

# Technical Manual



## MDT IP Interface

SCN-IP000.03

### **Further Documents:**

**Datasheet:**

[https://www.mdt.de/EN\\_Downloads\\_Datasheets.html](https://www.mdt.de/EN_Downloads_Datasheets.html)

**Assembly and Operation Instructions:**

[https://www.mdt.de/EN\\_Downloads\\_Instructions.html](https://www.mdt.de/EN_Downloads_Instructions.html)

**Solution Proposals for MDT products:**

[https://www.mdt.de/EN\\_Downloads\\_Solutions.html](https://www.mdt.de/EN_Downloads_Solutions.html)

## 1 Contents

1 Contents .....	2
2 Overview .....	4
2.1 Possible applications IP-Interface .....	4
2.2 Possible applications E-Mail Client .....	4
2.3 Possible applications Timeserver .....	4
2.4 Overview LEDS & Operation .....	5
2.5 Commissioning without Data Secure .....	6
2.6 Commissioning with Data Secure .....	7
2.7 Firmware Update .....	8
3 Safety – IP Secure/Data Secure .....	9
3.1 Safety mechanisms – IP Secure/Data Secure .....	9
3.2 Basic terms .....	9
3.2.1 FDSK .....	9
3.2.2 Secured Mode - Secure Mode .....	9
3.2.3 Non-secured mode - Plain Mode .....	9
3.2.4 Backbone Key .....	9
3.2.5 Commissioning Password .....	10
3.2.6 Authentication Code .....	10
3.2.7 Commissioning/ Secure Commissioning .....	11
3.2.8 Tunneling/Secure Tunneling .....	11
3.3 Mixed operation .....	12
3.4 Commissioning .....	12
3.5 Advanced security mechanisms .....	14
3.6 Requirements for KNX IP Secure/Data Secure .....	14
4 Settings – IP-Interface .....	15
4.1 Settings IP Interface with Secure .....	15
4.1.1 General .....	15
4.1.2 Device – Settings .....	16
4.1.3 Device – IP Configuration .....	17
4.2 Settings IP Interface without Secure .....	18
4.2.1 General .....	18
4.2.2 IP – Configuration .....	19
4.3 Example of assigning IP addresses .....	20

4.4	Communication settings .....	21
4.4.1	Procedure ETS 4.....	21
4.4.2	Procedure ETS 5.....	23
4.4.3	Set tunneling connections.....	24
4.4.3.1	Procedure for IP Interface without Secure .....	24
4.4.3.2	Procedure for IP Interface with Secure.....	25
5	Parameter → E-Mail Client .....	26
5.1	General settings .....	26
5.1.1	General .....	26
5.1.2	Web Interface .....	27
5.1.3	Time/Date.....	28
5.2	E-Mail functions.....	29
5.2.1	Status elements .....	29
5.2.2	Bit Alarms .....	31
5.2.2.1	Macros.....	32
5.2.3	Text Alarms.....	33
5.2.4	Status Reports.....	34
5.2.5	Specific behavior and error handling .....	35
5.3	Overview Communication Objects .....	36
5.4	Secure Group Address Communication .....	37
6	Web-Interface.....	38
6.1	Call of the Web-Interface .....	38
6.2	Overview Web Interface .....	39
6.3	Setting of E-Mail functionality.....	40
6.4	E-Mail – Error codes & remedy .....	43
6.5	Receive E-Mail as push message .....	43
6.6	Receive E-Mail as SMS .....	43
7	Index.....	44
7.1	Register of illustrations .....	44
7.2	List of tables .....	45
8	Attachment .....	46
8.1	Statutory requirements .....	46
8.2	Disposal routine.....	46
8.3	Assemblage .....	46
8.4	History.....	46

## 2 Overview

The MDT IP Interface, SCN IP000.03, has 2 parallel applications.

On the one hand there is one application for the IP Interface which allows access to the bus via Ethernet.

The second application is on the TP side and can send by KNX triggered emails, serve as a time server and provides access to the device via a Web Interface.

**Important: As these are two different applications, both applications need to be programmed independently. The IP interface gets two physical addresses!**

### Specifics:

- Use as a time server
- Extensive email functionality with status information from the KNX bus
- Supplied completely from the KNX bus, no additional power supply required!
- IP Secure for Interface application
- Data Secure for the email application

### 2.1 Possible applications IP-Interface

The MDT IP interface connects the KNX bus with an Ethernet network. Through the network, KNX telegrams can be sent to other devices or received from. For communication, the device uses the KNXnet / IP protocol of the KNX Association. It thus operates as a programming interface and replaces a RS232 or USB interface.

The IP interface includes a tunneling function for point-to-point connection.

The power is supplied via the KNX bus.

With the IP interface it is also possible to use the bus monitor in the ETS. Please note that the IP interface according to KNX specification can only be in either Bus Monitor mode **or** Tunneling mode.

### 2.2 Possible applications E-Mail Client

The email client can emit status reports, bit alarms and text alarms. All email events can be triggered via KNX telegrams. In addition, status reports can also be sent at fixed times - the email client has the functionality to work as a clock-master. All e-mails can be sent to up to 3 addresses simultaneously. The settings of the e-mail functionality can be carried out comfortably via the web interface.

### 2.3 Possible applications Timeserver

The IP Interface receives the date and time of the NTP server and can distribute them as the "master" to further KNX devices via the bus.

## 2.4 Overview LEDS & Operation

The figure below shows the structure of the device and the location of the LEDs:

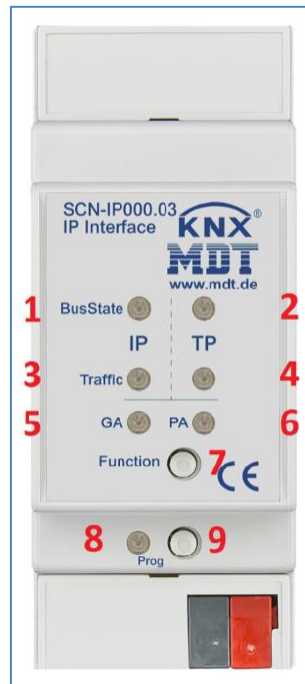


Figure 1: Structure – Hardware module

- |                       |                       |
|-----------------------|-----------------------|
| 1. LED BusState – LAN | 2. LED BusState – KNX |
| 3. LED Traffic – LAN  | 4. LED Traffic – KNX  |
| 5. No function        | 6. No function        |
| 7. Function button    | 8. Programming LED    |
| 9. Programming button |                       |

### Functionality of Programming-button:

- Short press:** programming LED lights **steadily red** -> IP interface is in the programming mode  
**Long press:** programming LED **flashes red** -> E-Mail client is in the programming mode

### Reset device:

If, for example, the applications are loaded in the wrong order or you want to switch from "Secure" to "without Secure", the IP interface must be reset.

Otherwise, programming errors may occur.

The procedure is as follows:

- Press the function button for at least 15 seconds, the LEDs 1, 2, 5, 6 lights up red/orange.
- Now release the function button (LEDs continue to light up as before).
- Now press the function button again for at least 3 seconds until all LEDs go out.
- The unit restarts. In the ETS it disappears under "Discovered interfaces".

Shortly afterwards it appears again with the default address (IP Interface 15.15.255).

The unit is now reset to factory settings.

The master reset also resets the secure settings to the FDSK (Factory Default Setup Key). This means that the device can only be downloaded with the FDSK

	Green	Red
<b>LED 1 Bus State – IP</b>	Off: LAN Error On: LAN OK	
<b>LED 2 Bus State – TP</b>	Off: KNX Bus: Error or not connected On: KNX Bus OK	
<b>LED 3 Traffic – IP</b>	Flashing: Bus load at LAN-side Off: No Bus load at LAN-side Speed up to 10 Mbit/s	Flashing: Transmission error at LAN side
<b>LED 4 Traffic - TP</b>	Flashing: Bus load at KNX side Off: No Bus load at KNX side	Flashing: Transmission error at KNX side

Table 1: Overview LEDs

## 2.5 Commissioning without Data Secure

The following procedure is recommended for commissioning the SCN-IP000.03:

1. Insert the application „SCN-IP000.03 – KNX IP Interface“
2. Configuration of the IP-Interface.
3. Transfer of the physical address and the application of the IP Interface. For this, the programming button has to be **pressed shortly**. The programming **LED lights steadily red**.
4. After successful transfer of the physical address and the application, the red LED turns off again.
5. Insert the application „SCN-IP000.03 – KNX IP Interface with email function“
6. Configuration of the E-Mail Client.
7. Transfer of the physical address and the application of the E-Mail Client. For this, the programming button has to be **pressed long**. The programming **LED flashes red**.
8. After successful transfer of the physical address and the application, the red LED turns off again.
9. Accessing the Web client to configure the e-mail addresses by opening an Internet browser and call the address: http:\\IP address: port, for example: http: \\192.168.1.178:8080 for the IP address 192.168 .1.178 and the http port 8080

**Important:** If the IP address of the IP Interfac gets changed subsequently, the device has to perform a reboot. This restart is not performed automatically by the application programming in the ETS4/5. Here, a manual restart will be required, which either by right-clicking on the device and selecting "Reset device" is executed or a short removing of the bus connector.

## 2.6 Commissioning with Data Secure

The following procedure is recommended for commissioning the SCN-IP000.03:

1. Insert the application „SCN-IP000.03 – KNX IP Interface with Secure“
2. Input of the FDSK (see sticker on the side of the device)
3. Configuration of the IP Interface.
4. Transfer of the physical address and the application of the IP Interface. For this, the programming button has to be **pressed shortly**. The programming **LED lights steadily red**.
5. After successful transfer of the physical address and the application, the red LED turns off again.
6. Insert the application „SCN-IP100.03 – KNX IP Interface with email function“
7. Input of the FDSK (see sticker on the side of the device)
8. Configuration of the E-Mail Client.
9. Transfer of the physical address and the application of the E-Mail Client. For this, the programming button has to be **pressed long**. The programming **LED flashes red**.
10. After successful transfer of the physical address and the application, the red LED turns off again.
11. Accessing the Web client to configure the e-mail addresses by opening an Internet browser and call the address: `http:\\IP address: port`, for example: `http: \\192.168.1.178:8080` for the IP address 192.168 .1.178 and the http port 8080

**FDSK Info:** The IP Interface has two FDSK (Factory Default Setup Key), one for each application. Therefore you will find two different keys on the right and left side of the interface.

**Important:** By deactivating "Secure commissioning" in the properties -> settings of the device, the device is operated "unsecure", i.e. in "plain mode". If you are prompted to enter the FDSK of the device, you can skip this dialog by clicking the "Later" button. Data Secure/IP Secure can also be activated later by activating "Secure commissioning" and the FDSK is present. Further details about IP Secure/Data Secure can be found at "3 Safety – IP Secure/Data Secure"

## 2.7 Firmware Update

If there is a new firmware version for the IP Interface, the update can be carried out directly on the device.

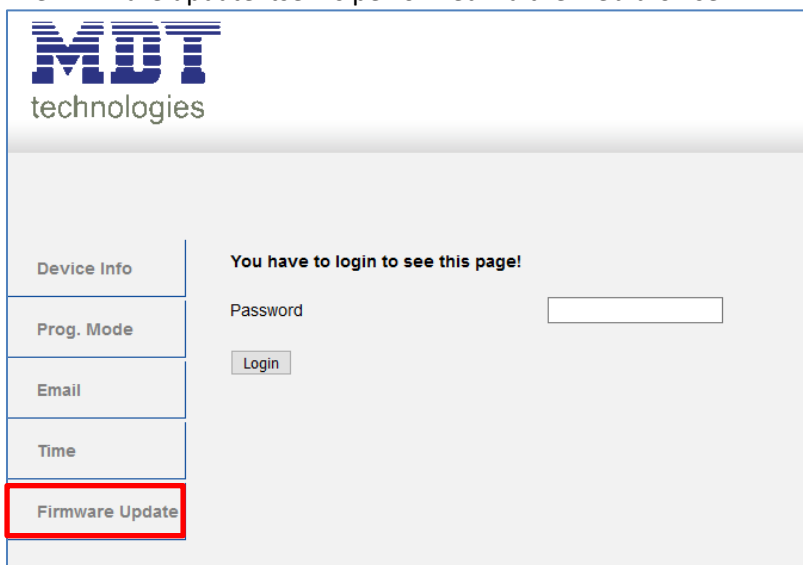
The required update file is available in "hex" format in the download area.

Link to the firmware files (Current devices):

[https://www.mdt.de/EN\\_Downloads\\_Productdata.html](https://www.mdt.de/EN_Downloads_Productdata.html)

MDT IP Interface <b>Firmwareupdate</b>	.03
MDT IP Router <b>Firmwareupdate</b>	.03

The firmware update itself is performed via the web browser:



The screenshot shows the MDT technologies web interface. At the top left is the MDT technologies logo. Below it is a navigation menu with items: Device Info, Prog. Mode, Email, Time, and Firmware Update. The 'Firmware Update' item is highlighted with a red rectangular border. To the right of the menu, there is a login prompt: 'You have to login to see this page!' followed by a 'Password' label, an empty text input field, and a 'Login' button.

A detailed description with procedure is available as a solution proposal at

**Important:**

**After an update, the unit is reset to factory settings. The physical address and application have to be reloaded!**

**Also, all settings in the web browser such as e-mail addresses etc. are reset to default settings. Therefore, make a note of the entered addresses etc. in advance.**



## 3 Safety – IP Secure/Data Secure

### 3.1 Safety mechanisms – IP Secure/Data Secure

KNX Data Security distinguishes between two mechanisms: IP Secure and Data Secure.

**KNX IP Secure** allows to encrypt and to authenticate messages sent by KNX devices to transmit them securely over the IP layer. This ensures that KNX tunneling or routing messages on IP cannot be read or manipulated. KNX IP Secure forms an additional "security shell" that protects the complete KNXnet IP data traffic.

**KNX Data Secure** enables the secure commissioning of devices that support data security and the encrypted transmission of group addresses between two devices that support Data Secure. For 2 devices to communicate securely with Data Secure, both devices must support Data Secure. However, it is also possible for a Data Secure device to communicate with a device that does not support Data Secure. In this case, however, only via an unsecured connection.

### 3.2 Basic terms

#### 3.2.1 FDSK

Every Secure device is delivered with the "Factory Device Setup Key" (FDSK). The system integrator/installer enters this key into the ETS, which generates a device-specific tool key from it. The ETS sends the tool key via the KNX bus to the device to be configured. This transmission is encrypted and authenticated with the FDSK key. After this initial commissioning, the device only accepts the received tool key. The FDSK is no longer required for further transmission - unless the device is reset via the master reset.

After initial commissioning, the FDSK of all devices in a project should be detached from the device sticker and stored in a project-specific manner. The IP interface has two FDSKs for each application one, therefore you will find two different keys on the right and left side of the interface.

#### 3.2.2 Secured Mode - Secure Mode

If a device is parameterised in such a way that it only transmits encrypted data, this is known as secure mode.

#### 3.2.3 Non-secured mode - Plain Mode

If a device is parameterised in such a way that it only transmits in unencrypted form, this is known as non-secured mode (plain mode).

#### 3.2.4 Backbone Key

If a KNX bus is connected to Data Secure via 2 IP Routers, they communicate encrypted with the backbone key. This key must be identical in all devices. The key is assigned independently by the ETS and cannot be changed.

### 3.2.5 Commissioning Password

The commissioning password is required in the ETS for the entire process/download during commissioning / device security of a KNX IP Secure device. It is also used to authenticate the ETS to the device.

It has to be different from passwords of possible secured, additional interfaces and represents the so-called management level for the device configuration by the ETS.

Only the ETS itself knows the commissioning password and can make changes to the device.

Passwords of secured additional interfaces can be distributed, e.g. to an external visualisation.

The commissioning password can be adapted by the user and is visible in the tab “Device -> Properties -> IP”:

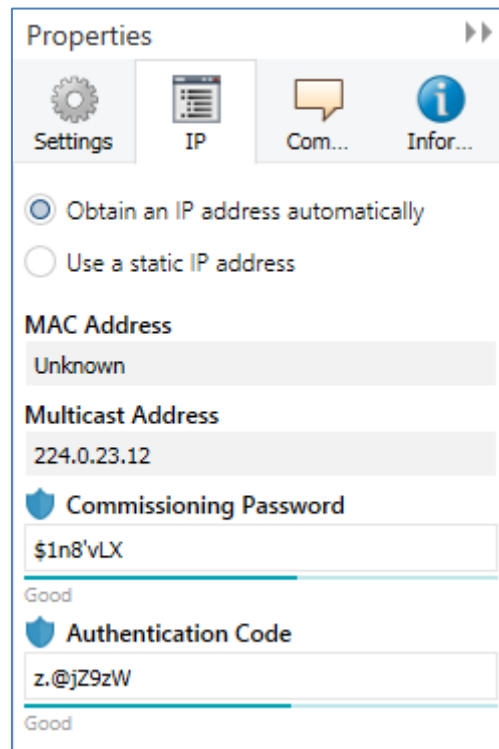


Figure 2: Commissioning Password/ Authentication Code

It is recommended to give each device an individual commissioning password and not a universal one in the entire project or even across projects. The ETS automatically assigns an individual password.

### 3.2.6 Authentication Code

The authentication code is required for authenticating KNX IP Secure devices.

As the FDSK is known outside of ETS, for example as QR Code or imprint on the device, this key has to be changed in the ETS project.

The FDSK is replaced by an individual authentication code for this ETS project and this KNX IP Secure device. Subsequent communication of the device with the ETS will then be done with this (new) authentication code (instead of the initial FDSK).

Each KNX IP Secure device therefore has an individual\* authentication code after commissioning which is different from the initial FDSK.

\* if not overwritten by the ETS user - in case of multiple devices - with an identical authentication code

The authentication code can be changed in ETS in the same way as the commissioning password, see Figure 2 above.

### 3.2.7 Commissioning/ Secure Commissioning

It can be decided for each device whether commissioning should be carried out in a secure or unsecured manner. If the commissioning is not secured, the device can be used as a normal device without Data Secure.

By default, the ETS sets all devices to Secure commissioning when inserted. This item can be changed by the user under Device ->Properties ->Settings:



Figure 3: Secure Commissioning/Secure Tunneling

### 3.2.8 Tunneling/Secure Tunneling

Tunneling refers to a KNX point-to-point connection on the TCP/IP network. For each IP Secure device, it can be decided whether the tunneling connections are transmitted "Secure" or "Plain", see Figure 3 above.

### 3.3 Mixed operation

#### IP Secure

Secured devices can only communicate with devices that are also secured. Mixtures of e.g. secured KNX IP Secure couplers with unsecured KNX IP Secure devices or normal KNX IP devices will not work.

#### Data Secure

With Data Secure, devices that support Data Secure can also communicate with devices that do not support Data Secure. A mixed operation in one project is therefore possible.

However, if all data of a group address are to be transmitted in encrypted form, all devices whose objects are connected to this group address must support Data Secure.

### 3.4 Commissioning

ETS requires the following procedure to put Secure devices into operation:

#### 1. Load product data

When loading the product database, you will normally be asked directly to enter the FDSK of the device:

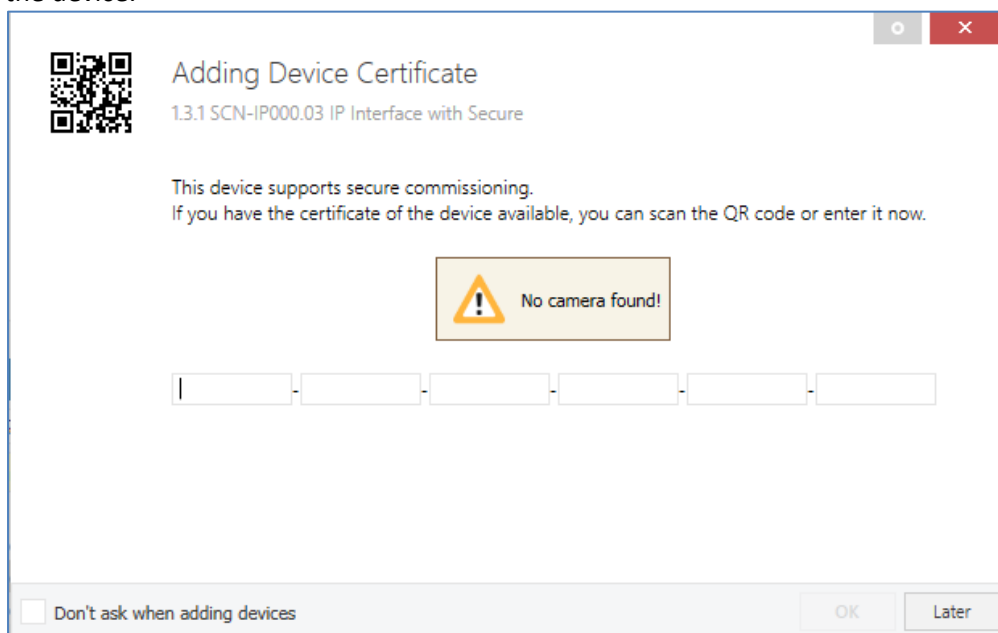


Figure 4: Enter FDSK

You can enter the FDSK manually or read the QR code from a camera. If you do not want to read the FDSK directly or if you do not have it at hand, you can do this later by confirming this dialogue with "Later".

To enter the FDSK later, select the respective project and choose the tab Security:

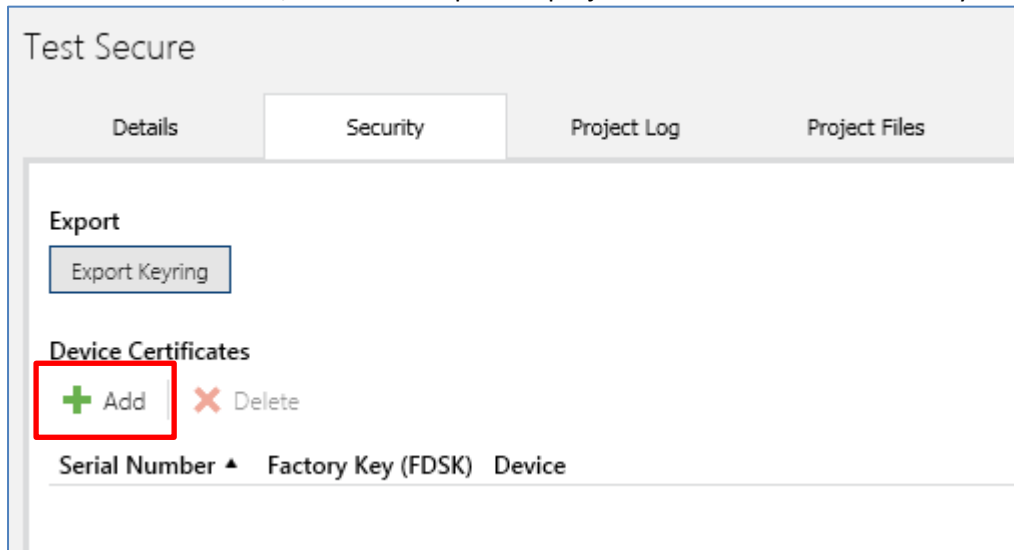


Figure 5: Subsequent input FDSK

Here you can now select the "Add" button and enter the FDSK or scan the QR Code. If the FDSK was detected correctly, the ETS decodes the FDSK into serial number and factory key. The ETS automatically assigns which key belongs to which device. Thus, you can simply enter all FDSK used in the project one after the other.

**2. Remove sticker/device certificate**

To prevent sabotage, the device certificate has to be kept in a safe place. It is therefore important to remove it before installing the device and keep it for the project.

**3. Adapt Commissioning Password/Authentication Code (optional)**

The Commissioning Password per device and Authentication Code per device can now be customized by the user. However, the ETS assigns initial passwords, so this does not necessarily have to be done. However, individual passwords should be assigned for each device.

**4. Download the application**

Now the application can be downloaded into the device.

**5. Distributing the Commissioning Password and Authentication Code**

If visualisation or remote access is required, the commissioning password and (optionally) the authentication code (authorisation of the other party for access to the project) need to be entered before the connection is established.

### 3.5 Advanced security mechanisms

In addition to the use of KNX IP Secure, the following guidelines should be taken into account during planning:

- Do not allow any ports of routers to access the Internet
- Secure LAN/WLAN system via a firewall
- If no external access to the KNX installation is required, the default gateway can be set to the value 0. This prevents communication to the Internet.
- Access to the KNX installation from the Internet should be realised via a VPN connection

### 3.6 Requirements for KNX IP Secure/Data Secure

**ETS 5.7.2** is required for commissioning Data Secure/IP Secure.

## 4 Settings – IP-Interface

The settings of the application "IP Interface **without Secure**" and "IP Interface **with Secure**" differ. Both settings are described below.

### 4.1 Settings IP Interface with Secure

#### 4.1.1 General

The following parameters can be set in the submenu "General":

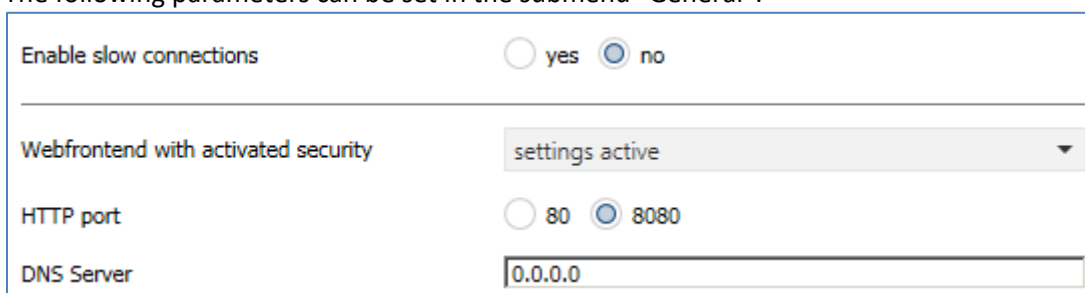


Figure 6: General Settings – IP Interface

The table below shows the settings for this submenu:

ETS-Text	Dynamic Range [Default value]	Comment
Enable slow conntctions	<ul style="list-style-type: none"> <li>• Yes</li> <li>• <b>No</b></li> </ul>	Adjust the timeout for tunnel connections. By default, slow connections are not supported and a short timeout is used for the UDP connection. This can be increased by supporting slow connections which may be necessary especially for tunnel connections over the internet.
Web frontend with activated security	<ul style="list-style-type: none"> <li>• Settings active</li> <li>• Only status</li> <li>• <b>Locked settings</b></li> </ul>	Setting the Web interface for firmware update/assignment of tunneling connection, etc: <b>Settings active:</b> All settings of the Web Interface are available to the user. <b>Only status:</b> Security-critical functions are only displayed as status in the Web Interface and no changes can be made. <b>Settings locked:</b> No Web Interface can be accessed.
HTTP port	<ul style="list-style-type: none"> <li>• 80</li> <li>• <b>8080</b></li> </ul>	Setting the HTTP port for the Web interface
DNS Server	any [0.0.0.0]	Entering the DNS address

Table 2: General Settings – IP Interface

### 4.1.2 Device – Settings

The following picture shows the settings of the IP Interface:

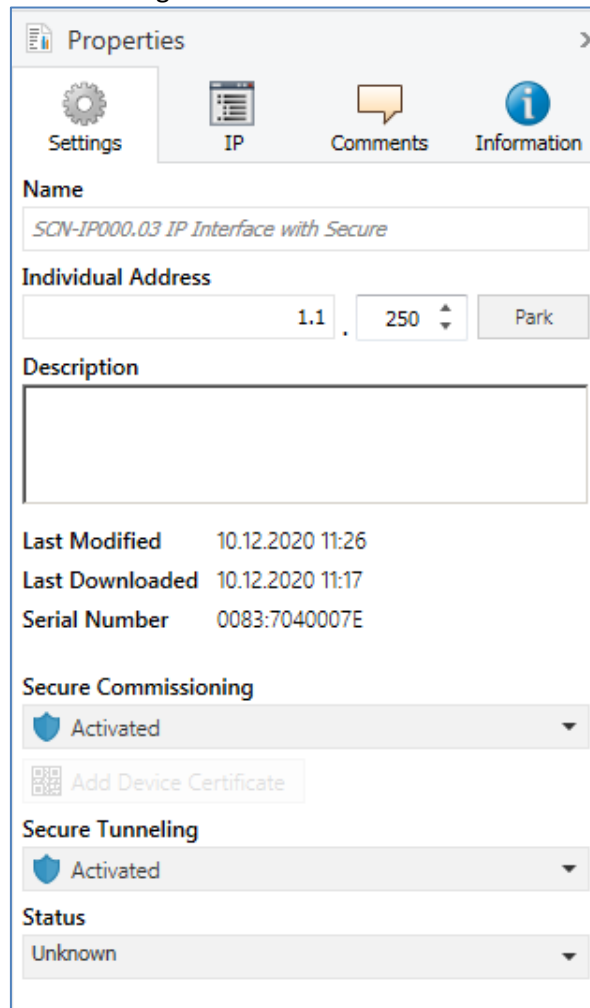


Figure 7: Device – Settings

#### Name

The name describes, among other things, how the connection is displayed in the ETS. Any name with a maximum length of 50 characters can be entered.

#### Secure commissioning

Activation/deactivation of Secure Commissioning. If a device is not commissioned safely, the secure functions are deactivated, see also “3 Safety – IP Secure/Data Secure”

#### Secure Tunneling

Activation/deactivation of Secure Tunneling. If Secure Tunneling is activated, the communication via the tunneling connection is encrypted, see also “3 Safety – IP Secure/Data Secure”



### 4.1.3 Device – IP Configuration

The following picture shows the IP settings of the unit:

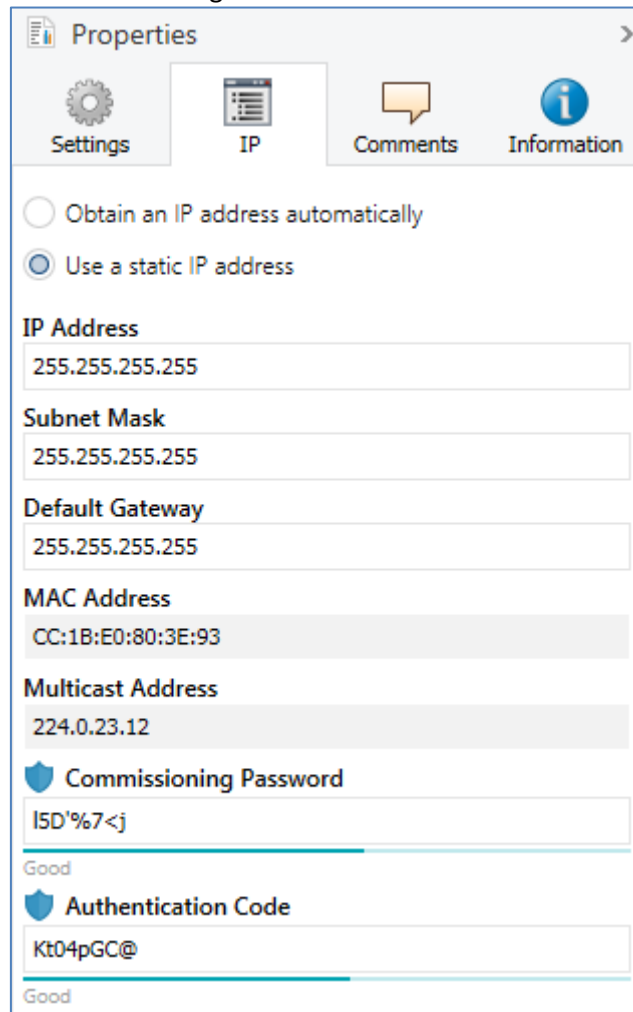


Figure 8: Device – IP Settings

#### Obtain an IP address automatically

The unit obtains the address automatically. A DHCP server needs to be available.

#### Use a static IP address

The user specifies a fixed IP address.

#### Subnet Mask/Standard Gateway

This can only be set with the setting "Use a static IP address".

The netmask is used by the unit to determine whether a communication partner is in the local network. If a partner is not in the local network, the unit does not send the telegrams directly to the partner, but to the gateway, which takes over the forwarding.

The setting of the gateway makes it possible for networks based on different protocols to communicate with each other.

Note: If the KNX IP Interface is only to be used in the local LAN, the entry 0.0.0.0 can remain. The network settings of the communicating PC can be read in the network settings of the PC.

**MAC Address**

Specified by the unit.

**Multicast Address**

The multicast address is specified by the backbone and can be changed in the project in the tab "Topology Backbone".

**Commissioning Password**

Set the start-up password (optional), see also "3 Safety – IP Secure/Data Secure".

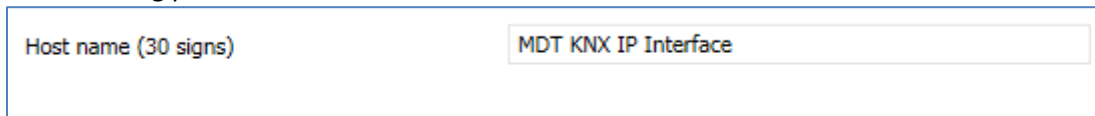
**Authentication Code**

Specify the authentication code (optional), see also "3 Safety – IP Secure/Data Secure".

## 4.2 Settings IP Interface without Secure

### 4.2.1 General

The following parameters can be set in the "General" submenu:



The screenshot shows a text input field with the label "Host name (30 signs)" and the value "MDT KNX IP Interface".

Figure 9: General Settings (without Secure)

The following table shows the setting options for this submenu:

ETS-Text	Dynamic Range [Default value]	Comment
Host name (30 signs)	any [MDT KNX IP Interface]	Any name can be chosen here, but it should be as meaningful as possible.

Table 3: General Settings (without Secure)

### 4.2.2 IP - Configuration

The following parameters can be set in the submenu "IP Configuration":

HTTP Port	<input type="radio"/> 80 <input checked="" type="radio"/> 8080
DHCP	<input checked="" type="radio"/> do not use <input type="radio"/> use
IP address	<input type="text" value="192.168.1.77"/>
Net mask	<input type="text" value="255.255.255.0"/>
Gateway	<input type="text" value="192.168.1.3"/>
DNS-Server	<input type="text" value="192.168.1.1"/>

Figure 10: Settings – IP Configuration (without Secure)

The following table shows the setting options for this submenu:

ETS-Text	Dynamic Range [Default value]	Comment
HTTP Port	<ul style="list-style-type: none"> <li>• 80</li> <li>• <b>8080</b></li> </ul>	Specifying of the http port
DHCP	<ul style="list-style-type: none"> <li>• <b>use</b></li> <li>• do not use</li> </ul>	Setting whether the IP address should be assigned automatically via DHCP or manually be set in further submenus
The following settings are displayed for "Do not use DHCP"		
IP-address	(0-255).(0-255).(0-255).(0-255) <b>0.0.0.0</b>	IP-address of the router ➤ only with manual IP address assignment
Net mask	(0-255).(0-255).(0-255).(0-255) <b>255.255.255.0</b>	Subnet mask of the network ➤ only with manual IP address assignment
Gateway	(0-255).(0-255).(0-255).(0-255) <b>0.0.0.0</b>	Gateway-address of the network ➤ only with manual IP address assignment
DNS	(0-255).(0-255).(0-255).(0-255) <b>0.0.0.0</b>	Domain Name Server of the network ➤ only with manual IP address assignment

Table 4: Settings – IP Configuration (without Secure)

The assignment of the IP address of the device can be done either manually or by a DHCP server, this is often available in DSL routers.

When selecting “DHCP - do not use”, the IP configuration can be set manually.

When selecting “DHCP – use”, a DHCP server must assign a valid IP address to the KNX / IP router. If there is no DHCP server available, the router restarts after a certain waiting period with an AutoIP address (address range of 169.254.1.0 to 169.254.254.255). Once a DHCP server is available, it automatically assigns a new IP address to the device.

### IP-address

The IP address must be allocated so that the bytes 1-3 are the same as those of the communicating computers. So the membership is given on the network. The 4th byte must be any available IP address (0-255) on the network, so as to avoid addressing conflicts.

The subnet mask is used for the device to determine whether a communication partner is located in the local network. Should not be a partner in the local network, the device does not send the telegrams directly to the partner but to the gateway, which handles the routing.

The setting of the gateway makes it possible for networks, which are based on different protocols to communicate with each other.

Note: If the KNX IP Interface is only be used in the local LAN, the entry can remain 0.0.0.0.

The network settings of the communicating computers can be read in the network settings of the PC.

## 4.3 Example of assigning IP addresses

A KNX IP interface to be accessed via PC. The PC has the following IP settings:

**IP address of the PC:**                               **192.168.1.30**  
**Subnet of the PC:**                                   **255.255.255.0**

Is the KNX IP Interface located in the same local LAN, i.e. it uses the same subnet, the assignment of the IP address is restricted by the subnet. That means in this example the IP address of the IP router has to be 192.168.1.xx. xx can be a number from 1 to 254 (with the exception of 30, which has already been used). It must be ensured, no numbers are assigned twice. The following settings can therefore be made in the IP Interface:

**IP address of the IP Interface:**               **192.168.1.31**  
**Subnet of the IP Interface:**                   **255.255.255.0**

## 4.4 Communication settings

If the IP configuration of the KNX Interface is valid, the device can be used as an interface to KNX. Therefore, connect the IP Interface to the KNX bus and the network.

### 4.4.1 Procedure ETS 4

**Attention: In ETS4 only the application "without Secure" can be used. Data Secure is only supported from ETS 5.7.2 on!**

In the "Settings" menu, select the "Communication" tab:

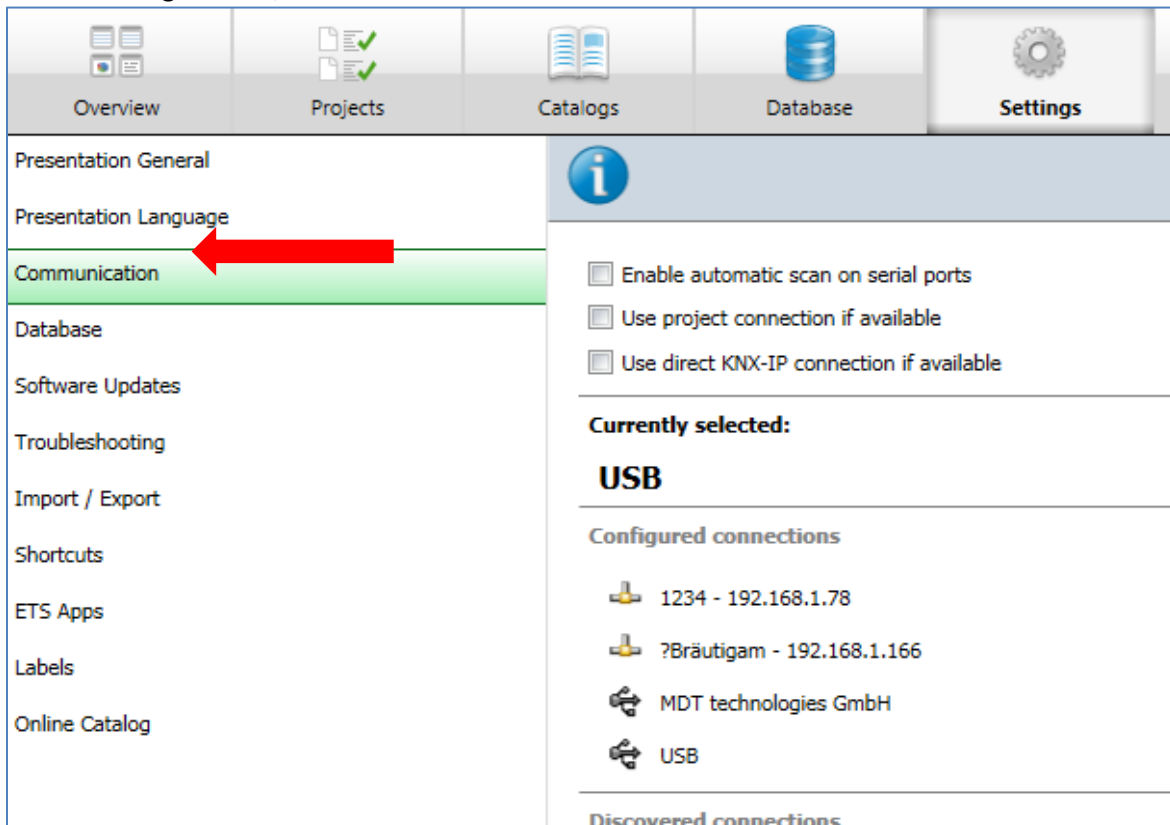


Figure 11: Settings ETS4 – Communication

Here the IP Interface should be listed in the “Discovered connections”:

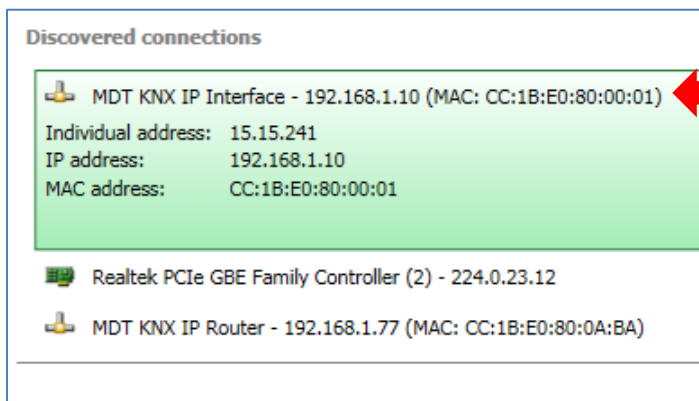


Figure 12: Settings ETS4 – Discovered connections

The connection can be chosen as active by clicking on "Select". Now the settings for this interface can be configured by selecting the button "Settings":

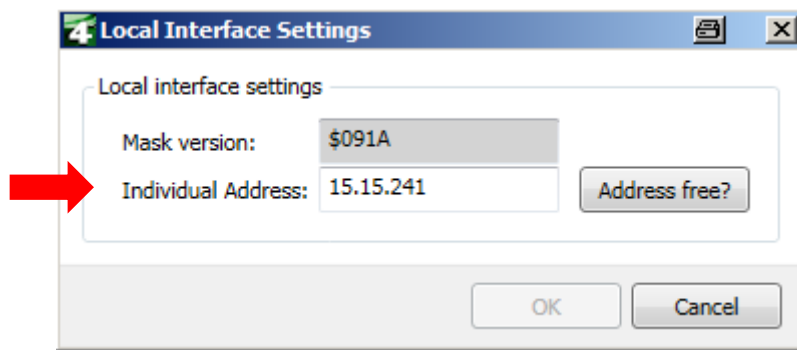


Figure 13: ETS4 – Local Interface Settings

Here, the first tunneling address can be assigned.

### 4.4.2 Procedure ETS 5

In the "Bus" menu, select the "Interfaces" tab:

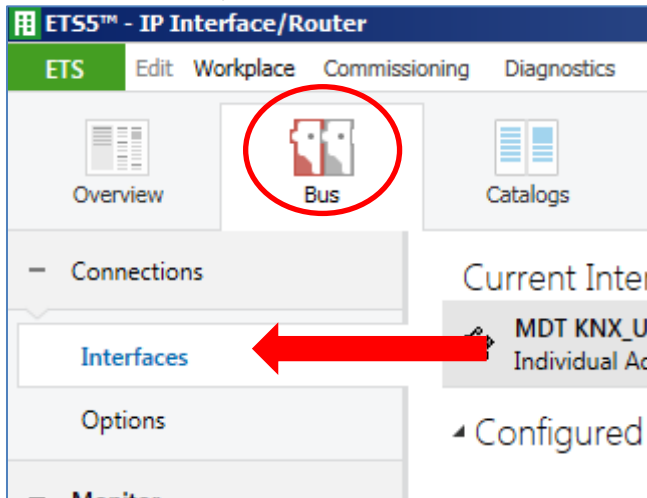


Figure 14: ETS5 – Bus - Interfaces

Here the IP Router/IP Interface should be listed in the “Discovered connections”:

Discovered Interfaces			
6.6.200 MDT KNX IP Interface	192.168.1.10:3671		CC:1B:E0:80:00:01
1.5.0 MDT KNX IP Router	192.168.1.77:3671		CC:1B:E0:80:0A:BA
MDT KNX_USB_Interface (MDT technologies)			

Figure 15: ETS5 – Discovered connections

After selecting the IP Router/IP Interface press button “Test”. If **OK** you can press button “Select”. Now device is shown as “Current Interface”

For the selected IP Router / IP Interface, the first tunneling connection can then be set:

**IP Tunneling**

**Name**  
MDT KNX IP Router

**Host Individual Address**  
1.5.0

**Individual Address**  
15.15.241 Address free?

**IP Address**  
192.168.1.77

**Port**  
3671

**MAC Address**  
CC:1B:E0:80:0A:BA



Figure 16: ETS5 – IP Tunneling connection

### 4.4.3 Set tunneling connections

#### 4.4.3.1 Procedure for IP Interface without Secure

The KNX IP router / KNX IP interface supports up to 4 simultaneous connections. The first physical address is adjusted as described under 4.4 in the ETS connections. In the Web-Interface, the further physical addresses can be assigned automatically by pressing the “Set” button in the menu “Prog.Mode”:


### KNX IP-Router

Status Programming Mode: Off

Change Programming Mode:

Individual Address            1. 0. 2  
     15.15.241

Tunneling Addresses            15.15.242  
     15.15.243  
     15.15.244

Set Tunneling Addresses         

Routing Multicast Address    239.0.0.0

Serial Number                    0104-262F000B

### TP Device

Status Programming Mode: Off

Change Programming Mode:

Individual Address            15.15.254

Serial Number                    0072-FFFF07B0

Figure 17: Set Tunneling Addresses (without Secure)

Now the 3 following physical addresses are assigned. If, for example, the IP Interface has got the first tunneling address assigned to the physical address 15.15.241 so the device provides further tunneling addresses automatically to 15.15.242, 15.15.243 and 15.15.244. When the first address was assigned to x.x.255, so the further tunneling addresses are not assigned automatically!



#### 4.4.3.2 Procedure for IP Interface with Secure

The addresses in the ETS 5 are set here.

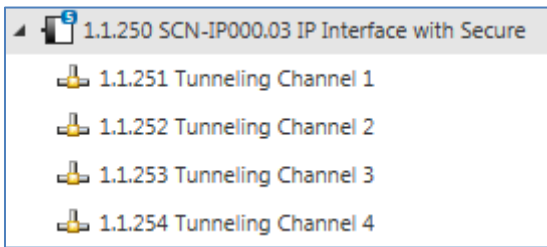


Figure 18: Set Tunneling Addresses in ETS5 (with Secure)

By selecting the tunneling channel, the name and address can be changed in the “**Properties**”.

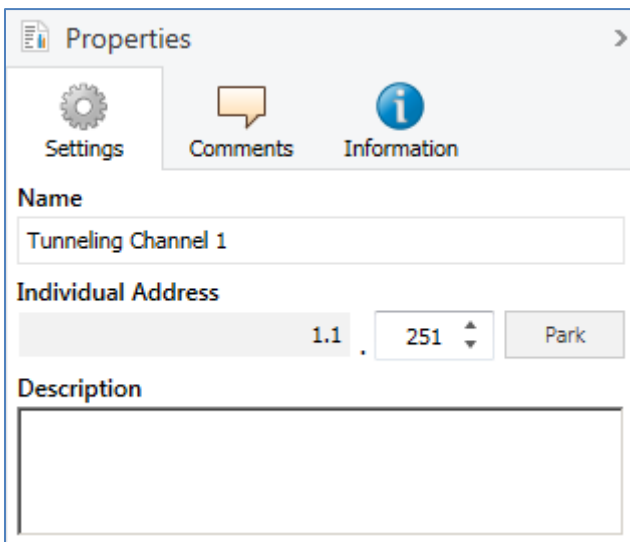


Figure 19: Set Tunneling Address ETS5 – Properties

## 5 Parameter -> E-Mail Client

### 5.1 General settings

#### 5.1.1 General

The following figure shows the general settings:

Startup delay time	10
Telegram Operation	10 min
Language for email content	<input checked="" type="radio"/> German <input type="radio"/> English
Device name	MDT IP Interface

Figure 20: General settings – E-Mail Client

#### Startup delay time

The Startup delay time determines the time between a bus voltage recovery and a functional device start.

#### Telegram Operation

With the help of the cyclic sending of the "Operation" telegram, a failure detection for this unit can be realised.

#### Language for email content

Here is selected in which language the email contents are sent.

#### Device name

The device name is displayed in the e-mail and can be integrated via macros in the email. It is advisable here to assign a meaningful name of the object, in which the IP interface is used. A name of up to 30 characters is allowed.

### 5.1.2 Web Interface

The following settings are available to set-up the web interface:

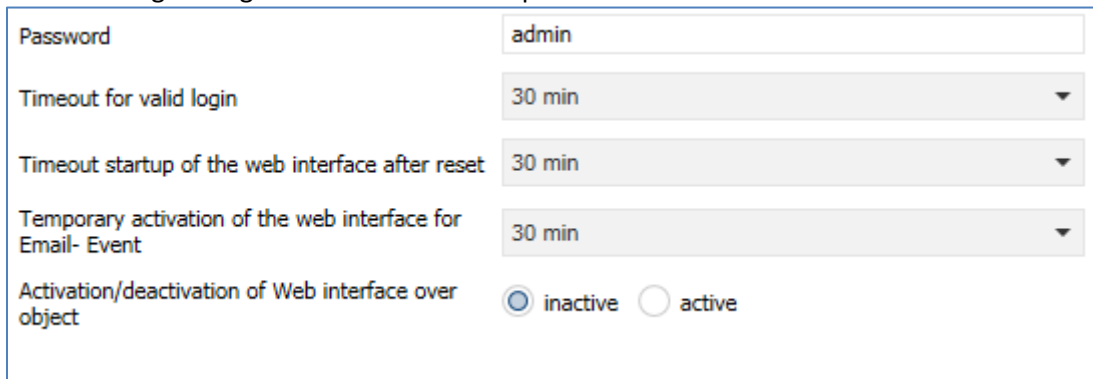


Figure 21: Settings – Web Interface

#### Password

The password is used to control access to the Web Interface. There should always be a password be entered!

Allowed characters: All characters from code page ISO 8859-1 excluding "space" and " &'\"'€ŠšŽžŒœÿ.

#### Timeout for valid login

The parameter specifies the time at which the web interface can be reached after a login. After the set time, the web interface is automatically locked.

#### Timeout startup of the web interface after reset

The parameter specifies the time how long the web interface can be reached after restarting (switching ON the bus voltage or reset via ETS). After the set time, the Web interface is no more accessible and can only be reached after a restart or after an activation of the web interface via object.

#### Temporary activation of the web interface for Email event

The parameter allows the temporal activation of the web interface after sending an email.

#### Activation/deactivation of the web interface over object

To activate via bus, regardless of any other settings, a communication object can be displayed to activate the web interface via object.

Following communication object appears for this purpose:

Number	Name	Length	Usage
55	Web interface	1 Bit	lock/unlock of Web Interface

Table 5: Communication object – lock/unlock Web-Interface

**Attention:** For security reasons it is recommended to disable the web interface after a certain time using the parameter "Timeout startup of the web interface after reset" or to activate the web interface only via object and deactivate when not in use!

### 5.1.3 Time/Date

The following settings are available for time and date:

Send cyclic system time each	10 min
Summer/Winter time change	<input type="radio"/> inactive <input checked="" type="radio"/> active
Time difference to universal time (UTC + ...)	(UTC +01:00) Amsterdam, Berlin, Bern, Rome, Vienn

Figure 22: Settings – Time/Date

#### Send cyclic system time each...

Setting whether the system time is to be sent cyclically.

#### Summer/Winter time change

Einstellung ob die Zeit automatisch zwischen Sommer- und Winterzeit umgestellt wird.

#### Time difference to universal time (UTC+...)

Setting the time zone

The following communication objects are displayed:

Number	Name	Length	Usage
2	Time	3 Byte	Sending Time
3	Date	3 Byte	Sending Date
4	Date/Time	8 Byte	Sending Date and Time

Table 6: Communication objects – Time/Date

## 5.2 E-Mail functions

The IP interface supports extensive email functionality. Thus, up to 30 status items are available, whose names and values can be displayed in the emails. The emails can be triggered via bit telegrams (bit alarms) or by sending text strings (Text alarms).

Furthermore can be sent up to 3 status reports, in which the 30 status items can be displayed. These status reports can be sent out by objects as well as at fixed times.

### 5.2.1 Status elements

The following settings are available for the status elements (here the example of status element 1):

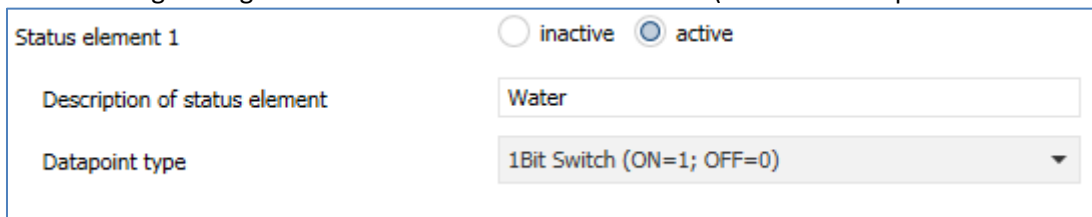


Figure 23: Settings – Status elements

Each state element, a display name and a data point type can be assigned. The display name can then be reported in the emails.

The following data point types with the corresponding values can be set:

#### Length: 1 Bit

Data point type	Value for 1	Value for 0
1 Bit Switch	On	Off
1 Bit Lock	Locked	Unlocked
1 Bit Up/Down	Down	Up
1 Bit Open/Closed	Closed	Open
1 Bit Heating/Cooling	Heating	Cooling
1 Bit Yes/No	Yes	No
1 Bit Present/Absent	Present	Absent
1 Bit Day	Day	Night
1 Bit Night	Night	Day

Table 7: Status elements – 1 Bit

### Length 1 Byte

Data point type	Dynamic range
1 Byte value	0-255
1 Byte Percent value	0-100%
1 Byte HVAC Status	0x01 -> Comfort 0x02 -> Standby 0x03 -> Night 0x04 -> Frost-/Heat protection
1 Byte HVAC Mode	The HVAC mode is evaluated bit by bit and displayed: Bit 0 -> 1 = Comfort Bit 1 -> 1 = Standby Bit 2 -> 1 = Night Bit 3 -> 1 = Frost-/Heat protection Bit 5 -> 0 = Cooling/ 1= Heating Bit 7 -> 1 = Frost alarm

Table 8: Status elements – 1 Byte

### Length 2 Byte

Data point type	Dynamic range
2 Byte unsigned value	0 – 65535
2 Byte signed value	-32768 – 32767
2 Byte floating value	-670760 – 670760

Table 9: Status elements – 2 Byte

### Length 4 Byte

Data point type	Dynamic range
4 Byte unsigned value	0 – 4 294 967 295
4 Byte signed value	-2 147 483 648 – 2 147 483 647
4 Byte floating value	Floating point according to IEEE 754

Table 10: Status elements – 4 Byte

### Length 14 Byte String

Data point type	Dynamic range
14 Byte String (ISO 8859-1)	Any string with max. 14 characters

Table 11: Status elements – 14 Byte

The following table shows the available communication objects:

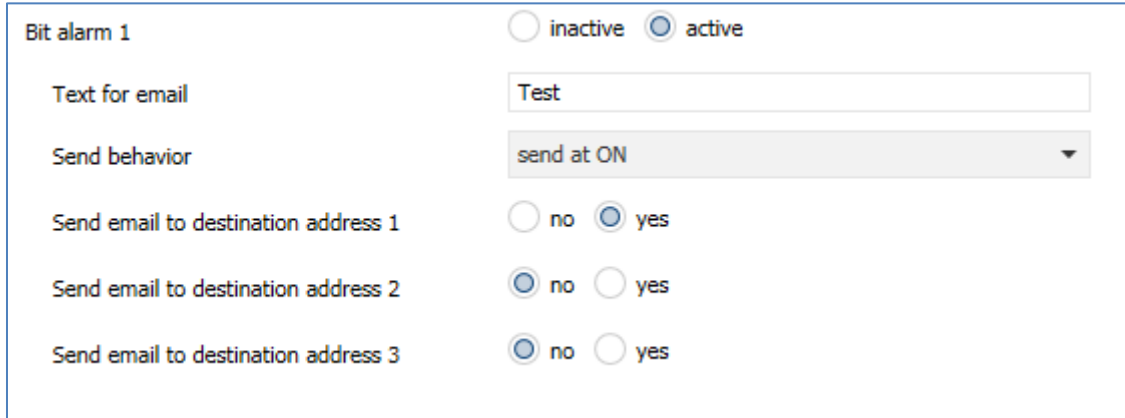
Number	Name	Length	Usage
21	Status element 1	1 Bit 1 Byte 2 Byte 4 Byte 14 Byte	Setting the value of the status element
<b>+1</b>	<b>next status element</b>		

Table 12: Communication objects – Status elements

### 5.2.2 Bit Alarms

Up to 10 "Bit Alarms" can be activated.

The figure below shows the available settings (here at the example of Bit alarm 1):



Bit alarm 1  inactive  active

Text for email

Send behavior

Send email to destination address 1  no  yes

Send email to destination address 2  no  yes

Send email to destination address 3  no  yes

Figure 24: Settings – Bit Alarm

The following table shows the settings available for an activated Bit alarm:

ETS-Text	Dynamic range [Default value]	Comment
Text for E-Mail	Any text, alternatively use of macros (see 5.2.2.1 Macros)	Setting of the text to be displayed in the email
Send behaviour	<ul style="list-style-type: none"> <li>▪ <b>send at ON</b></li> <li>▪ send at OFF</li> <li>▪ send at change to ON or OFF</li> <li>▪ send at change to ON</li> <li>▪ send at change to OFF</li> </ul>	Setting when the e-mail should be sent
Send email to destination address 1	<ul style="list-style-type: none"> <li>▪ yes</li> <li>▪ <b>no</b></li> </ul>	Setting whether to send to recipients 1
Send email to destination address 2	<ul style="list-style-type: none"> <li>▪ yes</li> <li>▪ <b>no</b></li> </ul>	Setting whether to send to recipients 2
Send email to destination address 3	<ul style="list-style-type: none"> <li>▪ yes</li> <li>▪ <b>no</b></li> </ul>	Setting whether to send to recipients 3

Table 13: Settings – Bit Alarm

The table below shows the available communication objects:

Number	Name	Length	Usage
11	Bit alarm 1	1 Bit	Triggering the first alarm bit
+1	<b>next Bit alarm</b>		

Table 14: Communication objects – Bit Alarm

### 5.2.2.1 Macros

In order to display values in emails, macros can be used. The following macros are available:

- **\$D\$** -> If this macro is inserted in the text, so the IP Interface replaces this by the device name.
- **\$T\$** -> If this macro is inserted into the text, so the IP Interface replaces this to the date and time at which the e-mail event was triggered.
- **\$Nxx\$** -> If this macro is inserted into the text so the IP Interface replace it with the name of the Status element "xx". Should, e.g. the name of the Status element 11 be displayed, so must be entered **\$N11\$**. For the Status element 1 it is enough to enter **\$N1\$**.
- **\$Vxx\$** -> If this macro is inserted into the text, so the IP Interface replaces this with the value of Status elements „xx“. Should, e.g. the value of the Status element 11 be displayed, so must be entered **\$V11\$**. For the Status element 1 it is enough to enter **\$V1\$**.
- A semicolon creates a line break, or writes the first part before the semicolon in the subject line of the email.

#### **Examples:**

For the following examples the device name "MDT" is given. The status element 1 has the name "light kitchen" and the data point type 1 bit switching.

- 1) Texts for E-Mail: **\$D\$ \$T\$ \$N1\$ \$V1\$**

An email with the subject "bit alarm: MDT" will be sent. The text of the e-mail is:

MDT date-time light kitchen OFF

Since nothing is separated by a semicolon, the whole text is put into the description field of the e-mail and used for the subject of the default-subject. The macros in the text field will be replaced by the IP Interface and lined up

- 2) Texts for E-Mail: **\$D\$; \$T\$; \$N1\$: \$V1\$**

An email with the subject "MDT" will be sent. The text of the e-mail is:

Date –Time

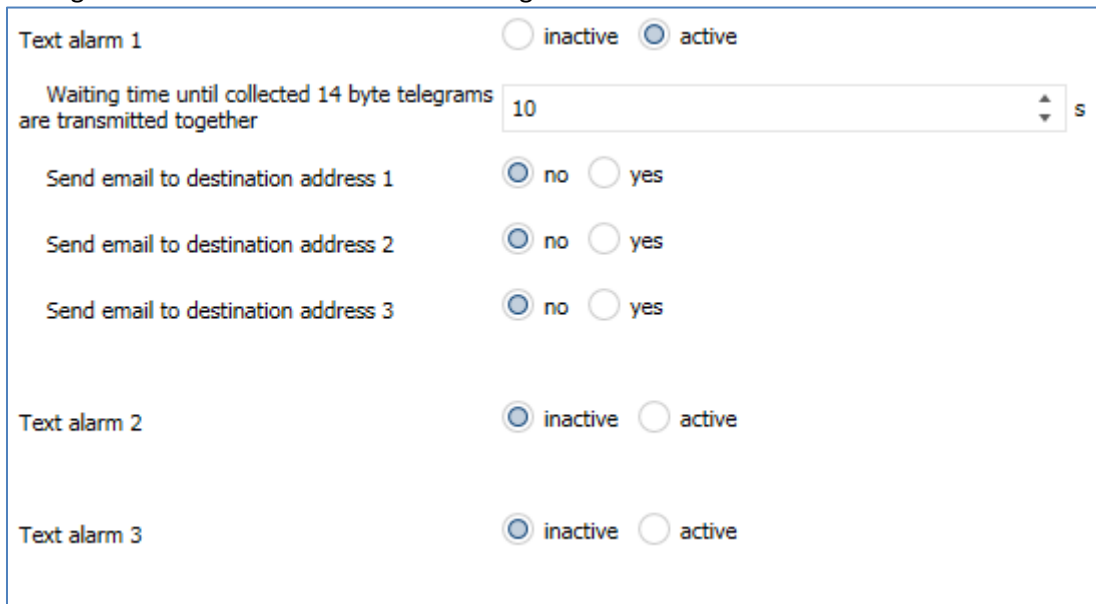
Light Kitchen: OFF (depending on the current value)

The semicolons separate the name of the device as subject and the text of the email. After that date, an additional line break is generated.



### 5.2.3 Text Alarms

The figure below shows the available settings:



Text alarm 1  inactive  active

Waiting time until collected 14 byte telegrams are transmitted together: 10 s

Send email to destination address 1:  no  yes

Send email to destination address 2:  no  yes

Send email to destination address 3:  no  yes

Text alarm 2:  inactive  active

Text alarm 3:  inactive  active

Figure 25: Settings – Text alarm

The following table shows the settings available for an activated text alarm:

ETS-Text	Dynamic range [Defaultwert]	Comment
Waiting time until collected 14 Byte telegrams are sent out together	1 ... 120 s [10 s]	Setting the time window in which text messages are combined into one email.
Send email to destination address 1	<ul style="list-style-type: none"> <li>▪ yes</li> <li>▪ no</li> </ul>	Setting whether to send to recipients 1
Send email to destination address 2	<ul style="list-style-type: none"> <li>▪ yes</li> <li>▪ no</li> </ul>	Setting whether to send to recipients 2
Send email to destination address 3	<ul style="list-style-type: none"> <li>▪ yes</li> <li>▪ no</li> </ul>	Setting whether to send to recipients 3

Table 15: Settings – Text alarm

A text alarm is triggered as soon as a value is written to the corresponding communication object. To send longer texts than 14 characters: After sending a value to the corresponding communication object, the IP Interface will wait the set waiting time.

If, within the set waiting time, another string has been sent to the communication object, all collected strings are sent one after another in the email.

The table below shows the available communication objects:

Number	Name	Length	Usage
8	Text alarm 1	1 Bit	Setting the value for the text alarm
+1	next Text alarm		

Table 16: Communication objects – Text alarms

### 5.2.4 Status Reports

The figure below shows the available settings (here at the example of Status report 1):

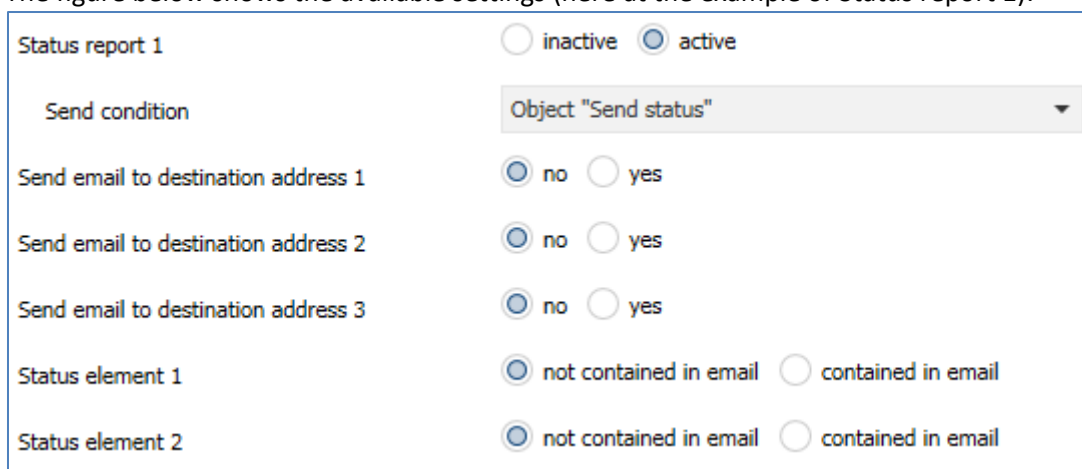


Figure 26: Settings – Status report

The following table shows the settings available for an activated status report:

ETS-Text	Dynamic range [Defaultwert]	Comment
Send condition	<ul style="list-style-type: none"> <li>▪ fixed day in the week</li> <li>▪ fixed date in month</li> <li>▪ <b>Object „Send status“</b></li> </ul>	Setting when the status report should be sent.
Send email to destination address 1	<ul style="list-style-type: none"> <li>▪ yes</li> <li>▪ <b>no</b></li> </ul>	Setting whether to send to recipients 1
Send email to destination address 2	<ul style="list-style-type: none"> <li>▪ yes</li> <li>▪ <b>no</b></li> </ul>	Setting whether to send to recipients 2
Send email to destination address 3	<ul style="list-style-type: none"> <li>▪ yes</li> <li>▪ <b>no</b></li> </ul>	Setting whether to send to recipients 3
Status element 1-30	<ul style="list-style-type: none"> <li>▪ <b>not contained in E-Mail</b></li> <li>▪ contained in E-Mail</li> </ul>	Setting whether the status element should be displayed in the email

Table 17: Settings – Status report

The status report can be sent cyclically, once a week, once a month as well as being transmitted via object.

Each activated Status element can be integrated in the status report. All activated Status elements are displayed in the status report as follows:

- “Name of the status element: value of the status element”

The table below shows the available communication objects:

Number	Name	Length	Usage
5	Status report 1	1 Bit	Sending the status report; is displayed only when the send condition is set to “object”
<b>+1</b>	<b>next Status report</b>		

Table 18: Communication objects – Status report

### 5.2.5 Specific behavior and error handling

In the e-mail functionality the following points should be noted:

- From technical reasons, between two e-mails is a 5 second break provided for an error-free processing.
- E-mails are sent only with current time. Therefore, it is checked whether ever a time via NTP was received. If not, the emails are sent out after 5 minutes with the start date 01/01/1970 00:00.  
Time via NTP server is monitored hourly. If no time is received, this is output via object 53 "NTP time server - error" with a "1". As soon as a time is received again, a "0" is sent.

The following table shows the corresponding communication object:

Number	Name	Length	Usage
53	NTP Time Server – Error	1 Bit	Sending an error

Table 19: Communication object – NTP Time Server Error

#### Error code-object:

The error code object is set and sent when ...

- The email was 4 times tried to transmit and this failed every time and the previous email delivery was without error or it was the first email after a restart. Between the attempts, the subsequent delays will be respected:
  - Delay before first repeat: 10 seconds
  - Delay before second repeat: 1 minute
  - Delay before third repeat: 10 minutes
- The email was tried 1 time to be sent and it failed, and the previous e-mail delivery was also flawed.

The following table shows the corresponding communication object:

Number	Name	Length	Usage
52	E-Mail – Error code	1 Byte	Sending an error

Table 20: Communication object – E-mail Error code

#### E-Mail buffer:

It can be buffered 10 emails.

- From the 8th Mail in the buffer, an alarm will be sent to the bus.
- When the buffer is full, additional email requests are rejected
- All values that are displayed in the bit alarm emails respectively status emails can only send the currently valid value at the time of shipment.

##### Example:

- T=0: Status element 3 = OFF
- T=10: Status element 3 = ON
- If at the time t=0 the mail delivery is triggered (for example, via object), the e-mail but only at the time t=10s is emitted, the value "On" in the email will be inserted.

The following table shows the corresponding communication object:

Number	Name	Length	Usage
51	E-Mail buffer – Overflow	1 Bit	Indicates an overflow of the e-mail buffer

Table 21: Communication object – E-mail buffer

**Error code and email buffer are reset if a transmission was successful or the error condition is no longer fulfilled.**

### 5.3 Overview Communication Objects

The following table shows the standard settings for the communication objects:

Standard Settings									
No.	Name	Function	Length	C	R	W	T	U	
<b>Common Objects</b>									
1	Operation	Send status	1 Bit	X	X		X		
2	Time	Send current time	3 Byte	X	X		X		
3	Date	Send current date	3 Byte	X	X		X		
4	Date/Time	Send current date and time	8 Byte	X	X		X		
51	E-Mail buffer	Overflow	1 Bit	X	X		X		
52	E-Mail	Error code	1 Byte	X	X		X		
53	NTP Time Server	Error	1 Bit	X	X		X		
54	Web interface	Lock status	1 Bit	X	X		X		
55	Web interface	Lock	1 Bit	X		X			
<b>Email Function</b>									
5	Status report 1	Send E-Mail	1 Bit	X		X			
+1	<b>next Status report</b>								
8	Text alarm 1	Send E-Mail	14 Byte	X		X			
+1	<b>next Text alarm</b>								
11	Bit alarm 1	Send E-Mail	1 Bit	X		X			
+1	<b>next Bit alarm</b>								
21	Status element 1	according to parameters	1 Bit 1 Byte 2 Byte 4 Byte 14 Byte	X	X		X		
+1	<b>next Status element</b>								

Table 22: Overview – Communication objects

### 5.4 Secure Group Address Communication

If a group address is to be transmitted in encrypted form, all devices whose communication objects communicate with this group address must support Data Secure.

The IP Interface supports up to 255 secure group addresses with a maximum of 64 different secure devices.

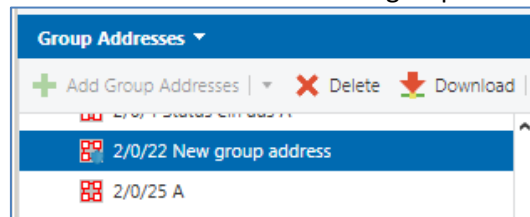
If two communication objects that both support Data Secure are connected to a group address, the ETS automatically sets this group address to "Security active". This is indicated by a blue protection shield in the Security tab:

	Security	Object ^	Device
↔		1: Operation - Send status	1.1.26 SCN-IP100.03 Email for IP Router with Secure
↔		1: Operation - Send status	1.1.31 SCN-IP000.03 Email for IP Interface with Secure

Figure 27: Secured group address

Using the Security tab in the group address settings, you can explicitly disable or enable security for this group address. The "automatic" setting is the default setting. In this way, the ETS decides independently whether the group address can be transmitted safely and activates this if possible:

- Open Workplace "Group Addresses" -> select the relevant group address ->



In "Properties" for the group address you get:

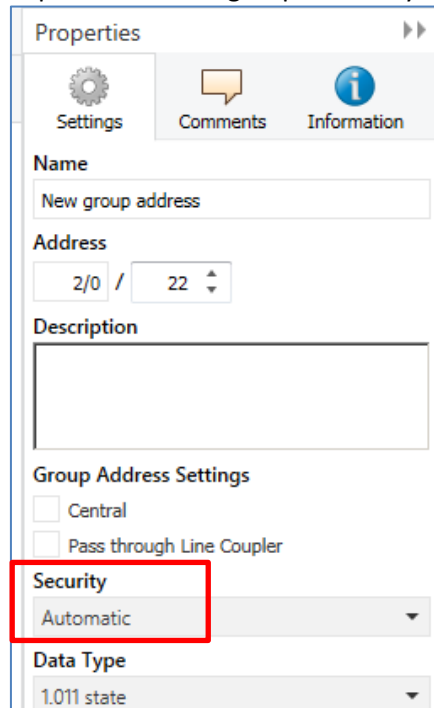


Figure 28: Changing the security settings for the group address

## 6 Web-Interface

### 6.1 Call of the Web-Interface

The web interface can be accessed in 2 types:

#### 1.) Via the Browser:

For this, open your default browser and insert the following address in the address bar:  
http://ip-address:Port

**Example:** The following settings are made for the IP interface:

HTTP Port	<input type="radio"/> 80 <input checked="" type="radio"/> 8080
DHCP	<input checked="" type="radio"/> do not use <input type="radio"/> use
IP address	<input type="text" value="192.168.1.178"/>
Net mask	<input type="text" value="255.255.255.0"/>
Gateway	<input type="text" value="192.168.1.3"/>
DNS-Server	<input type="text" value="192.168.1.1"/>

Figure 29: Web Interface – Example IP Configuration

Here insert <http://192.168.1.178:8080> to the address bar.

The IP address of the IP interface can also be viewed in the ETS settings under Bus -> Interfaces.

#### 2.) Via the Windows Explorer:

Go to the Windows Explorer and open the folder “Network”. Here your IP interface should appear with the specified host name. Double-click on the interface your default browser is invoked with the correct address.

## 6.2 Overview Web Interface

After calling up the web interface, the login window appears:

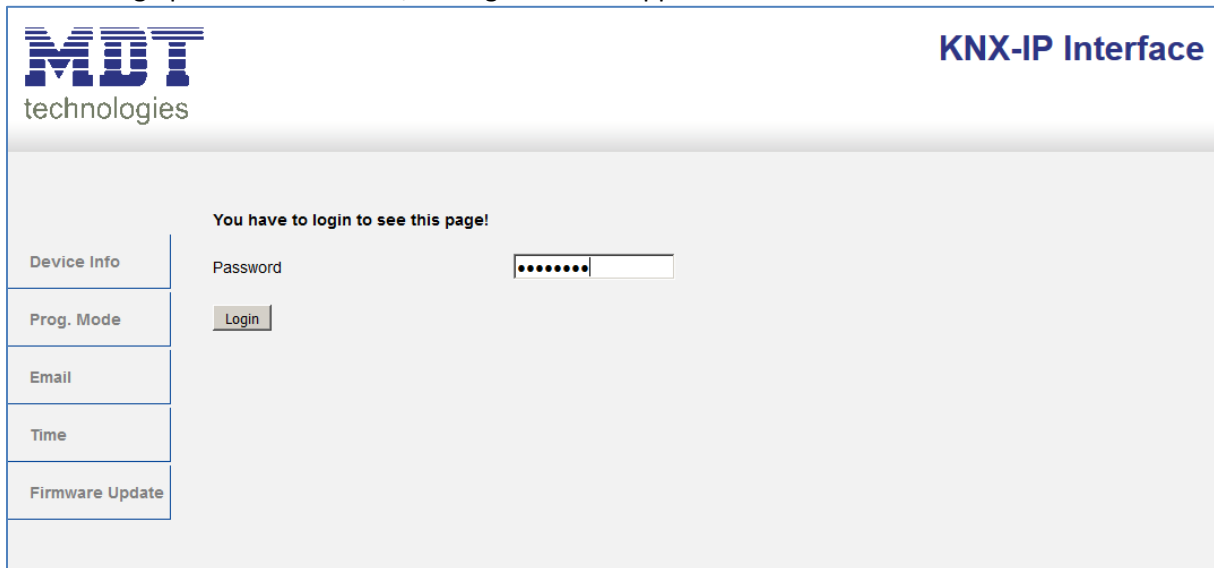


Figure 30: Web Interface – Login window

After a successful login, the menus can be selected on the left side. The menus have the following functions:

- **Device Info**  
The menu “Device Info” contains information and settings of the IP Interface, such as MAC address, IP address, network settings, software version, etc.
- **Prog. Mode**  
In the menu “Prog. Mode” the programming LEDs for the TP and the IP side can be switched ON and OFF. Furthermore, the allocated physical addresses, the tunneling addresses and serial number can be seen.
- **Email**  
In the menu “Email” the e-mail functionality can be set, see also 6.3 .
- **Time**  
In the menu “Time”, information concerning the time server can be viewed.
- **Firmware Update**  
It is possible to perform a firmware update for the IP Interface.  
For more information see **Fehler! Verweisquelle konnte nicht gefunden werden..**  
If you have any questions, please contact MDT Support at [support@mdt.de](mailto:support@mdt.de).

### 6.3 Setting of E-Mail functionality

To set up E-mail functionality, open the menu “E-mail” and click "Settings":

**Destination E-Mail Test:**

E-Mail Address 1: knx@mdt.de

E-Mail Address 2:

E-Mail Address 3:

Status: no error

Server Response:

[Settings](#) ←

Figure 31: Web Interface – Destination E-Mail Test

Subsequently, the following menu opens:

**Email settings**

**Outgoing (SMTP) settings:**

SMTP server address:

SMTP server port:

E-Mail Address:

Username:

Password:

**Destination E-Mail Address:**

E-Mail Address 1:

E-Mail Address 2:

E-Mail Address 3:

Figure 32: Web Interface – E-Mail settings



Now the sending E-mail address and the destination addresses (up to 3) can be set. The following settings have to be made for the sending email address:

- **SMTP server address**  
Here the outgoing mail server has to be specified.
- **SMTP server port**  
Here the port is specified for the outgoing mail.
- **E-Mail Address**  
Specification of the sending email address.
- **Username**  
The name needs to be entered with which you log on to your e-mail address. This can vary depending on the provider and can be e.g. a complete e-mail address, a user name or an ID.
- **Password**  
Enter the password you use to log in to your e-mail address.

**Note:** The following example is made with the German provider “WEB.DE”. For details regarding the specifications of other providers (outside Germany) please check with your local provider.

If searching for server data e.g. at web.de, the following data are given:

**Serverdaten**

POP3 steht für die englische Abkürzung "Post Office Protocol Version 3". Per POP3 werden E-Mails von einem Server in ein E-Mail-Programm übertragen und gleichzeitig vom jeweiligen Server gelöscht.

**Posteingang:**  
 Server: **pop3.web.de**  
 Port: **995**  
 Verschlüsselung: **SSL-Verschlüsselung**  
 (Steht in einem Programm "SSL" nicht zur Verfügung, genügt es, die Option "Verschlüsselung" zu aktivieren.)

**Postausgang:**  
 Server: **smtp.web.de**  
 Port: **587**  
 Verschlüsselung: **STARTTLS**  
 (Steht in einem Programm "STARTTLS" nicht zur Verfügung, nutzen Sie bitte das Protokoll "TLS". Existiert auch hierfür keine Option, genügt es, die Option "Verschlüsselung" zu aktivieren.)

Welche Ordner werden per POP3 abgerufen?

Figure 33: Example 1 – Server data (German)

Thus, in the field „SMTP server address“ the value „smtp.web.de“ can be entered and in the field „SMTP server port“ the value „587“

At the provider web.de it is further required that the sending of e-mails via external programs needs to be activated in the settings:

**WEB.DE Mail über POP3 & IMAP**

Wenn Sie Ihre E-Mails mit Outlook oder einem anderen E-Mail-Programm abrufen möchten, müssen Sie dazu POP3 und IMAP aktivieren. Bitte verwenden Sie die angezeigten Zugangsdaten.

E-Mails per externem Programm (Outlook, Thunderbird) versenden und empfangen

Für die wichtigsten E-Mail-Programme bieten wir Ihnen Schritt-für-Schritt-Anleitungen an.

POP3

**Serverdaten für den POP3 Abruf:**

POP3-Server	<b>pop3.web.de</b>
SMTP-Server	<b>smtp.web.de</b>

Figure 34: Example 2 – Server data (German)

In addition to the above described vendor web.de, the following providers are tested with the settings listed below:

**gmx.de**

SMTP server address: mail.gmx.net

SMTP server port: 587

**1&1**

SMTP server address: smtp.1und1.de

SMTP server port: 587

**Telekom**

SMTP server address: smtpmail.t-online.de

SMTP server port: 465

**HotMail, now: outlook.com/de**

SMTP server address: smtpmail.live.com

SMTP server port: 587

**Strato**

SMTP server address: smtp.strato.de

SMTP server port: 587

All data of the email providers are on the state of the manual, see front page, and are not guaranteed.

Into the “Destination E-mail address” insert all email addresses (max. 3) to which you want to send an email.

Then you close the menu by the OK button.

In the following menu the e-mail configuration can be tested:



Figure 35: Web Interface – Destination E-Mail Test

After successful configuration, a test e-mail to the set destination addresses can be triggered. Then the status is displayed and if so, an error is displayed. The significance of the error codes is shown in next chapter 6.4 E-Mail – Error codes & remedy

## 6.4 E-Mail – Error codes & remedy

Status in the web interface always shows the status of the last sent email. If an error occurs, the error codes have the following meanings:

- Error 0: No error (250 Requested mail action okay, completed: id=0LgK3g-1alfqB1ZsS-00nhnX)
  - Last E-Mail was sent without problems.
- Error 4: unable to connect to server
  - Wrong Port specified
    - Check Port
- Error 6: invalid sending Email address
  - Sending-E-Mail address is invalid
  - Sending-E-Mail address not accepted by server
    - Check the settings for the E-Mail address
- Error 8: invalid receiving Email address
  - Destination E-Mail address is invalid
    - Check destination E-Mail address
- Error 9: Socket unexpectedly closed
  - Restart the device and if necessary reprogram
- Error 12: Unknown/unsupported server authentication request (535 Authentication credentials invalid)
  - Invalid username or password
    - Check username and/or password

## 6.5 Receive E-Mail as push message

E-mails can be received as a push message to the phone. Therefore, certain services need to be used. Thus, e.g. be used for Apple devices, the service Prowl: <http://www.prowlapp.com/> can be used. By using push messages, emails are immediately displayed as "Notification" on the device.

## 6.6 Receive E-Mail as SMS

To convert emails into SMS and send this, a number of providers offer this service in certain packages, for example, Telekom. If your email provider does not support any SMS-service for e-mails, so third parties like SMS77 - <https://www.sms77.de/> - can be used.

## 7 Index

### 7.1 Register of illustrations

Figure 1: Structure – Hardware module .....	5
Figure 2: Commissioning Password/ Authentication Code.....	10
Figure 3: Secure Commissioning/Secure Tunneling.....	11
Figure 4: Enter FDSK.....	12
Figure 5: Subsequent input FDSK.....	13
Figure 6: General Settings – IP Interface .....	15
Figure 7: Device – Settings .....	16
Figure 8: Device – IP Settings.....	17
Figure 9: General Settings (without Secure) .....	18
Figure 10: Settings – IP Configuration (without Secure) .....	19
Figure 11: Settings ETS4 – Communication.....	21
Figure 12: Settings ETS4 – Discovered connections .....	21
Figure 13: ETS4 – Local Interface Settings .....	22
Figure 14: ETS5 – Bus - Interfaces .....	23
Figure 15: ETS5 – Discovered connections .....	23
Figure 16: ETS5 – IP Tunneling connection.....	23
Figure 17: Set Tunneling Addresses (without Secure).....	24
Figure 18: Set Tunneling Addresses in ETS5 (with Secure).....	25
Figure 19: Set Tunneling Address ETS5 – Properties.....	25
Figure 20: General settings – E-Mail Client.....	26
Figure 21: Settings – Web Interface.....	27
Figure 22: Settings – Time/Date.....	28
Figure 23: Settings – Status elements.....	29
Figure 24: Settings – Bit Alarm .....	31
Figure 25: Settings – Text alarm .....	33
Figure 26: Settings – Status report .....	34
Figure 27: Secured group address .....	37
Figure 28: Changing the security settings for the group address .....	37
Figure 29: Web Interface – Example IP Configuration.....	38
Figure 30: Web Interface – Login window .....	39
Figure 31: Web Interface – Destination E-Mail Test .....	40
Figure 32: Web Interface – E-Mail settings .....	40
Figure 33: Example 1 – Server data (German).....	41
Figure 34: Example 2 – Server data (German).....	41
Figure 35: Web Interface – Destination E-Mail Test .....	42

## 7.2 List of tables

Table 1: Overview LEDs.....	6
Table 2: General Settings – IP Interface.....	15
Table 3: General Settings (without Secure).....	18
Table 4: Settings – IP Configuration (without Secure) .....	19
Table 5: Communication object – lock/unlock Web-Interface .....	27
Table 6: Communication objects – Time/Date.....	28
Table 7: Status elements – 1 Bit.....	29
Table 8: Status elements – 1 Byte .....	30
Table 9: Status elements – 2 Byte .....	30
Table 10: Status elements – 4 Byte .....	30
Table 11: Status elements – 14 Byte .....	30
Table 12: Communication objects – Status elements.....	30
Table 13: Settings – Bit Alarm.....	31
Table 14: Communication objects – Bit Alarm.....	31
Table 15: Settings – Text alarm .....	33
Table 16: Communication objects – Text alarms.....	33
Table 17: Settings – Status report.....	34
Table 18: Communication objects – Status report.....	34
Table 19: Communication object – NTP Time Server Error.....	35
Table 20: Communication object – E-mail Error code.....	35
Table 21: Communication object – E-mail buffer.....	35
Table 22: Overview – Communication objects .....	36

## 8 Attachment

### 8.1 Statutory requirements

The above-described devices must not be used with devices, which serve directly or indirectly the purpose of human, health- or lifesaving. Further the devices must not be used if their usage can occur danger for humans, animals or material assets.

Do not let the packaging lying around careless, plastic foil/ -bags etc. can be a dangerous toy for kids.

### 8.2 Disposal routine

Do not throw the waste equipment in the household rubbish. The device contains electrical devices, which must be disposed as electronic scrap. The casing contains of recyclable synthetic material.

### 8.3 Assemblage



#### **Danger to life due to electric current!**

All activities on the device should only be done by an electrical specialist. The county specific regulations and the applicable KNX-directives have to be observed.

### 8.4 History

V1.0	- First Version of the 3rd generation of IP Interfaces – SCN-IP000.03	05/2019
V1.1	- General corrections; descriptions "Update", "Reset" extended	12/2020