Product Manual

SMART CONNECT KNX Remote Access

1-0003-004

Documentation valid for:

Product database entry:	v7.2
Firmware:	v7.0
Remote Access Windows Client:	from v1.42
Document issued:	07.08.2024

Legal Information

SMART CONNECT KNX Remote Access Product Manual
Status: 07.08.2024

ise Individuelle Software und Elektronik GmbH
Osterstraße 15
26122 Oldenburg, Germany

Products to which reference is made in this document can be either brands or registered trademarks of the respective rights holder. Ise Individuelle Software und Elektronik GmbH and the author make no claim to these brands. The brands are named solely for the purpose of providing the necessary description.

Trademark

KNX is a registered trademark of the KNX Association.

Feedback and information about products

If you have any questions regarding our products, please contact us via e-mail at sales@ise.de. We would be pleased to receive your ideas, suggestions for improvements and criticism via e-mail at support@ise.de.

Contents

1 About this documentation

This documentation will accompany you through all phases of the product life cycle of SMART CONNECT KNX Remote Access. You will learn for example how to assemble, install, commission and configure the device.

All descriptions in this documentation relating to configuration in the ETS refer to the variant "ETS Professional" in the version 6.

Explanations for the concepts of KNX do not form part of this documentation.

1.1 Target group

This documentation is aimed at qualified electricians and KNX processors.

Only qualified electricians may assemble and install the SMART CONNECT KNX Remote Access. Specialist knowledge of KNX is a prerequisite.

Anyone may configure the SMART CONNECT KNX Remote Access. We recommend that configuration is done by a system integrator with sound specialist knowledge of KNX and using the ETS.

1.2 Symbols and typographical conventions

Symbol / label	Meaning
ℹ	Warning of possible material damage
⚠	General warning
⚡	Warning of electrical voltage

Table 1: Symbols and safety notes

Symbol / label	Meaning
F1	PC button
<<Inscription>>	Text on software interface
💡	Troubleshooting tip
ℹ	Important additional information

Table 2: Special symbols and typographical conventions

2 About SMART CONNECT KNX Remote Access

2.1 Proper use

The SMART CONNECT KNX Remote Access enables safe remote access to your KNX installation. A VPN connection can also be established with your Ethernet-based home network. In order to carry out remote maintenance with the ETS, the Remote Access Windows Client gives you access to:

- the IP interfaces in the KNX installation
- the devices contained in the remote network.

The SMART CONNECT KNX Remote Access is a KNX system device and complies with the KNX guidelines.

Important

ise Individuelle Software und Elektronik GmbH assumes no liability for damage caused by improper use or use for purposes other than or contrary to the intended purpose.

Configuration: Compatible ETS versions

Simple integration into the KNX System (can be completely configured via ETS):

- ETS5 or higher;
- Product database entry: Download the product database entry from our website www.ise.de or from the ETS online catalogue free of charge.

KNX Secure

SMART CONNECT KNX Remote Access is KNX Secure.

The device is compatible with KNX Secure. KNX Secure offers protection against manipulation in building automation and can be configured in the ETS project.

- The required KNX Secure certificate or the FDSK (Factory Default Setup Key) that it contains can be found on a sticker on the side of the device and is also enclosed with the device.
- For maximum security, we recommend removing the sticker from the device.
- Keep the certificate in a safe place.
- You cannot restore the certificate yourself.
- Please contact our support team if you should lose the certificate despite utmost care.

2.2 System

The SMART CONNECT KNX Remote Access is connected to the KNX installation via KNX/TP.
The device is connected to the Internet via IP in order to enable access to the KNX system.
The configuration of the remote access can be performed on https://my.ise.de.
Communication between the SMART CONNECT KNX Remote Access and my.ise is encrypted as per AES specifications and is secured with digital certificates.

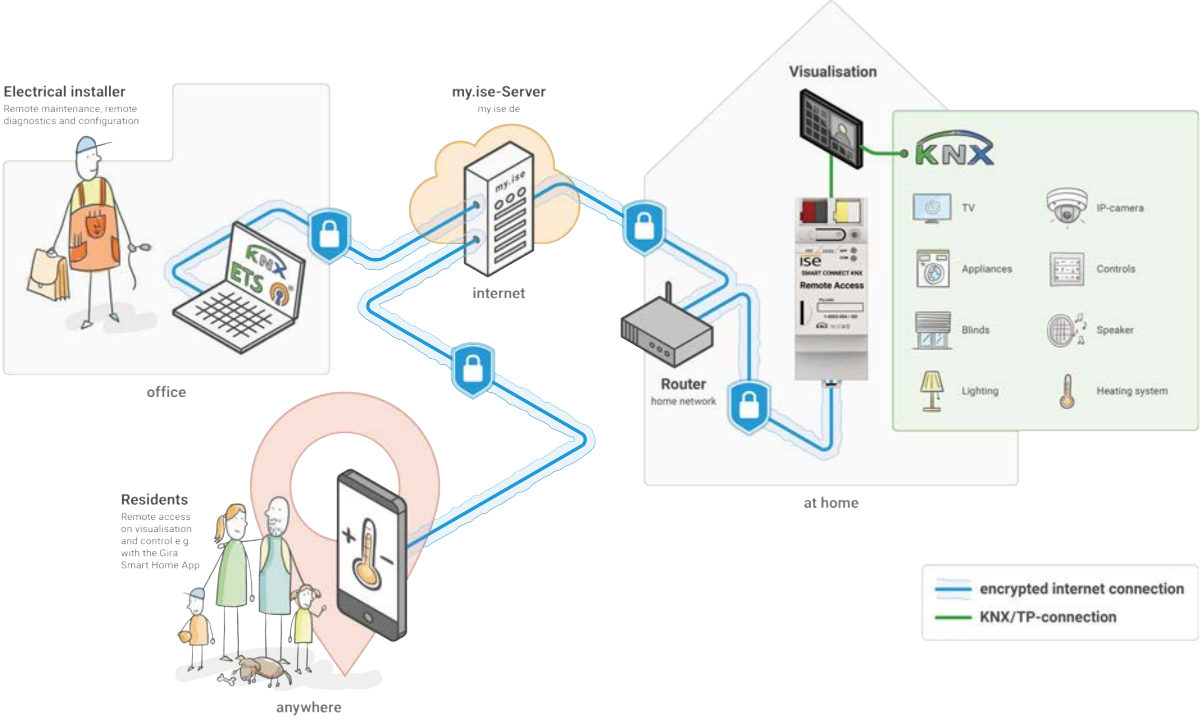


Figure 1: Remote access system chart

2.3 Functions and use cases

- To access the KNX devices remotely, connect the SMART CONNECT KNX Remote Access with the KNX installation.
- The SMART CONNECT KNX Remote Access is connected to the home network over Ethernet. It then connects to the my.ise server automatically through your existing Internet access https://my.ise.de ► see Using the my.ise server, p. 7
- Among other things, VPN network coupling (either Layer 2 or Layer 3) provides access to KNX installations, visualization interfaces and files in the home network. This means uncomplicated access to the KNX system and other applications is also possible for smartphone apps. The VPN access can be controlled and monitored via KNX group objects.
- Notifications can be triggered via KNX telegrams, saved to my.ise and forwarded by means such as a push notification (Android or iOS), an e-mail, a phone call or text message.
- Records and graphs. The SMART CONNECT KNX Remote Access can record values from the KNX system and shown them in graphs on the device website. The graphs can also be embedded in external visualisations or websites.

- Use as a data logger. The SMART CONNECT KNX Remote Access features a card reader for microSDXC cards up to 1 TB. The KNX telegrams in an ETS-compliant format can be recorded on the memory card for analysis purposes. The card memory can be used as a ring memory or as a read-only memory.
- Use as a time server. The SMART CONNECT KNX Remote Access can transmit the time and date to the bus at configurable intervals. It is possible to initiate transmission of the current time and the current date using a trigger.
- Administration of remote access options and access rights on my.ise ► see my.ise functions, p. 7
- Access to the HTML pages from any networked end device ► see Access to websites in the remote network, p. 8
- KNX communication with the ETS via KNXnet/IP, IP direct download and Eiblib/IP via the Remote Access Windows Client ► see Remote access options, p. 12
- Configuration access to the Gira HomeServer with the HomeServer Expert via the Remote Access Windows Client.
- Access to Windows computers using the remote desktop connection through the Remote Access Windows Client.
- Freely configurable TCP port redirects via the Remote Access Windows Client.
- KNX/TP connection with integrated IP interface (tunnelling server) for KNX access using ETS or other software. Three concurrent connections can be set up for using the download and the groups and bus monitor.
- Status signalling and access management of the secured connections using KNX group objects.
- The remote access also functions via a mobile phone network access even if it does not have a unique IP address accessible from the outside, as is usually the case for UMTS or LTE.
- For your internet router, communication from your SMART CONNECT KNX Remote Access will not differ from an encrypted connection in your browser, in a similar way to online banking, for example.

Functional enhancements from updates

You can obtain functional enhancements for the SMART CONNECT KNX Remote Access with a new version of the firmware. Simply download the latest firmware and the relevant product manual from our website www.ise.de.

► see Updating the firmware via the device website, p. 41

2.4 Using the my.ise server

The my.ise server can be accessed at https://my.ise.de.
The my.ise server acts as the point of exchange during remote access to the end devices in your building.
The SMART CONNECT KNX Remote Access uses the standard protocols HTTPS, TLS/SSL and WebSocket to communicate with the my.ise server. The my.ise server does not save the transmitted data. It merely forwards them instead. The server is operated in Germany in compliance with the strict European data protection guidelines.

Note on cookies

Use of the my.ise server requires the use of cookies in the browser for technical reasons.

You have the following options to use the my.ise server:

- Registration of a new user for initial login.
- Login as an existing registered my.ise user.

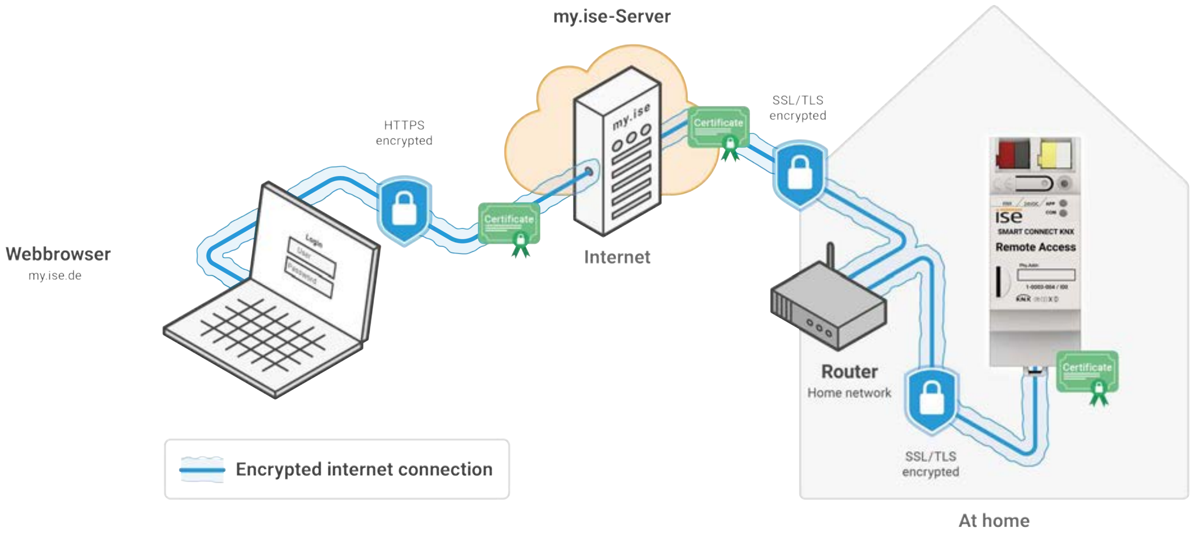


Figure 2: Overview of secure access with my.ise

my.ise functions

The following functions are available to manage your SMART CONNECT KNX Remote Access on my.ise:

- Setting up users and access groups and managing access rights
- Adding further devices
- Retrieving device data
- Configuring the VPN access
- Creating forwardings for notifications
- Accessing notifications received
- Adding links to access web interfaces in the remote network
- Setting up application accesses for using supported apps

Access to websites in the remote network

Network devices with an integrated web server, such as cameras or network printers, can be reached via the SMART CONNECT KNX Remote Access and automatically receive their name under the domain httpaccess.net.
You can access the network device concerned in a web browser using this name. Communication over the Internet is encrypted. The user authentication is verified based on the access rights configured on my.ise for your SMART CONNECT KNX Remote Access.

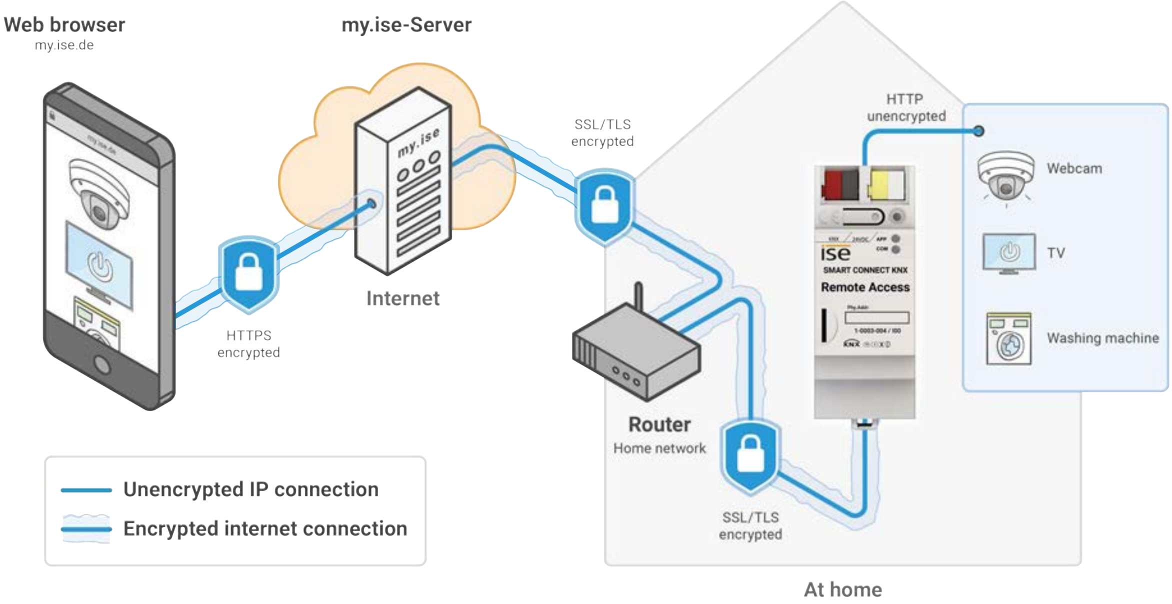


Figure 3: Secure device access to websites via my.ise

2.5 Remote Access Windows Client

The Remote Access Windows Client is an application that provides secure access to devices on the remote network via the Internet. To ensure this is the case, the Remote Access Windows Client is installed and launched on the same PC as the ETS.

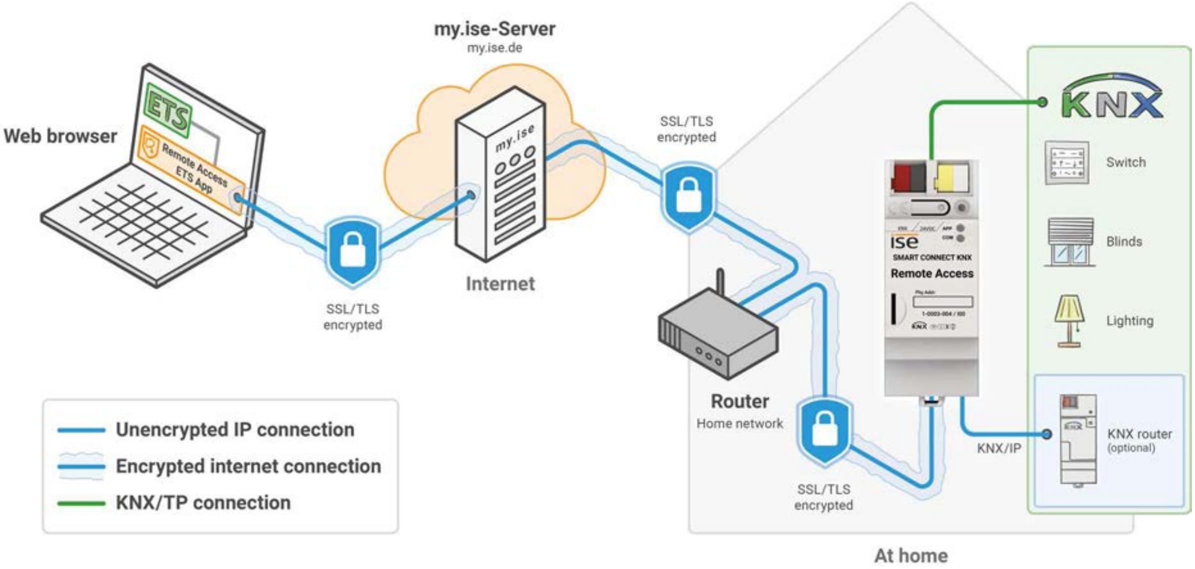


Figure 4: Secure access to the KNX installation via my.ise

The Remote Access Windows Client establishes an encrypted connection to the SMART CONNECT KNX Remote Access via my.ise. This connection is made available to other applications on your computer and on your local network so that they can access devices on the remote network.

No client is necessary to access devices using HTTP. You can use my.ise directly.

The Remote Access Windows Client is currently available for Microsoft Windows from version 8.

Use cases

The Remote Access Windows Client is used in the following use cases:

- Remote access to KNX installation using the KNX/IP protocol
- Remote configuration of a Gira HomeServer with the Gira Expert
- Remote access via other TCP protocols (e.g. remote desktop link RDP)

Installing the Remote Access Windows Client

1. Scroll down to the download section on the product page.
2. Download the appropriate installation file for Windows (x86) or (x64).
3. Execute the installation file on the same PC as the ETS.

2.5.1 General Remote Access Windows Client settings

1. Launch the client.

2. Use the gear icon ⚙ to open the general settings. You will find information on specific settings in the following table.

Setting	Description
Activate ETS access for the entire local area network (LAN) (only for this PC apart from that)	• Activated: All clients running on the same local network have access to the KNX/IP devices. • Disabled: The KNX/IP devices are available only to the current client. The client is the PC on which your ETS is running. The PC is identified by its IP address. The KNX/IP devices are displayed under <<Discovered interfaces>> in the ETS.
Automatically activate secure remote access to the Gira Home Server for new device configurations	Make this setting if you will use the Gira HomeServer for your projects on a regular basis.

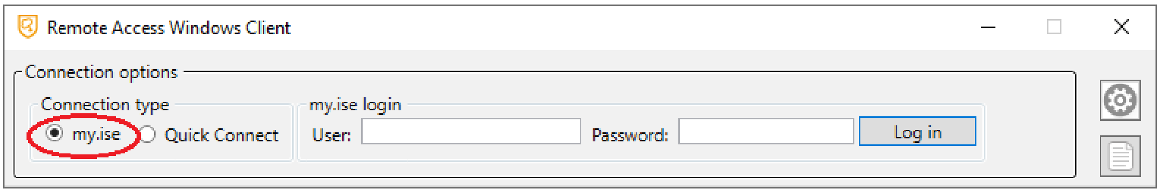
Table 3: Remote Access Windows Client settings

2.5.2 Establishing a connection using a my.ise login

Requirement: You are registered as a user on my.ise.

1. Launch Remote Access Windows Client.

2. Select <<my.ise>> as the connection type.



Remote Access Windows Client

Connection options

Connection type: ● my.ise ○ Quick Connect

my.ise login

User:

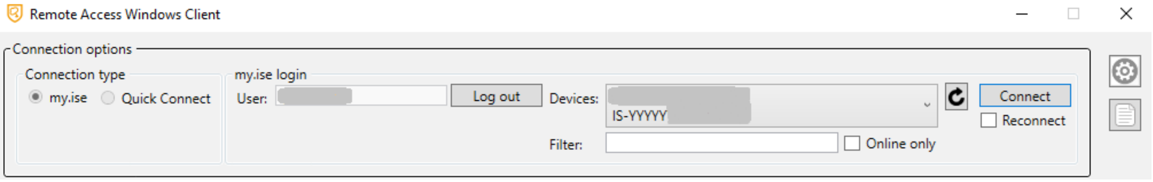
Password:

Figure 5: Connection type my.ise

3. Log on using the same user data as for my.ise.

4. Select the required device.

Use the filter if you have multiple devices. Either enter a text or limit the selection to the devices currently logged onto my.ise using the <<Online only>> function.


Remote Access Windows Client

Connection options

Connection type

● my.ise ○ Quick Connect

my.ise login

User: [redacted] Log out

Devices: IS-YYYYY[redacted]

Filter: □ Online only

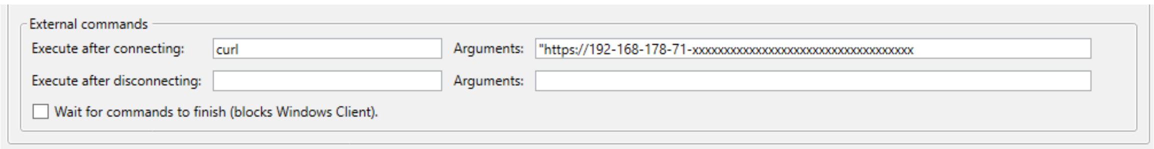
Connect

□ Reconnect

Figure 6: Device selection for my.ise Login

5. Select remote access based on your use case. Remote access via KNX/IP is activated by default (see Remote access options, p. 12).

6. If required, define external commands that should be executed after a connection is established or cancelled.
   Enter the name of the command or program with its path into the left input field. Complete the <<Arguments>> input field with all the parameters that need to be transferred to execute the command.


External commands

Execute after connecting: curl Arguments: "https://192-168-178-71-xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx

Execute after disconnecting: Arguments:

□ Wait for commands to finish (blocks Windows Client).

Figure 7: External commands

Combine external commands using the <<Reconnect> function under the <<Connect>> button. The client uses this function to try to reconnect automatically after disconnection.

7. Click on <<Connect>> after you have defined all the required settings.

   You can measure the communication speed if there is an active connection 🕒 .
   What is measured is the time from which a request is transmitted into the target SMART CONNECT KNX Remote Access network until a response is received from the SMART CONNECT KNX Remote Access.

You will find detailed connection information in the logbook 📄.

You can use the <<Disconnect>> button or close the client to disconnect an active connection.

2.5.3 Remote access options

Remote access via KNX/IP

All KNX/TP tunnelling servers and discovered KNX/IP devices in the remote network will appear in the ETS Connection Manager if remote access is gained via KNX/IP.

Label the discovered KNX/IP devices with a prefix such as RA- to avoid mixing them up with other devices in your own network.

Remote access via TCP

If you wish to gain access via a Remote Desktop on a PC, for example, go to the gear icon and enter the IP adress or DNS name (hostname) of the target computer in the remote network. It is highly likely that the TCP port in the remote network (standard port RDP 3389) on your PC is already assigned. In this case, you need to use another free local TCP port as the standard RDP port. Recommended are ports 40000 and above.

If you have chosen another port as the standard RDP port for the local TCP port, make the entry for the remote desktop connection as follows:

Example: 127.0.0.1:40000

Gira HomeServer remote configuration

Enter either the HomeServer's IP address or the HomeServer's local DNS name on the remote network for remote access to the Gira HomeServer.

You can use the specified default values for the Gira experts. Click on the gear icon if you would like to change the port specifications anyway. Ports lower than 1023 have usually been assigned and are not recommended.

Gira HomeServer Version 4.7.0 and above uses Port 443.

> As soon as connection has been established via my.ise, you can transfer the project to the HomeServer. To do so, launch the Gira Expert and select the <<Other address>> option in the <<Transfer project>> dialogue. Enter the IP address 127.0.0.1 and the configured port.

You can use the specified default values in the case of an Eiblib/IP protocol.

> Add an <<Eiblib/IP>> connection in the ETS and assign 127.0.0.1 as the server address and the configured local ports.

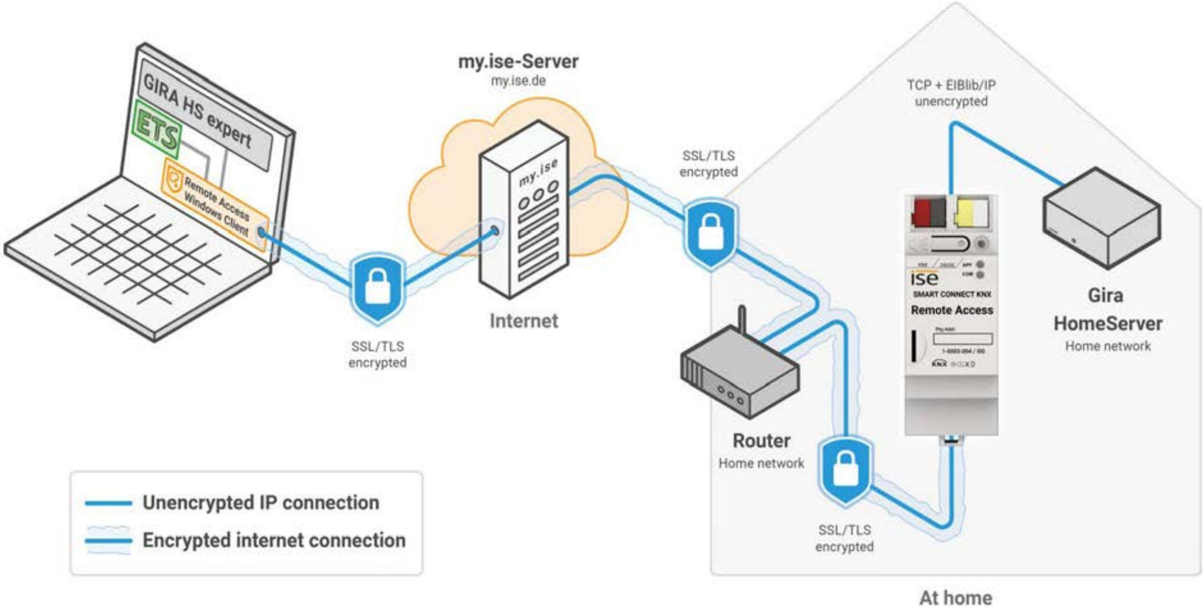


Figure 8: Secure Gira HomeServer configuration via remote access

3 Important notes

3.1 General safety instructions

Warning

Danger from incorrect use

Incorrect use can result in damage to the device, fire or other dangers.

- Only qualified electricians may install and mount electrical devices.
- Follow the instructions in this product manual.
- This product manual is part of the product and must remain with the customer.

3.2 Storage and transport

Store the device in its original packaging. The original packaging provides optimum protection during transport. Store the device in a temperature range of -25 °C to +70 °C.

3.3 Cleaning and maintenance

The SMART CONNECT KNX Remote Access is maintenance-free.

If necessary, clean the device with a dry cloth.

Important

Device damage due to improper opening

- Never open the housing.
- If you suspect that the device is damaged, contact our support team.
- We provide a warranty in accordance with statutory requirements.
- Send the device back to us postage free with a detailed error description only if our support team asks you to.

4 Technical data

Power supply and connections	
Rated voltage:	DC 24 to 30 V Supply via external DC
Power consumption:	2 W
Connections:	• KNX: Bus connection terminal (black/red) • External power supply: Power supply terminal (white / yellow) • IP: 2x RJ45 (integrated switch)
microSD card slot	microSD cards up to 1 TB (SDXC)

Ambient conditions	
Installation environment temperature:	0 °C to +45 °C

Device dimensions	
Installation width:	36 mm (2 HP)
Installation height:	90 mm
Installation depth:	74 mm (DRA Plus)

KNX SPECIALIST	
Communication:	KNX: KNX/TP
Installation method:	S-mode
Medium:	TP1-256

IP	
Communication:	Ethernet 10/100 BaseT (10/100 Mbit/s)

Approvals and protection type	
Approvals / certifications:	CE, KNX
Protection type:	IP20 (compliant with EN 60529)
Protection class:	III (compliant with IEC 61140)

Supported web browsers
Current versions of Mozilla Firefox, Microsoft Edge, Apple Safari and Google Chrome.

5 Device design

Stated directions always relate to the device in its installed position.

5.1 Front

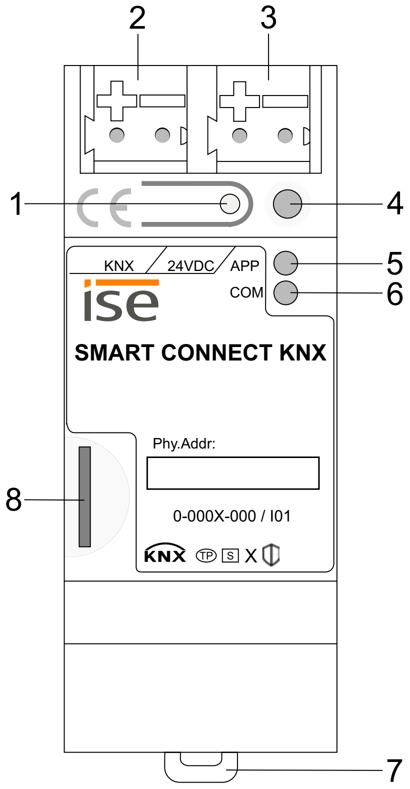
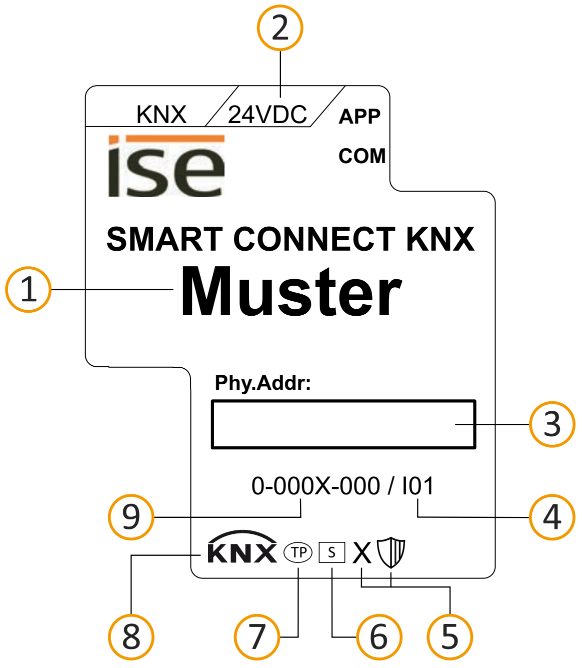


Figure 9: Front

No.	Description	
1	Button:	Programming button
2	Connection:	KNX/TP
3	Connection:	External power supply
4	LED:	"Programming" (red)
5	LED:	“APP”: Operation indication (green)
6	LED:	“COM”: Communication KNX/TP (yellow)
7	Holding device:	Release lever for top-hat rail terminal
8	Connection:	microSD card slot Use of microSD cards up to 1 TB (SDXC)

5.2 Data on device sticker

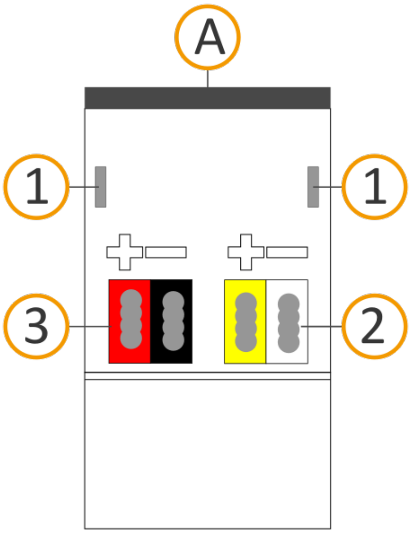


No.	Description
1	Product name
2	Rated voltage
3	Individual address: Enter the assigned individual address in the field with a permanent marker.
4	Index
5	KNX Secure
6	Installation method, here "S-mode"
7	Transfer medium, here "TP"
8	KNX certification
9	Order number

Figure 10: Device sticker

5.3 Top

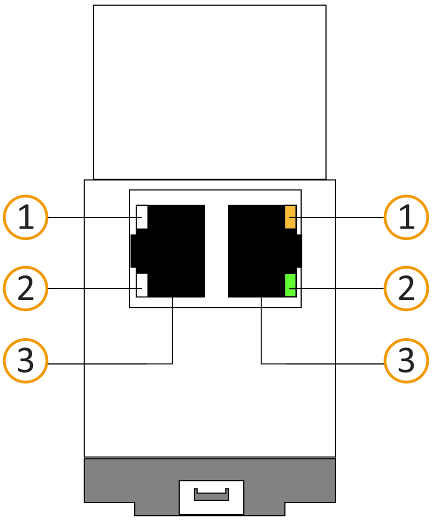
The openings for securing the cover cap are located on the top of the device.



No. / Index	Description
1	Opening for securing the cover cap
2	Attached power connection terminal
3	Attached bus connection terminal
A	Back of device

Figure 11: Top of device

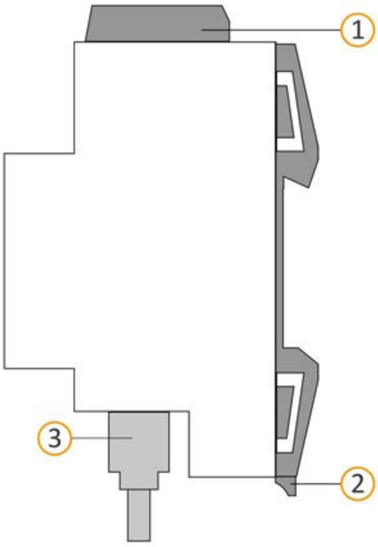
5.4 Underside



No.	Description
1	"Communication" LED
2	"Connection speed" LED
3	IP: 2x RJ45 (integrated switch)

Figure 12: Network connections

5.5 Device side



No.	Description
1	Attached cover cap
2	Release lever for top-hat rail terminal
3	RJ45 cable (not included in the scope of supply) connected to RJ45 socket.

Figure 13: Device side

6 Installation

6.1 Scope of supply

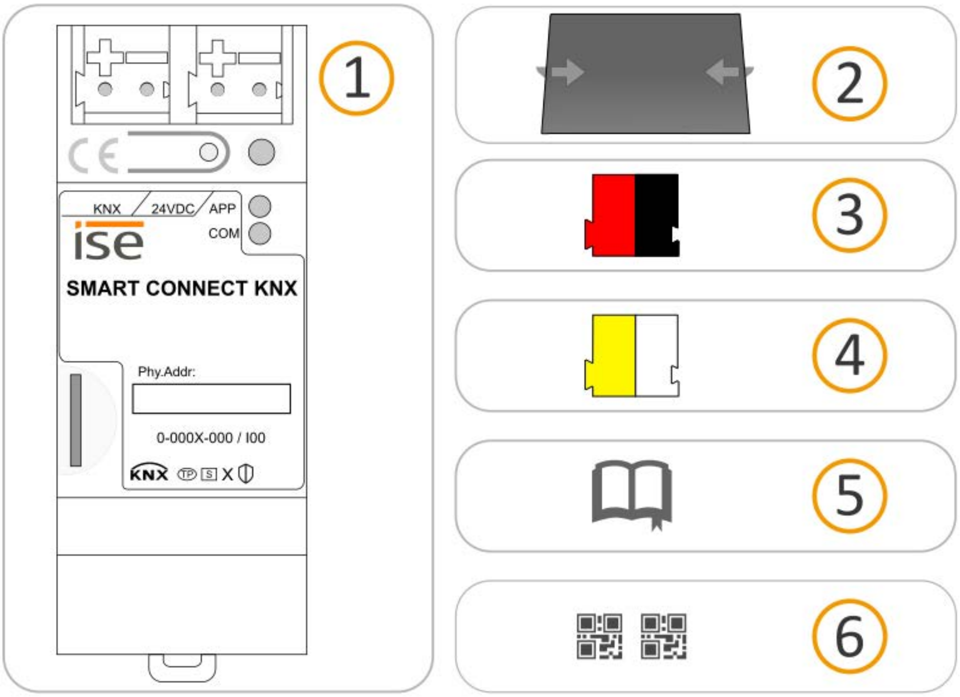


Figure 14: Scope of supply

No.	Objects supplied	Explanation
1	Device	SMART CONNECT KNX Remote Access
2	Cover cap	To protect connections from dangerous voltages.
3	Bus connection terminal	To connect the KNX/TP bus lines.
4	Power connection terminal	To connect the external power supply.
5	Installation instructions	This product manual also provides you with the information from the installation instructions but with additional details, application examples and configuration instructions.
6	Sticker set	Additional set of stickers with data for KNX Secure, initial device password and registration ID. The same stickers are attached to the side of the device.

The installation instructions are part of the product.
Give these instructions to your customer.

6.2 Checking the installation conditions

Before starting with the mounting process, check that the requirements for the planned installation environment have been met.

Important

Device functional fault due to incorrect ambient temperature in the installation environment

- Pay attention to the temperature of the installation environment: min. 0 °C to max. +45 °C.
- Do the not mount the SMART CONNECT KNX Remote Access above heat-emitting devices.
- Ensure that there is sufficient ventilation/cooling.

Pay attention to the device depth (see figure 15, item 1): DRA Plus, 74 mm.

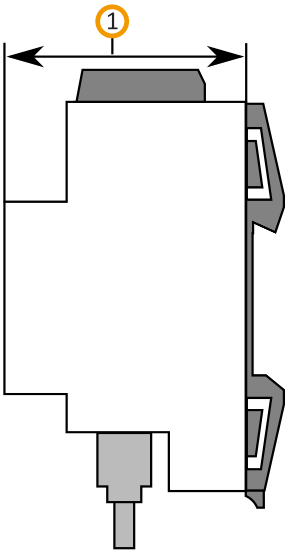


Figure 15: Device depth

6.3 Mounting the device

Only qualified electricians may assemble and install the SMART CONNECT KNX Remote Access. Specialist knowledge of the installation regulations is a prerequisite.

Warning

Danger from incorrect use

Incorrect use can result in damage to the device, fire or other dangers.

- Only qualified electricians may install and mount electrical devices.
- Follow the instructions in this product manual.
- This product manual is part of the product and must remain with the customer.

Warning

Danger of electric shock

An electric shock can result from touching live parts in the installation environment.
Electric shock can cause death.
Pay attention to the installation regulations:

- Route the KNX/TP bus line with the sheathing intact until it is close to the bus connection terminal.
- Firmly press the bus KNX/TP bus line into the bus connection terminal as far as it will go.
- Install bus line leads without sheathing (SELV) reliably disconnected from all non-safety low-voltage cables (SELV/PELV).
- Maintain the specified clearance.
- Attach the cover cap supplied.
- For more information see also the VDE regulations governing SELV (DIN VDE 0100-410/"Safe separation", KNX installation regulation).

Mounting and connecting the device

1. Snap the device vertically onto the top-hat rail (installation position: network connections at bottom).

2. Connect the KNX/TP bus line (referred to below as the bus line) to the KNX connection of the device (see figure 16, item 1) by means of the supplied bus connection terminal (see figure 16, item 2). Polarity: left/red: “+”, right/black:

   a. Attach the bus connection terminal (see figure 16, item 2).

   b. Route the bus line with the sheathing intact until it is close to the bus connection terminal.

   c. Firmly press the bus line into the bus connection terminal as far as possible.

   d. Route the bus line to the back.

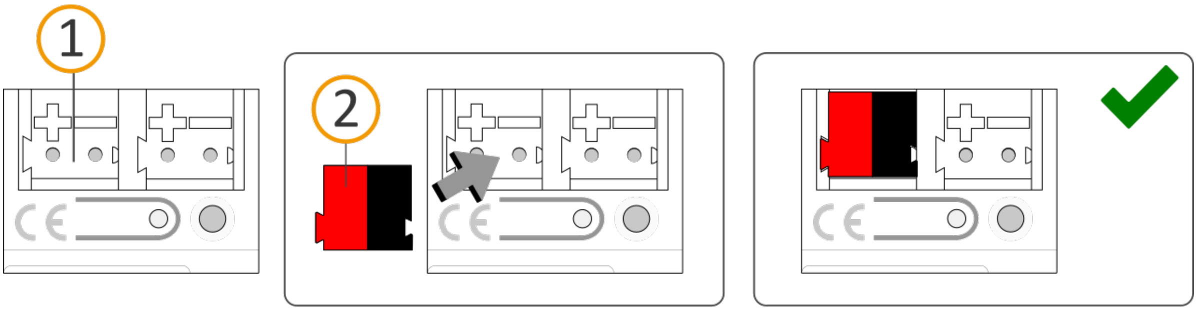


Figure 16: Connect the bus line

3. Connect the external power supply to the power supply terminal (see figure 17, item 1) by means of the supplied power connection terminal (see figure 17, item 2).
   Polarity: left/yellow: “+”, right/white: “–”.

   a. Attach the power connection terminal (see figure 17, item 2).

   b. Route the power line with the sheathing intact until it is close to the power connection terminal.

   c. Firmly press the power line into the power connection terminal as far as possible.

   d. Route the power supply line to the back.

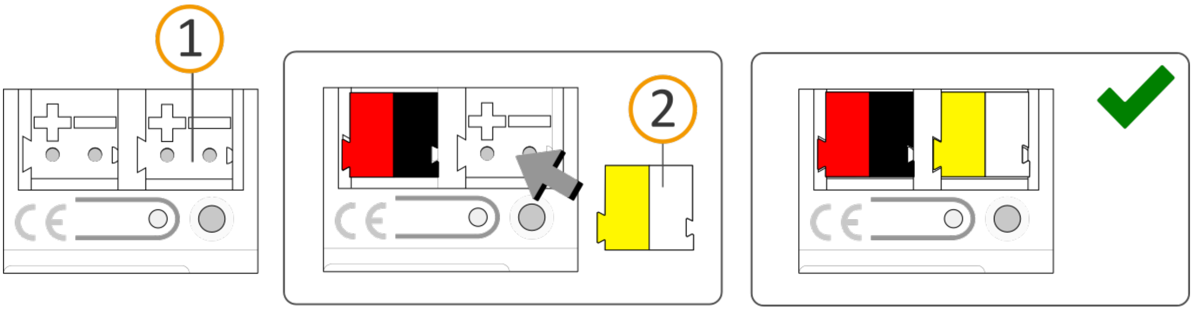


Figure 17: Connect the power supply

Important

Functional fault in all devices due to incorrectly dimensioned power supply

The following applies if you use the non-choked auxiliary supply output of a KNX power supply as an additional power supply:
The operating currents of all KNX/TP devices on the line section must not exceed the rated current of the power supply.

4. Attach the cover cap supplied:

   a. Route all cables to the back. The openings for fastening the cover cap (see figure 18, item 1) must be clear. All cables must be between the openings.

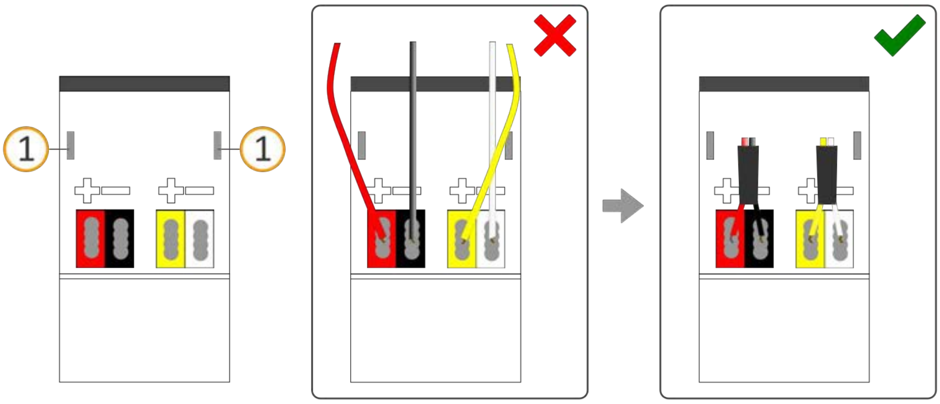


Figure 18: Cable routing

   b. Attach the cover cap over the connection terminals.

   c. Press the cover cap together gently.

   d. Insert the cover cap’s fastening claws into the openings until you feel the cover cap engage.

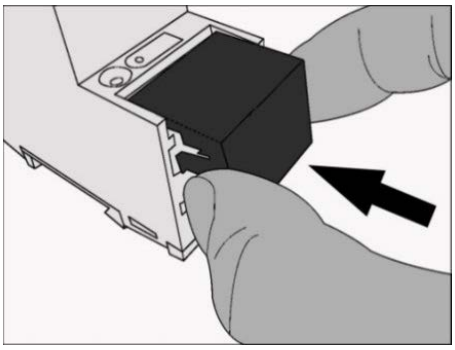


Figure 19: Attaching the cover cap

5. Connect the network:

   a. Make sure that your network infrastructure (router, DNS server) is in operation.

   b. The network connections are on the underside of the device.

   c. Connect the IP network cable (RJ45 cable) to one of the device's network connections (RJ45 socket).

The RJ45 sockets are the same. The free RJ45 socket can be used to connect another IP device.

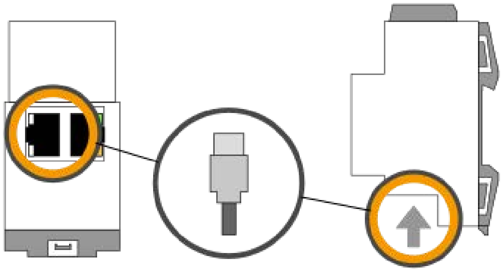


Figure 20: Connect the IP network cable

7 Device website

You can access the SMART CONNECT KNX Remote Access via the device website.
The device website is run on your installed browser. You do not require any additional software. As soon as the device is available you can access the device website via the IP.

An overview of the functions can be found in ▶ table 4 on p. 27.

7.1 Accessing the device website

Call up the device website by actioning one of the following:

- Enter the device's IP address in the address bar of your browser.
- Alternatively, select the device in the network environment category <<Other devices>> (see figure 21, item 1): Double click on the device icon (see figure 21, item 2).

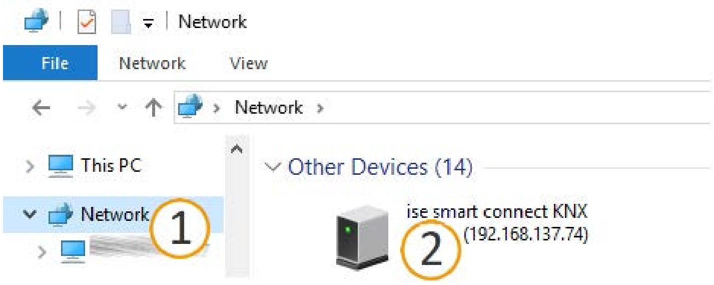
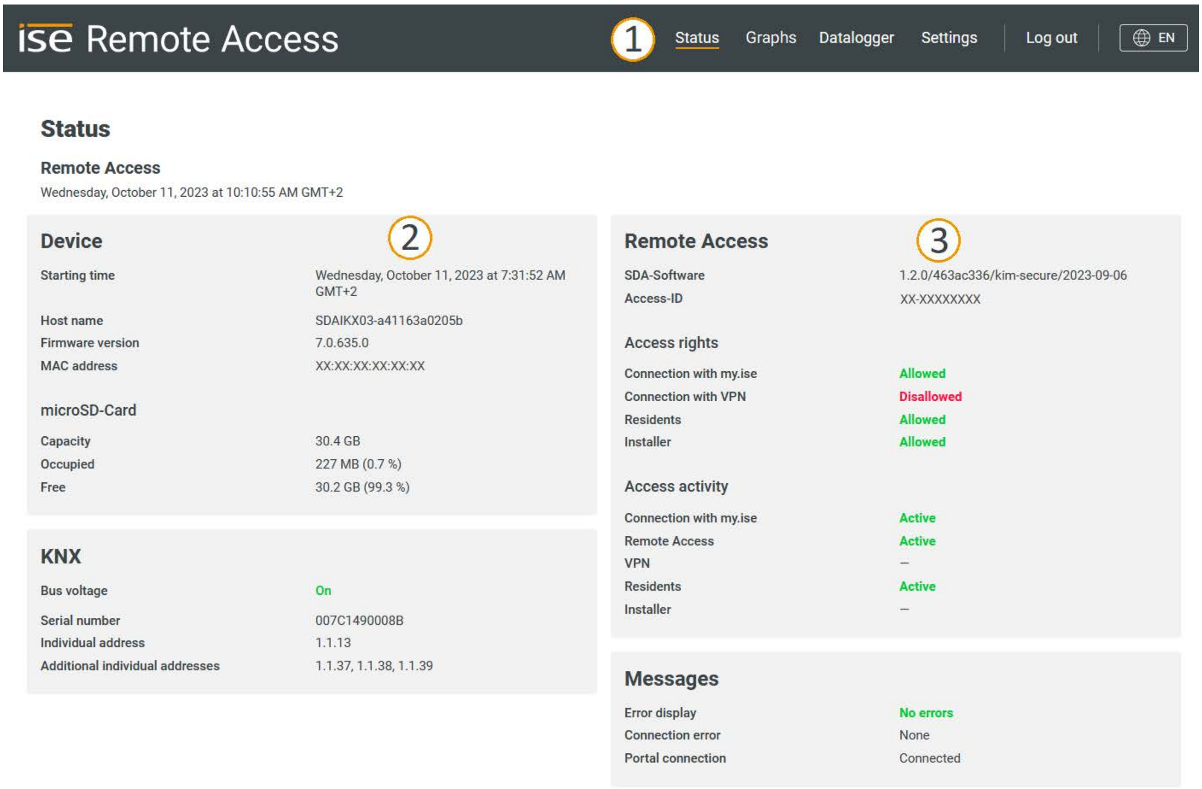


Figure 21: Accessing the device website via the network environment

The device website is password protected. The registration ID is also used as an initial password after a factory reset. You can change the password in <<Settings>> after successful login.

7.2 Getting to know the interface of the device website



Status

Remote Access
Wednesday, October 11, 2023 at 10:10:55 AM GMT+2

Device

Starting time	Wednesday, October 11, 2023 at 7:31:52 AM GMT+2
Host name	SDAIKX03-a41163a0205b
Firmware version	7.0.635.0
MAC address	XX:XX:XX:XX:XX:XX

microSD-Card

Capacity	30.4 GB
Occupied	227 MB (0.7 %)
Free	30.2 GB (99.3 %)

KNX

Bus voltage	On
Serial number	007C1490008B
Individual address	1.1.13
Additional individual addresses	1.1.37, 1.1.38, 1.1.39

Remote Access

SDA-Software	1.2.0/463ac336/kim-secure/2023-09-06
Access-ID	XX-XXXXXXXX

Access rights

Connection with my.ise	Allowed
Connection with VPN	Disallowed
Residents	Allowed
Installer	Allowed

Access activity

Connection with my.ise	Active
Remote Access	Active
VPN	–
Residents	Active
Installer	–

Messages

Error display	No errors
Connection error	None
Portal connection	Connected

Figure 22: Device website homepage/status page

Item	Element	Function
1	Menu bar	Call up other pages or run functions.
2	Page	The <<Status>> page is shown.
3	Information	Display of specific information.

Menu	Description
Status	Information: • System information • System configuration • Application information
Graphs	Showing the recorded data in graphs ▶ Parameters – graphs, p.50
Data logger	Access to the data logger archive and download of data logger files ▶ Parameter – data logger, p.55
Settings	Functions: • ▶ Download of log files, p. 75 • Change password • Restart device • ▶ Reset to factory settings, p. 39 • Switch device to programming mode • ▶ Change logging mode, p. 75 • ▶ Configure network settings, p. 39 • ▶ Update firmware, p. 41
Log out	Logging out from the device website
Language selection	Select one of the following languages: • German • English • Dutch • Spanish • French • Italian

Table 4: Overview

ℹ After a restart of the SMART CONNECT KNX Remote Access, the connection status to the my.ise server may show incorrect values for a short time. The web page will not be updated automatically. Use the refresh function in your browser to do so.

8 Commissioning and configuration

After installing the device and connecting the bus, power supply and network, the device can be commissioned.

8.1 Quick start

If you are already familiar with KNX and how to install KNX gateways, you can use this quick start to set up the SMART CONNECT KNX Remote Access for the first time.

Logging onto my.ise

1. Register on my.ise https://my.ise.de.
2. Click on <<Add device>>.
3. Enter registration ID (see enclosed sticker).
4. Add name and description for easier identification.

Downloading the Remote Access Windows Client

Not in the same network as the SMART CONNECT KNX Remote Access?
Use the Remote Access Windows Client:

5. Access product page and scroll to the download section.
6. Download suitable Remote Access Windows Client for Windows (x86) or (x64).
7. Execute installation file to run on the same computer as the ETS.

Connecting device via the Remote Access Windows Client

8. Start up Remote Access Windows Client in Windows start menu.
9. Log on with the same user data as for my.ise.
10. Select the SMART CONNECT KNX Remote Access in the selection list and connect.

Incorporating the device into ETS

11. Click on the <<Bus>> tab in the ETS.
12. Enter individual address. Individual address on delivery: 15.15.255.
13. Test input by clicking on <<Test>>.

8.2 Reading off the device status using the LEDs

The following status indicators (LEDs) can be found on the front panel.

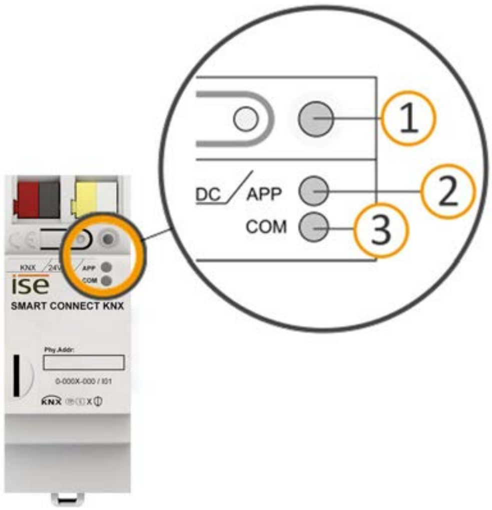


Figure 23: Status indicators (LEDs) on the front of the device

No.	Element	Description
1	"Programming" LED (red)	Programming mode active/inactive display
2	LED "APP" (green)	Serves as a status indicator for the application
3	LED "COM" (yellow)	KNX/TP communication traffic display

Table 5: Status indicators

The "Programming" LED shows independently of the operating mode whether the device is in programming mode or not.

Colour	Description
🔴 (Red, continuously on)	Programming mode is active. ▶ Assign individual address, S. 37
○ (off)	Programming mode is deactivated.

Table 6: Status of the device – Programming mode

The status indicators for the network are on the underside of the device.

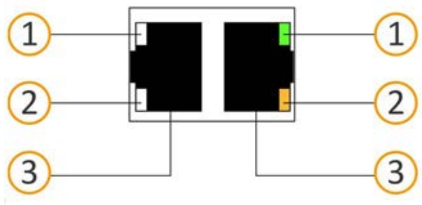


Figure 24: Network LEDs

No.	Element	Description
1	"Connection speed" LED	• LED lights up green: 100 Mbit/s • LED is off: 10 Mbit/s (There is no connection if LED 2 also off. Check whether the cable is correctly connected.)
2	"Communication" LED	• LED lights up yellow-orange: Connected but currently no telegram traffic • LED flashes yellow-orange: Telegram traffic
3	IP connection	2x RJ45 (integrated switch)

Table 7: Device status – network

8.2.1 LEDs during device start-up

The "APP" and "COM" LEDs have different meanings depending on the phase in the operating mode. After the power supply is switched on or after power returns, the device indicates its status using the following LED combinations:

APP	COM	Description
Correct operation		
○ (off)	🟡 (yellow)	Device starting up.
🟢 (green)	🟡 (yellow)	Device booted up and ready for operation.
Error		
○ (off)	○ (off)	No power supply. • Check the connections and the power supply.
○ . 🟢 . ○ . 🟢 . ○ . 🟢 (off).(green).(off).(green).(off).(green) Rapid flashing	○ (off)	The firmware cannot be started. • Contact support team.
○ ... 🟢 ... ○ ...🟢 ... 🟡 ... ○ ... 🟡 ...○ ... (off)...(green)...(off)...(green)... (yellow)...(off)...(yellow)...(off)... LED "APP" and "COM": Slow flashing (about 1 Hz) in an alternating pattern		The newly loaded firmware cannot be started. The system is trying to activate the previous firmware (invalid firmware). • Contact support team.

Table 8: Device status – device starting up

8.2.2 LEDs in operation

LED status after successful device start-up:

APP	Description
🟢 (green)	The device is working perfectly (normal operation). In general, the connection to my.ise is allowed (group object 1). The device connects to the my.ise server but remote access is not active. Redirects are possible.
○ (off)	The device is currently starting up or is out of operation. • Wait until the device start-up process is complete. • If the device is still out of operation, check the connections and the power supply.
🟢 ... ○ A slow flash (about 1 Hz), then 2 s pause	The connection with my.ise is deactivated via the group object 1. The device does not connect to the my.ise server. Remote access is not possible due to technical reasons.
🟢 ... ○ ... 🟢 ... ○ ... 🟢 ... ○ (green).(off).(green).(off).(green).(off) Three slow flashes (about 1 Hz), then 2 s pause	Remote access is allowed for at least one access group and there is at least one active connection.

Table 9: "APP" LED in operation

COM	Description
🟡 (yellow)	The KNX connection has been established. No KNX telegram traffic. The LED is also deemed to be continuously on if brief irregular interruptions occur.
○ . 🟡 . ○ . 🟡 . ○ . 🟡 (off).(yellow).(off).(yellow).(off).(yellow). Rapid flashing	KNX connection has been established. KNX telegram traffic.
Error	
○ (off)	Connection to KNX is interrupted. • Check whether the KNX and voltage connections are mixed up. • Check the bus connection. • Check whether the power supply is correctly connected.

Table 10: "COM" LED in operation

8.3 Configuration

The device is configured in the ETS (Engineering Tool Software). The ETS is available with a different range of functions from the KNX Association (www.knx.org).

All descriptions in this documentation on configuration in the ETS refer to the ETS Professional version 6.

Help on the ETS is available in the integrated ETS Online Help.
Press the [F1] button.

Note:
The SMART CONNECT KNX Remote Access is configured as follows when delivered and after a factory reset:

- Remote access is activated for the Residents and Installers access groups and for Quick Connect.
- The individual address for the device is 15.15.255. The address for the three other three individual interfaces (tunnelling server) is 15.15.254.

Work steps

1. Add the SMART CONNECT KNX Remote Access as a device in the ETS, ▶ see Creating the device in the ETS, p. 34.
2. Assign an individual address to the device in the ETS and up to three individual interface addresses in accordance with the KNX topology.
3. Select the option <<Receive IP address automatically>> or select <<Use a permanent IP address>> and complete the following fields: IP address, IP subnet mask and standard gateway address, ▶ see Setting the IP address, IP subnet mask and standard gateway address, p. 36.
4. Set the general parameters, ▶ see Parametrisation, p. 47.
5. Link the group addresses to the group objects.
6. The SMART CONNECT KNX Remote Access is now ready for commissioning using << Program ETS>> and for functions testing.

Note:

We recommend downloading via the direct IP connection due to the significantly shorter transfer times. In the ETS main toolbar, select the icon <<Bus interface>> → the cogwheel for settings next to <<Automatic>> → <<Direct IP connection if supported by target device>>.

8.3.1 Creating the device in the ETS

Depending on whether the product database entry already exists in the ETS catalogue or whether the device is already being used in your existing project, different work steps are required in order to use the current version.

Work steps	
Device already exists in the ETS catalogue?	
Yes	No
Update product database. During an update, the old product database entry is replaced by the new one.	Importing product database entry. There are numerous possibilities for importing a new product database entry. Below we will assume that you have downloaded the product database entry yourself. ▶ see Importing a new product database entry, p. 34.
Device in existing project should be updated?	
Yes	No
You must update the device properly so that the existing links to group addresses are maintained. ▶ see Update the product in the existing project (only product database v7.2), p. 35.	Add the device to your topology in the usual way.

Table 11: Work steps – creating the device in the ETS

Importing a new product database entry

Requirement: You have now downloaded the product database entry (product file) from our website at www.ise.de.

1. Start the ETS and select the <<Catalog>> panel in your project.
2. Select the <<Import>> button in the toolbar.
3. In the <<Open product file>> window, open the product file and press on the <<Open>> button to confirm your selection.
4. Follow the further instructions in the ETS. If necessary, call up the Online Help with the [F1] button.

Update the product in the existing project (only product database v7.2)

Requirement: Importing a new product database entry, p. 34

1. In the ETS, open the project for which the device is to be updated.
2. Open the <<ETS apps>> tab in the ETS settings.
3. Download the ise Service App under <<ETS App Store>> and install it.
4. Licence the app. **Instructions for app licencing** can be found at https://support.knx.org.
5. Use the service app for product updates.

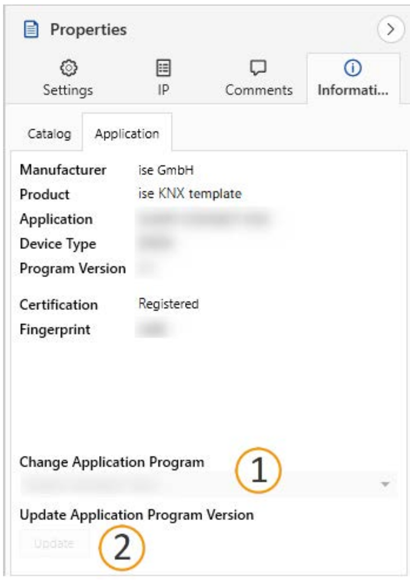
Updating a product in the existing project

Requirement: New product database entry exists in the catalogue.

1. In the ETS, open the project for which the device is to be updated.
2. Search for the new product database entry in the catalogue and add the new version of the device to the devices in your project.
3. Select the old version of the device in your topology.
4. Under <<Properties>>, select the <<Information>> → <<Application>> tab.
5. Select the <<Update>> button under the item <<Update Application Program Version>> (see figure 25, item 2).

> If you change the value under <<Change Application Program>> (see figure 25, item 1), user-defined settings such as links to group addresses will be lost.

6. Select the newly added device and delete it again from your topology.



Manufacturer	ise GmbH
Product	ise KNX template
Application	[redacted]
Device Type	[redacted]
Program Version	[redacted]
Certification	Registered
Fingerprint	[redacted]

Change Application Program

Update Application Program Version

Figure 25: Updating the application program

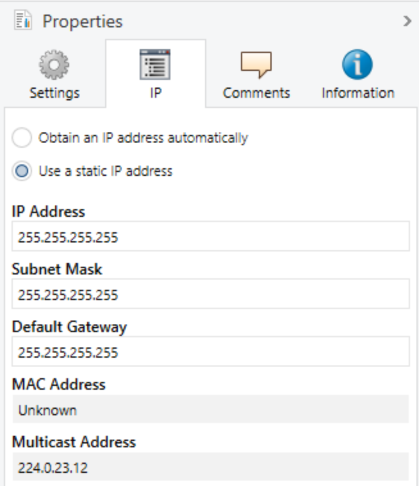
8.3.2 IP settings

Besides the individual address in the KNX network, an IP address, the subnet mask and the address of the standard gateway in the IP data network must be assigned to the SMART CONNECT KNX Remote Access.

You can enter the settings manually in the ETS or receive them automatically (obtain the data from a DHCP server, e.g. integrated in the router of the data network).

Setting the IP address, IP subnet mask and standard gateway address

1. In the ETS, select the device in your topology.
2. Under <<Properties>> select the <<IP>> tab.
3. You will find the available selection options in figure 26 and Table 12 “Settings for manual IP address entry or for receiving automatically”, p. 36.



○ Obtain an IP address automatically

● Use a static IP address

IP Address: 255.255.255.255

Subnet Mask: 255.255.255.255

Default Gateway: 255.255.255.255

MAC Address: Unknown

Multicast Address: 224.0.23.12

Figure 26: IP settings

Setting	Description
Receive IP address automatically	The address data are automatically obtained from a DHCP server on the data network. The DHCP server must assign a valid IP address to the SMART CONNECT KNX Remote Access. ℹ If there is no DHCP server available, the device starts up after a waiting time with an automatic IP address in the address range of 169.254.1.0 to 169.254.254.255. As soon as a DHCP server is available, the device is automatically assigned a new IP address.
Use a permanent IP address	Enter the data manually You can obtain the permitted IP address range and the subnet mask and standard gateway from the router configuration interface.

Table 12: Settings for manual IP address entry or for receiving automatically

Serious misconfiguration

Default values are set if you want to use the setting <<Use static IP address>> but then forget to fill in the appropriate fields. Devices with the default value 127.001 as fixed IP address will not start up properly.
Reset the device to its factory settings. ► Resetting to factory settings, p. 39.
If problems should persist, contact Support.

8.3.3 Programming an individual address

The individual address that you issued in the ETS must be assigned to the device. We refer here to "programming". To do this you must put the device into programming mode.

Assigning an individual address

Requirements: Device and bus voltage switched on. Programming LED is off.

1. Briefly press the programming button (see figure 27, item 1). Alternatively, you can also press the programming button on the device website. The programming LED (see figure 27, item 2) lights up red.

2. In the ETS, assign the individual address to the device in accordance with the KNX topology and execute programming in the ETS.

3. On the device, enter the assigned individual address with a permanent marker in the field <<Phy.Addr.>>.

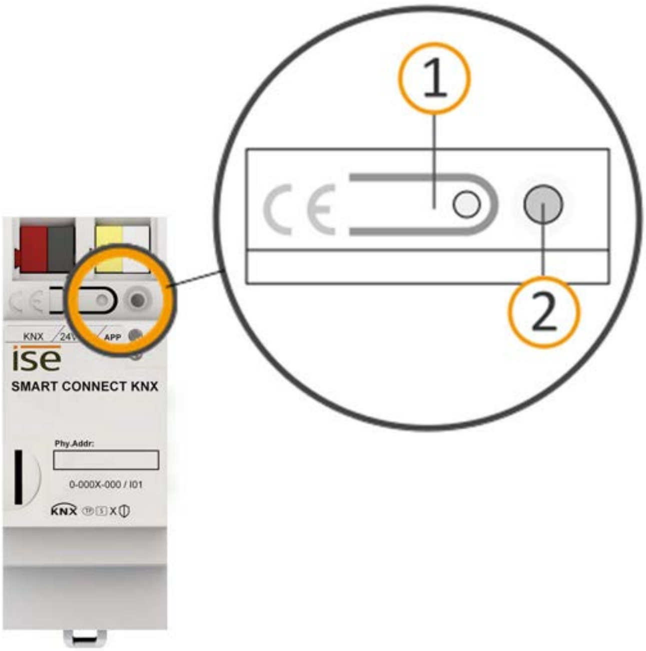


Figure 27: Programming

Recognising successful assignment of the individual address:

- Device: The programming LED on the device is off.
- ETS: The completed transfer is indicated on the <<History>> tab by a green marking. Programming flag <<Adr>> is set and <<Cfg>> is not set. More information about this and other flags is available from the ETS documentation.

After the IP address is assigned, you can also conveniently set the device to programming mode on the device website instead of pressing the programming button on the device itself.

Tunnelling server

The SMART CONNECT KNX Remote Access has access to three tunnelling servers (KNX/IP - interfaces). These interfaces can also be used for downloading and in the group and bus monitor modes. An individual address must be assigned to each tunnelling server in the <<Properties>> tab in the ETS. If you do not require all three interfaces, you can also enable addresses using the <<Park>> function.

8.3.4 Network settings via the device website

Requirement: The device website is open.

1. Select <<Settings>> in the menu bar.
2. In the <<Network>> area, select the ⚙ button under <<IPv4 settings>>.
   The network settings dialogue will open.
3. In the input field <<DNS address>>, enter the IP address of your DNS server.
4. Click on <<Save>> below the input field. The system accepts the configuration.

> If you program the device from the ETS or select <<Reset device>> for the device, the DNS server will be reset to the standard gateway. You will then need to re-configure the DNS server on the device website.

8.3.5 Resetting to factory settings

When you reset the device to the factory settings, it behaves as if it were in the state of delivery. The device is then unconfigured:

- The device remains in the existing projects.
- The device's registration remains unchanged.
- The device keeps the version of the application program in the ETS.
- The entire parametrisation is rejected.
- The IP settings are reset.
- The device website password is reset to the initial password.
- The device now has the following as the individual address once more: 15.15.255.

> The green app LED lights up green after the factory reset.
> ► See Table 8 “Device status – device starting up”, p. 31.

You have the following possibilities for resetting the device to the factory settings:

- Manual: Press the programming button on the device in a particular sequence.
- Automated: You select the <<Reset device>> function on the device website.

⚠ **Warning**

Danger of electric shock
An electric shock can result from touching live parts in the installation environment. Electric shock can cause death.
Pay attention to the installation regulations:

- Route the bus line with the sheathing intact until it is close to the bus connection terminal.
- Firmly press the bus line into the bus connection terminal as far as possible.
- Install bus line leads without sheathing (SELV) reliably disconnected from all non-safety low-voltage cables (SELV/PELV).
- Maintain the specified clearance.
- Attach the cover cap supplied.
- Also see also the VDE regulations governing SELV (DIN VDE 0100-410/"Safe separation", KNX installation regulation) for more information.

Manually resetting the device to the factory settings

Requirement: The device must be switch off without voltage.

1. Press the programming button (see figure 27, item 1) and keep it pressed while you attach the power connection terminal.
2. Do not release the programming button until the following LEDs are all flashing slowly at the same time:
   - Programming LED (see figure 23, item 1)
   - APP LED (see figure 23, item 2)
   - COM LED (see figure 23, item 3)

   Usual duration: approx. 30 seconds.
3. Release the programming button briefly.
4. Press the programming button again and keep it pressed until following LEDs are all flashing rapidly at the same time:
   - Programming LED (see figure 23, item 1)
   - APP LED (see figure 23, item 2)
   - COM LED (see figure 23, item 3)
5. Release the programming button.

The device is reset to the factory settings. You do not have to restart the device.

Resetting the device to the factory settings via the device website

1. Open the device website ▶ see Accessing the device website, p. 25.
2. On the <<Settings>> page, select the <<Reset device>> button.
3. Confirm the confirmation prompt.

As soon as the device has been completely reset to the factory settings, the login opens.
To log in, you need to enter the Initial Device Password. You do not need to restart the device.

8.4 Updating firmware

You can obtain functional enhancements for the SMART CONNECT KNX Remote Access with a new version of the firmware. The current firmware and corresponding product manual are available on our website at www.ise.de.

So that you can use the new functions, it is necessary for the versions of the firmware being used and the product database entry are compatible.

8.4.1 Updating the firmware via the device website

You can only import a firmware version that is newer than the current version on the device. Previous versions cannot be imported.

There are two ways to update:

- Online: Import firmware online.
- Offline: Import firmware offline. For devices without Internet connection in the installation environment.

Import firmware online

1. Open the device website.
2. Select <<Settings>> in the menu bar.
   You will see the currently installed firmware version in the <<Firmware>> area. If a new firmware version is available for the device it will be indicated to you.
3. Click on the <<Start update>> button.

Import firmware offline

Requirement: You have downloaded the current firmware version from the www.ise.de website.

1. Open the device website.
2. Select <<Settings>> in the menu bar.
3. In the <<Firmware>> area, select the button <<Choose firmware-file>>.
4. In Explorer, select the desired firmware file and confirm your selection with the <<Open>> button.
5. Start the firmware installation by clicking <<Perform update>>.

If the new firmware is incompatible with the configuration of the previous firmware, a corresponding message is displayed. There is a distinction between the following cases here:

- The new version provides new functions. After the update, the device functions with the same range of functions as before. New functions cannot be used until an ETS download of a newer product database entry is made.
- The new version is completely incompatible with parametrisation in the version currently being used. An ETS download is absolutely necessary. We recommend unloading the ETS application program before the update and configuring the device with a new product database entry after the update.

If an incompatibility arises, the update must be confirmed again for security reasons.

8.4.2 Compatibility between product database entry and firmware version

To ensure you can use the device’s new functions, the firmware version used must be compatible with the version of the device's application program in the project. The application program is part of the product database entry.

The application program version can be found in the ETS under <<Properties>> in the <<Information>> tab ➔ <<Application>> under <<Program version>>.

Compatibility at a glance

The versions are fully compatible if the main version of the application program and the firmware are identical.

The version numbers are structured according to the following scheme: <Main version no.>.<Sub-version no.>

Example: Full compatibility with same main version numbers

- Firmware version: 2.3
- Application program version: 2.0

In order to use all new functions, it may be necessary to update the application program, ▶ see Update the product in the existing project (only product database v7.2), p. 35.

Incompatibility at a glance

If the new firmware has a higher main version number than the application program, there may be an incompatibility depending on the version. In the SMART CONNECT KNX Remote Access with firmware version 7, an application as of version 6.2 can be loaded.

Example: Incompatibility if the main version number of the firmware is higher

- Firmware version: 2.3
- Application program version: 1.3

Establishing compatibility

In case of incompatibility, you will need to uninstall the application program.

- The device remains in the existing projects.
- The device keeps the version of the application program in the ETS.
- The entire parametrisation is rejected.
- User data in the ETS is preserved.

Requirement: New product database entry exists in the catalogue.

1. In the ETS, open the project for which the device is to be updated.
2. Search for the new product database entry in the catalogue and add the new version of the device to your project.
3. Select the old version of the device in the topology for your project.
4. In the <<Topology>> window in the menu bar, select the <<Unload>> ➔ <<Unload application>> button.

   After uninstalling, the device behaves as in the state of delivery. The device is then unconfigured. Then start configuration as usual. ► see Configuration, p. 33.

5. Under <<Properties>>, select the <<Information>> ➔ <<Application>> tab.
6. Click on the <<Update>> button under the <<Update Application Program Version>>.
7. Select the newly added device and delete it again from your topology.

8.5 Firewall configuration

The SMART CONNECT KNX Remote Access communicates with my.ise via a HTTPS connection only. All data are exchanged via this connection in both directions, meaning that no additional configuration is required for the firewall.
If you wish to limit network access to specific domains and ports or IP addresses, we recommend configuring exceptions. You will find an overview with the remote access relevant domains, ports and IP addresses at https://my.ise.de.

8.6 Setting up VPN

You need an OpenVPN client to be able to access your home network via VPN.

Download the OpenVPN software at https://openvpn.net/community-downloads/ and install it on your PC. Compatibility between Version 2.6.6 and the SMART CONNECT KNX Remote Access’s VPN function has been assured.

If you intend to use VPN on your smartphone, download the OpenVPN Connect app from the Apple App Store or the Google Play Store and install it on your smartphone.

Prerequisite for setting up VPN

- A user account has been created at https://my.ise.de.
- The SMART CONNECT KNX Remote Access is connected to the Internet.
- The SMART CONNECT KNX Remote Access is registered on my.ise.
- A released version of the OpenVPN client was downloaded and installed on the PC or smartphone.

VPN setup

1. Log onto my.ise.
2. In the function overview, click on <<VPN access>>.
3. Select the access type and the volume of data traffic.
4. Wait until the configuration file has been created and then download the file.
5. Open the OpenVPN client and import the configuration file.
6. Enable the VPN connection in the OpenVPN client.

If you want to create the VPN access for several users, each user needs their own user account on my.ise. Repeat steps 4 to 6 for each user.

Test whether the established configuration works first before creating VPN access for additional users.

VPN settings on my.ise

Administrators can make the following settings under <<VPN access>>:

- Enable/disable VPN access.
- Enable VPN access for individual users.
- Change properties.
- Download VPN configuration file.
- Delete VPN access.

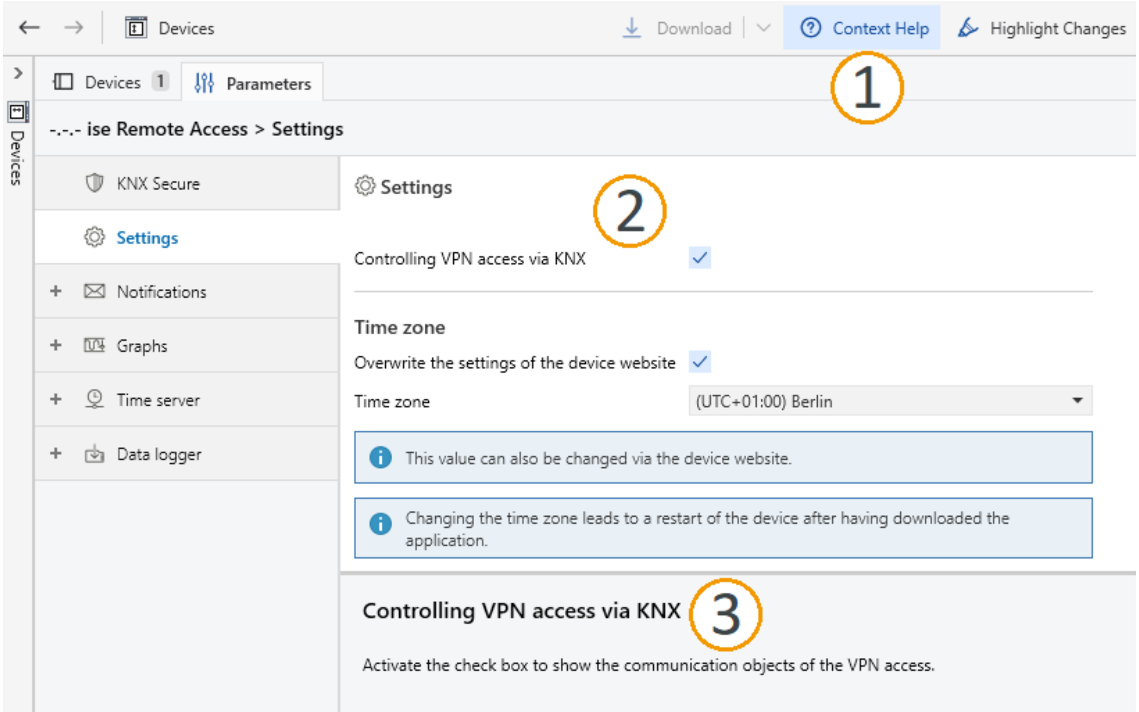
ℹ If you change properties under <<VPN access>>, the current configuration files will be invalid. For each user created, a new configuration file will be generated, which you must download and import into the OpenVPN client for the corresponding user.

9 Parametrisation

The parameters to be configured depend on your specific application. The context help in the ETS explains the parameters.

Calling up the context help in the ETS

1. Enable the <<Context help>> button in the <<Parameter>> tab in the toolbar.
2. Click on the desired parameter.
3. The corresponding explanation appears in the lower area of the parameter dialogue.



-.-.- ise Remote Access > Settings

Settings

Controlling VPN access via KNX ✓

Time zone

Overwrite the settings of the device website ✓

Time zone (UTC+01:00) Berlin

This value can also be changed via the device website.

Changing the time zone leads to a restart of the device after having downloaded the application.

Controlling VPN access via KNX

Activate the check box to show the communication objects of the VPN access.

Figure 28: ETS context help

9.1 Parameters – notifications

KNX group objects and system events such as the login/logout of a SMART CONNECT KNX Remote Access to/from my.ise can be used to generate notifications on my.ise. Besides static texts, they may also contain values from the KNX bus or even an attachment, such as a camera image. These notifications can be transmitted via push message (iOS and Android), email, phone or SMS.

In accordance with the selected number of notification objects, group objects and parameter pages are made available (notification 1 = group object 101, notification 2 = group object 102...).
The data types and properties are defined on the parameter pages.

To trigger a notification, a group address of the group object to be triggered must be linked to the group object of the notification.

Note:

Attachments containing notifications are limited to a data volume of 250 kB.
If they are larger, they are simply not sent. An error message is output on my.ise.

A notification has the following properties:

- Creation date
- Category
- Subject
- Contents
- Priority (low, high, alarm or system)
- Optional attachment, such as an IP camera image

Notification via KNX

The database entry contains 50 KNX group objects for receiving values from the KNX bus and generating notifications from them.

The following data types are supported:

- Boolean (1 bit)
- Counter (1 byte), e.g. number of open windows
- Percent (1 byte), e.g. brightness or blind position
- Floating point number (2 bytes), e.g. inside or outside temperature
- Text (14 bytes), e.g. alarm text

In addition to selection of the data type, filters such as limits or value ranges can be indicated to generate the required notifications.

The two text properties, "Subject" and "Text," can be comprised of static texts in which the value received from the KNX can be used for each placeholder.

A web address can also be specified for downloading an attachment from a web server (e.g. an IP camera) and attaching it to a message.

Suppressing notifications

If you do not wish to be notified of every change, you can specify a threshold value (as an absolute value). Notification of changes will then only be notified when this threshold value is exceeded.

9.2 Parameters – graphs

KNX group objects and the values transmitted by them can be used to generate graphs on the device website of the SMART CONNECT KNX Remote Access. For this, up to 200 records which are used for saving the transmitted values on the device are made available in the ETS.

Parameterising of the records

1. Open the <<Graphs>> tab and the <<Settings>> subtab in the ETS.
   In accordance with the selected number of records, group objects and parameter pages are made available (record 1 = group object 201, record 2 = group object 202...).
2. Go to the parameter page of a record.
3. Assign a self-explanatory name to find the record again in the group objects and on the device website.
4. Select a data point type. It must correspond to the data point type of the group object whose values are to be recorded.
5. Select a data type (unit). For a correct representation, the data type and its unit must correspond to the transmitted value.
6. Use the summary of the received values to improve the performance when loading the graphs.
   These parameters are not available for 1-bit objects.

Note:

If the ETS parameters of a recording are changed, all previous data for this recording will be deleted from the device when it is programmed again.

Generating records

Requirement: Devices with the corresponding group objects and the associated group addresses have already been created in the ETS project.

1. Select a group object that is to provide the values for the corresponding record.
2. Link the group address of the selected group object with the group object of the corresponding record.

After having programmed the device, the received values are recorded in the internal device memory.
The microSD card is not used for this.
On the device website, the records can be represented in graphs.

Note:

Always link the record only to one group address.
Otherwise there may be undesired representations in the graph.

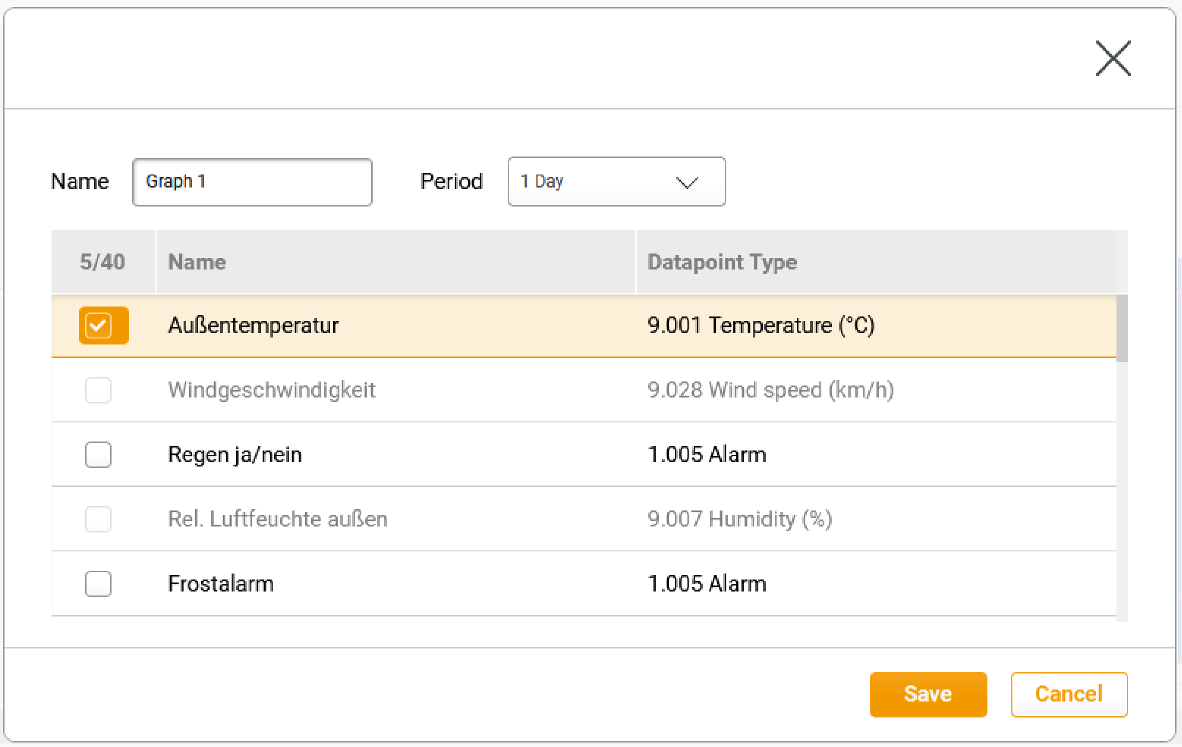
Storage of recordings

Recordings are stored in the device's ring buffer. Around 80 million individual data records can be stored on the device. If the remaining memory capacity falls below a certain level, the oldest data is deleted to make room for new recordings. Only a factory reset allows you to actively delete the data.

Configuration of graphs on the device website

1. Log in to the device website of the SMART CONNECT KNX Remote Access.
2. Select << Graphs>> in the menu bar.
3. Click <<Add graph>>.
4. Assign a name and select the time period to be represented.
   Please note that the representation of long time periods may lead to longer loading times.
5. Select the record to be represented in this graph.

- Up to 40 records can be shown in one graph.
- The representation of 1-bit bars is limited to 20.
- A graph can show max. two Y axes. For this reason, only two different non binary data point types are allowed in one graph.



Name: Graph 1

Period: 1 Day

5/40	Name	Datapoint Type
☑	Außentemperatur	9.001 Temperature (°C)
□	Windgeschwindigkeit	9.028 Wind speed (km/h)
□	Regen ja/nein	1.005 Alarm
□	Rel. Luftfeuchte außen	9.007 Humidity (%)
□	Frostalarm	1.005 Alarm

Figure 29: Adding a graph

Representation of the graphs

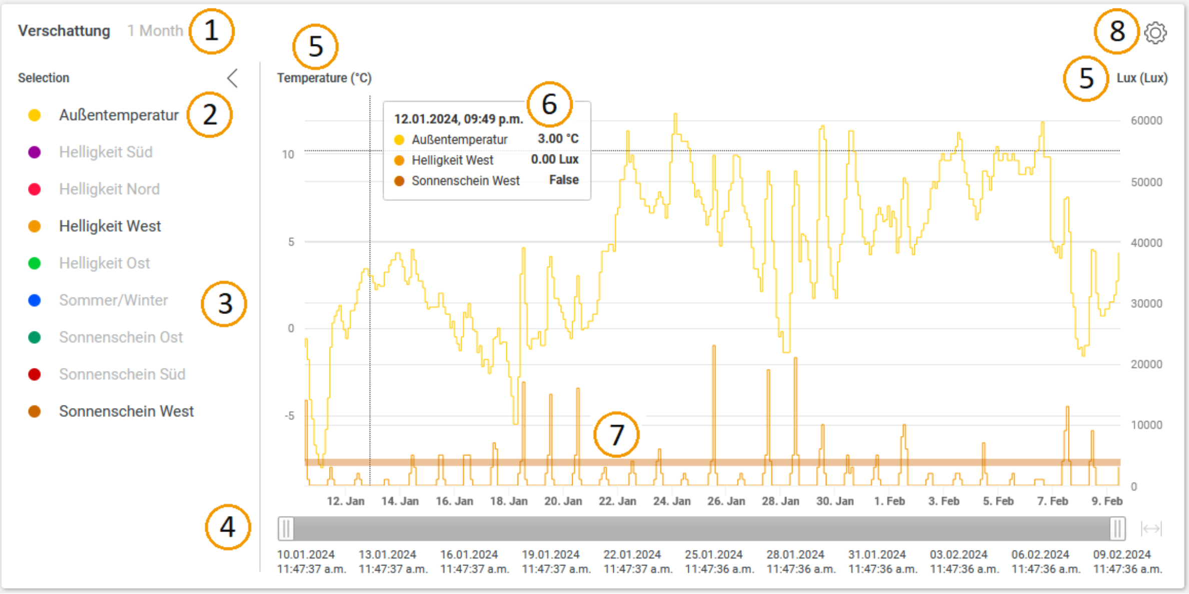


Figure 30: Graphs on the device website

No.	Element	Explanation
1	Name/time period	Representation of the assigned name and the time period.
2	Record (shown)	Only the selected records are shown in the graph.
3	Record (hidden)	Click the records to hide them.
4	X axis	Representation of the selected time period. In the area below, it is possible to zoom in individual sections by moving the slider.
5	Y axis	Representation of the data type (unit) selected in the ETS.
6	Information window	The values at the mouse pointer position are displayed in an information window. A maximum number of 10 values are displayed.
7	1-bit bar	Representation of 1-bit values as true (dark) or false (light).
8	Settings	Adapting and editing the graph.

Table 13: Legend of the graphs

Embedding the graphs

You can embed the generated graphs into a KNX visualisation or to a website. You can choose between integrating an inline frame and calling up a website via a link.

1. Use the cogwheel symbol on the graph to open the settings.
2. Click <<Embed>>.
3. Select the type of use and copy the code or link (CRTL + C).
4. Open the application into which the graph is to be embedded.
5. Insert the inline frame code or the link at a suitable position in this application.

Note:

If you access the device website locally, clicking <<Embed>> generates a URL that you can use to access the graph on the device's local network.
If you access the device website remotely, clicking <<Embed>> generates a URL that you can use to access the graph remotely.

Exporting graphs

You can export the records of a graph to a CSV file.

1. Use the cogwheel symbol on the graph to open the settings.
2. Click <<CSV export>>.
3. The export is started automatically and can be found in the download area of your browser.

Note:

The time period selected during the configuration of the graph is exported. Depending on the software used, it is possible that only a limited number of values is shown.
If not all values are included in the file, reduce the time period or configure less records in one graph.
The values of hidden records are also transferred to the CSV export.

9.3 Parameter – time server

As a time server, the SMART CONNECT KNX Remote Access can transmit the current time to the KNX bus at configurable intervals. The transmitted time is obtained from the system time. This time is synchronised via the NTP server configurable on the device website. The interval for sending the group object 52 <<Date and time>> is defined via the parameters <<Send time>> (group object 50) and <<Send date>> (group object 51).
The shorter interval is used if the parameter values differ.

The device can be configured for various UTC time zones. The <<Time zone>> parameter used for this is located in the <<Settings>> parameter view.

Time changeover is taken into account either automatically depending on the time zone set or not at all. A <<Generic Time Zone w/o DST>> must be parametrised to ensure that no automatic time changeovers are carried out.

The time server will then only transmit the date and time if, as a minimum, a successful NTP synchronisation has been performed since the device start-up. This is to prevent a possibly incorrect system time from being sent.

With the parameter <<Time server>>, a group object 53 is provided with which the sending of the time/date can be triggered (trigger).

The time server function is deactivated on delivery.

9.4 Parameter – data logger

The data logger function is enabled using the <<Data logger>> parameter in the <<Data logger – Settings>> parameter view. By ticking the check box, the data logger is started directly. If a microSD card is inserted into the device or if there is already a microSD card in the device, logging begins automatically if it is not deactivated via the group object 57 <<Activate data logger>>.

The data logger status is sent via the group object 58 <<Data logger – state>>. However, the data logger state can also be queried directly. If the data logger is active, the group object has the value 1. The group object <<Data logger – state>> takes the value 0 and sends it if

- the microSD card has been removed,
- there is no more memory capacity on the microSD card or
- the data logger has been activated using the <<Activate data logger>> group object 57.

The <<Format>> parameter in the same parameter view can be used to configure whether an ETS3 (.trx) or an ETS4/ETS5/ ETS6 (.xml) compliant data format should be used. The data logger files are named and saved on the microSD card according to the following format:

```
Year
-----Month
-------------Day
------------------2010_01_06_TP1.xml
```

If there is a loss of voltage resulting in the time/date being lost, a file name may possibly be repeated. In such a case, a tilde (~) is added to the end of the file name; if a name is repeated again, a tilde is added with a successive number (~1).

The microSD card memory can be used as read-only memory or as a ring memory.
When used as a ring memory, the remaining memory is monitored. When the remaining memory capacity drops below 2.5 MB, the oldest log file is deleted to create space for new data. When the card is used as a read-only memory, logging is automatically ended as soon as microSD card is full until a new microSD card with sufficient memory capacity is inserted.

The SMART CONNECT KNX Remote Access supports SDXC card up to a maximum of 1 TB.
The cards must be formatted with exFAT.

Important

Deactivate logging before removing the microSD card to avoid damage to the card.

Group objects 59 and 60 are available for monitoring the memory status.

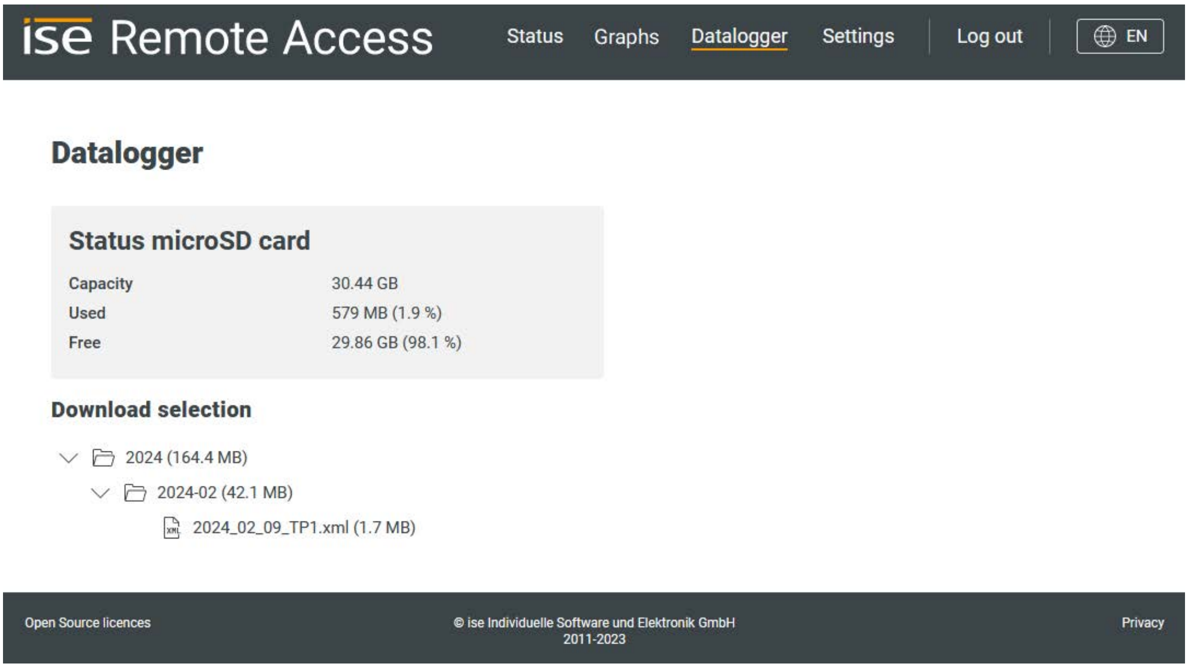
Note:

If the NTP server is not available, a default time is used in the event of a power failure. Further logging is based on this time until the NTP server is available again.

Access to the data logger archive

Access to the data logger archive can be gained on the device website. The menu item is also available for deactivated data loggers to download old files if necessary. The microSD card’s status is also displayed besides the saved files.

When a microSD card is inserted, the data logger files stored on the microSD card are listed under <<Download selection>>. They are grouped by year and month. The years and months are minimised by default and can be fully revealed by pressing the arrows.



Datalogger

Status microSD card

Capacity	30.44 GB
Used	579 MB (1.9 %)
Free	29.86 GB (98.1 %)

Download selection

- 2024 (164.4 MB)
  - 2024-02 (42.1 MB)
    - 2024_02_09_TP1.xml (1.7 MB)

Figure 31: Data logger archive

The file size is displayed in byte(s) next to a month or an individual file. You can start downloading an XML file by clicking on the download icon next to it.

Note:

If you are not able to decrypt secure telegrams in the ETS group monitor, restart the ETS and repeat decryption.

10 Group objects

The SMART CONNECT KNX Remote Access provides the following group objects to connect group addresses.

Important information regarding all group objects which signal an active connection:

When using the HTTP access, i.e. without Remote Access Windows Client, the connection to the device will not end immediately after the pages are loaded or the browser is closed. HTTP connections may take up to five minutes to close. The associated group objects do not signal closing until this process is complete. The connection is terminated synchronously if the Remote Access Windows Client is used.

Limitations and authorisations of access rights via Group objects

If the SMART CONNECT KNX Remote Access is added in an ETS project, its group objects may allow or prohibit KNX access options. The access rights limitations defined via the KNX in the remote installation always override the definitions on my.ise. In this way, remote access can be deactivated completely regardless of the settings on my.ise through the use of group telegrams. Likewise, all communication with my.ise can be disabled using group telegrams.

10.1 Remote access

1 |	
Name	Allow connection to my.ise
Function	Allows the device to establish a connection to the my.ise server or prohibits it from establishing one. If it is forbidden to establish a connection, the device cannot be accessed from outside.
Possible values	0: Prohibit 1: Allow
Data width	1 bit
Data point type/data type	1.003/enable
Direction	Write
Flags (CRWTUI)	C-W---

Table 14: Allow connection to my.ise

2 |	
Name	Allow connection to my.ise – state
Function	Indicates whether the device is allowed to connect to the my.ise server.
Possible values	0: Prohibited 1: Allowed
Data width	1 bit
Data point type/data type	1.003/enable
Direction	Read
Flags (CRWTUI)	CR-T--

Table 15: Allow connection to my.ise – state

3 | 5	
Group objects	3: Resident 5: Installer
Name	Grant "Residents" or "Installers" remote access
Function	Allows or prohibits remote access for members of the group concerned.
Possible values	0: Prohibit 1: Allow
Data width	1 bit
Data point type/data type	1.003/enable
Direction	Write
Flags (CRWTUI)	C-W---

Table 16: Grant remote access

4 | 6	
Group objects	4: Resident 6: Installer
Name	Grant "Residents" or "Installers" remote access – state
Function	Indicates whether remote access is allowed for members of the group concerned.
Possible values	0: Prohibited 1: Allowed
Data width	1 bit
Data point type/data type	1.003/enable
Direction	Read
Flags (CRWTUI)	CR-T--

Table 17: Grant remote access – state

9 |	
Name	Allow VPN access
Function	Enables or disables VPN access for all users approved for the VPN on my.ise.
Possible values	0: Disable 1: Enable
Data width	1 bit
Data point type/data type	1.003/enable
Direction	Write
Flags (CRWTUI)	C--W---

Table 18: Allow VPN access

10 |	
Name	Allow VPN access – state
Function	Shows whether VPN access is permitted.
Possible values	0: Prohibited 1: Allowed
Data width	1 bit
Data point type/data type	1.003/enable
Direction	Read
Flags (CRWTUI)	CR-T--

Table 19: Allow VPN access – state

20 |	
Name	Connection to my.ise – state
Function	Indicates whether connection to my.ise is established. Group object 31 provides more detailed information.
Possible values	0: Disconnected 1: Connected
Data width	1 bit
Data point type/data type	1.011/state
Direction	Read
Flags (CRWTUI)	CR-T--

Table 20: Connection to my.ise – state

21 |	
Name	Remote access connection – state
Function	Indicates whether at least a remote connection is currently active, regardless of the connection type.
Possible values	0: Not active 1: Active
Data width	1 bit
Data point type/data type	1.011/state
Direction	Read
Flags (CRWTUI)	CR-T--

Table 21: Remote access connection – state

22 | 23	
Group objects	22: Resident 23: Installer
Name	Remote access connection "Resident" or "Installer" – state
Function	Indicates whether a remote access connection is active for members of the group concerned.
Possible values	0: Not active 1: Active
Data width	1 bit
Data point type/data type	1.011/state
Direction	Read
Flags (CRWTUI)	CR-T--

Table 22: Remote access connection “Group” – state

25 |	
Name	VPN access – state
Function	Shows whether an active VPN connection currently exists.
Possible values	0: Not active 1: Active
Data width	1 bit
Data point type/data type	1.011/state
Direction	Read
Flags (CRWTUI)	CR-T--

Table 23: VPN access – state

10.2 Connection error

30 |	
Name	Error indication
Function	Indicates a connection error which is described by group object 32. Further details can be found on the SMART CONNECT KNX Remote Access's device website.
Possible values	0: No alarm 1: Alarm
Data width	1 bit
Data point type/data type	1.005/alarm
Direction	Read
Flags (CRWTUI)	CR-T--

Table 24: Error indication

31 |	
Name	my.ise connection info
Function	Diagnostic information on the my.ise connection.
Details	Supplies more precise information on the my.ise connection status displayed by group object 20.
Data width	14 byte
Data point type/data type	16.001/Character String (ISO 8859-1)
Direction	Read
Flags (CRWTUI)	CR-T--

Table 25: my.ise connection info

32 |	
Name	Connection error info
Function	Additional diagnostic information in case of a my.ise connection error.
Details	Supplies more precise information on the connection error displayed by group object 30.
Data width	14 byte
Data point type/data type	16.001/Character String (ISO 8859-1)
Direction	Read
Flags (CRWTUI)	CR-T--

Table 26: Connection error info

10.3 Time server

50 |	
Name	Time
Function	Transmits the current time periodically and on request.
Details	The interval can be parameterised. If you read this object directly when it is not yet possible to enquire a valid NTP time, you will receive the current system time, which may differ from the correct time.
Data width	3 byte
Data point type/data type	10.001/time of day
Direction	Read
Flags (CRWTUI)	CR-T--

Table 27: Time

51 |	
Name	Date
Function	Transmits the current date periodically and on request.
Details	The interval can be parameterised. If you read this object directly when it is not yet possible to enquire a valid NTP time, you will receive the current system date, which may differ from the correct time.
Data width	3 byte
Data point type/data type	11.001/date
Direction	Read
Flags (CRWTUI)	CR-T--

Table 28: Date

52 |	
Name	Date and time
Function	Transmits current date and time periodically and on request.
Details	The interval is determined based on the lower interval between group objects 50 and 51. If you read this object directly when it is not yet possible to enquire a valid NTP time, you will receive the current system time and, which may differ from the correct time and date.
Data width	8 byte
Data point type/data type	19.001/date time
Direction	Read
Flags (CRWTUI)	CR-T--

Table 29: Date and time

53 |	
Name	Transmit date/time trigger
Function	Triggers the transmission of the date and time.
Details	1-bit object to trigger the transmission of the current time/date if the object is assigned any value. No values are transmitted if no NTP query has been successful yet.
Data width	1 bit
Data point type/data type	1.017/trigger
Direction	Write
Flags (CRWTUI)	C-W---

Table 30: Transmit date/time trigger

54 |	
Name	NTP query – state
Function	Indicates if it was possible to query a valid time from the NTP server.
Possible values	0: NTP query was not successful 1: NTP query was successful
Data width	1 bit
Data point type/data type	1.002/Boolean
Direction	Read
Flags (CRWTUI)	CR-T--

Table 31: NTP query – state

10.4 Data logger

55 |	
Name	microSD card error
Function	Shows whether the microSD card presents an error.
Possible values	0: No error 1: Error
Data width	1 bit
Data point type/data type	1.002/Boolean
Direction	Read
Flags (CRWTUI)	CR-T--

Table 32: microSD card error

56 |	
Name	microSD card error code
Function	Indicates the current error code.
Possible values	0: microSD card OK 1: microSD card full 2: microSD card not inserted 4: an error has been detected on microSD card (e.g. incorrectly formatted)
Data width	1 byte
Data point type/data type	20.*/1-byte
Direction	Read
Flags (CRWTUI)	CR-T--

Table 33: microSD error code

57 |	
Name	Activate data logger
Function	Enables or deactivates logging and indicates state on request.
Possible values	0: Disable 1: Enable
Data width	1 bit
Data point type/data type	1.001/switch
Direction	Write
Flags (CRWTUI)	CRW---

Table 34: Activate data logger

58 |	
Name	Data logger – state
Function	Indicates whether the data logger is currently logging data.
Possible values	0: Not active 1: Active
Data width	1 bit
Data point type/data type	1.002/Boolean
Direction	Read
Flags (CRWTUI)	CR-T--

Table 35: Data logger – state

59 |	
Name	microSD card – memory state
Function	Indicates whether the microSD card memory is full.
Possible values	0: Not full 1: Full
Data width	1 bit
Data point type/data type	1.002/Boolean
Direction	Read
Flags (CRWTUI)	CR-T--

Table 36: microSD card — memory state

60 |	
Name	microSD card – filled memory capacity
Function	Indicates the percentage of microSD card memory that is full.
Possible values	0 to 255 is equal to 0 to 100 %
Data width	1 byte
Data point type/data type	5.001/percentage (0 to 100%)
Direction	Read
Flags (CRWTUI)	CR-T--

Table 37: microSD card – filled memory capacity

10.5 Notifications

The following group objects provide five possible data point types. The data point type is determined by selecting the corresponding parameters.

101…150	
Name	Notification No. 1/…/50
Function	Creates a notification on my.ise. The boolean value can be sent in the notification.
Possible values	0: Disable 1: Enable
Data width	1 bit
Data point type/data type	1.001/switch
Direction	Write
Flags (CRWTUI)	C-W---

Table 38: Trigger notification – boolean

101…150	
Name	Notification No. 1/…/50
Function	Creates a notification on my.ise. The percentage value can be sent in the notification.
Possible values	0 to 255 is equal to 0 to 100 %
Data width	1 byte
Data point type/data type	5.001/percentage (0 to 100%)
Direction	Write
Flags (CRWTUI)	C-W---

Table 39: Trigger notification – percentage

101…150	
Name	Notification No. 1/…/50
Function	Creates a notification on my.ise. The counter value can be sent in the notification.
Possible values	0 to 255
Data width	1 byte
Data point type/data type	5.010/counter pulses (0 to 255)
Direction	Write
Flags (CRWTUI)	C-W---

Table 40: Trigger notification – counter

101…150	
Name	Notification No. 1/…/50
Function	Creates a notification on my.ise. The float value can be sent in the notification.
Possible values	List of 2 bytes separated by a space or comma
Data width	2 bytes
Data point type/data type	9.*/2-byte float value
Direction	Write
Flags (CRWTUI)	C-W---

Table 41: Trigger notification – float value

101…150	
Name	Notification No. 1/…/50
Function	Creates a notification on my.ise. The text value can be sent in the notification.
Possible values	Freely selectable text
Data width	14 bytes
Data point type/data type	16.001/Character String (ISO 8859-1)
Direction	Write
Flags (CRWTUI)	C-W---

Table 42: Trigger notification – text

10.6 Records

The following group objects provide seven possible data point types. The data point type is determined by selecting the corresponding parameters.

201…400	
Name	Record No. 1/…/200
Function	Records the value for the graphs.
Data width	1 bit
Data point type/data type	1.* /1-bit
Direction	Write
Flags (CRWTUI)	C-W-U-

Table 43: Record – DPT 1.*

201…400	
Name	Record No. 1/…/200
Function	Records the value for the graphs.
Data width	1 byte
Data point type/data type	5.* /8-bit unsigned value
Direction	Write
Flags (CRWTUI)	C-W-U-

Table 44: Record – DPT 5.*

201…400	
Name	Record No. 1/…/200
Function	Records the value for the graphs.
Data width	2 bytes
Data point type/data type	7.* /2-byte unsigned value
Direction	Write
Flags (CRWTUI)	C-W-U-

Table 45: Record – DPT 7.*

201…400	
Name	Record No. 1/…/200
Function	Records the value for the graphs.
Data width	2 bytes
Data point type/data type	9.* /2-byte float value
Direction	Write
Flags (CRWTUI)	C-W-U-

Table 46: Record – DPT 9.*

201…400	
Name	Record No. 1/…/200
Function	Records the value for the graphs.
Data width	4 bytes
Data point type/data type	12.* /4-byte unsigned value
Direction	Write
Flags (CRWTUI)	C-W-U-

Table 47: Record – DPT 12.*

201…400	
Name	Record No. 1/…/200
Function	Records the value for the graphs.
Data width	4 bytes
Data point type/data type	13.* /4-byte signed value
Direction	Write
Flags (CRWTUI)	C-W-U-

Table 48: Record – DPT 13.*

201…400	
Name	Record No. 1/…/200
Function	Records the value for the graphs.
Data width	4 bytes
Data point type/data type	14.* /4-byte float value
Direction	Write
Flags (CRWTUI)	C-W-U-

Table 49: Record – DPT 14.*

11 Troubleshooting

The device LEDs give you information on operating state errors as well as faults after configuration:

► See LEDs during device start-up, p. 31.

► See LEDs in operation, p. 32.

You will find solutions for displayed error codes and possible configuration errors in the following table. If the following solutions are not successful, check the configuration and the status of the access groups on my.ise and on the device website. Error codes are displayed on the device website under <<Status>>.

Issue	Troubleshooting
The COM LED does not light up.	Check the KNX cabling and the LED status displays as per Section "LEDs in operation" on page 32.
The APP LED lights up continuously.	Check the general authorisation for the my.ise connection via KNX Group Objects 1 and 2.
The APP LED flashes constantly and slowly at 1 Hz.	Check the device parametrisation in the ETS as specified in Chapter "Creating the device in the ETS" on page 34.
The device is not visible in the Windows network environment.	Check the network cabling and parametrisation of the device IP in the ETS as specified in Section "Setting the IP address, IP subnet mask and standard gateway address" on page 36.
The device is displayed as offline on my.ise.	Check the Internet connection. If you do not use DHCP, check the specified DNS server. Check the device website for further error information. If the check did not identify any faults, restart the unit on the device website.

Table 50: Troubleshooting

11.1 Generating log files

Support uses log files to obtain information to help analyse your problem. You generate these log files via the device website and download them as a ZIP file.

You configure the scope of the information contained in the log files using the logging mode.
Our Support may ask you to configure the logging mode.

1. Open the device website ► See Accessing the device website, p. 25.

2. On the <<Settings>> page in the <<General>> field, select the corresponding button under <<Logging mode>>.

<<normal>>	Basic information is collected.
<<extended>>	Detailed information is collected.

ℹ <<extended>> logging mode has a negative influence on performance. Only activate this mode if Support requests the extended log files.
Deactivate this mode again as soon as you have generated the log files.

3. Click the <<Download log file>> button. The log files are compiled and downloaded as a ZIP file.

11.2 Contacting Support

If you have a problem with your SMART CONNECT KNX Remote Access and require support, contact us:

- E-mail to support@ise.de
- Call us on tel.: +49 441 680 06 12
- Fax us: +49 441 680 06 15

We will need the following data in order to help you:

- To identify the device: Product name or order number
- Registration ID
- MAC address (optional)
- Product database entry version
- Version of the firmware
- ETS version
- A meaningful error description including the error code (if there is one)

Gladly also:

- Log files
- Screenshot of <<Status>> on the device website

11.3 FAQs – Frequently asked questions

How do I find the IP address of my SMART CONNECT KNX Remote Access?

You will find the IP address on the device website; see “Accessing the device website” on page 25.

How much Internet data traffic do I consume if I have connected the SMART CONNECT KNX Remote Access to my.ise?

Approx. 400 bytes of data traffic occurs per minute to maintain the connection. This corresponds to approx. 560 KB/day or 16.5 MB/month. My.ise does not regard this data volume as user data in the sense of limiting the data volume in the licence agreement for the SMART CONNECT KNX Remote Access.

Which communication channel to my.ise is used by SMART CONNECT KNX Remote Access?

The SMART CONNECT KNX Remote Access communicates with my.ise using an HTTPS connection via default port 443 only. Using this one connection, all data are exchanged in both directions so that it is generally not necessary to make a configuration of the firewall. If you wish to limit network access to specific domains and ports or IP addresses, we recommend configuring exceptions. You will find an overview with the remote access relevant domains, ports and IP addresses at https://my.ise.de.

Why do I need to activate cookies to use my.ise?

My.ise cookies are used to secure accesses and the connection. These cookies do not track. Exchange with third parties only takes places if user accounts are linked to third parties.

Are there software updates for my SMART CONNECT KNX Remote Access?

You will find information on software updates at “Updating firmware” on page 41.

With which protocols can I access devices on the remote network?

You can access devices on the remote network which are accessible via HTTP without needing to install the Remote Access Windows Client software. This means almost all devices which have a browser-based user interface. These devices are found automatically via SSDP. With client, all TCP-based protocols, such Telnet, SSH, HTTPS, Window Remote Desktop, FTP and many more, work alongside KNX/IP and the Gira HomeServer.

Why do the group objects concerned not report that a connection is no longer available immediately after my browser is closed when I use HTTP to gain access?

Read the entry instruction at “Group objects” on page 57 for more information.

How can I configure the three individual addresses for the KNX/IP ETS interfaces (tunnelling server) in the ETS project?

Read Section “Tunnelling server” on page 38 for more information.

Can I use the three KNX/IP ETS interfaces for downloading and the group and bus monitor?

Yes, the interfaces support all download operations and the group and bus monitor.

Can the website of my SMART CONNECT KNX Remote Access also be reached over the Internet?

Yes, the device website can be accessed securely over the Internet.

Why is the device website for my SMART CONNECT KNX Remote Access not displayed?

The browser or the particular browser version used is not supported.

We support current market standard browsers such as Google Chrome, Microsoft Edge and Mozilla Firefox in their current versions as a minimum (as of the date this documentation was printed). However, we recommend that you keep your browser up to date for security reasons alone if nothing else.

Why does the ETS report an error that it is not possible to write on a protected area when downloading the application program?

Please ensure that your ETS version is up to date. We are only able to guarantee that the SMART CONNECT KNX Remote Access will provide its full capabilities if you use the latest version of the ETS.

Is the my.ise server really necessary?

There is currently no flawless technical solution available today which fulfils our requirements for stability and security. Using a server is the only way to provide remote access which is virtual always functional and does not require complicated configuration.

What kind of data does the server save?

The server only saves the data which are absolutely essential for providing the service. In addition to the data you specified during login and the data visible in the user interface, this includes information on the quantity and point in time of the data volume transferred. The server does not save user data at any time.

Is operation of the server within Germany guaranteed?

Yes. Our my.ise server and the data server (for even distribution of the data traffic) are all guaranteed to be operated in Germany. To ensure high availability, the servers are rented from reputable hosting providers as the so-called root server so that no unauthorised third party can access the server and data. The restrictive General Data Protection Regulation (GDPR) applies when operating in Germany

Why does the licence exclude continuous use (24/7) and include a data volume limitation?

Since all data needs to pass through the my.ise server (see above), continuous use is very performance intensive, particularly in the case of video streaming, for example. Certain limitations are therefore necessary to guarantee good performance at all times. You are welcome to contact us if you have use cases which exceed these conditions. Licence models with expanded scope have not been ruled out for the future.

If I access a website using my.ise, it no longer functions correctly, even though it functions locally. Why might that be?

Not all websites can be loaded from the remote network via my.ise. More complex sites in particular, such as those with Java implementations, may not work. If this should happen, you are welcome to send an e-mail to our support team with a precise product description, screenshots and a brief error description. We try to support as many products as possible using secure my.ise-HTTP access.

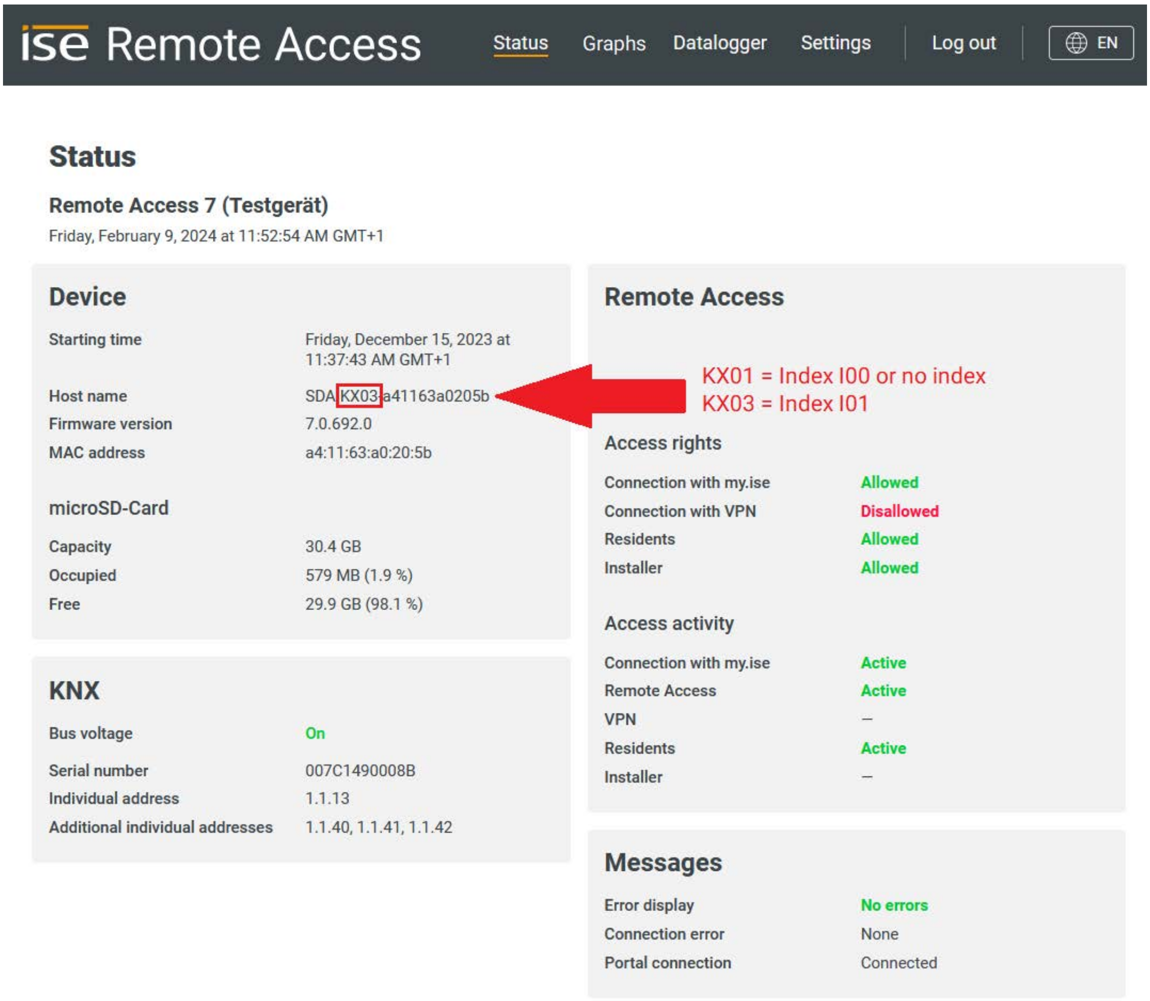
Why do I see the previously configured IP and individual addresses after unloading the application on the device website?

The device website is not updated until the page is refreshed after unloading.

Where can I find the index status?

Since 2019, the SMART CONNECT KNX Remote Access has been provided with an index. If various firmware versions are available to download for SMART CONNECT KNX Remote Access, the index status provides information on the firmware to be used.

The index status is shown on the device sticker (see figure 10).
If you are not on site, you can determine the index status via the device website:



Status

Remote Access 7 (Testgerät)
Friday, February 9, 2024 at 11:52:54 AM GMT+1

Device

Starting time	Friday, December 15, 2023 at 11:37:43 AM GMT+1
Host name	SDA-KX03-a41163a0205b
Firmware version	7.0.692.0
MAC address	a4:11:63:a0:20:5b

microSD-Card

Capacity	30.4 GB
Occupied	579 MB (1.9 %)
Free	29.9 GB (98.1 %)

KNX

Bus voltage	On
Serial number	007C1490008B
Individual address	1.1.13
Additional individual addresses	1.1.40, 1.1.41, 1.1.42

Remote Access

KX01 = Index I00 or no index
KX03 = Index I01

Access rights

Connection with my.ise	Allowed
Connection with VPN	Disallowed
Residents	Allowed
Installer	Allowed

Access activity

Connection with my.ise	Active
Remote Access	Active
VPN	–
Residents	Active
Installer	–

Messages

Error display	No errors
Connection error	None
Portal connection	Connected

Figure 32: Index in host name

12 Disassembly and disposal

If you want to disassemble the device, due to a defect, for example, proceed in reverse order to installation.

Removing the cover cap

⚠ **Warning**

Danger from incorrect use

Incorrect use can result in damage to the device, fire or other dangers.

- Only qualified electricians may install and disassemble electrical devices.
- Follow the instructions in this product manual.

⚠ **Warning**

Danger of electric shock

An electric shock can result from touching live parts in the installation environment. Electric shock can cause death.

- Enable the device.
- Cover up live parts in the vicinity.

1. Gently press in the cover cap at the side (see figure 33, item 1).

2. Pull off the cover cap upwards (see figure 33, item 2).

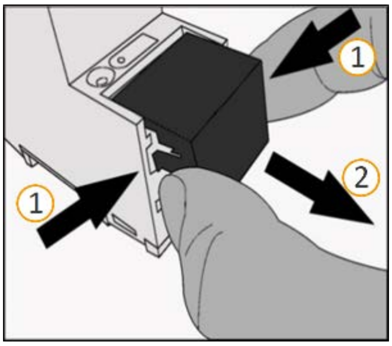


Figure 33: Removing the cover cap

Detaching the device from the top-hat rail

Requirement: Power supply, bus line and network connection are disconnected.

1. Insert a screwdriver (see figure 34, item 1) into the release lever (see figure 34, item 2) and push the release lever down (see figure 34, item 3).

2. Take the device off the top-hat rail.

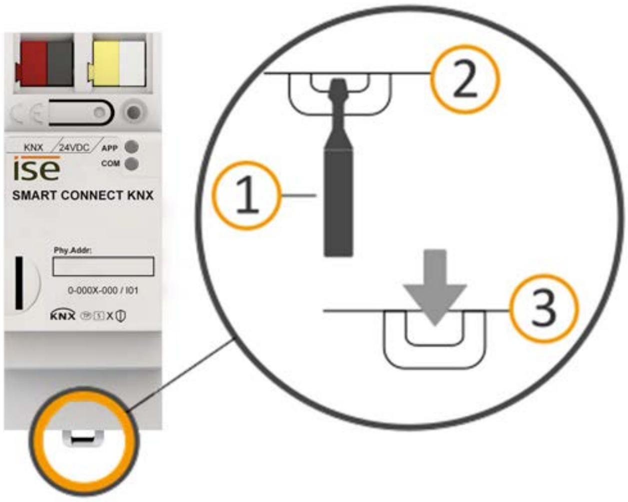


Figure 34: Detaching the device from the top-hat rail

Disposal

Make an active contribution to protecting the environment by disposing of all materials in an environmentally-responsible way.

Packaging and box	
♻	Dispose of the packaging material appropriately, in a card, paper or plastic recycling bins.

Device	
	Old devices must not be disposed of with domestic refuse! You can dispose of your old device free of charge at designated collection facilities or, if necessary, you can hand it in to your specialist dealer. Contact your local authority for recycling details.

13 Glossary

Access groups

Users can be enabled to use the SMART CONNECT KNX Remote Access via the my.ise server. Access can be allowed or prohibited separately using the KNX button to divide users into access groups. Access is enabled for both groups by default.

Residents: Access group for building residents.

Installers: Access group for external service providers.

Authentication key

If a software, such as a visualisation software, opens an my.ise connection, the software must identify itself to my.ise. A user creates an authentication key on my.ise for this purpose. This replaces the user's login data (e-mail and password).

Catalogue

Abbreviated name for “Online Catalog“ of the ETS. The catalogue is a product database. The catalogue contains all KNX-certified or -registered devices. The device data are saved as a product database entry.

Connector

KNX gateway to link the home network with the my.ise server to enable remote access. SMART CONNECT KNX Remote Access and connector are used as synonyms of one another.

Data volume, traffic

Designates the user data volume transferred over the my.ise server. Widely different volumes of data are transferred in different applications. KNX communication produces small data volumes whereas live streaming from a webcam produces comparatively large data volumes. The volume of data transferred has an impact on the my.ise server. The transfer volume is per month and limited SMART CONNECT KNX Remote Access to a maximum of 2 GB. See “Maximum permissible transfer volume” on page 86.

Device website

Applications used to check device status, update loading and the display of device information.

DPT, DP type, data point type

The data point type is the standard coding for data transmitted via group telegrams.

ETS (Engineering Tool Software)

The device is configured in the ETS software. The ETS is available with a different range of functions from the KNX Association (www.knx.org).

FDSK (Factory Default Setup Key)

The FDSK is an integral part of the KNX Secure certificate and is used to ensure secure communication between devices in the "KNX IP Secure Device" category. The combination of FDSK and the device’s serial number can provide each device with a unique identification. Together, they form the device certificate.
Depending on the use case, the certificate may be required for initial authentication in the ETS or for encryption of communication.

The KNX Secure certificate is printed on a sticker on the side of the device. A second sticker is enclosed with the product.

Firmware update tool

Software which is embedded in the device hardware and is used to operate the device. Functional enhancements for the device are available with a new firmware version.

Flags (CRWTU)

Every group object has flags with which the group object obtains methods: C=Communication, R=Read, W=Write, T=Transfer, U=Update, I=Initialise.

Home network

The computer network (Ethernet) in your home. Your network devices are connected to the SMART CONNECT KNX Remote Access via the home network.

httpaccess.net

Part of the my.ise server for configuration-free access to devices which have an integrated web server.

Local network

Local network refers to the network containing the computer with which is used to access a device in the remote network via my.ise. Access is gained either via my.ise or the Remote Access Windows Client.

my.ise login

Access with my.ise login to devices behind a SMART CONNECT KNX Remote Access.

my.ise server

Central server in the my.ise infrastructure to manage access to the SMART CONNECT KNX Remote Access.
We operate the server in Germany in compliance with the stringent European data protection guidelines. Accessible under https://my.ise.de.

Network device

A device with an IP connection installed in the home network which is accessed via my.ise.

Notifications

A message system which saves messages generated by system events (e.g. logging a SMART CONNECT KNX Remote Access onto/off my.ise) or by KNX group objects and forwards them via push notification, e-mail, phone or text message on request.

Ownership transfer

Refers to the my.ise server function to change ownership of a SMART CONNECT KNX Remote Access. This occurs on a regular basis when a new building installation is transferred from the installer to the owner, hence the term "ownership transfer".

Product database entry (also catalogue entry)

Data relating to a device in the "Online Catalog" of the ETS. The product database entry contains all data to allow the device to be configured in the ETS. The product database entry is provided in the form of a file by the device manufacturer. The latest version of product data entries for the ise Individuelle Software und Elektronik GmbH can be downloaded free of charge from our website www.ise.de.

The product database entry is often also called the "catalogue entry".

Registration ID

Each SMART CONNECT KNX Remote Access has a unique registration ID (formerly connector ID), which is printed on a sticker on the side of the device. The registration ID is used to link a SMART CONNECT KNX Remote Access with a my.ise account. A second sticker is enclosed with the product.

Remote access

Secure access to a device in the home network via the my.ise server and a SMART CONNECT KNX Remote Access.

Remote Access Windows Client

PC software which allows other applications to communicate via remote access.

Remote connection ID

The remote connection ID is a shortened variant of the registration ID and comprises the first two blocks of the registration ID.

Remote network

The network containing the SMART CONNECT KNX Remote Access is referred to as a remote network.

Secure connection

Designates an encrypted and authenticated (on both sides) communication connection between two communication partners.

TLS, SSL

Internet standard (as per RFC 5246) for an encrypted and optionally authenticated communication protocol. SSL stands for "Secure Socket Layer." The protocol was renamed to TLS, or "Transport Layer Security," in 1999. Both terms are synonyms. This protocol is widely used, especially as a HTTPS security layer.

Updates

You will find information on new versions of the firmware in this documentation under the search term "Update".

User role, role

A my.ise user has one of the following roles on a SMART CONNECT KNX Remote Access enabled for them:

A “user” may use the device to access the home network.
An “administrator” is also able to enable the device for other users, cancel authorisations and define user roles and access groups.

The “owner” of a SMART CONNECT KNX Remote Access is the person legally responsible for it. The owner’s rights are identical to those of the administrator. Every SMART CONNECT KNX Remote Access linked to a my.ise account has exactly one owner. The owner can be changed by <<Ownership transfer>>.

Website

Information on the device's application can be found in this documentation under the search term "Device website".

14 Licence Agreement SMART CONNECT KNX Remote Access

Hereinafter are the contract terms for your use of the software as the "licensee".

On accepting this agreement and installing the SMART CONNECT KNX Remote Access software or putting the SMART CONNECT KNX Remote Access into use, you conclude an agreement with ise Individuelle Software und Elektronik GmbH and agree to abide by the terms in this agreement.

14.1 Definitions

Licensor: ise Individuelle Software und Elektronik GmbH, Oldenburg (Oldb), Osterstraße 15, Germany

Licensee: The legal recipient of the SMART CONNECT KNX Remote Access software.

Firmware: Software which is embedded into the SMART CONNECT KNX Remote Access hardware and is used to operate the SMART CONNECT KNX Remote Access.

SMART CONNECT KNX Remote Access: The SMART CONNECT KNX Remote Access software designates all of the software provided for the SMART CONNECT KNX Remote Access product, including the operating data. This includes, in particular, the firmware and the product database.

14.2 Object of the agreement

The object of this agreement is the SMART CONNECT KNX Remote Access software provided on data storage devices or through downloads, the Remote Access Windows Client software, the provision of my.ise and the associated documentation in written and electronic format.

14.3 Software usage rights

14.3.1 Firmware and Remote Access Windows Client

The licensor grants the licensee the non-exclusive, non-transferable right to use the SMART CONNECT KNX Remote Access software for an unlimited time in accordance with the following conditions for the purposes and applications specified in the valid version of the documentation (which shall be provided in printed format or also as online help or online documentation).

The licensee is obliged to ensure that each person who uses the program only does so as part of this license agreement and observes this license agreement.

14.3.2 my.ise

The Licensor provides the Licensee with a my.ise server at https://my.ise.de to use with the firmware and the Remote Access Windows Client. The Licensor currently utilises the services of ise Individuelle Software und Elektronik GmbH for this purpose. The Licensor may cancel operation of the my.ise server for due cause on giving 5 years' notice. In this case, the Licensor must make the my.ise software available to the Licensee as a source code upon request to enable the Licensee to host the server software themselves and thus ensure continued use of my.ise.

14.4 Restriction of rights of use

14.4.1 Maximum permissible transfer volume

The licence excludes the use of continuous remote access for purposes such as visualisation or location networking. The Licensor regards repeated, uninterrupted use for more than 12 hours at a time to be continuous use.The transfer volume is per month and limited SMART CONNECT KNX Remote Access to a maximum of 2 GB.
The Licensor reserves the right to use technical means to implement the usage limits specified above.

14.4.2 Copying, modification and transmission

The licensee is not authorised to use, copy, modify or transfer the SMART CONNECT KNX Remote Access software in whole or in part in any way other than as described herein. Excluded from this is one (1) copy produced by the licensee exclusively for archiving and backup purposes.

14.4.3 Reverse engineering and conversion technologies

The Licensee is not authorised to apply reverse-engineering techniques to the SMART CONNECT KNX Remote Accesssoftware or to convert the SMART CONNECT KNX Remote Access software into another type. Such techniques include, in particular, disassembly (conversion of an executable program's binary-coded computer instructions into an assembler language which humans can read) or decompilation (conversion of binary-coded computer instructions or assembler instructions into source code in the form of high-level language commands).

14.4.4 Firmware and hardware

The firmware may only be installed and used on the hardware (SMART CONNECT KNX Remote Access) approved by the licensor.

14.4.5 Transfer to a third party

The SMART CONNECT KNX Remote Access software must not be passed on or made accessible to third parties.

14.4.6 Renting out, leasing out and sub-licensing

The Licensee is not authorised to rent or lease the SMART CONNECT KNX Remote Access software or grant sub-licences to the program.

14.4.7 Software creation

The Licensee requires written approval from the licensor to create and distribute software which is derived from the SMART CONNECT KNX Remote Access software.

14.4.8 The mechanisms of licence management and copy protection

The mechanisms of the licence management and copying protection of the SMART CONNECT KNX Remote Access software must not be analysed, published, circumvented or disabled.

14.5 Software development

The licensor is entitled to collect and process information about the parameterisation of the SMART CONNECT KNX Remote Access, providing that this information is collected in a manner that prevents any conclusions from being drawn about the identity of the licensee. This information is exclusively intended for the targeted development of the SMART CONNECT KNX Remote Access and the related provision of software updates and product support.

14.6 Property and confidentiality

14.6.1 Documentation

The SMART CONNECT KNX Remote Access software and its documentation (which shall be provided in printed format or also as online help or online documentation) are business secrets of the licensor and/or the object of copyright and/or other rights and shall continue to belong to the licensor. The Licensee shall observe these rights.

14.6.2 Transfer to a third party

Neither the software, the data backup copy nor the documentation (which shall be provided in printed format or also as online help or online documentation) may be passed on to third parties at any point in time – in whole or in part, for a fee or free of charge.

14.7 Modifications and subsequent deliveries

The SMART CONNECT KNX Remote Access software and the documentation (which shall be provided in printed format or additionally as online help or online documentation) shall be subject to possible changes by the licensor. You will find the latest software and documentation versions at www.ise.de.

14.8 Warranty

The SMART CONNECT KNX Remote Access software works together with software from third parties. No warranty is provided for software from third parties. For more information ► see Open Source Software, p.89.

14.8.1 Software and documentation

The SMART CONNECT KNX Remote Access software and the documentation (which shall be provided in printed form or additionally as online help or online documentation) shall be provided to the Licensee in the respective valid version. The warranty period for the SMART CONNECT KNX Remote Access software is 24 months. The licensor shall provide the following warranty during this time:

- The software shall be free of material and manufacturing defects when turned over to the customer.
- The software shall function as described in the documentation enclosed with it in its respective valid version.
- The software shall be executable on the computer stations specified by the licensor.

The warranty shall be fulfilled with the supply of spare parts.

14.8.2 Limitation of warranty

Otherwise, no warranty shall be provided that the SMART CONNECT KNX Remote Access software and its data structures are free from errors. Nor does the warranty cover defects due to improper use or other causes outside the Licensor’s control. Any additional warranty claims shall be excluded.

14.9 Liability

The licensor shall not be liable for damages due to loss of profit, data loss or any other financial loss resulting as part of the use of the SMART CONNECT KNX Remote Access software, even if the licensor is aware of the possibility of damage of that type.

This limitation of liability is valid for all the Licensee’s damage claims, regardless of the legal basis. In any case, liability is limited to the purchase price of the product.

The exclusion of liability does not apply to damage caused due to wilful intent or gross negligence on the part of the Licensor. Furthermore, claims based on the statutory regulations for product liability shall remain intact.

14.10 Applicable law

This agreement is subject to the laws of the Federal Republic of Germany.
The place of jurisdiction is Oldenburg (Oldb).

14.11 Termination

This agreement and the rights granted herein shall terminate if the Licensee fails to fulfil one or more provisions in this agreement or terminates this agreement in writing. In such a case, the supplied SMART CONNECT KNX Remote Access software and the documentation (which is provided in printed format or also as online help or online documentation), including all copies, must be returned immediately without the Licensor specifically requesting their return. No claim to reimbursement of the price paid shall be accepted in such a case.

The licence to use the SMART CONNECT KNX Remote Access software shall expire upon termination of the agreement. The SMART CONNECT KNX Remote Access product must be taken out of operation in such a case. Further use of the SMART CONNECT KNX Remote Access without a licence is forbidden.

The commissioning and visualisation software must be uninstalled and all copies must be destroyed or returned to the Licensor.

14.12 Subsidiary agreements and changes to the agreement

Subsidiary agreements and changes to the agreement shall only be valid in writing.

14.13 Exception

All rights not expressly mentioned in this agreement are reserved.

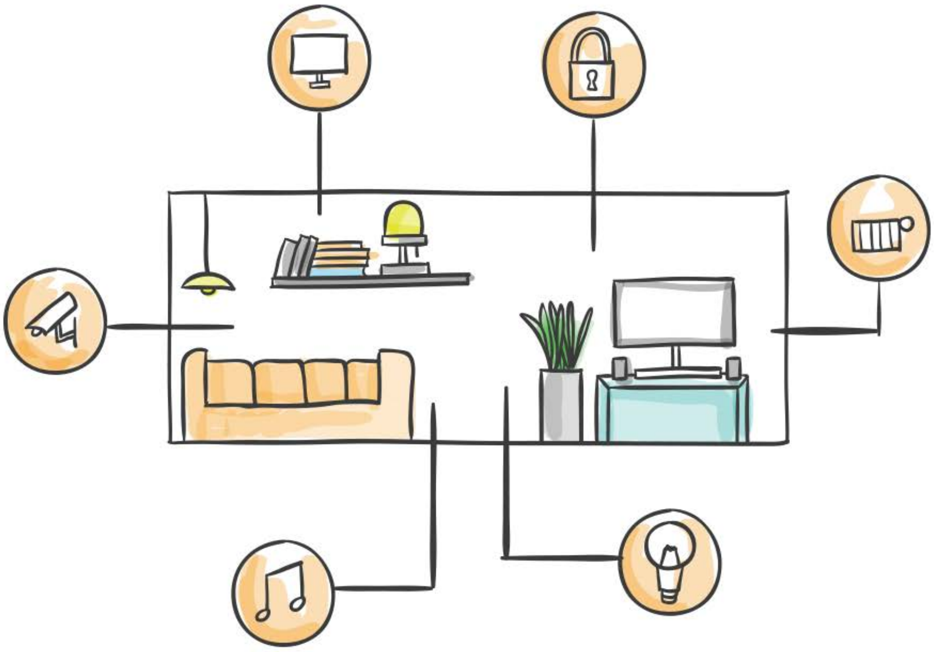
15 Open Source Software

This product uses software from third-party sources which are published within the framework of various Open Source licences.

The individual software packages used and their licences are listed and described on the device website for this product and can be accessed in the status bar.

The source code for the Open Source Software used in this product can be obtained by sending an e-mail to support@ise.de

This offer is valid for 3 years after the service for this product has been discontinued.



ise Individuelle Software und Elektronik GmbH
Osterstraße 15
26122 Oldenburg, Germany

Phone: +49 441 680 06 11
Fax: +49 441 680 06 15
E-mail: sales@ise.de