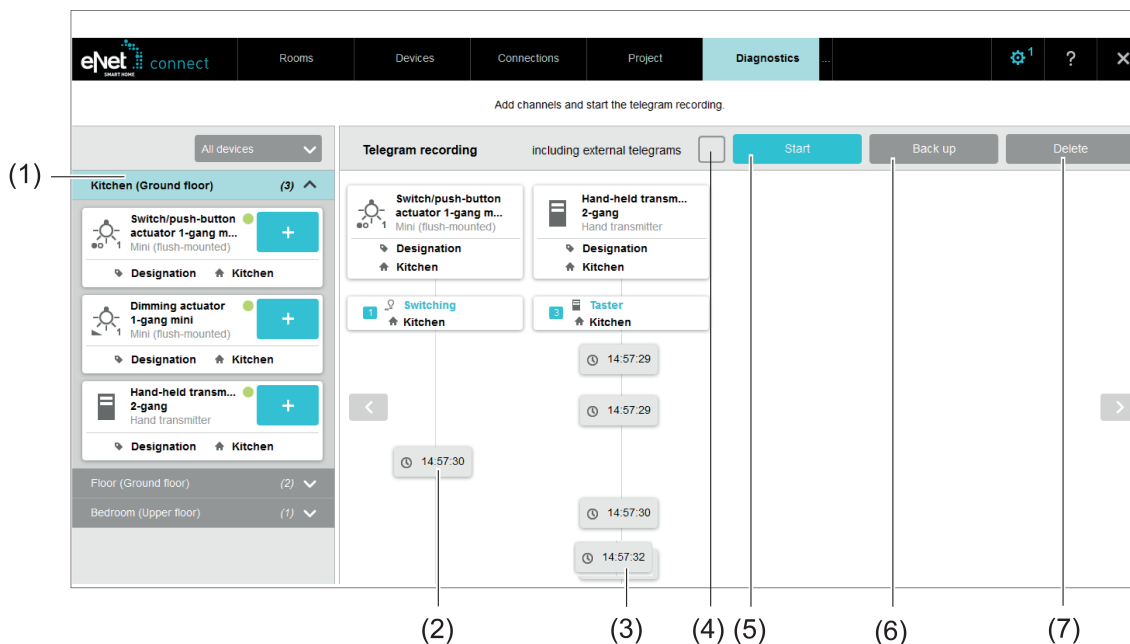
Figure 18: Diagnostics view - Telegram recording

(1) Device selection
(2) Recorded telegrams of an actuator channel
(3) Recorded telegrams of a sensor channel via repeater (doubled display of the time stamp)
(4) External telegrams are additionally recorded when the checkbox is checked
(5) Start/stop recording
(6) Back up recording
(7) Delete recording

**Procedure:**

■ In the **Diagnostics** view, select the menu item **Telegram recording**.

Up to 10 channels can be selected for telegram recording. In this case, to record all telegrams received from the eNet server, no channels must be selected, but the telegram recording must be started directly instead.

■ If necessary, select filter to limit the selection of devices.
■ Select the channel for the telegram recording using the ⊞ button.
■ Select **Start recording**.

A maximum of 50 telegrams are displayed.

■ Stop telegram recording using the **Stop recording** button.

ⓘ The telegram recording can be continued using the **Start recording** button.

The time of the telegrams is displayed in the result of the telegram recording. If the telegram was transmitted via a repeater, this is indicated by the double display of the time stamp (Figure 18).

ⓘ Delete the telegram recording using the **Delete recording** button. The recorded telegrams are deleted permanently.

## 11.3 Export and evaluate telegrams

The recorded telegrams can be exported as a table in csv format in order to perform evaluations in other software (e.g. MS Excel).

The following information on each telegram is listed in the table:

- Time when the eNet server received the telegram

- Device UID, a freely assigned device-specific number
- Serial number of the device that can also be viewed in the **Information** window
- Device type as an abbreviation of the device name
- Device name, which is also displayed in the device display
- Device location and designation of the device
- Channel number, type, location and name of the device channel that has transmitted the telegram
- Display showing whether the telegram was received via a repeater

**Procedure:**

- Select **Back up recording**.

  A table in csv format is generated and can either be opened directly or saved locally on the computer.

ℹ️ In the .csv file, semicolons and UTF-8 character encoding are used.

**Evaluation of the telegram recordings**

- Cumulative occurrence of external telegrams can be a possible cause for the overload of the system and can impede communication in the eNet system. External telegrams are recorded by the diagnostics and can be recognized by the fact that they only have one time stamp.
- Individual actuators or sensors can be examined as to whether they transmit telegrams. Assuming that the eNet server is within range, device faults can hereby be excluded.
- If no telegrams are recorded, the cause can be due to the fact that the range between the eNet server and device (actuator and/or sensor) is not sufficient. The use of repeaters can ensure better telegram reception. The measurement can then be repeated with the repeater.

# 12 System overview and advanced settings

## 12.1 System overview

In the system overview, various actions pertaining to the project can be performed in the active project. The system overview is recalled using the ⚙ menu via **Settings**.

### 12.1.1 Update

**Update of the eNet server**

If, in the system settings of the eNet Server, the automatic search for an update is set and an update is available, then it is displayed here. It is possible to switch to the system settings to perform the update.

**Update for devices**

If updates are available for devices, then the update can be programmed to either all the devices or only a selection of devices via the **Update devices** function. The expected programming time is displayed in the device selection dialogue as an estimate of the update period

ⓘ  During a device update, the connection between the computer and eNet Server must be maintained and the web browser must remain open with the commissioning interface during the complete update operation. This is particularly important for an update of battery-powered eNet devices and to display messages which can appear during the operation. For this reason, ensure that the computer does not switch off automatically during the period of the update or switches to the standby state and that that the computer is supplied with power via a power supply unit.

ⓘ  During an update, work with the commissioning interface is limited. Areas and rooms can still be created, catalogue devices added and connections and scenes created.

ⓘ  Before an update of the solar sun sensor, the charging level of the energy storage is checked. If the charging level is too low, no update is started. The sun sensor must first be charged in a very bright place beforehand, see the operating manual of the sun sensor.

ⓘ  With battery-operated devices, always replace the battery with a new one before performing an update.

ⓘ  If connections were added to the project through manual commissioning, then a project comparison must be carried out before an update.

### 12.1.2 Messages

If the eNet system contains devices with a weak battery, then these devices can be displayed here. Weak batteries should be replaced with new batteries.

ⓘ  The battery status is also displayed in the device information of the device and in the **eNet SMART HOME app**.

### 12.1.3 Devices

If changes are made to devices in the commissioning interface, then the devices must be programmed. These devices can be programmed here in one step. If necessary, actuate battery-operated devices.

### 12.1.4 Connections

**Programming / deactivating all connections**

All the connections can be prepared and then programmed in a single step. The precondition for this is that all the battery-operated devices involved in programming are ready for reception. Deactivation of all the connections can also be carried out in one step, if, for example, the whole eNet system is to be decommissioned.

**Connections to unknown devices**

The devices of the project which are connected to unknown devices are displayed. Unknown devices are devices which have not yet been added to the project. If unknown connections

exists, then all the unknown connections can be deleted from the devices in the project (see chapter 8.12. Delete connections).

### 12.1.5 Signal quality measurement

Only the devices contained in the programmed connections are taken into account for the signal quality measurement via the **system overview**. This means that the measurement can only be started when there is at least one programmed connection. In contrast to the signal quality measurement in the **Diagnostics** view, the eNet Server is not included in the measurement itself.

ⓘ  With this signal quality measurement, the logic links between devices, which were created via scenes and If-Then rules in the **eNet SMART HOME app** are not taken into account. This signal quality measurement in the Diagnostics view can be used for this (see chapter 11.1. Measuring the signal quality).

ⓘ  The results of the last signal quality measurement can be output in the project report (see chapter 10.2. Create project report).

ⓘ  During the measurement, work with the commissioning interface is limited. Areas and rooms can still be created, catalogue devices added and connections and scenes created.

### 12.1.6 Logout / Help

**Log out other users**

The administrator can log out all the users that have logged onto the eNet Server. This also affects the users accessing the eNet Server via the app.
If, for example, a user is in the system settings and the administrator wishes to change something in the system settings, they can use this function to obtain access to the system settings. Note that any unsaved system settings performed by the user but not yet calibrated with the eNet Server are lost.

**Displaying help dialogues**

The help dialogues can be displayed again for which the **Do not show this dialog again** checkbox was checked.

## 12.2 Advanced settings

The applications described below can be accessed using the **Display advanced settings** button.

### 12.2.1 Log messages

Changes to these settings should only be made after consulting Service.

**Messages of the eNet Server**

To aid support of the eNet Server, it is possible to export the messages of the eNet Server if there is a fault.

**Log level**

Setting of the log levels applies to the messages of the eNet Server. The **Major** log level only takes error messages into account. The other levels, **Warnings**, **Information** and **Debug**, also take other messages into account. The range of the messages increases from the **Major** level to the lowest **Debug** level.
The default setting **Warnings** should not be changed without consulting Service, as other settings can lead to unnecessarily extended runtimes of the eNet Server. If there is an error, Service will specify a different log level, if this is wise.

### 12.2.2 Maintenance

Changes to these settings should only be made after consulting Service.

**Activate display of exceptional errors**

Additional error messages can be displayed for troubleshooting.

**Communication Timeout**

If the response time of the eNet Server to a request of the commissioning interface is longer than the set value for the communication timeout, then the process is aborted and an error message is generated. 185,000 ms (approx. 3 min) is preset.

**Delete local storage**

Data saved by the commissioning interface in the web browser can be deleted. In the commissioning interface, the consequence of this is the reloading of the catalogue data and reconstruction of the connections.

# 13 Appendix

## 13.1 Index

## 13.2 Copyright notice and disclaimer

Information about the software licences and copyright can be accessed using the **?** menu.

## 13.3 References

You can find a Quick Start Guide as an introduction to working with the eNet Server, the eNet system manual and additional information on the eNet system at **www.enet-smarthome.de**.