Documentation date:

19/06/2019

Product Manual

ISE SMART CONNECT KNX REMOTE ACCESS

Order No. 1-0003-004

Valid for application software v5.0, firmware version v5.0 and SDA client from version v1.6

Table of contents

1 Product description

1.1 Functions

- Secure data transfer from anywhere in the world to your home over the Internet, starting with the first data packet, thanks to the secure portal server https://securedeviceaccess.net
- Access to the HTML pages of each network end device (e.g. camera) as if you were at home
- KNX communication with the ETS via KNXnet/IP, IP direct download and Eiblib/IP using the SDA client for Windows
- Configuration access to the Gira HomeServer with the HomeServer Expert via the SDA client for Windows
- Access to Windows computers using the remote desktop connection through the SDA client for Windows
- Many other use cases using freely configurable TCP port forwarding through the SDA client for Windows
- Notifications can be triggered via KNX telegrams, saved on the server and forwarded via e-mail, voice call or text message.
- KNX/TP connection with integrated IP interface (tunnelling server) for KNX access using the ETS or other software (max. three simultaneous connections) for downloading and use of the group monitor and bus monitor
- Status signalling and access management of the secured connections through KNX communication objects
- Access functions even if the Internet access device does not have a unique Internet IP address, e.g. usually the case with UMTS and LTE
- No configuration necessary if DHCP is used
- An integrated Ethernet switch (two RJ45 connections) simplifies the connection of multiple IP devices. This enables multiple ISE SMART CONNECT KNX REMOTE ACCESSs or other IP devices in the distribution to be connected without the aid of other active components.
- Supports accelerated transfer from the ETS to the ISE SMART CONNECT KNX REMOTE ACCESS or other KNXnet/IP devices using the direct KNX-IP connection.
- Configuration of the ISE SMART CONNECT KNX REMOTE ACCESS is carried out using the latest version of the ETS4 or ETS5. The application accesses ETS functions not supported by earlier ETS versions. This is why previous versions of ETS cannot be used for configuration.
- ISE SMART CONNECT KNX REMOTE ACCESS can be used as a data logger. It incorporates a card reader for microSDHC cards up to 32 GB. The KNX EIB telegrams in an ETS4-compliant format can be recorded to the card for analysis purposes. The card memory can be used as a ring memory or as a ROM.
- As a clock, ISE SMART CONNECT KNX REMOTE ACCESS can send the time and date to the bus at configurable intervals. It is possible to trigger the sending of the current time and the current date via a trigger.

1.2 KNX Secure Ready

ISE SMART CONNECT KNX REMOTE ACCESS is prepared for KNX Secure. The necessary FDSK (Factory Default Setup Key) are located on the side of the device as a sticker and are also included within the device packaging. Devices without these stickers are not "Secure Ready".

For maximum safety, we recommend removing the stickers on the device.

You cannot restore the FDSK yourself.

- Keep the FDSK safe.
- If you lose the FDSK despite all care, please contact our support.

1.3 How does Secure Device Access work?

This section describes the mode of operation of the Secure Device Access infrastructure (abbreviated "SDA"). It presents the components which make up "Secure Device Access" and describes how these components work together so that you can access your home securely from anywhere.

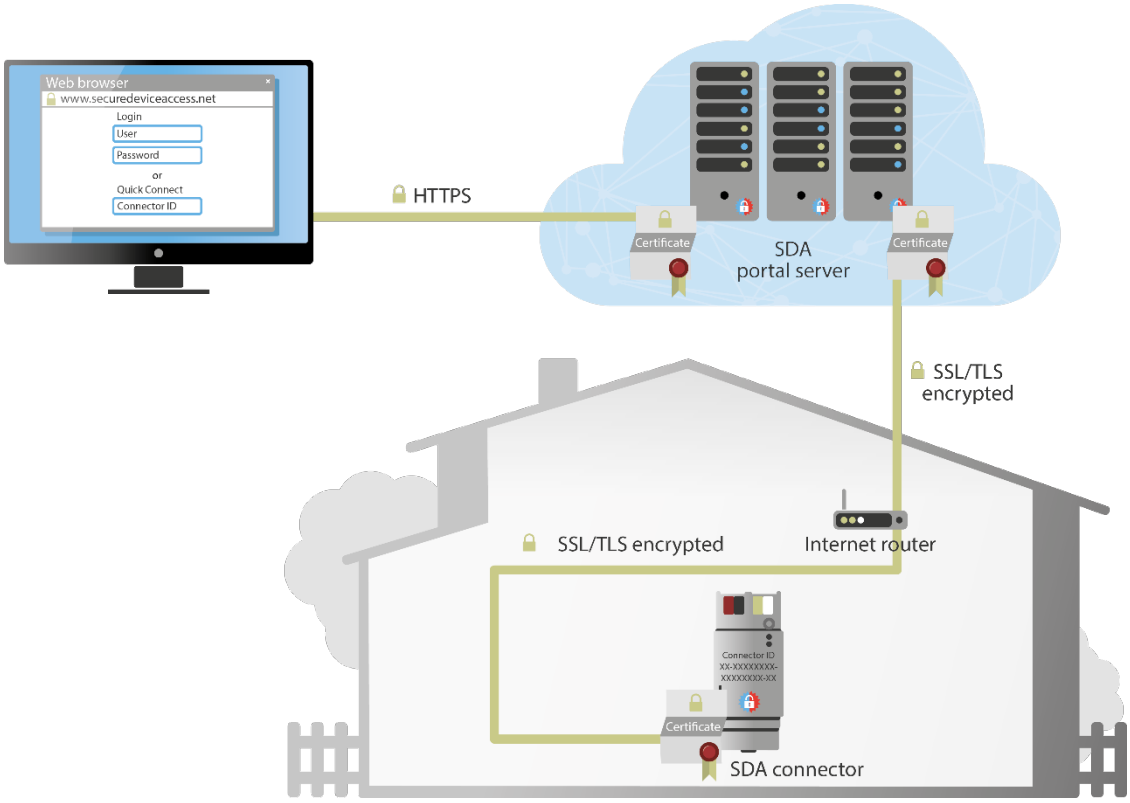


Figure 1: Overview of secure access with “Secure Device Access”

1.3.1 ISE SMART CONNECT KNX REMOTE ACCESS, "SDA connector" in general

The ISE SMART CONNECT KNX REMOTE ACCESS (referred to as the "SDA connector" in the following) is installed in your home and prepares your home network for secure access over the Internet.

The SDA connector is simply connected to the home network via Ethernet. It then connects to the SDA portal server automatically through your existing Internet access. Communication between the SDA connector and SDA portal server is encrypted as per AES and secured with digital certificates (for details, see Section 1.3.4 "HTTPS proxy httpaccess.net").

Depending on the network protocols supported by the respective device, access occurs directly through the SDA portal server or through the "SDA client" software available for Windows (see Section 1.3.7 "Client software (SDA client)").

If you have a KNX installation in your house, you can connect it to the ISE SMART CONNECT KNX REMOTE ACCESS using the KNX connection if desired. This enables you, or your electrical installer, to access your KNX devices from anywhere, e.g. with the ETS.

1.3.2 Quick Connect

Each SDA connector is provided with a unique cryptographically secure "registration ID" (previously called Connector ID) ex works. The registration ID is printed on the SDA connector and is linked to the actual device through a digital certificate.

Using the registration ID, you can access your end devices immediately after unpacking and connecting them without any additional logging in.

Part of the registration ID is randomly generated and therefore cannot be guessed. Whoever knows the registration ID of your SDA connector can access your devices. This could be an advantage or a disadvantage, depending on the application.

To prevent access via "Quick Connect," you can link your SDA connector to an account on the SDA portal server at any time. Access is then no longer possible via "Quick Connect" unless you enable this explicitly again.

1.3.3 SDA portal server

You can manage your SDA connector through the portal server (accessible under https://securedeviceaccess.net). Through the portal server, you can also provide access to your SDA connector, and thus to your KNX and network devices, to other users.

Any number of SDA connectors can be assigned to an account on the portal server.

If you or persons authorised by you wish to access end devices in your building, the portal server always plays the part of the exchange. The portal server does not save the transferred data, but only forwards them on.

We operate the server in Germany in compliance with the stringent European data protection guidelines.

Note: Use of the SDA portal server requires the use of cookies in the web browser for technical reasons.

1.3.4 HTTPS proxy httpaccess.net

Most network devices today, such as cameras and network printers, have an integrated web server for access with a web browser. Access through the SDA portal server is especially easy in such cases. Each network device which can be accessed via an SDA connector automatically receives its own name under the domain httpaccess.net. Using this name, you can access the corresponding network device from anywhere using a web browser.

Naturally, all of this communication over the Internet is also encrypted, and user authentication occurs according to the access authorisation set on the portal server for your SDA connector.

For your convenience, the SDA portal server manages a list of links of the end devices which are accessible via httpaccess.net. If the network device supports UPnP, which is often the case, the portal server can enter it automatically in the list of links.

1.3.5 Communication – Secure, reliable and easy-to-handle

For communication with the portal server, the SDA connector uses the popular standard protocols HTTPS, TLS/SSL and WebSockets.

All data are encrypted as per AES. Not a single bit of your data is transferred unencrypted.

The SDA connector and SDA portal server authenticate each other with digital certificates and RSA key pairs. The certificates are issued by our own certification office. This makes us immune to counterfeit certificates from the thousands of certification agencies around the world which pop up time and again.

By using standard protocols, and since the SDA connector actively connects to the SDA portal server, we achieve the best possible compatibility with the existing infrastructure. To your Internet router, communication of the SDA connector is no different from the encrypted connection of your web browser, e.g. for online banking or Google searches.

The advantage to you here is that the SDA connector functions easily without the need for complex configuration. Unpack it, connect it, you're done. This is a major advantage compared to other approaches to secure remote access, such as VPN and SSH tunnelling.

In contrast to other solutions, Secure Device Access can even be carried out over a mobile phone connection, even if it doesn't have a unique IP address which can be reached externally.

1.3.6 SDA notifications

KNX group objects and system events such as the logging in/logging out of an SDA connector to/from the portal can be used to generate messages in the portal server, i.e. so-called SDA notifications. In addition to static texts, they can also contain values from the KNX or even an attachment, such as a camera image.

These notifications can be configured for forwarding via e-mail, phone or text message.

Note: Attachments are limited to 250 kByte. A bigger data volume will not be transferred and no error message be sended.

1.3.7 Client software (SDA client)

The SDA client software (referred to as the SDA client in the following) is installed by you to your Windows computer. Through the SDA client, other applications running on your computer are able to access your devices without having to support the SDA protocol themselves.

The SDA client is currently available for Windows. Other platforms will follow.

The SDA client establishes an encrypted connection to the SDA connector via the SDA portal server. 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.

Depending on use case, the FDSK is required for initial authentication in the ETS or for the encryption of communication.

Examples:

- With the ETS, you can configure KNX devices via KNXnet/IP.
- With the GIRA HomeServer Expert, you can configure a HomeServer.
- You can access a Windows computer using a remote desktop connection.
- Using SSH and/or X Windows, you can access a Linux computer or embedded Linux devices.
- Through freely configurable TCP port forwarding, many other use cases are supported.

1.4 Definitions and explanation of terms

Connector ID

Former name of the registration Id (long or full connector ID) or remote access ID (short connector ID).

Secure Device Access, or SDA

Designates the entire system which provides secure access to your home over the Internet. See Section 1.3 "How does Secure Device Access work?."

Portal server, SDA portal server

Main server of the Secure Device Access infrastructure on the Internet. Accessible under https://securedeviceaccess.net. Using this server, you can manage access to your SDA connectors. See Section 1.3.3 "SDA portal server."

SDA connector, ISE SMART CONNECT KNX REMOTE ACCESS

The SDA connector is a small electronic device connected to your home network which links it to the portal server. See Section 1.3.1 "ISE SMART CONNECT KNX REMOTE ACCESS, "SDA connector" in general."

Registration ID

Each SDA connector has a unique registration ID (formerly called connector ID) printed on the device. This registration ID serves the following purposes:

- Secure access without having to log in to the portal (Quick Connect)
- Linking of an SDA connector to a portal account

The registration ID is random and cannot be guessed.

Remote access ID

Each SDA connector has a unique registration ID printed on the device. This registration ID consists of four blocks separated by a hyphen. Within the configuration, for example in the SDA or the Gira Project Assistant (GPA), a shortened variant of the registration ID is displayed. This shortened variant is called remote access ID and only consists of the first two blocks.

Quick Connect

Access to devices behind an SDA connector without having to log in to a portal by simply entering the registration ID. See Section 1.3.2. "Quick Connect." Quick Connect is the counterpart of Portal Connect.

Portal Connect

Access to devices behind an SDA connector after logging in to the portal. See Section 1.3.3. "SDA portal server." Portal Connect is the counterpart of Quick Connect.

SDA client

Computer software which enables other applications to communicate via SDA without their having to know anything about SDA.

Device, network device

A device with a network or KNX connection installed in your home which is to be accessible via SDA.

SDA notifications

A message system which saves messages generated by system events (e.g. logging in/logging out of an SDA connector to/from the portal) or KNX group objects and forwards them via e-mail, phone or text message as desired.

httpaccess.net

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

User name

User name for logging in to the portal server. The user name used for SDA is always an e-mail address.

Password

Password belonging to a user name for authentication via the SDA portal server.

Access group

You can enable your SDA connector for other people via the SDA portal server. You can assign these people to the "residents" and "installers" access groups. Using KNX buttons, you can grant or prohibit access separately according to the access group.

Installer

Access group for external service providers. Access is blocked from this group as standard.

Resident

Access group for house residents. Access is granted for this group as standard.

Home network

The computer network (Ethernet) in your home. Your network devices are connected to the SDA connector via the home network.

Remote access

Secure access to a device on your home network via the SDA portal server and an SDA connector.

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 security layer of HTTPS.

Data volume, traffic

Designates the user data volume transferred over the SDA portal server. Widely different volumes of data are transferred in different applications. KNX communication results in small data volumes, whereas live streaming from a webcam results in comparatively large data volumes. The volume of data transferred puts a strain on the SDA portal server. For this reason, there are different invoicing models for different applications with a limitation on the permissible data volume.

User role

A portal user has the role of either "user" or "administrator", depending on the SDA connector authorised for him/her.

A "user" may use the SDA connector to access the home network. An "administrator" is additionally able to authorise the SDA connector for other users, cancel authorisation and define user roles and access groups.

Owner

The "owner" of an SDA connector is the legally responsible person. The owner always has the "administrator" user role. Every SDA connector linked to a portal account has exactly one owner. The owner can be changed by "handing over the keys."

Handing over the keys

Designates the function of the SDA portal server for changing ownership of an SDA connector. This occurs on a regular basis when a new building installation is transferred from the installer to the owner, hence the term "handing over the keys." See also Section 3.10.1.

Authentication key

Authentication keys are used by software which wants to open an SDA connection, such as a visualisation, to authenticate itself with the portal. They are created explicitly by the user in the portal and are a "replacement," so to speak, for a portal user name/password so that a user never has to enter his or her personal login data into an application or even provide it to third parties. See also Section 3.9.3 "Authentication keys."

Local network

Designates the network containing the computer with which I want to access a device in my installation (see also "Remote network") via SDA. Access occurs either via the portal or the SDA client. In the case of KNX, this is the computer on which the ETS is started.

Remote network

This designates the network containing the SDA connector. SDA provides secure access to the remote network via the Internet using the SDA connector.

2 Application scenarios

2.1 Important general information

2.1.1 Quick Connect vs. SDA portal

The easiest and quickest usage type is Quick Connect. With Quick Connect, remote access of the installation occurs solely by entering the registration ID (see also Section 1.3.2 "Quick Connect") printed on the device. This has the advantage of not having to log a user into the portal. An example use case would be a ISE SMART CONNECT KNX REMOTE ACCESS at a construction site in connection with a UMTS/LTE router to be usable by all co-workers quickly and in an uncomplicated way.

All the access options (ETS, HTTP, HomeServer etc.) are available, regardless of whether Quick Connect or the SDA portal is used.

2.1.2 Limitations and authorisation of access rights via KNX communication objects

If the ISE SMART CONNECT KNX REMOTE ACCESS is added in an ETS project, its communication objects can be used to prohibit or grant access options via KNX, even at run-time. The access rights limitations defined via the KNX in the remote installation always outweigh the definitions in the portal. In this way, SDA remote access can be deactivated completely regardless of the settings in the SDA portal through the use of group telegrams. All communication to the SDA portal can be deactivated likewise through the use of group telegrams.

2.2 Access to websites on the remote network

SDA permits secure access to websites on the remote network. For this purpose, the unencrypted (HTTP) data on the remote network (see Figure 2) are transported to the SDA portal server via an encrypted SSL/TLS connection and then to the web browser via an HTTPS connection.

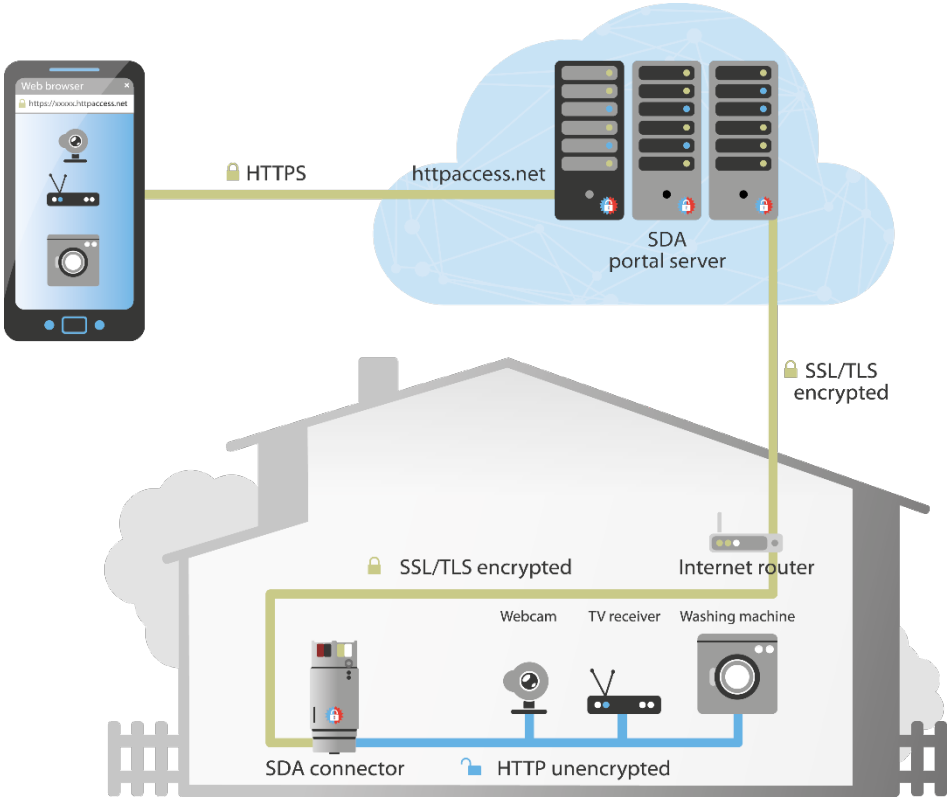


Figure 2: Secure access to websites via "Secure Device Access"

HTTP access to websites on the remote network is easiest through the SDA portal. Access via Quick Connect or Portal Connect is quickly configured here. A description of this can be found in Sections 3.2 "HTTP access via Quick Connect" and 3.5 "HTTP access via Portal Connect."

2.3 Access to KNX installations

The SDA client enables secure access to KNX installations over the Internet. For this purpose, the SDA client is installed to the computer and started parallel to the ETS. Since the KNX/IP protocol is completely unprotected today, the SDA connector transfers all KNX/IP data encrypted with SSL/TLS to the SDA portal server while it in turn exchanges the data with the SDA client with SSL/TLS encryption. The SDA client then provides the KNX/IP data for the ETS unencrypted locally on the computer with the ETS so that the ETS can be used completely transparently as usual.

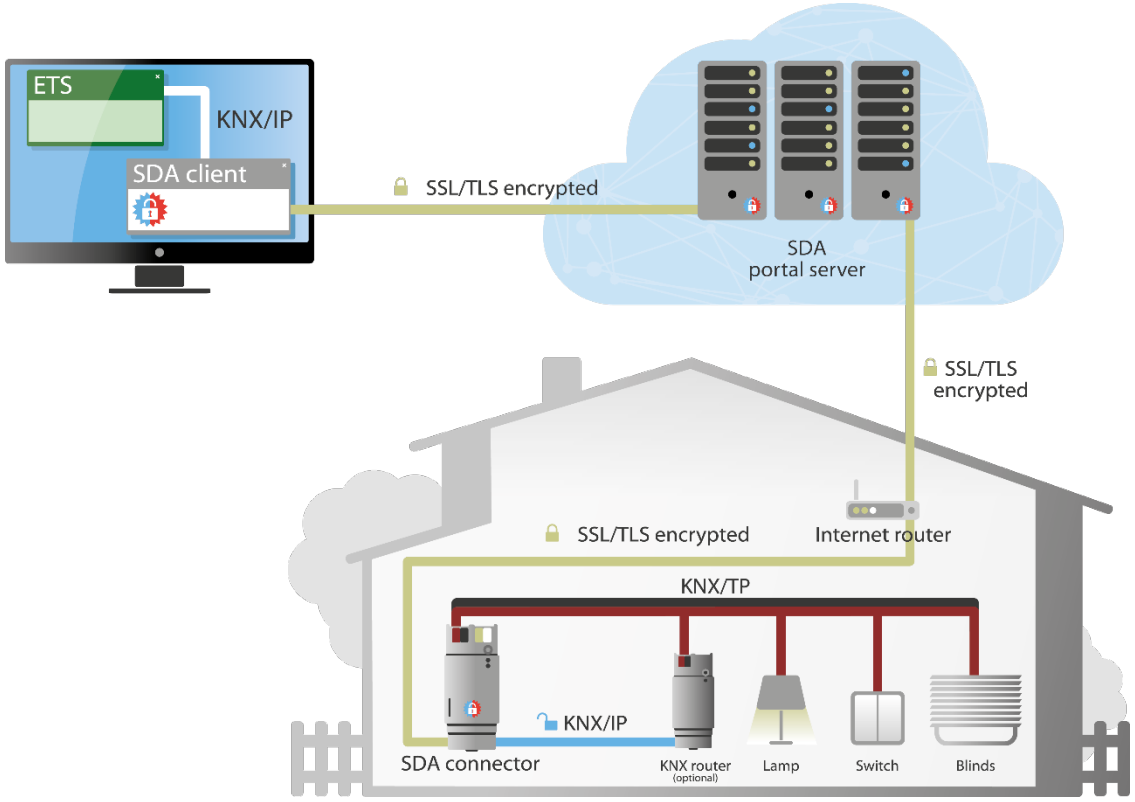


Figure 3: Secure access to the KNX installation via "Secure Device Access"

Once a connection to a specific SDA connector has been established using the SDA client (see Section 4.2 "Connecting to an SDA connection using the SDA client"), the KNX/IP interfaces available on the remote network appear in the ETS as if the ETS itself were on the remote network. To avoid mix-ups with other devices on your own network, it is possible to append text (e.g. "SDA –") to the device name normally displayed in the ETS. In addition, it is also possible to make available only the KNX/IP interface of the SDA connector for simplicity's sake. In addition to the KNX/IP interfaces, all devices which can be loaded directly via IP (see Section 9.3 "Accelerate transfer: Select transfer path *KNX-TP* or *IP*") are made known to the ETS so that these accelerated downloads also work via SDA. Additional information on this can also be found in Section 4.3. "Configuration of the access options of an SDA connector."

2.4 SDA notifications

SDA notifications were conceived for saving information from the installation, e.g. about KNX group objects, on the portal in a message database. System events, such as the logging in and logging out of an SDA connector to/from the portal can be recorded in this way.

An SDA notification possesses the following properties:

- Creation date
- Category ("System" or freely selectable text)
- Subject
- Contents
- Severity (low, high, alarm or system)
- Attachment (optional), such as an IP camera image

2.4.1 SDA notification via KNX

The database entry contains 50 KNX group objects for receiving values from the KNX 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 (e.g. limits or value ranges) in which notifications are to be created can be specified.

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.

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.

In addition, a web address can be specified for loading an attachment from a web server (e.g. IP camera) and attaching it to a message.

The concrete descriptions of these functions can be found in the parameter dialogue in the ETS.

2.5 Configuration of the Gira HomeServer

The Gira HomeServer is accessed in a very similar way to the KNX installation.

On the one hand, access to the KNX installation occurs through the Gira HomeServer using the Eiblib/IP protocol, and on the other, the configuration is supported with the Expert. All data are also encrypted upon transmission over the Internet here.

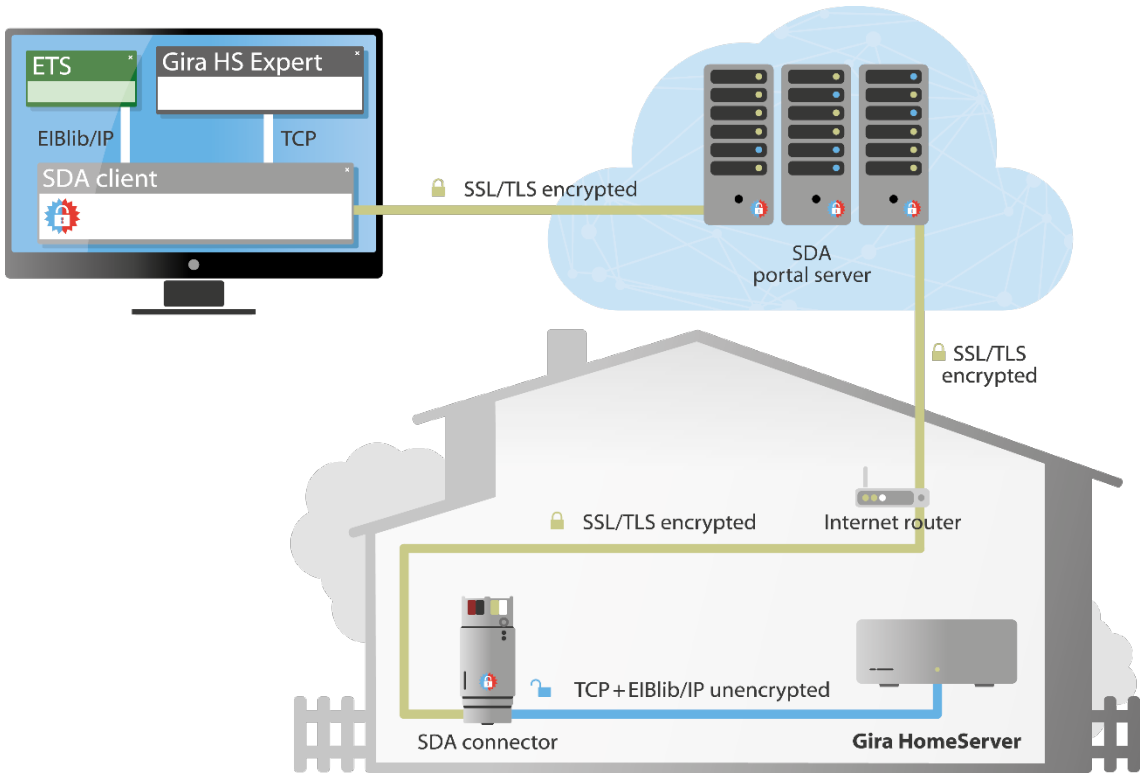


Figure 4: Secure configuration of the Gira HomeServer with "Secure Device Access"

Note: Since automatic detection is not possible for the Eiblib/IP and the HomeServer configuration protocol, the following must be observed for the use of these protocols via SDA: The SDA client makes available protocol transmission locally over IP address 127.0.0.1, i.e. if an Eiblib/IP connection is configured in the ETS for example, 127.0.0.1 (instead of the IP address of the Gira HomeServer on the remote network) must then be entered for the IP address for use via SDA. The same applies for downloading with the Expert. Additional information on this can be found in Section 4.3.2. "Remote configuration of Gira HomeServer and the use of Eiblib/IP."

2.6 Access through other TCP protocols

Using SDA, it is in principle possible to use nearly all TCP-based protocols securely over the Internet.

The Remote Desktop Protocol (RDP), among others, is widely used. Microsoft defined this protocol for remote access to Windows computers. Together with the SDA client, you can easily configure access. Additional information can be found in Section 4.3.3 "Using other TCP protocols via SDA."

Should you not have a protocol or not be sure about its proper use, please visit our forum or send an e-mail to our support team (support@ise.de).

2.7 User rights and access groups

Regardless of the access type, i.e. websites, KNX, HomeServer, remote desktop connection etc., access rights for the predefined access groups "residents" and "installers," as well as "Quick Connect," can be configured for each relationship between the SDA connector and portal user and controlled dynamically using KNX communication objects.

A typical scenario after handing over the keys could look like this:

- With the SDA connector, one or more portal users of my electrical trade company/system integrator are linked in the role of the "installer" for maintenance purposes.
- With the SDA connector, one or more portal users are linked in the role of "resident" (typically all family members) for visualisation on a smartphone and website access.
- The SDA connector is configured using the parameters in the ETS in such a way that the users with the "residents" access group always have access; in addition, the users of the "installers" access group do not have access as standard.
- If the installer wants to access the system for a maintenance appointment or due to a call from the home owner, he/she contacts the home owner. The home owner then gives the installer access by authorising access in his/her visualisation or using the corresponding communication object. Automatic deactivation of access after a certain period of time is also easy to arrange using logic.
- For security-sensitive residents, it is also possible to deactivate SDA access completely using a button or visualisation. The SDA connector then no longer reports to the portal, and remote access is impossible.
- The SDA connector indicates connection establishment via SDA using KNX communication objects to make appropriate processing in a visualisation/logic (e.g. e-mail when someone connects) easily possible.

In addition, software access (e.g. visualisations) can be controlled using authentication keys. Each user can create any number of these keys for each SDA connector to which he/she has access, e.g. for visualisation (see Section 3.9.3 "Authentication keys").

3 Usage of the SDA portal server

The portal server can be reached under the secured address https://securedeviceaccess.net.

3.1 Start page

Using the start page of the portal, you obtain corresponding access to configuration settings and websites on the remote network by entering a user or registration ID (text field “connector ID”).

Specifically, the page offers the following functions:

- Login with a user already registered with the portal.
- Registration of a new user for initial login.
- Use of HTTP access via Quick Connect with the registration ID printed on the device.

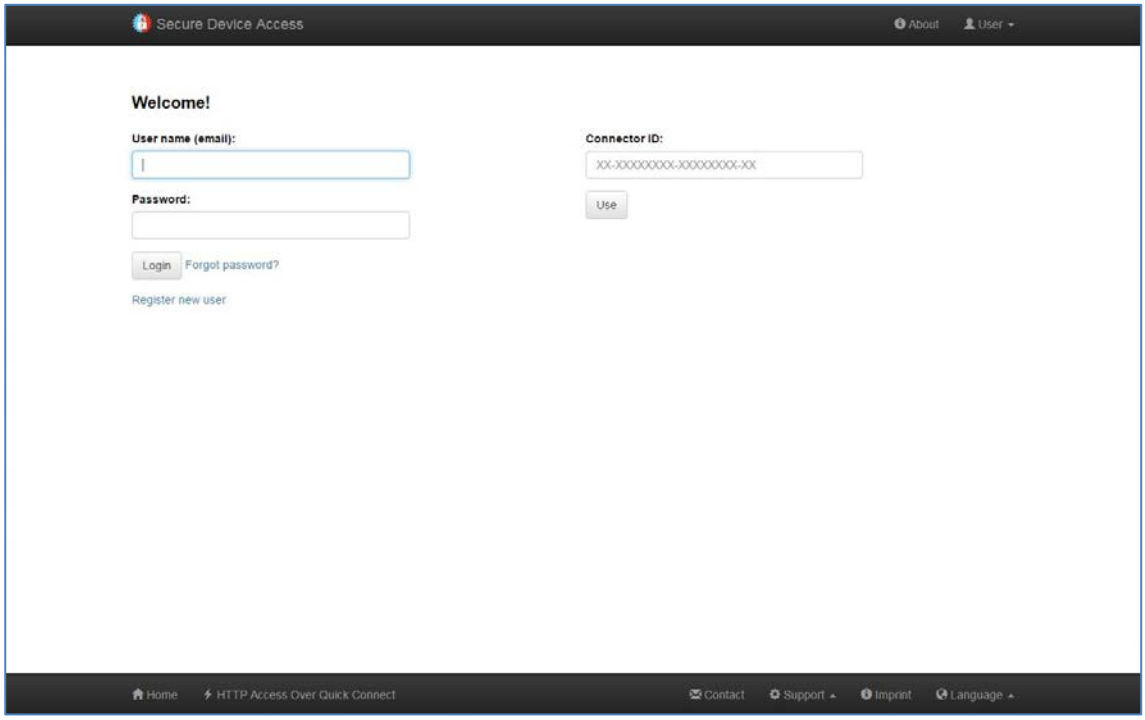


Figure 5: SDA portal – Start page

3.2 HTTP access via Quick Connect

If you decide on use via Quick Connect, you can use the SDA portal without logging in a registered user to visit websites of devices on the remote network.

After entering the registration ID (text field “connector ID”) on the start page and pressing the "Use" button, you are brought to a page which temporarily saves the links to devices in the installation which have just been used. In addition, you can search for devices on the remote network using the "Find devices" button. A link is automatically created for each found device here. Most devices, such as printers, DSL routers, IP cameras, all products of the ISE SMART CONNECT series and lots more are included here. In technical terms, the Simple Service Discovery Protocol (SSDP for short) is used here.

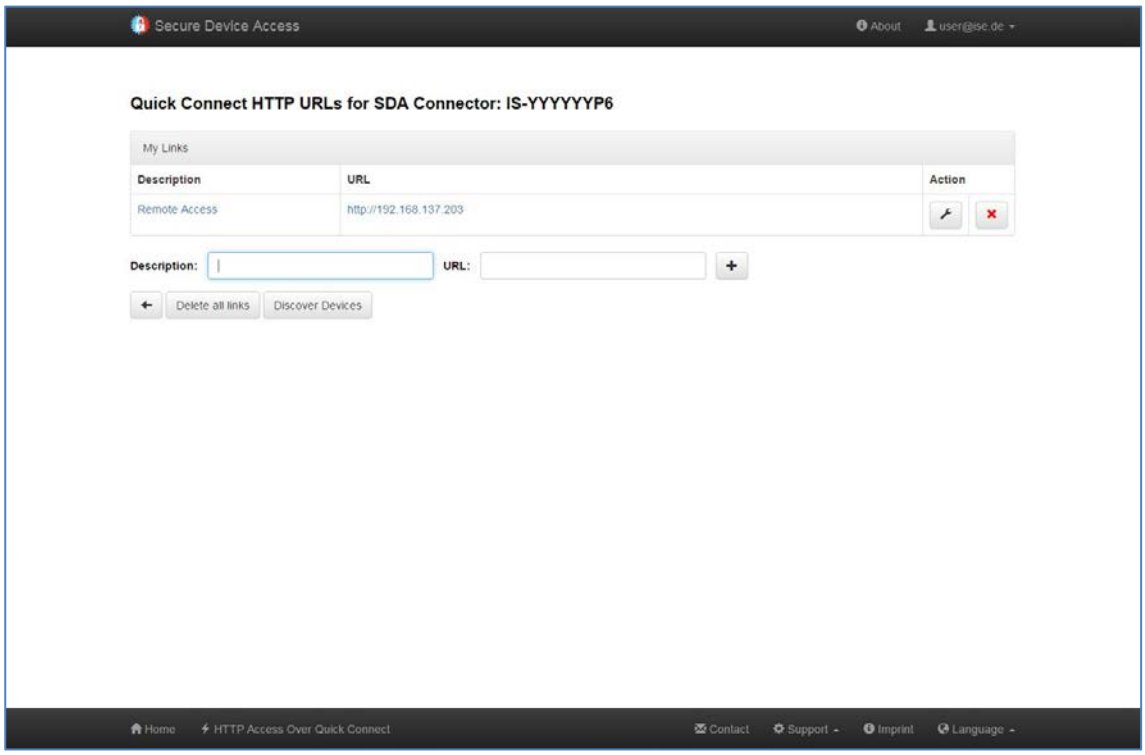


Figure 6: Access to HTTP websites via Quick Connect

You can enter an HTTP path in the remote network manually in the "URL" field (e.g. "192.168.1.200/index.html") along with a description of the link so that you always have quick access to your devices.

Not all websites can be loaded from the remote network via SDA. More complex pages, in particular, may not function. In such cases, we ask that you send an e-mail to our support team (see Chapter 12 "Troubleshooting and support") with a precise description of the product, screen shots and a brief error description.

The following actions are available for created links:

Action	Description
	Edit the URL
	Delete the link

3.3 User registration

If you do not wish to work with Quick Connect, you can register as a user with the SDA portal. This is either required or very helpful, in particular in cases where you would like to grant user rights differently to different people or allow access to your network via the ISE SMART CONNECT KNX REMOTE ACCESS by several people.

Registration is carried out using the currently common standard of e-mail address verification. A link in an e-mail automatically sent to the specified e-mail address after the start of registration must be confirmed. This ensures that login is not possible from an unauthorized e-mail address. The procedure is automated so that it only takes a few minutes.

3.4 SDA connector management

After successful user registration and login to the SDA portal, you will see the list of all devices linked to your user. It is usually empty for the first login.

You can be linked to a device in the following ways:

1. Using the operating elements below the list of your devices, you add a new SDA connector via the registration ID (text field “connector ID”) and thus become the owner (for important notes, see Section 3.11 "Owners and transfer of ownership").
2. Another user gives you access rights on an SDA connector which is administered by the other user.
3. Another user transfers ownership to you (for important notes, see Section 3.11 "Owners and transfer of ownership").

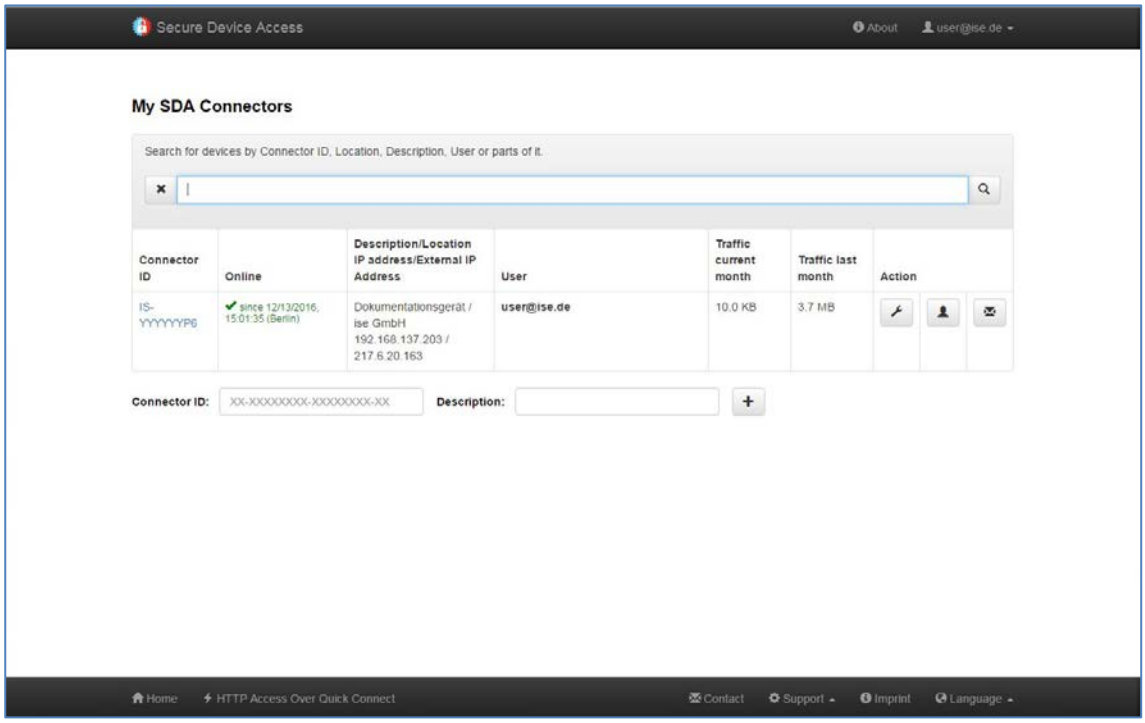


Figure 7: SDA connectors of the logged in user

In the list of SDA connectors linked to your user, you can access websites on the remote network using the links after the corresponding SDA connector in the "Remote Access ID" column.

In the "Online" column, you receive information on the current connection status of the SDA connector. The time specification is displayed in accordance with the time zone setting of your user. If the device is currently not logged in to the portal server, i.e. it is "offline", the text appears in red. Otherwise, it is green.

The "Location/Description" column contains text fields which are filed in as desired by the user. The location is a property on the SDA connector and is thus the same for all users. The description text can be filled in as desired by any user linked to the SDA connector. This enables an installer, for example, to specify when the owner is entered as the "At home" location after the address is transferred.

The owner and administrators see all users linked to the device in the "User" column. A normal user does not see the other users for data protection reasons. When a device is linked to a user for the first time, this user is the owner (see Section 3.11 "Owners and transfer of ownership").

The owner is always shown in **bold**.

The following two columns show the previously used data volume for the current month and the previous month. For information on the data volume available and the usage conditions, see Chapter 13 "ISE SMART CONNECT KNX REMOTE ACCESS software licence agreement."

Up to five actions can be available (depending on the user rights):

Action	Description
	Display and change properties and expanded information of an SDA connector (see Section 3.6 "More detailed information on an SDA connector" and Section 3.7 "Displaying and changing properties of an SDA connector")
	Manage access rights for other users (see Section 3.9 "Managing access rights for users")
	View and manage SDA notifications (see Section 3.10 "SDA ")

3.5 HTTP access via Portal Connect

Access to remote websites via SDA with a logged-in user (Portal Connect) essentially corresponds to access via Quick Connect in terms of functionality (see Section 3.2). "HTTP access via Quick Connect."

It is possible, however, to deactivate the "Discover Devices" function for users without administrator rights here. See also Section 3.9 "Managing access rights for users" for this.

3.6 More detailed information on an SDA connector

The portal server retains information on a logged in SDA connector which is very important for diagnosing problems, in particular.

This includes:

- The registration ID
- The IP address of the SDA connector on the remote network
- The Internet IP address over which the SDA connector communicates with the portal. This is the external IP address of the Internet gateway, e.g. your Fritz!Box
- The SDA software version (also called the SDA service version) currently running on the SDA connector

3.7 Displaying and changing properties of an SDA connector

This page displays detailed information on the SDA connector. Using the button, the complete registration ID can be made visible. You can then copy it to the clipboard with the button.

The location and Quick Access can also be changed for the SDA connector if the logged-in user has access rights for this. The automatic creation of SDA notifications when logging in/logging out the SDA connector or SDA client can also be activated.

Handing over the keys serves to transfer the owner (see below), e.g. when transferring from the craftsmen to the owner and for deleting a connector from the portal. This function only makes sense if the SDA connector is sold, as all user rights etc. are irreversibly removed.

This is not possible as long as you are the owner of the SDA connector!
See also Section 2.7 " User rights and access groups."

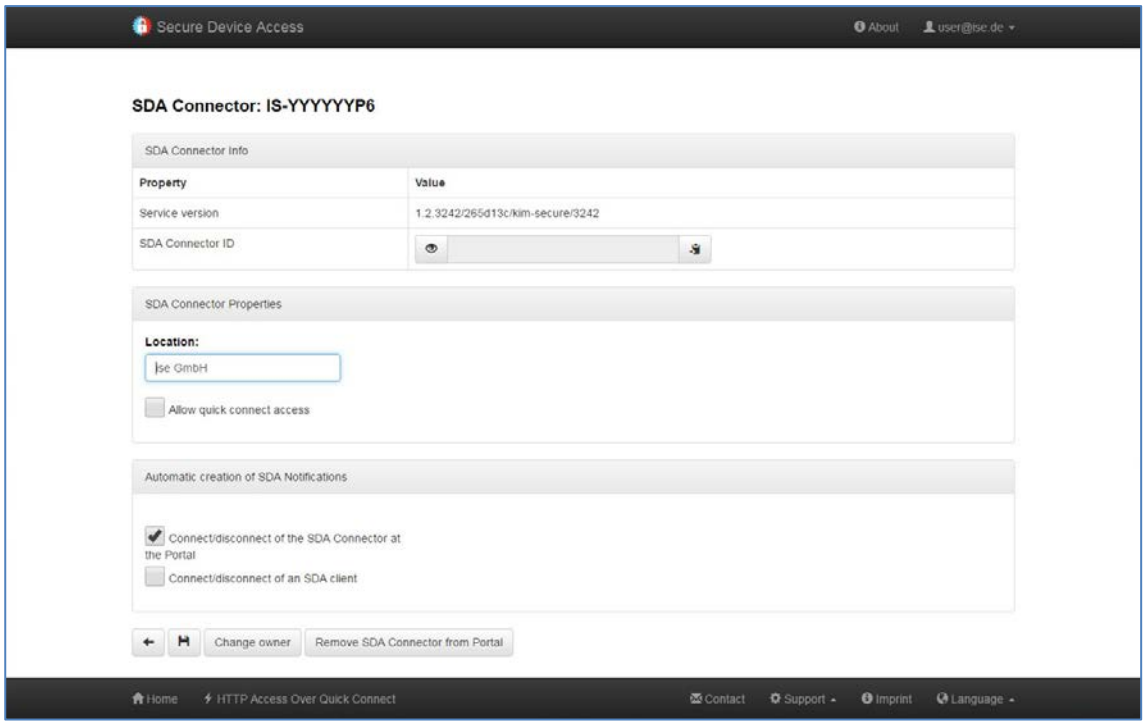


Figure 8: Displaying and changing properties of an SDA connector

3.8 Managing access rights for users

The SDA portal enables differentiated configuration of access rights based on users for each SDA connector.

The following can be defined for each user (if the currently logged in user possesses the corresponding rights):

User	Description
Role	Possible options here include "owner", "administrator" and "user", whereby the owner is an administrator with a special position (see Section 3.11 "Owners and transfer of ownership"), which is why only administrators and users are referred to in the following (see below).
Access groups	Possible options here include "residents" and "installers," whereby a user can optionally be assigned to neither of the groups or even both groups (see below).

Besides the addition of new users to an SDA connector, user rights can of course also be restricted again and the connection of an SDA connector to a user can also be fully deleted.

The rights of users without administrator rights can be restricted for SDA notifications and the "Discover Devices" function.

In addition, the logged-in user can manage his/her authentication key here. These keys are used as SDA login information, e.g. by visualisations together with the remote access ID, so that the user's own information does not need to be forwarded.

Owners and administrators may have the right to make configurations for other users or to restrict them. Figure 9 shows the actions:

Action	Description
	Edit user
	SDA notifications forwarding rules
	Rights
	Authentication key
	Delete

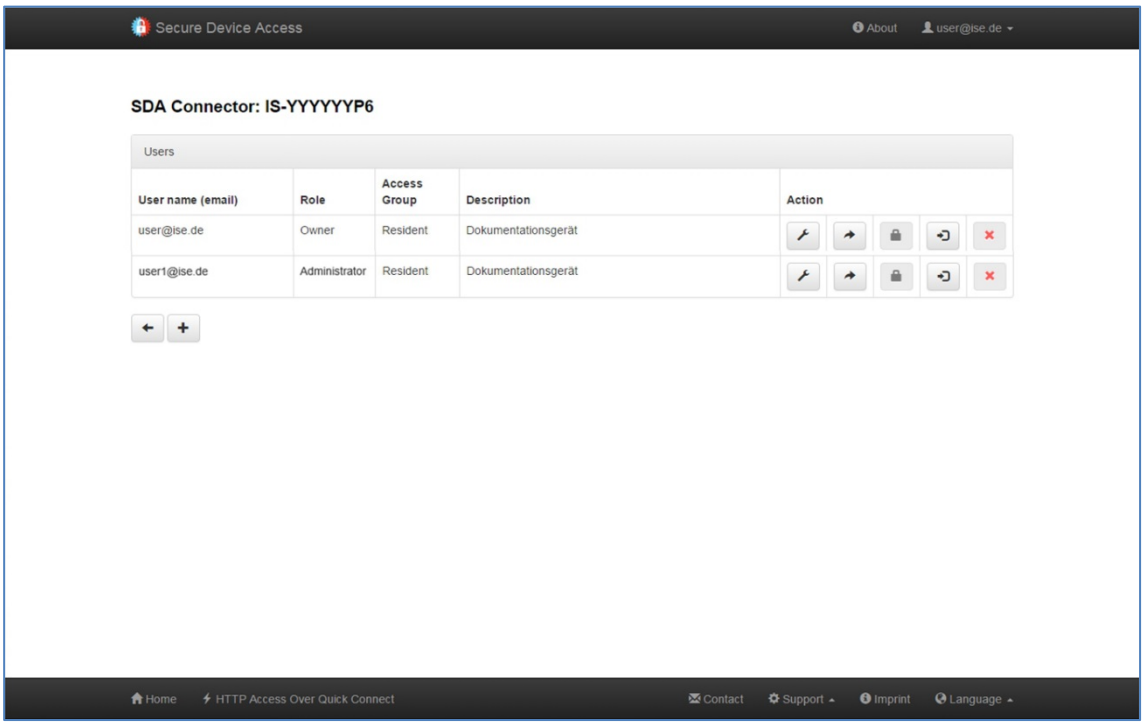


Figure 9: Managing access rights for users

3.8.1 The role of a user on an SDA connector

The difference between an administrator and user lies in the right to make changes to configurations on the SDA portal. Any administrator can manage all the properties and user rights for the SDA connector (except for ownership). The user can at most view the properties.

For a user without administrator rights, you can configure whether the user is able to search for devices (see Section 3.5 "Managing access rights for users").

The role of a user in connection with an SDA connector is solely based on the configuration options on the SDA portal and has absolutely nothing to do with the access rights to the remote network via SDA! Only the access groups are used for this purpose (see Section 3.9.2 "The access groups of a user on an SDA connector")!

3.8.2 The access groups of a user on an SDA connector

Using the access groups, it is possible to grant access to the remote network permanently or temporarily based on groups. Using KNX communication objects, residents and installers can be activated or deactivated for both groups at any time. In addition, Quick Connect can be activated and deactivated via the KNX. For this purpose, please read Chapter 8 "Configuration in the ETS."

The access groups of a user in connection with an SDA connector are solely based on the right to access the remote network via SDA, for example to visit websites or to access the KNX installation with the ETS. If you would like to change the configuration options on the SDA portal for a user, use the roles for this purpose (see Section 3.9.1 "The role of a user on an SDA connector")!

3.8.3 Authentication keys

Software access (e.g. visualisations) can be controlled using authentication keys. Each user can create any number of these keys for each SDA connection to which he/she has access, e.g. for visualisation.

For each generated key, there is a text field which describes the use of the key. The keys can be deleted again at any time (e.g. if a smartphone is lost). The same key is never generated twice, meaning that a lost key becomes irreversibly unusable upon deletion.

To facilitate the setup of an application for the use of an authentication key, an activation key can be generated via the button. This can be used by the application to transfer the associated authentication key from the SDA portal to the application. An activation key is valid for a maximum of 24 hours and can be used as often as you like. The automatic deactivation of the activation key takes place at the time specified in the “Date end activation” column. It is recommended to deactivate an activation key manually upon completion of the application setup via the button in order to prevent possible misuse. Since the activation key is considerably shorter than an authentication key, an activation key is more vulnerable.

The following actions are available for created authentication keys:

Action	Description
	Authentication key display
	Generation of an activation key for the authentication key
	Removal of an activation key for the authentication key
	Copying of the authentication key to the clipboard
	Deletion of the authentication key

3.9 SDA notifications

The letter icon () brings you to the notification list of a connector. All notifications are displayed sorted chronologically. Any attachments, such as camera images, can be opened directly via a link.

These notifications can also be forwarded according to configurable rules (see Section 3.10.1 "Forwarding rules for SDA "). Using the delete action (✖), rules can be deleted.

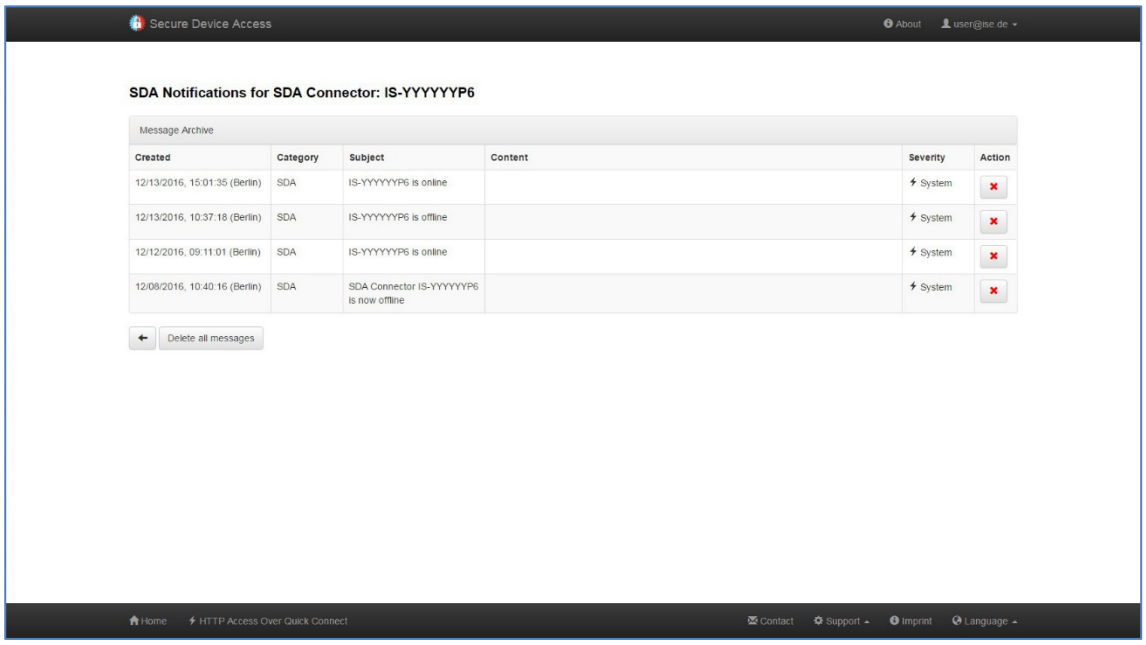


Figure 10: SDA notifications

3.9.1 Forwarding rules for SDA notifications

As an administrator, you can specify the forwarding rules for SDA notifications. You can access the corresponding selection by selecting the forwarding rules action (➦) in the user overview (see Section 3.9 "Managing access rights for users").

The SDA notifications can be forwarded in different ways when created, namely via:

- E-mail (default is the user ID of the portal; multiple addresses can be specified)
- SMS (uses sms77.de as the provider; multiple addresses can be specified)
- Telephone voice call which reads the SDA notifications aloud; available in many different languages (uses sms77.de as the provider)
- IFTTT, Maker Channel (uses IFTTT.com; for experienced users only)
  see Section “Using SDA notifications as triggers in IFTTT”, p. 28

For the use of functions based on sms77.de or IFTTT, a separate account must be set up at sms77.de. The corresponding access data must be stored in the "External Services" menu item for the user-specific data!

Each forwarding rule makes it possible to select and forward SDA notifications according to their severity and/or category (text filter; if it contains at least one word, the filter condition is fulfilled).

Any number of forwarding rules can be configured, and all the active ones can be evaluated upon receipt of an SDA notification. The deactivation option makes it possible to create rules which are required more often, but not always, e.g. only when you are on holiday.

Example: You want all notifications of the category "SDA" and the severity "System" to be forwarded to you via e-mail (including e.g. the online/offline messages). For this purpose, carry out the following:

- Add a forwarding rule.
- Deactivate all severity levels except "System."
- Activate "Category forwarding" and the input of "SDA" in the text field which is then activated.
- Activate "Email forwarding." Your SDA user ID appears as the default value. You can also configure e-mail for the reception of forwarded notifications.
- Save the forwarding rule. It is activated automatically.

The SDA notifications generated by the system, e.g. for online/offline status of the SDA connectors, are always generated with the "System" severity and "SDA" category. All severities up to "System" and any categories can be used when SDA notifications are used via KNX objects.

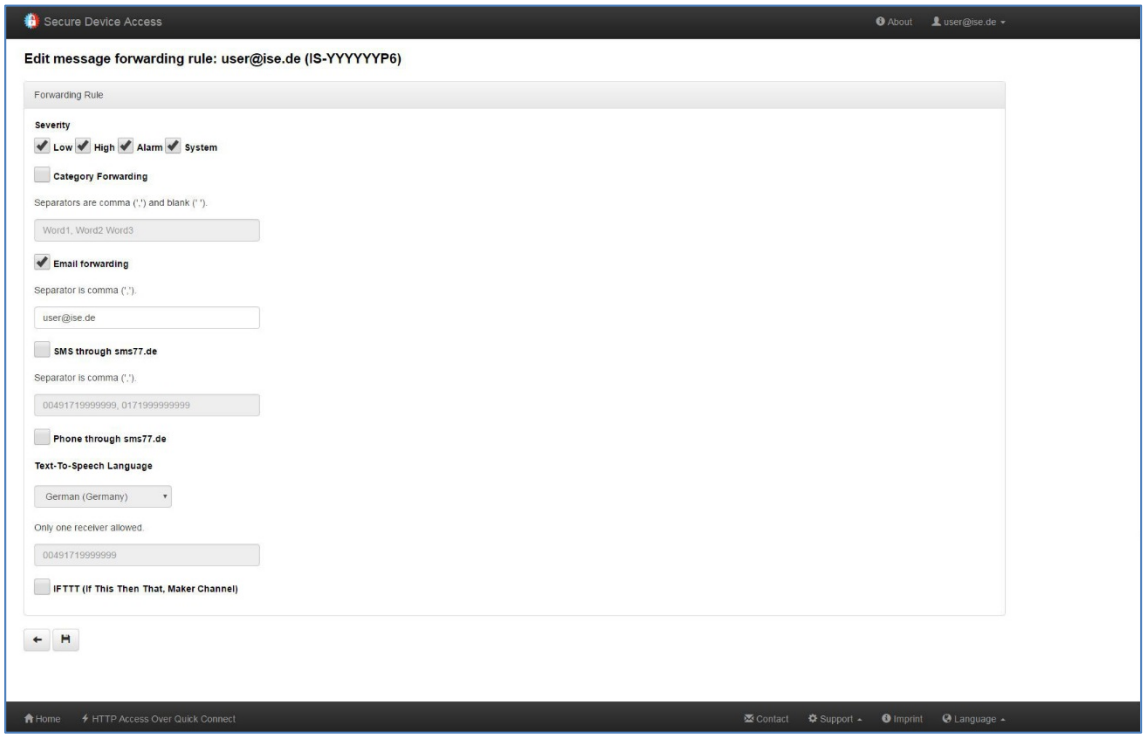


Figure 11: SDA notifications – Forwarding rules

3.9.2 Using SDA notifications as triggers in IFTTT

SDA notifications can be forwarded to IFTTT. These SDA notifications then serve as a trigger in IFTTT. SDA notifications cannot be used as an action.

The description of the IFTTT concepts is not part of this documentation.

To forward SDA notifications, you can define an unlimited number of forwarding rules in the SDA portal. You can configure forwarding to IFTTT for each of these forwarding rules.

IFTTT does not know the individual forwarding rules from the SDA. Every forwarding rule that is configured for the IFTTT is therefore linked to the same trigger (event name = sda_notification).

Procedure:

1. Link IFTTT with the SDA portal.
2. Create forwarding rules in the SDA portal and configure them for IFTTT.
3. Create an applet in the IFTTT portal and use the SDA notifications as triggers.

Linking IFTTT with the SDA portal

Configuration instructions in IFTTT are subject to change. IFTTT is not a product from ise Individuelle Software und Elektronik GmbH. We do not guarantee the topicality or accuracy of documentation for third-party products.

1. Determine IFTTT API key:
    a. Log in to the IFTTT portal.
    b. Enter <<Webhooks>> in the search box.
    c. Select the Service Webhooks tile.
    The Service Webhooks page will open.
    d. Select the <<Connect>> button.
    e. Select the <<Settings>> button (top right).
    f. The API key is part of the URL. Copy the last part of the URL (everything after “use/”)
2. Enter the API key in the SDA portal:
    a. Log in to the SDA portal.
    b. In your user drop-down list on the menu bar, select the entry <<External services>>.
    c. In the section <<IFTTT (If this then that) login data >> enter the IFTTT API key in the <<API Key>> field.
    d. Select the button (save).

Example 1: IFTTT-URL

Displayed URL: https://maker.ifttt.com/use/wBXU7D6GY5SjAjilFf8r9

API key: wBXU7D6GY5SjAjilFf8r9

Creating forwarding rules in the SDA portal and configuring them for IFTTT.

1. Log in to the SDA portal.
2. In the drop-down list in menu bar, select the entry <<My SDA connectors>>.
3. Select the action (user) in the desired device line.
4. Select the action (forwarding rules) in the desired user line.
5. If required, create a new forwarding rule or edit an existing one.
6. Configure the forwarding rules as usual.
7. To activate IFTTT, select the checkbox <<IFTTT (If This Then That, maker channel>>.
8. Select the button (save).

Creating an applet in the IFTTT portal and using the SDA notifications as triggers

Configuration instructions in IFTTT are subject to change. IFTTT is not a product from ise Individuelle Software und Elektronik GmbH. We do not guarantee the topicality or accuracy of documentation for third-party products.

1. Log in to the IFTTT portal.
2. Create a new applet:
    a. Select <<My Applets>> from the menu.
    b. On the <<Applets>> page, select the <<New Applet>> button.
    c. Start the configuration of this service by selecting the blue text “+ this”.
    d. In the <<Choose a service>> step, search for <<Webhook>>.
    e. Select the Service Webhooks tile.

    The Service Webhooks page will open.
    f. In the <<Choose trigger>> step, select the tile <<Receive a web request>>.
    g. In the <<Complete trigger fields>> step, enter the following text accurately as <<Event Name>>: sda_notification

    The SDA notifications are configured as triggers.

    Now configure the desired action as usual.

3.10 Owners and transfer of ownership

From the moment when an SDA connector is not used solely via Quick Connect, but instead is added to a user using the portal for the first time, the SDA connector has an owner. From that point on, there is always exactly one owner. The owner is always displayed in **bold** in the display of users which are connected to the SDA connector.

The owner is the person who is legally responsible for the use of remote access. At the time of building, this is usually the electrical installer or system integrator. When the keys change hands to the owner of the installation, ownership is usually transferred.

The owner of an SDA connector can take away all rights of all other users, including other administrators, at any time, whereas no-one can refuse access to him/her.

Should the SDA connector or SDA access be misused with regard to the licence agreement or other legal regulations (violation of data protection or personal rights by cameras etc.), the owner is liable at first instance.

Ownership can be transferred in the SDA portal. The "Hand over the keys" button on the page for displaying and changing the SDA connector properties is provided for this purpose. The owner is changed using a secure procedure:

1. The current owner presses the "Hand over the keys" button, enters the user name of the desired new owner and submits the request.
2. The desired new owner receives an e-mail containing a link for accepting the transfer of ownership. For security purposes, the same applies for the current owner.
3. When the desired new owner and current owner have accepted the request, both receive a corresponding e-mail and ownership is transferred.

If the request is not confirmed by the desired new owner or the current owner, ownership is not transferred.

4 Usage of the SDA client

The SDA client is an application which is installed on a computer with which devices on the remote network are to be accessed securely over the Internet if the HTTP protocol is not used. The SDA client is not required for accessing websites on the remote network with a web browser. See Section 2.2 "Access to websites on the remote network."

The most typical applications for the SDA client include

- Accessing KNX installations via the KNX/IP or Eiblib/IP protocol
- Configuring a Gira HomeServer with the Expert

In addition, SDA supports the use of many other TCP-based IP protocols such as the Remote Desktop Protocol (RDP) from Microsoft for remote access to a Windows computer.

The SDA client is currently available for Microsoft Windows versions 7 and up.

You can find the current version of the SDA client installation application under https://www.ise.de/en/products/ise_smart_connect_KNX_Remote_Access under Downloads.

4.1 General settings

To open the general settings, use the button “gear” (top right, see "Figure 12: SDA client", (1)).

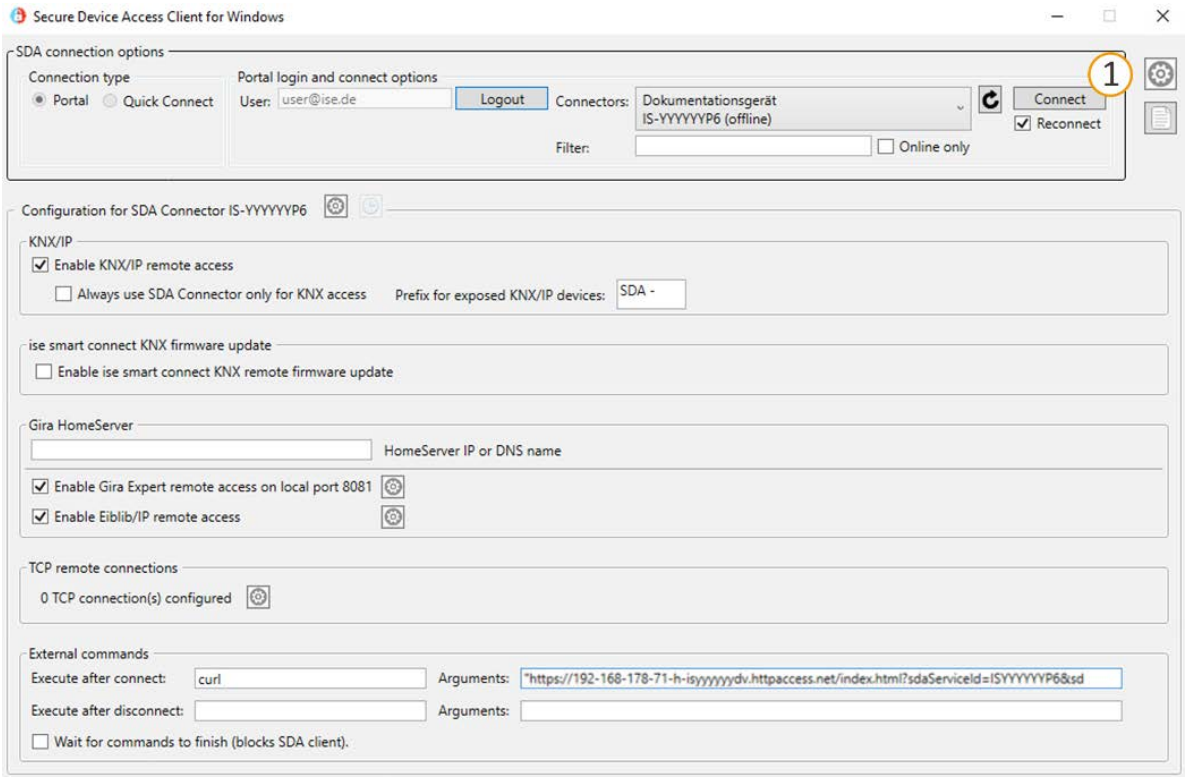


Figure 12: SDA client – Open the general settings

In the general setings you can activate expanded logging for troubleshooting if problems occur. You can also delete the log files or create a ZIP archive of them which can then be attached to an e-mail should support be required. In addition, you can specify whether the SDA client should remember the last password used

Table 1: General settings - details about specific options

Option	Description
Enable ETS access for complete LAN (otherwise for this PC only)	Defines for which clients all KNX/IP devices are available that can be accessed remotely via ISE SMART CONNECT KNX REMOTE ACCESS. The client is the PC running your ETS. The PC is identified by its IP address. The KNX/IP devices are displayed in the ETS under <<Discovered Interfaces>>. To find these KNX/IP devices faster in the ETS, you can define a prefix for their names (area <<KNX/IP>>> setting <<Prefix for exposed KNX/IP devices>>). • Activated: All clients running in the same local network have access to the KNX/IP devices. • Deactivated: The KNX/IP devices are only available for the current client. The setting wil be used the next time you connect to the SDA Connector (button <<Connect>>>).
Enable Gira HomeServer secure remote access features by default for new SDA Connector configurations	Activate Gira HomeServer support for new SDA connector configurations as standard (see following sections). This makes sense if you use the Gira HomeServer in your projects on a regular basis.
Connection timeout	Connection timeout for the connection to the SDA portal. 3 seconds is a good value for both a normal Internet connection from home or the office and frequently for mobile Internet connections of 3G and up as well. Should you wish to use SDA with a slower Internet connection from time to time, however, you can increase the timeout value.
Check ETS4 version	Due to possible limitations when using the automatic search function of the KNX/IP connections with ETS versions older than ETS4.2, it is also possible to run a compatibility check with ETS4 here. See also Section 4.3.1 "Access to a KNX installation via KNX-IP" for this.

4.2 Connecting to an SDA connection using the SDA client

There are two options for establishing a connection to an SDA connector: Quick Connect (see Section 1.3.2. "Quick Connect") and Portal Connect (see Section 1.3.3. "SDA portal server").

For this reason, you first select the connection type after starting the SDA client.

4.2.1 Establishing a connection via Quick Connect

Select "Quick Connect" as the connection type (see Figure 13). Then enter the registration ID in the ”connector ID” field. If you would like to use an SDA connector which you have already used at an earlier point in time with Quick Connect, you can also select it from the list.

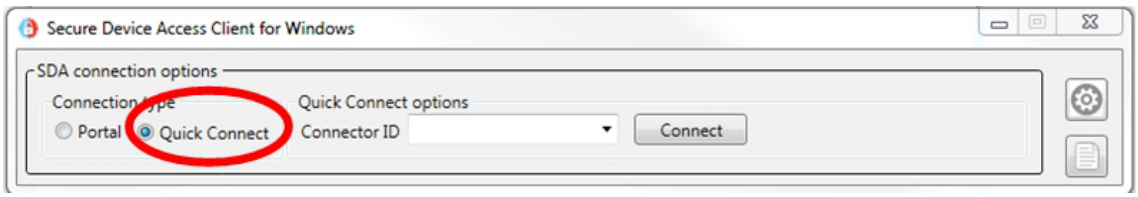


Figure 13: Connecting SDA connector via Quick Connect

After entering a valid registration ID, its configuration will appear. If the SDA connector is being used with this client for the first time, a default configuration is created.

Once you have adjusted the configuration to suit your applications (see Section 4.3 "Configuration of the access options of an SDA connector" ff.), you can establish the connection using the "Connect" button.

4.2.2 Establishing a connection via Portal Connect

Select "Portal Connect" as the connection type (see Figure 14). Then enter your portal user name (**Note:** This is always an e-mail address) and the associated password.

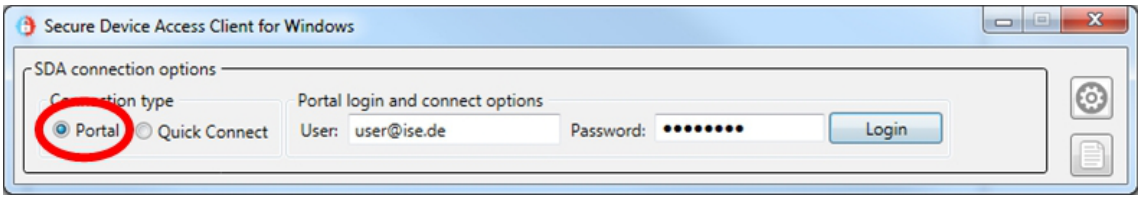


Figure 14: Logging in to the SDA portal server

Once you have then logged in to the SDA portal server using the "Login" button, a list of all SDA connectors for which your user possesses access rights appears.

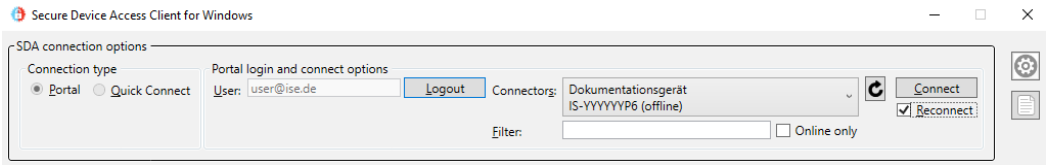


Figure 15: Using SDA connector via Portal Connect

After selecting an SDA connection from the list, its configuration will appear. If the SDA connector is being used with this client for the first time, a default configuration is created.

Once you have adjusted the configuration to suit your applications (see Section 4.3 "Configuration of the access options of an SDA connector" ff.), you can establish the connection using the "Connect" button.

You can also select the option “Reconnect”. If Reconnect is activated, the Windows Client will automatically attempt to re-establish the connection if it is aborted (e.g. Through DSL Reconnect). This option can also be used together with the execution of “External Commands” (see Section 4.3 "Configuration of the access options of an SDA connector") if necessary.

If you are working with multiple SDA connectors, you have the option of using a filter. You can enter a text and limit the selection to the connectors currently logged in ("online") to the portal.

4.3 Configuration of the access options of an SDA connector

In addition to HTTP access, for which an SDA client is not required, the standard use of the ISE SMART CONNECT KNX REMOTE ACCESS is the secure remote accessing of KNX installations via the KNX/IP protocol. For this reason, the configuration for this service is always visible and activated as standard.

In addition to KNX/IP, the SDA client also offers easy access for secure remote configurations of the Gira HomeServer. A project can be updated using the HomeServer Expert here, and a bus connection can also be established over the Eiblib/IP protocol.

It is also possible to use TCP remote access connections directly, e.g. for the Microsoft Remote Desktop Protocol (RDP).

The use, and thus also the configuration, of access to a Gira HomeServer or additional TCP connections is optional and can thus be activated or deactivated using the settings of the respective SDA connector (see figure 16).

The “External Commands” option can be used to execute external programs both after a connection has been established and terminated.

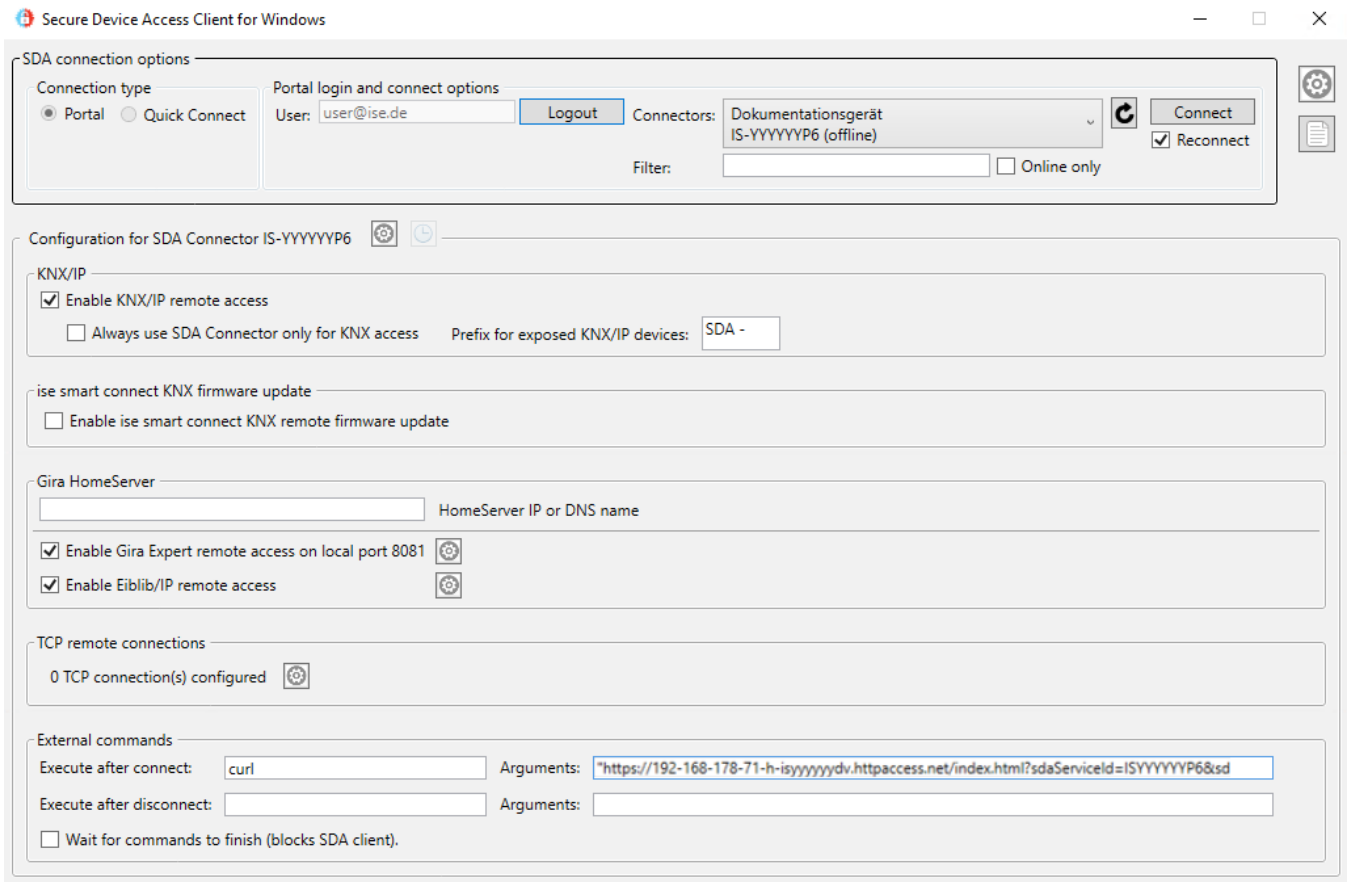


Figure 16: SDA connector configuration options

4.3.1 Access to a KNX installation via KNX-IP

The configuration for secure KNX/IP remote access is comprised of three options. KNX/P access can always be deactivated if you only require quick access to a computer via Remote Desktop and don't need KNX/IP, for example.

If KNX/IP access is permitted, all KNX/IP tunnelling servers and KNX/IP devices found on the remote network which support fast IP download are reported on the computer with the ETS as standard so that they appear in the Connection Manager of the ETS. (Heed the important note on use with ETS4 versions prior to ETS4.2 at the end of this chapter.) To see at a glance which devices are connected via SDA, a prefix of your choice with up to eight characters can be entered.

If desired, you can also make only the tunnelling server of the ISE SMART CONNECT KNX REMOTE ACCESS accessible via SDA, e.g. because there are many devices on the remote network and you are in a hurry.

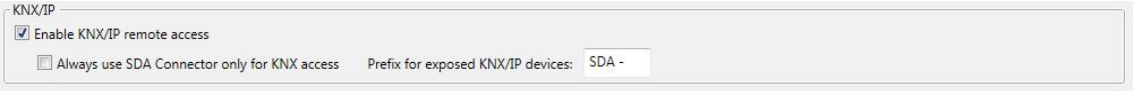


Figure 17: KNX/IP remote access configuration

Important note: If **ETS4 versions prior to ETS4.2** are used, problems can arise during automatic detection of the KNX/IP interfaces in the ETS4 where they do not appear. In this case, the interfaces must be configured manually in the ETS4!

For this purpose, you manually create a new connection in ETS4, issue the desired name and copy the corresponding IP address and port from the SDA client to the input fields in the ETS4. The SDA client provides assistance here if a connection is open by offering buttons for copying the corresponding values to the clipboard. Refer to the following figure for this.

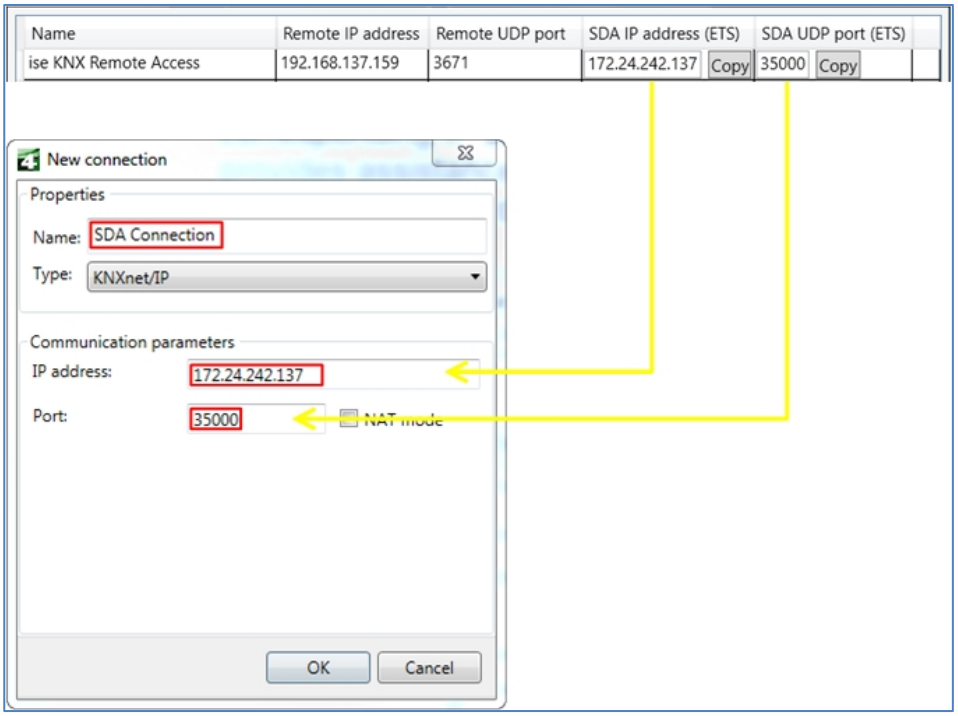


Figure 18: Manual KNX/IP interface configuration for ETS prior to ETS4.2

Note: The SDA client remembers the locally used port (starting with 35000) for each tunnelling server from the remote network so that the manually established connections remain valid later on for a new SDA connection to the same installation.

Note: SDA communication is specially optimised for KNX communication so that it still functions reliably even with slow Internet connections.

4.3.2 Remote configuration of Gira HomeServer and the use of Eiblib/IP

To ensure secure remote access to the Gira HomeServer, the IP address or local DNS name of the HomeServer in the installation, i.e. the remote network, must be entered.

It is then possible to authorise remote access for the HomeServer Expert. Since the HomeServer is configured over port 80, which is usually already in use on computers, we recommend port 8081. Any other available port can be used, however. Ports below 1000 are not recommended, though.

Note: HomeServer version 4.7.0 and newer use port 443 for configuration; the port has to be adapted using the button “gear” next to Gira Expert option.

As standard, ports 50000, 50001 and 50002 are used for the Eiblib/IP protocol. These ports are usually available on the local computer, so adjustments are generally not necessary here.

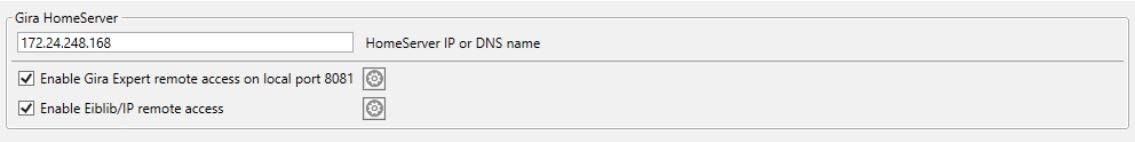


Figure 19: Gira HomeServer remote access configuration

To be able to load the HomeServer on the remote network with the Expert via SDA, you must select the "Other address" option in the "Transfer project" dialog box with an active SDA connection; always enter 127.0.0.1 as the IP address, followed by the configuration port (default is 8081).

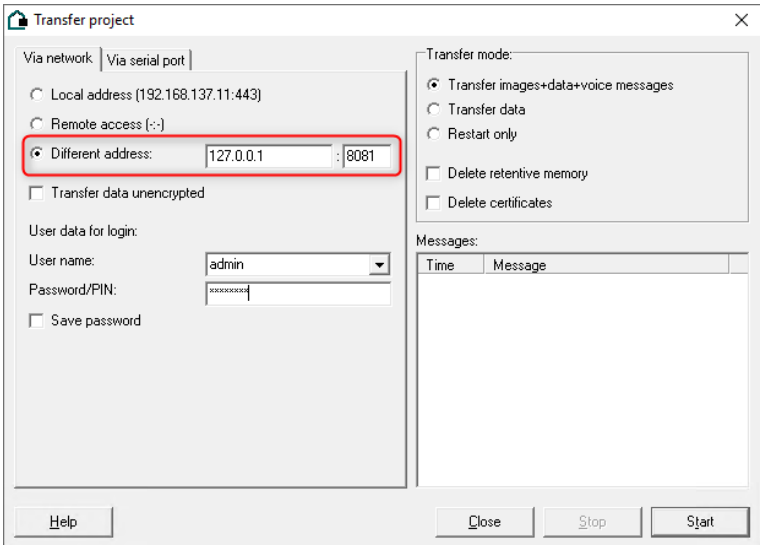


Figure 20: Transferring a project with the Expert via SDA

To use Eiblib/IP with the HomeServer, you must create a connection of type "Eiblib/IP" in the ETS as usual. As with the Expert, the server address 127.0.0.1 is always to be entered here. The ports can retain their default values (50000, 50001, 50002).

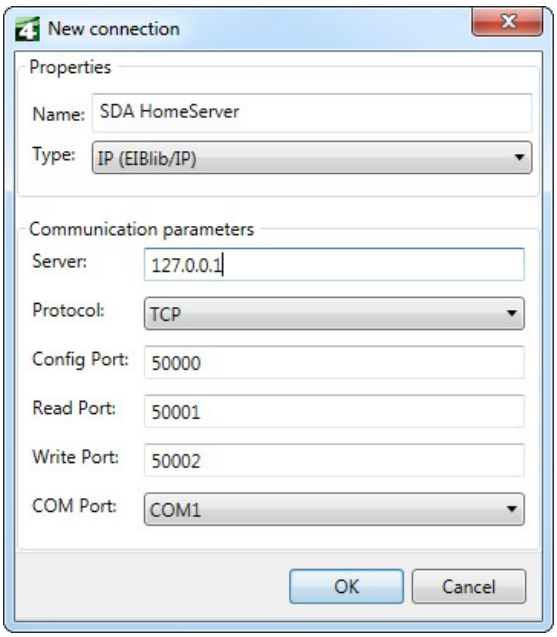


Figure 21: Using the HomeServer with Eiblib/IP via SDA for KNX connection

4.3.3 Using other TCP protocols via SDA

Through the "TCP remote access connections" settings, you can use other TCP-based IP protocols via SDA. The Microsoft Remote Desktop Protocol (RDP), for example, is well known. This protocol is used by the Microsoft Remote Desktop connection application. Here as well, it is generally the case that the port is already used locally by the computer, which is why the translation to a port is required (as in the example in the following figure).

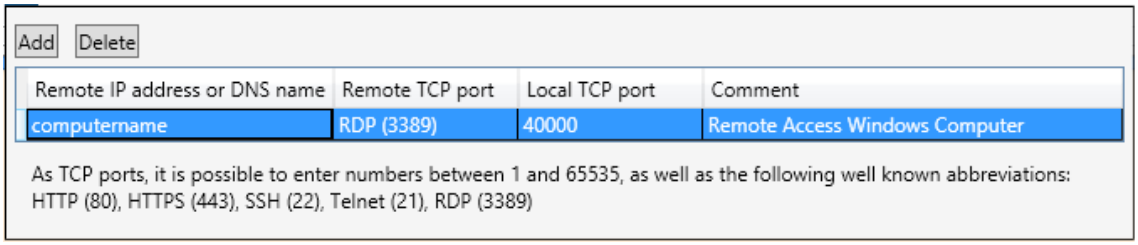


Figure 22: TCP remote access configuration

Note: It is often the case that you can no longer use the TCP port which must be addressed on the device on the remote network (3389 in this example, the standard port for RDP) on your computer, for example because you have installed software to your computer which is already using this port. In this case, you must find another port which is available. It can help to use ports starting with 40,000 here, for example (as in our example).

If you then want to establish a remote desktop connection to the target computer via SDA ("computername" in our example), you will still have to enter the port if it does not correspond to the default port. In our example, the connection can be established as follows.

Figure 23: Using the remote desktop

Note: Writing the port with a preceding ":" directly after the so-called host name is common syntax for the explicit specification of a port (only required if not the default port). With HTTP, e.g. http://127.0.0.1:40003/index.html.

Protocols such as Telnet and SSH can also easily be used via SDA.

4.3.4 Executing external commands/programs

The “External Commands” option can be used to execute external programs both after a connection has been established and terminated.

This means that files can be loaded or copied to the remote system using curl, for instance, or a program can be stopped in the event of an aborted connection and started again upon reconnection. The commands for automation are particularly easy to use in combination with the Reconnect option for connections (see above).

Figure 24: Configuration of external commands

In the left input field, the name of the command or program is entered, with path if necessary. All parameters required for execution are entered in the corresponding argument input field.

You can also configure whether to wait for the termination of the external commands.

Important: Waiting for a command blocks the Window Client completely until the program finishes.

4.4 Starting the SDA connection and status display

Starting the secure connection to the SDA connector is carried out in the same way for both Quick Connect and Portal Connect via the "Connect" button. Should an error occur when the connection is being established, a corresponding error message will be displayed.

If the connection is established successfully, configuration options are deactivated, as the connection cannot be modified when the connection is active.

In the top element, green text with the date and time of the start of the connection and IP information of the local computer and the SDA connector on the remote network is displayed. This serves diagnostic purposes and is very helpful for providing information to experts.

For all three connection types (KNX/IP, Gira HomeServer and TCP), a button with an information graphic is likewise displayed after start-up. Should errors occur with individual connections, e.g. if not a single KNX/IP device was found or a TCP connection could not be established, a button with a warning triangle also appears. All the buttons have tool tips and also display the text in an input field when you press them. In the following figure, a TCP connection could not be established.

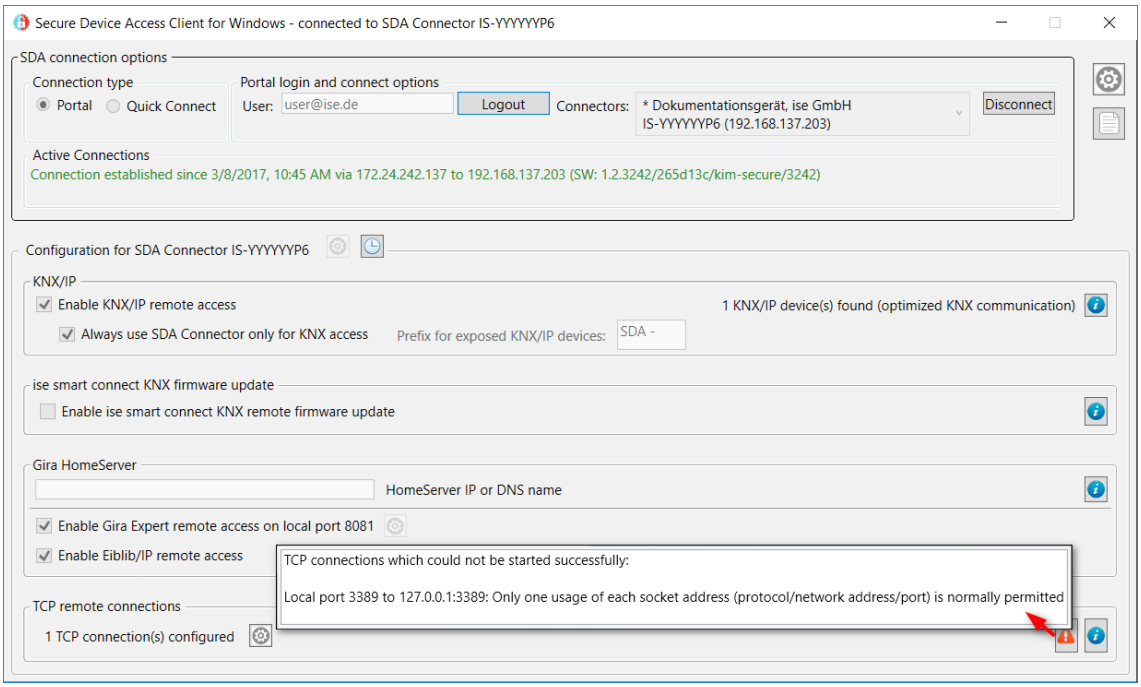


Figure 25: Status information in the SDA client after connection establishment

Important note: By far the most frequently occurring problem is a configuration which uses a local port which is already in use by another application. In the example in the figure, this is port 50000. In this case, the operating system error message is "Normally, each socket address (protocol, network address or connection) may only be used once". In this case, please select a different local port!

Note for experts: Detailed connection information will be provided under to experts in a log book window.

4.5 Measuring communication speed

By pressing the button you can make a time measurement for a communication round trip, i.e. the time from the transmission of a request to the target network of the SDA connector to the reception of a response from the SDA connector, once a connection has been established. With fast connections, this time is in the range of 30–40 milliseconds. With slow connections, it can take several seconds.

Important note: If the communication round trip takes over 5 seconds on average, KNX communication is problematic.

4.6 Closing an SDA connection

When you are finished, close the active connection by pressing the "Disconnect" button. The connection is also closed automatically when the SDA client is closed.

5 Time server

As a time server, ISE SMART CONNECT KNX REMOTE ACCESS can send the current time to the KNX bus at configurable intervals. For this, first you activate the "Time server" parameter in the "General" parameter view so that the parameter page “Time server” becomes visible (see section 8.4.1 "Parameter page *General*"). You configure then the respective desired interval with the "Send time" and "Send date" parameters. The time sent is obtained from the system time. This is synchronised with a NTP server which can be configured via device website. The interval for sending the communication object 52 “Date and time” to the KNX bus is the shorter one of the parameters "Send time" (communication object 50) and "Send date" (communication object 51) if they differ.

The device can be configured for various UTC time zones. The "Time zone" parameter used for this is located in the "General" 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 parameterised so that no automatic time changeovers are carried out.

The time server will only send the date and time if at least one successful NTP synchronisation has been executed after device start-up. This is to prevent the sending of a wrong system time.

With the time server function, a communication object is provided with which the sending of the time/date can be triggered (trigger). For more details, see section 8.5 "Connecting group addresses to group objects".

The time server function is deactivated at delivery.

6 Data logger

ISE SMART CONNECT KNX REMOTE ACCESS can be used as a data logger. The data logger functionality is controlled via the "Data logger" parameter in the "General" parameter view (see section 8.4.1 "Parameter page *General*"). If it is set to "Yes", the data logger functionality is always activated. 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 "Activate data logger" communication object.

The data logger state is sent via the "Data logger status" communication object. The data logger status can also be queried directly. As long as the data logger is active, the communication object has the value 1. The communication object “Data logger status” assumes the value 0 if:

- the microSD card is removed,
- no memory capacity is available on the microSD card, or
- the data logger is deactivated via the "Activate data logger" communication object.

The data logger supports two types of memory management. The microSD card memory can be used as static or cyclic buffer.

When used as cyclic buffer, the remaining memory is monitored. When the remaining memory capacity drops below 2.5 Mbyte, the oldest log file is deleted to create space for new data.

When used as static buffer, logging is automatically ended as soon as the microSD card is full until a new card with sufficient capacity is inserted.

Via the "Data logging format" parameter in the same parameter view, it can be configured whether an ETS 3 (.trx) or an ETS 4/ ETS 5 (.xml) compliant data format should be used. The data logger can be activated or deactivated via the "Activate data logger" communication object.

Naming and saving the log files on the microSD card is in accordance with the following scheme:

Year
-----Month
----------Day
----------2010_01_06_TP1.trx

If there is a loss of voltage and a resulting loss of time/date, a file name can be repeated. In this case, a tilde (~) is attached to the end of the file name, for further repetitions, consecutive numbers (~1) are added to the tilde.

ISE SMART CONNECT KNX REMOTE ACCESS supports SDHC cards up to a maximum of 32 GB. The cards must be formatted with FAT32.

Important note: To prevent damage to the card, you should deactivate logging before removing the microSD card.

Various communication objects are available for monitoring the memory status. The current card status and the occupancy level are queried via these communication objects. For more details, see section 8.5 "Connecting group addresses to group objects".

Important note: If the NTP server cannot be reached after a power failure, a default time is used. Further logging is based on this time, until the NTP server is available again.

6.1 Access to the data logger archive

Via the device website, the data logger archive can be accessed. The menu item is also available when the datalogger is deactivated in order to download old files if necessary. In addition to the actual files, the status of the microSD card is also displayed.

When the microSD card is inserted, the log files stored on the microSD card are listed under “Content”. These are grouped by year and month. By default, the years and months are minimized and can be expanded by the plus sign next to the year / month.

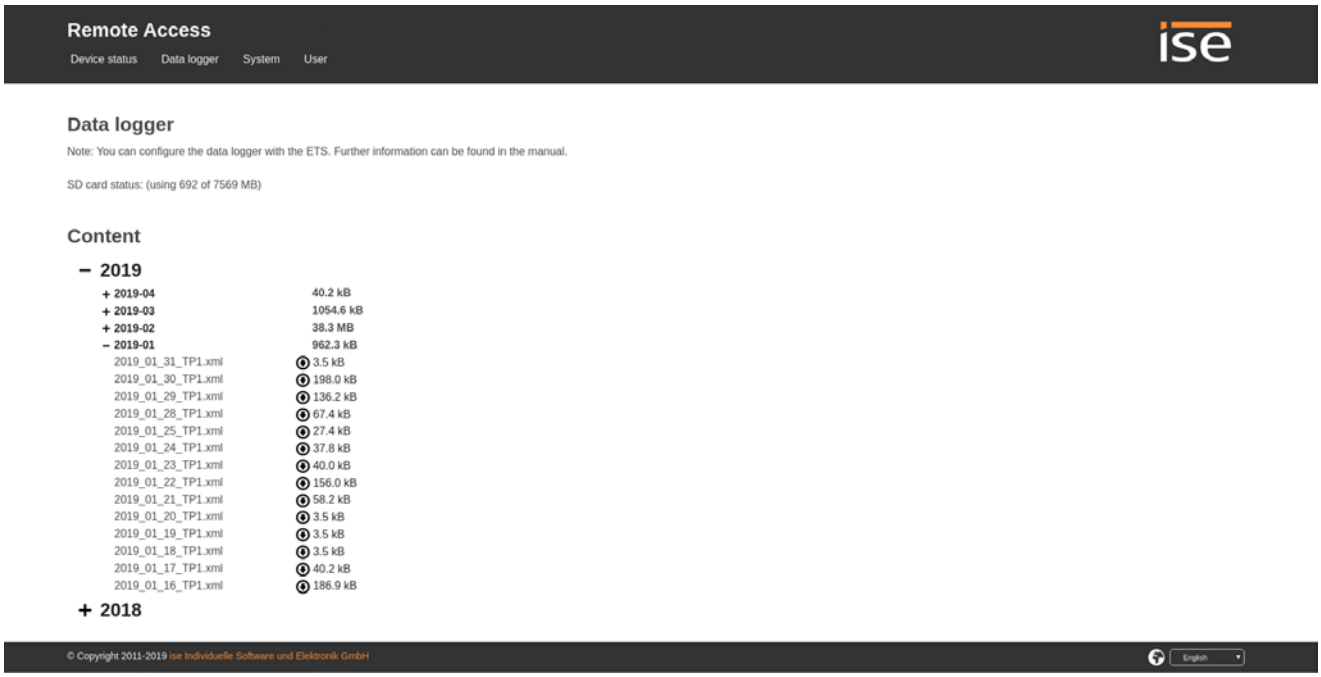


Figure 26: Data logger archive

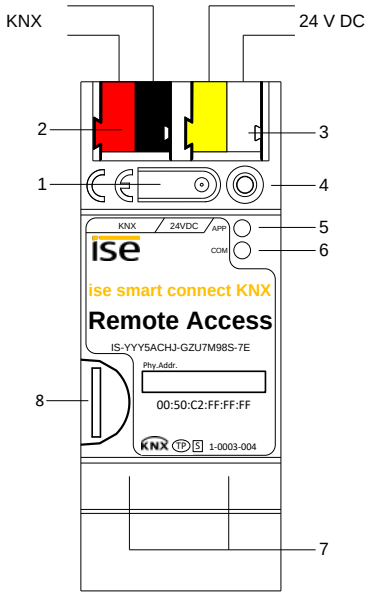
The number next to a month or a single file indicates the file size in bytes.

Push the download symbol to start the download of a xml-file.

Important note: Encrypted telegrams cannot be decrypted via ETS.

7 Installation, electrical connection and operation

7.1 Device design



Dimensions:

Width (W):

36 mm (2 HP)

Height (H):

90 mm

Depth (D):

74 mm

Figure 27: ISE SMART CONNECT KNX REMOTE ACCESS

1	Programming button for KNX	Switches to the device in the ETS programming mode or vice versa.
2	KNX connection (twisted pair)	On left: (+/red) On right: (–/black)
3	Connection Power supply	DC 24 to 30 V, 2 W (at 24 V) On left: (+/yellow) On right: (–/white)
4	KNX programming LED (red)	Red: Device is in ETS programming mode
5	LED APP (green)	Green: Normal operation off/flashes: For start or diagnosis code, see 9.2.1/0
6	LED COM (yellow)	Yellow: Normal operation (brief dark phases indicate KNX telegram traffic) off/ flashes: For start or diagnosis codes, see 9.2.1/0
7	Ethernet connection	LED 10/100 speed (green) On: 100 Mbit/s Off: 10 Mbit/s LED link/ACT (orange) On: Connection to IP network Off: No connection flashes: Data reception on IP
8	MicroSD card holder	A microSD card must be inserted for the data logger to be able to record telegrams. Media size: Up to 32 GB microSDHC Format: FAT32

7.2 Safety notes

Electrical devices may only be installed and mounted by a qualified electrician. In doing so, the applicable accident prevention regulations must be observed. Failure to observe the installation instructions can result in damage to the device, fire or other dangers.

DANGER!
Electric shock if live parts are touched. Electric shock may lead to death.
Isolate connection cables before working on the device. Cover up live parts in the vicinity!

Please see the operating instructions enclosed with the device for more information.

7.3 Mounting and electrical connection

Mounting the device

- Snap it on to the top-hat rail as per DIN EN 60715, vertical mounting; network connections must face downward.

A KNX data rail is not required; the connection to KNX-TP is established using the accompanying bus connection terminal.

Observe temperature range (0 °C to +45 °C); do not install over heat-emitting devices and ensure sufficient ventilation/cooling if necessary.

Connecting the device

- Connect the KNX-TP bus line to the KNX connection of the device using the included KNX bus connection terminal. The bus line must be led to near the device terminal with the sheathing in tact! Bus line leads without sheathing (SELV) must be installed isolated in such a way that they are securely protected from all non-safety-low-voltage lines (SELV/PELV) (comply with ≥ 4 mm spacing or use cover; see also VDE regulations on SELV (DIN VDE 0100-410/"Secure isolation", KNX installation specifications)!
- Connecting the external power supply to the power supply connection (3) of the device using a KNX device connection terminal, preferably yellow/white.
  Polarity: left/yellow: (+), white/right: (-).

  Note: If the "non-choked" auxiliary power output of a KNX power supply is used as an auxiliary energy source, you must ensure that the overall current consumption (including all KNX-TP devices) on the line segment does not exceed the rated voltage of the power supply.
- Connection of one or two IP network lines to the network connection of the device (7).

Mounting/removing a cover cap

A cover cap can be mounted for protection of the KNX bus and power supply connections from dangerous voltage, particularly in the connection area.

The cap is mounted with an attached bus and power supply terminal and a connected bus and power supply line to the rear.

- Mounting the cover cap: The cover cap is pushed over the bus terminal until you hear and feel it lock into position (comp. Figure 28A).
- Removing the cover cap: The cover cap is removed by pressing it slightly on both sides and pulling it off towards the front (comp Figure 28B).

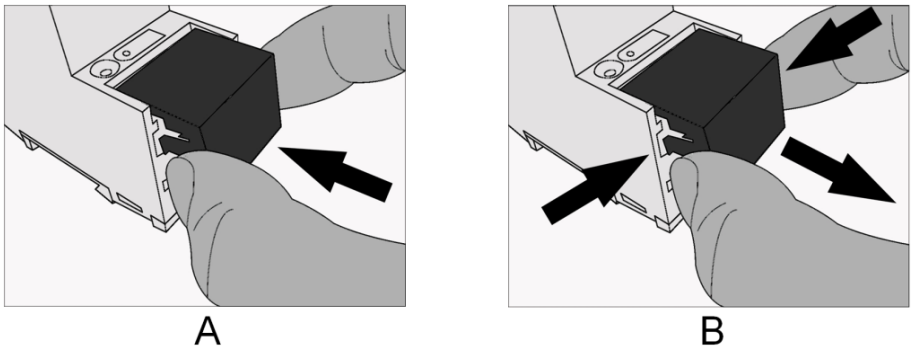


Figure 28: Mounting / removing cover cap

8 Configuration in the ETS

Note: Upon delivery and also after a factory reset, the ISE SMART CONNECT KNX REMOTE ACCESS is configured as follows before it is loaded with ETS for the first time:

- Remote access is always activated, namely for the "residents" user group and via "QuickConnect".
- The physical address is 15.15.255, and the three additional physical addresses for the tunnelling server all have the address 15.15.254.

Configuration of the ISE SMART CONNECT KNX REMOTE ACCESS is divided into the following steps:

Preparations:		**For explanations, see**
1	Mount device, connect it to KNX bus connection and auxiliary voltage.	→ Chapter 7
2	Install the ISE SMART CONNECT KNX REMOTE ACCESS on the IP network with an Internet connection.	

Configuration via ETS:		
After installing the device and connecting the bus, power supply and Ethernet, the device can be commissioned. The preparatory configuration is carried out using the Engineering Tool Software, ETS, available from the KNX Association, see www.knx.org.		
1	Create the ISE SMART CONNECT KNX REMOTE ACCESS as a device in the ETS.	→ Section 8.1
2	Assign the physical address of the device and the maximum three physical addresses of the interface as usual according to the KNX topology.	
	As one of the first devices on the market to do so, the ISE SMART CONNECT KNX REMOTE ACCESS utilises the ETS option (ETS4 and later) where interface addresses can already be configured in the ETS project. The ETS also makes sure here that overlapping with other devices in the project does not occur. For this reason, we strongly recommend using this function!	→ Section 8.2
3	Set IP address, IP subnet mask and default gateway address of the ISE SMART CONNECT KNX REMOTE ACCESS or select "Obtain an IP address automatically (from a DHCP server)".	→ Section 8.3
4	Set general parameters, incl. DNS server for the ISE SMART CONNECT KNX REMOTE ACCESS.	→ Section 8.4.1
5	Connect group addresses to group objects as usual.	→ Section 8.5
6	The ISE SMART CONNECT KNX REMOTE ACCESS is now ready for commissioning via *"Program ETS"* and for testing of the functions.	

8.1 Configuration step 1 – Create ISE SMART CONNECT KNX REMOTE ACCESS as device in the ETS

If it has not yet been done, import the ETS device application to the ISE SMART CONNECT KNX REMOTE ACCESS once in the device catalogue of its ETS, for example using the "*Import Products*" function on the start page of the ETS.

You can download the ETS application from our website under www.ise.de free of charge.
The other explanations in this document refer to

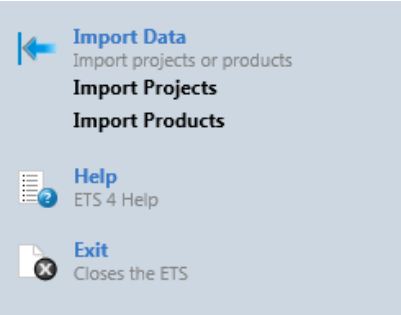


Figure 29: Product import via the ETS4 start page

Hardware		Application software	
Device:	ISE SMART CONNECT KNX REMOTE ACCESS	Application:	**ISE SMART CONNECT KNX REMOTE ACCESS**
Manufacturer:	ise GmbH	Version:	**V5.0**
Order No.	1-0003-004		
Version:	V1.0		
Design:	DRA (series installation)		

If you already have an ETS project with a previous database entry, you can also update the application program. To do this, drag the new database entry to the project and then select the device with the old database entry. Now select *"Information"* in the device *"Properties"* and then select the *"Application"* tab (ETS 4.2) or the *"Application program"* tab (ETS 5).

You can now use the "*Update application program*" button (ETS 4.2) or the "*Update*" button (ETS 5) to replace the old database entry. Existing links with group addresses are not lost. The newly added device can now be deleted again.

In ETS 4.2, you require a special license for this. From ETS 5, this is possible with every license.

8.2 Configuration step 2 – Assigning physical addresses

The ISE 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. In addition to the physical address of the device, the device also has (up to) three additional physical interfaces.

As with many products today, they can be configured via the interface settings after opening the KNX/IP connection in the ETS. In this case, you must be very careful to ensure that the addresses have not already been used for other purposes.

Starting with ETS4, it is possible to specify the number of additional addresses for products so that they are configurable in the ETS. A list with the additional addresses appears for this purpose below the input window for the physical address in the device properties in the ETS. In this case, the ETS ensures the uniqueness of the addresses in the project and is loaded into the device automatically when programming the physical address.

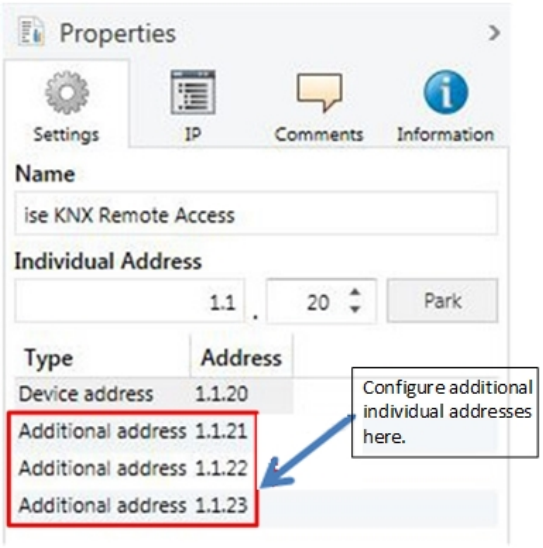


Figure 30: Configuring addresses

If you do not require all three interfaces, you can also enable addresses using the "Park" function. When adding a device, the ETS usually pre-sets the additional addresses automatically.

8.3 Configuration step 3 – Setting the IP address, subnet mask and address of the default gateway

In addition to the physical address on the KNX network, the ISE SMART CONNECT KNX REMOTE ACCESS must also be assigned an address on the IP data network. This includes the following information:

- IP address
- Subnet mask
- Default gateway address
- DNS server

This can occur in two ways, either

- automatically by obtaining the data from a DHCP server (e.g. Integrated into the data network route) or
- via manual setting in the ETS.

Proceed as follows for this purpose:

1. Select the device in the ETS.

2. Display the device properties in the sidebar on the ETS as shown in Figure 31.

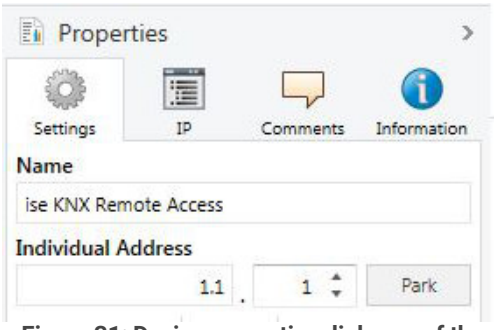


Figure 31: Device properties dialogue of the ETS

3. Select the "IP" tab accordinglyFigure 32. Then select either
   ⊙ *Obtain an IP address automatically (default)*

   The address data are automatically obtained from a DHCP server on the data network.
   or
   ⊙ *Use the following address*

   and enter the data manually.
   You can usually obtain the permissible IP address range and the subnet mask and default gateway from the router configuration interface.

   Important: If the device is not used with DHCP, the DNS entry must be set correctly in the parameters of the device (see Section 8.4 “Setting parameters”)!

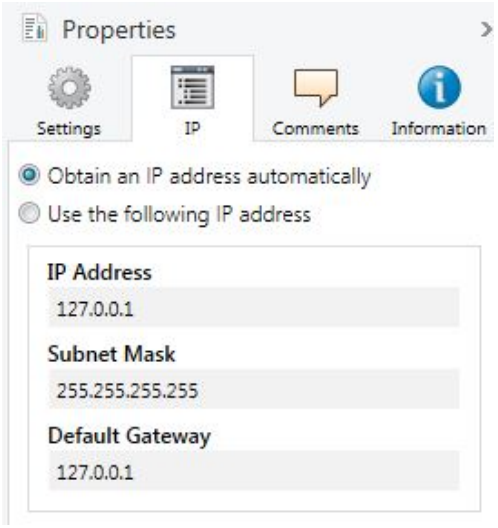


Figure 32: Setting of the IP address data of the device on the “IP” tab in the sidebar of the ETS

If the ⊙ *Obtain an IP address automatically* setting is used, a DHCP server must issue the ISE SMART CONNECT KNX REMOTE ACCESS a valid IP address.

If a DHCP server is not available for this setting, the device starts up after a waiting time with an auto IP address (address range from 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.

8.4 Setting parameters

8.4.1 Parameter page *General*

The default value of each parameter is marked in **bold**.

Parameter	Entry/Selection	Remarks
DNS server (if not using DHCP)	**Default gateway**	The IP address of the default gateway is used (see Section 8.3 Configuration step 3 – Setting the IP address, subnet mask and address of the default gateway).
	individual DNS server IP address	With this parameter, it is possible to set up an individual IP address of the DNS server.
	0.0.0.0	The individual DNS server IP address. If 0.0.0.0 is used, the default gateway is used.
Time server	**No** Yes	The device works as a time server and sends the current time and date to the KNX bus at configurable intervals.
Data logger	**No** Yes	This parameter determines whether the data logger function is activated. The corresponding communication objects are only available when it is activated.
Time zone	**(UTC+01:00) Europe/Berlin** Other UTC time zones	The time zone to be used is selected here. There are several time zones with identical UTC deviations. In some of these time zones, summer/winter time switchover is at a different time. One of the "Generic Time Zone w/o DST" time zones must be selected so that no automatic time changeovers are carried out. **Important note: If this setting is changed, ISE SMART CONNECT KNX REMOTE ACCESS will restart directly after the application has been programmed!** **Important note: The option to disable NTP via the device website has been deactivated since firmware version 5.0. If you have disabled NTP, it will be automatically enabled using the default NTP server pool.ntp.org.**
Portal access in general	**as before restart**	After a restart, the general portal access status is set to the last known value before the restart. If the general portal access status is enabled before the restart, for example, the portal access status is also enabled after a restart.
	enabled	Enables the device to establish a connection to the SDA portal server after each restart.
	disabled	Prohibits the device establishing a connection to the SDA portal server after each restart.
Remote access for the "residents" group, "installers" group or via "Quick Connect" after a restart.	**as before restart**	After a restart, the remote access status of the respective group or "Quick Connect" is set to the last known value before the restart. If the remote access status is enabled before the restart, for example, the remote access status is also enabled after a restart.

Parameter	Entry/Selection	Remarks
	enabled	Enables remote access for the respective group or "Quick Connect" after each restart.
	disabled	Prohibits remote access for the respective group or "Quick Connect" with each restart.
Number of SDA notification objects	**0**|1...|49|50	The number of SDA notifications objects is specified here (max. 50). The "101 ff" group objects are visible according to the selection.
Separator for floating-point numbers	**","** "."	

8.4.2 Parameter page *Time server*

The parameter page *Time server* is only visible when the timer server is activated on the parameter page *General*.

Parameter	Entry/Selection	Remarks
Send time	**every minute** every hour every day	The interval for sending the time to the bus is configured with this parameter.
Send date	**every minute** every hour every day	The interval for sending the date to the bus is configured with this parameter.

8.4.3 Parameter page *Data logger*

The parameter page *Data logger* is only visible when the data logger is activated on the parameter page *General*.

Parameter	Entry/Selection	Remarks
Format		This parameter determines which format the data should be logged in on the microSD card.
	ETS4/ETS5	The data is stored in an ETS4-compliant format (.xml) which is also readable by the ETS5.
	ETS3	The data is stored in an ETS3-compliant format (.trx).
Memory type	cyclic buffer **static buffer**	This parameter specifies how the microSD card memory is to be used.
Memory status type		Only visible when "Memory type" is set to "static buffer". This parameter specifies what type the status object of the card occupancy level should be.

Parameter	Entry/Selection	Remarks
	binary	A 1-bit object is used. The value "1" means that the microSD card is full, "0" means that there is still space on the microSD card for logging
	value (0-255)	A 1-byte object is used. The value range is between 0 – 255. The value "255" corresponds to a card occupancy level of 100%.

8.4.4 Parameter page *Notifications*

The parameter page *Notifications* is only visible when the number of notifications is greater 0 on the parameter page *General*.

According to the number of SDA notifications selected above, the DP types and other parameters of the respective SDA notifications can now be specified (SDA notification 1 = group object 101, SDA notification 2 = group object 102 etc.).

Table 2 SDA notification "N"

Parameter	Entry/Selection	Remarks
Data type	**Boolean (1 bit, DPT 1.001)** Percent (1 byte, DPT 5.001) Counter (1 byte, DPT 5.010) Floating point (2 bytes, DPT 9.*) Text (14 bytes, DPT 16.001)	The desired data type of the respective SDA notification can be selected.
Notifications for changed value only	" "	Always send notification.
	"✓"	Send notification only if the value in the group telegram has changed.
Threshold value	0-1000 Specification as integer.	Suppress notifications. Only send notifications again if the threshold value is exceeded. The threshold value is the deviation from the last value (as an absolute number) that generated a notification. 0. No threshold value. You will receive a notification every time a change occurs.
Threshold base	**1: No factor** Value according the selection list	Factor with which the threshold value is multiplied if necessary.
Filter	Text	The filter can be comprised of a fixed value or up to two conditions. With DPT 1.001 (boolean), the filter is possible via a selection list.
Priority	**Low** High Alarm	

Parameter	Entry/Selection	Remarks
Category	Text	Can be used to filter the SDA notifications and their forwarded notifications on the SDA portal.
Subject	Text	Used when sending e-mails as "Subject."
Text	Text	Used when sending e-mails as "Text."
Add attachment	„“ „✓“	
URL of the attachment	Text	Only http requests are supported. Observe the maximum permissible file size of 250 kB.

8.5 Connecting group addresses to group objects

The following group objects are available for the connection of group addresses at the ISE SMART CONNECT KNX REMOTE ACCESS.

Important note for all group objects which signal an active connection: When HTTP access is used, i.e. without an SDA client, the connection to the device (if permitted) is not closed immediately after loading the pages or closing the browser. This relates to the technical optimisation of HTTP access in the SDA portal server. HTTP connections can require up to five minutes until they are closed. This means that the corresponding group objects which signal an active connection also do not signal closing until this point in time. If the SDA client is used, on the other hand, the connection is closed synchronously.

Object	Name	Direction	Data width	DP type	Flags (CRWTU)
1	Grant portal access	Write	1 bit	1.003	C-W--
Rubric:	Remote access	Data type:	Enable		
Function:	Allows or prohibits the connection of the device to the SDA portal server. If connection establishment is prohibited, the device is never accessible from the outside.				
Description:	1 = Allow, 0 = Prohibit				

Object	Name	Direction	Data width	DP type	Flags (CRWTU)
2	Grant portal access – Status	Read	1 bit	1.003	CR-T-
Rubric:	Remote access	Data type:	Enable		
Function:	Indicates whether the device is allowed to connect to the server.				
Description:	1 = Allowed, 0 = Prohibited				

Object	Name	Direction	Data width	DP type	Flags (CRWTU)
3 (residents) 5 (installers) 7 (Quick Connect)	Grant remote access	Write	1 bit	1.003	C-W--
Rubric:	Remote access	Data type:	Enable		
Function:	Allows or prohibits remote access for each of the members of the group or via "Quick Connect".				

Description: 1 = Allow, 0 = Prohibit

Object	Name	Direction	Data width	DP type	Flags (CRWTU)
4 (residents) 6 (installers) 8 (Quick Connect)	Grant remote access – Status	Read	1 bit	1.003	CR-T-

Rubric: Remote access

Data type: Enable

Function: Indicates whether remote access is granted for members of the group or via "Quick Connect".

Description: 1 = Allowed, 0 = Prohibited

Object	Name	Direction	Data width	DP type	Flags (CRWTU)
20	State portal connection	Read	1 bit	1.011	CR-T-

Rubric: Remote access

Data type: Status

Function: Indicates whether connection to portal is established. For detailed information see group object 31.

Description: 1 = Connected, 0 = Disconnected

Object	Name	Direction	Data width	DP type	Flags (CRWTU)
21	State any remote connection	Read	1 bit	1.011	CR-T-

Rubric: Remote access connection

Data type: Status

Function: Indicates whether at least a remote connection is currently active, regardless of the connection type.

Description: 1 = Active, 0 = Not active

Object	Name	Direction	Data width	DP type	Flags (CRWTU)
22 (residents) 23 (installers) 24 (Quick Connect)	State any remote connection	Read	1 bit	1.011	CR-T-

Rubric: Remote access connection

Data type: Status

Function: Indicates whether in each case a remote access connection is currently active for the group or via "Quick Connect".

An active connection is signalled for another group if necessary if access was granted to a member of this group via "Quick Connect" or based on membership in another group.

Description: 1 = Active, 0 = Not active

Object	Name	Direction	Data width	DP type	Flags (CRWTU)
30	Error indication	Read	1 bit	1.005	CR-T-

Rubric: Connection error

Data type: Alarm

Function: Indicates a connection error which is described by group object 32. Further details can be found on the website of the ISE SMART CONNECT KNX REMOTE ACCESS device.

Description: 1 = Alarm, 0 = No alarm

Object	Name	Direction	Data width	DP type	Flags (CRWTU)
31	Portal connection info	Read	14 bytes	16.001	CR-T-

Rubric: Connection error

Data type: Character (ISO 8859-1)

Function: Diagnostic information about the portal connection

Description: Supplies more precise information on the portal connection status displayed by communication object 20.

Object	Name	Direction	Data width	DP type	Flags (CRWTU)
32	Connection error info	Read	14 bytes	16.001	CR-T-

Rubric:	Connection error	Data type:	Character (ISO 8859-1)
Function:	Additional diagnostic information in case of a portal connection error.		
Description:	Supplies more precise information on the connection error displayed by communication object 30.		

Object	Name	Direction	Data width	DP type	Flags (CRWTU)
50	Time	Read	3 bytes	10.001	CR-T-

Rubric:	Time server	Data type:	Time of day
Function:	Sends cyclically and on request the current time.		
Description:	3 byte object for sending the current time. The interval can be parameterised (see section 8.4.2 "Parameter page *Time server*"). If you read this object explicitly before a valid NTP time could be obtained, the current system time is returned which can differ from the correct time.		

Object	Name	Direction	Data width	DP type	Flags (CRWTU)
51	Date	Read	3 bytes	11.001	CR-T-

Rubric:	Time server	Data type:	Date
Function:	Sends cyclically and on request the current date.		
Description:	3 byte object for sending the current date. The interval can be parameterised (see section 8.4.2 "Parameter page *Time server*"). If you read this object explicitly before a valid NTP time could be obtained, the current system date is returned which can differ from the correct date.		

Object	Name	Direction	Data width	DP type	Flags (CRWTU)
52	Date and time	Read	8 bytes	19.001	CR-T-

Rubric:	Time server	Data type:	Date/Time
Function:	Sends cyclically and on request current date and time.		

Description:	8 byte object for sending the current date and time. The interval is determined by the shorter interval of the parameters for the communication objects 50 "Time" and 51 "Date" (see section 8.4.2 "Parameter page *Time server*"). If you read this object explicitly before a valid NTP time could be obtained, the current system time and date is returned which can differ from the correct time and date.

Object	Name	Direction	Data width	DP type	Flags (CRWTU)
53	Trigger send date/time	Write	1 bit	1.017	C-W--

Rubric:	Time server	Data type:	Trigger
Function:	Triggers the sending of date and time.		
Description:	1-bit object for triggering the sending of the current time/date if the object has been assigned any desired value. If no NTP query has been successful yet, no values will be sent.		

Object	Name	Direction	Data width	DP type	Flags (CRWTU)
54	NTP status	Read	1 bit	1.002	CR-T-

Rubric:	Time server	Data type:	Boolean
Function:	Indicates whether a valid time could be requested by the NTP server.		
Description:	1-bit object for display of the status of the last NTP query. If the NTP query was successful and the system time has been reset as a result or if there was an error during the previous query, the object is assigned a "1". If the last NTP query was not successful, the object is assigned a "0".		

Object	Name	Direction	Data width	DP type	Flags (CRWTU)
55	SD card error	Read	1 bit	1.002	CR-T-

Rubric:	Data logger	Data type:	Boolean
Function:	Indicates whether there is currently an error with the SD card.		
Description:	1-bit object for signalling an SD card error. When a "1" is assigned to the object, an SD card error has occurred.		

Object	Name	Direction	Data width	DP type	Flags (CRWTU)

Object	Name	Direction	Data width	DP type	Flags (CRWTU)
56	SD error code	Read	1 byte	20.*	CR-T-

Rubric: Data logger
Data type: -

Function: Indicates the current error code (0 = no error).

Description: 1-byte object for signalling a microSD card error.

0 = microSD card OK

1 = microSD card full

2 = microSD card not inserted

4 = Fault has occurred in microSD card (e.g. incorrectly formatted)

Object	Name	Direction	Data width	DP type	Flags (CRWTU)
57	Activate data logger	Write	1 bit	1.001	CRW--

Rubric: Data logger
Data type: Switch

Function: Activates (1 = default) or deactivates (0) the logging and indicates the status on request.

Description: 1-bit object to activate the data logger. When a "1" is assigned to the object, the data logger is active. If a "0" is assigned to it, it is deactivated.

Object	Name	Direction	Data width	DP type	Flags (CRWTU)
58	Data logger status	Read	1 bit	1.002	CR-T-

Rubric: Data logger
Data type: Boolean

Function: Indicates whether the data logger is currently recording data.

Description: 1-bit object which reflects the state of the data logger. If the object has a value of "1", the data logger is active. A "0" means that the data logger is inactive.

Object	Name	Direction	Data width	DP type	Flags (CRWTU)
59	SD card memory state	Read	1 bit	1.002	CR-T-

Rubric: Data logger
Data type: Boolean

Function: Indicates if the SD card memory is exhausted (1 = full).

Description: 1-bit object for display of the occupancy level of the SD card. When a "1" is assigned to the object, the SD card is full. If it is assigned a "0", then there is still space for logging on the SD card.

Object	Name	Direction	Data width	DP type	Flags (CRWTU)
60	SD card memory occupancy	Read	1 byte	5.001	CR-T-

Rubric:	Data logger	Data type:	Percentage (0..100%)
Function:	Shows how many % of the SD card memory is occupied.		
Description:	1-byte object for displaying the memory occupancy of the SD card. The value range is 0-255 (equivalent to 0-100%).		

Object	Name	Direction	Data width	DP type	Flags (CRWTU)
101 - 150	Notification trigger no. 1/2/3/.../49/50	Write	1 bit	1.001	C-W--

Rubric:	Switching	Data type:	On/Off
Function:	Sends an SDA notification to the SDA portal server. The boolean value can be sent in the SDA notification.		
Description:	This is one of five possible DP types for the 50 group addresses "101 to 150." The specification of the DP type is made through a corresponding selection under the general parameters (see Section 8.4.4 "Parameter page *Notifications*").		

Object	Name	Direction	Data width	DP type	Flags (CRWTU)
101 - 150	Notification trigger no. 1/2/3/.../49/50	Write	1 byte	5.001	C-W--

Rubric:	Percent	Data type:	Percent (0 to 100%)
Function:	Sends an SDA notification to the SDA portal server. The boolean value can be sent in the SDA notification.		
Description:	This is one of five possible DP types for the 50 group addresses "101 to 150." The specification of the DP type is made through a corresponding selection under the general parameters (see Section 8.4.4 "Parameter page *Notifications*").		

Object	Name	Direction	Data width	DP type	Flags (CRWTU)
101 - 150	Notification trigger no. 1/2/3/.../49/50	Write	1 byte	5.010	C-W--
Rubric:	Meter	Data type:			
Function:	Sends an SDA notification to the SDA portal server. The boolean value can be sent in the SDA notification.				
Description:	This is one of five possible DP types for the 50 group addresses "101 to 150." The specification of the DP type is made through a corresponding selection under the general parameters (see Section 8.4.4 "Parameter page *Notifications*").				

Object	Name	Direction	Data width	DP type	Flags (CRWTU)
101 - 150	Notification trigger no. 1/2/3/.../49/50	Write	2 bytes	9.*	C-W--
Rubric:	Floating point	Data type:	KNX floating point		
Function:	Sends an SDA notification to the SDA portal server. The boolean value can be sent in the SDA notification.				
Description:	This is one of five possible DP types for the 50 group addresses "101 to 150." The specification of the DP type is made through a corresponding selection under the general parameters (see Section 8.4.4 "Parameter page *Notifications*").				

Object	Name	Direction	Data width	DP type	Flags (CRWTU)
101 - 150	Notification trigger no. 1/2/3/.../49/50	Write	14 bytes	16.001	C-W--
Rubric:	Text	Data type:	Character (ISO 8859-1)		
Function:	Sends an SDA notification to the SDA portal server. The boolean value can be sent in the SDA notification.				
Description:	This is one of five possible DP types for the 50 group addresses "101 to 150." The specification of the DP type is made through a corresponding selection under the general parameters (see Section 8.4.4 "Parameter page *Notifications*").				

9 Commissioning

9.1 Operation

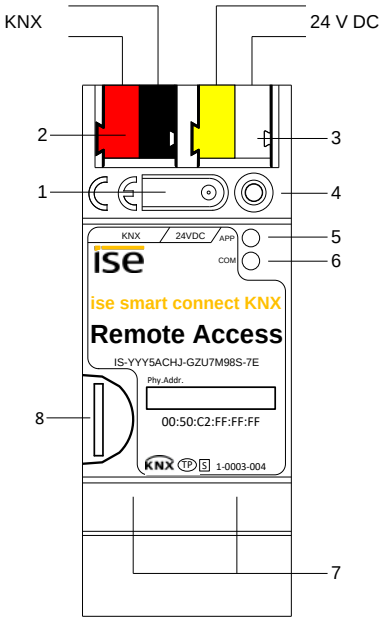


Figure 33: ISE SMART CONNECT KNX REMOTE ACCESS

1	Programming button for KNX	Switches to the device in the ETS programming mode or vice versa.
2	KNX connection (twisted pair)	On left: (+/red) On right: (–/black)
3	Connection Power supply	DC 24 to 30 V, 2 W (at 24 V) On left: (+/yellow) On right: (–/white)
4	KNX programming LED (red)	Red: Device is in ETS programming mode
5	LED APP (green)	Green: Normal operation off/flashes: For start or diagnosis code, see 9.2.1/0
6	LED COM (yellow)	Yellow: Normal operation (brief dark phases indicate KNX telegram traffic) off/flashes: For start or diagnosis codes, see 9.2.1/0
7	Ethernet connection	LED 10/100 speed (green) On: 100 Mbit/s Off: 10 Mbit/s LED link/ACT (orange) On: Connection to IP network Off: No connection flashes: Data reception on IP
8	MicroSD card holder	A microSD card must be inserted for the data logger to be able to record telegrams. Media size: Up to 32 GB microSDHC Format: FAT32

9.2 LED status displays

The device features three status LEDs on the upper housing side and four status LEDs on the network connections.

The LED displays have **different meanings**

- while the device is starting and
- during operation.

9.2.1 LED status display upon device start-up

After the power supply (DC 24 V on the yellow-white connection terminal) is switched on or after a return in voltage occurs, the device indicates its status through the following LED combinations:

LED "APP" (green)	LED "*COM*" (yellow)	Meaning	
○ **Off**	○ Off	**Error:** No power supply: Please check connections and power supply.	×
○ **Off**	● Yellow	Device starting up.	✓
○.....● **Green Flash slowly (approx. 1 Hz)**	● Yellow	**Note:** The device is fully started up, but not yet configured. An ETS download is necessary.	×
○.....● **Green Flash quickly**	○ Off	**Error:** Please contact support. The firmware cannot be started.	×
●...○...●...○...●... **Green** ○...●...○...●...○... **Yellow** **Flash slowly alternately (approx. 1 Hz)**		**Error:** Please contact support. The newly loaded firmware cannot be started. The system is trying to activate the previous firmware (invalid firmware).	×

9.2.2 LED status display in operation

Once device start-up is complete, the meaning of the LEDs is as follows:

LED "*APP*" (green)	Meaning
● **Green**	Normal operation: Portal access is generally permissible (group object 1) and the device connects to the portal server, but remote access is not currently active. Forwarded notifications are available.
○ **Off**	Device in start-up procedure or out of operation: Wait until the start-up procedure is complete or check the power supply.
●...○ **One slow flash at 1 Hz, followed by a 2 s pause**	Note: Portal access not allowed (group object 1). The device is not connecting to the SDA portal server, and remote access is not technically possible.
●...○...●...○...●...○ **Three slow blinks at 1 Hz, followed by a 2 s pause**	Note: Remote access is allowed for at least one group or "Quick Connect", and there is at least one active connection. Remote access is thus in use.

LED "COM" (yellow)	Meaning
● **Yellow**	Normal operation: KNX connection is established, no KNX telegram traffic.
●...○...●...○...●...○ **Rapid yellow flashing with brief dark phases**	Normal operation: KNX connection is established, KNX telegram traffic.
○ **Off**	Error: Connection to KNX is interrupted. Check the bus connection

9.3 Accelerate transfer: Select transfer path *KNX-TP* or *IP*

Programming (transfer from the ETS to the device) occurs in the programming environment of the ETS. An additional KNX data interface is not required for transfer (bus connection via bus connection terminal). The ETS can reach the device from both the IP page and the KNX-TP page.

Due to considerably shorter transfer times, we recommend downloading from the device's IP page.

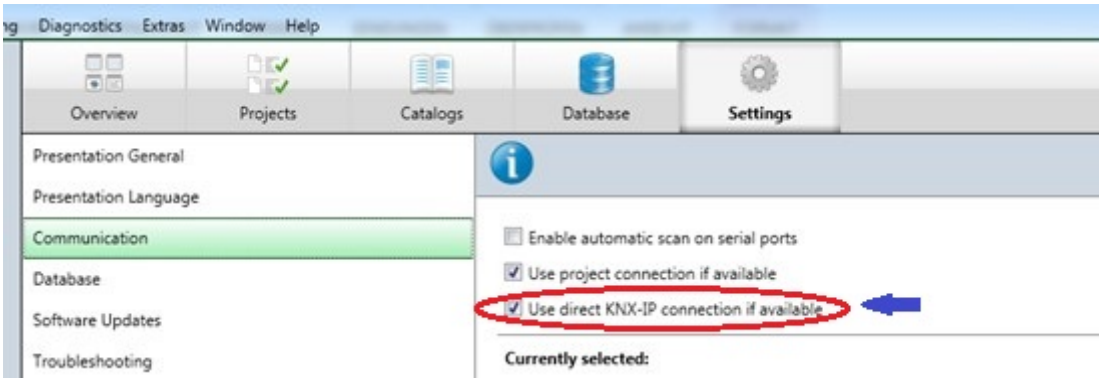


Figure 34: The *"Use direct KNX-IP connection if available"* setting accelerates the transfer from the ETS to the device

For transfer of the ETS via the IP page, set the setting

☑ ***Use direct KNX-IP connection if available.***

on the ETS start page, → *Settings* tab → *Communication* entry.

9.4 Programming the physical address of the device

- Ensure that the device and bus voltage are switched on.
- Ensure that the programming LED (4) is not illuminated.
- Press programming button (1) briefly – Programming LED (4) lights up red.
- Program physical address using the ETS.

After a successful programming procedure,

- LED (4) will go out.
- The ETS shows the completed transfer with a green marking under *History* in the sidebar (normally at the right-hand window edge).
- The ETS sets the commissioning tick on the device for "Adr" and "Cfg".

You can now note down the physical address on the device.

Important note: The additional addresses of the tunnelling server, which the ISE SMART CONNECT KNX REMOTE ACCESS brings along and which supports up to three connections, are also configured via the ETS in the properties of the device.

9.5 Transferring application programs and configuration data

After programming the physical address, the application program, parameter settings and group address connections can be transferred to the device.

A connection to the device can be further established via IP or KNX for this purpose.

1. For this purpose, select *"Programming application program*". The download lasts approx. 15 seconds with a direct IP connection or about 2 minutes if using TP.
2. After the download, please wait approx. 15 seconds while the device copies the data and installs the application.
3. Commissioning is complete.

9.6 Logging in on device website

You can accessISE SMART CONNECT KNX REMOTE ACCESS via the "Device website" application".

Calling up the device website start page

Call up the device website by doing 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 (see Figure 35): Double click on the device icon.

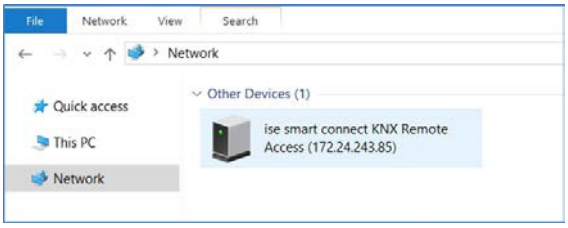


Figure 35: Calling up the device network via network environment

The device website start page is displayed. The device website is password protected.

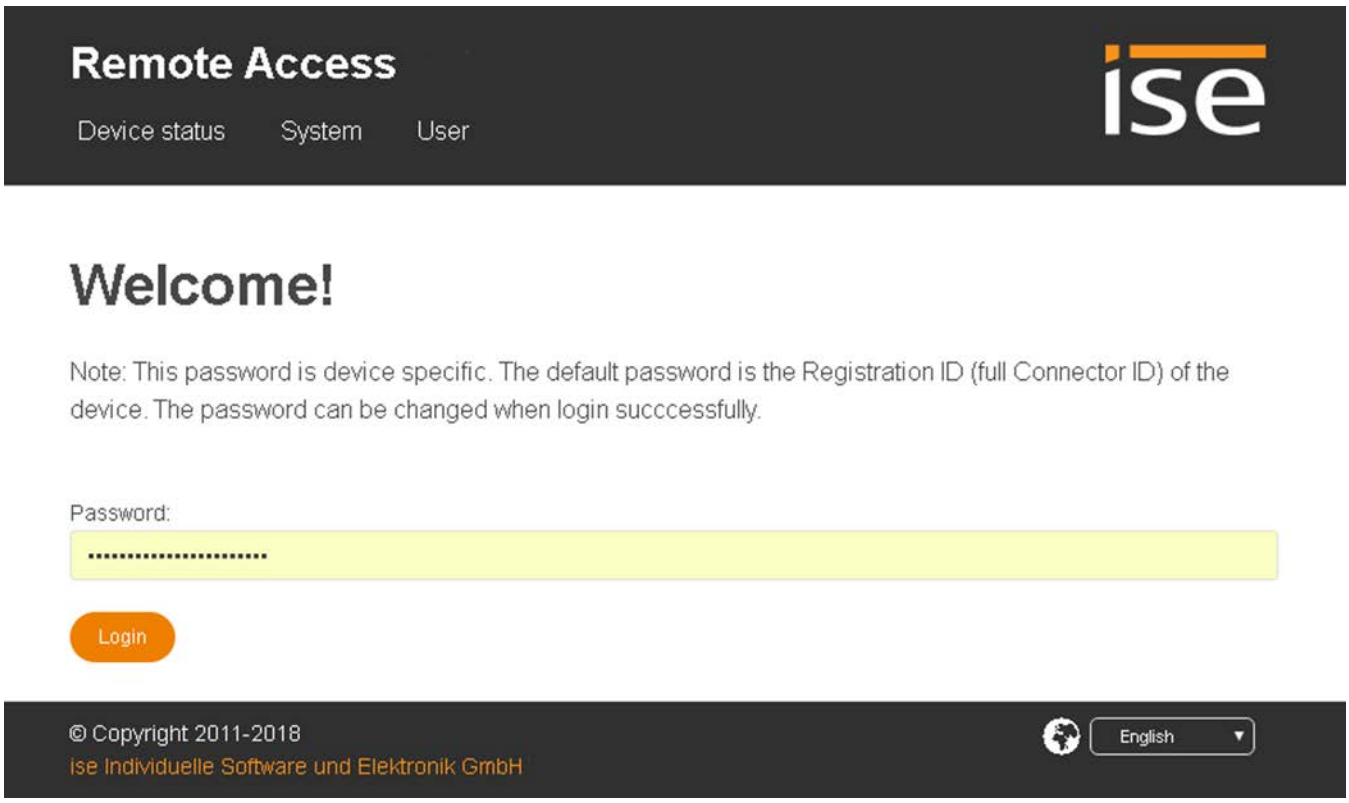


Figure 36: Device website start page

Logging in on device website

1. When you log in for the first time, enter the device's registration ID in the "password" field.
   You will find the registration ID on a device product sticker (1). Observe the use of upper-case and lower-case characters (case sensitive).
2. Select the "Log in" button.
3. Once you have logged in, change your password.

If you reset the device to factory settings, you will need to use the initial password "Device registration ID".

Changing password

1. In the "User" menu bar, select → "Change password".
2. On the "Change password" page, enter your current password and the new password.
3. Select the "Save" button.

9.7 Factory reset

The following physical KNX address is factory pre-set: 15.15.255.

Following the factory reset, the device behaves as in the state of delivery. The device registration ID is once again used as the password for the device website. The device is unconfigured. This can be recognized after starting up the device from the slowly flashing green APP LED (5).

9.7.1 Using the programming button on the device

The device can be reset to the factory settings through a sequence during start-up.

- Make sure that the device is switched off.
- Press and hold programming button (1) and switch on the device.
- Press and hold programming button (1) until the programming LED (4), the RUN LED (5) and the KNX LED (6) flash slowly simultaneously.
- Briefly release the programming button (1), then press and hold it again until the programming LED (4), the RUN LED (5) and the KNX LED (6) flash quickly simultaneously.
- The factory reset is being carried out; release programming button.
- The device need not be restarted following a factory reset.

The factory reset can be cancelled at any time by interrupting the sequence.

9.7.2 Using the website of the device

The factory reset can also be triggered from the website of the device.

- Call up with device website and log in (see Section 9.6 “Logging in on device website”, p. 69).
- Select *Device Status* in the upper menu bar on the website.
- Select *Factory Reset* in the upper menu bar on the status page.
- Confirm the factory reset when the security prompt appears.
- The next displayed page, *Factory Reset*, indicates that the factory reset is being carried out. As soon as this is complete, the start page is loaded again.

9.8 Displaying information over the website

Calling up the website is described in Section 9.6 "Logging in on device website” p. 69.

The start page of the device shows the system information, system configuration and application information after successful login.

Important note: If the ISE SMART CONNECT KNX REMOTE ACCESS was just restarted, the displayed connection status with the portal server can display incorrect values for a moment after start-up if they are being updated for the first time at the same time.

In general, the website is not updated automatically. For this purpose, please use the corresponding function of your web browser.

9.9 Firmware update of the device

9.9.1 Firmware update using the device website

The ISE SMART CONNECT KNX REMOTE ACCESS makes it possible to install firmware updates using the device website. For this purpose, select the *Update Firmware* menu item on the device website. The ISE SMART CONNECT KNX REMOTE ACCESS will now automatically search the update server for a newer version and show the current firmware version and the versions of any available updates. If a newer version is available, the associated description of the version is also displayed.

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

1. The new version provides new functionality. 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 catalogue entry occurs.
2. 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 catalogue entry after the update.

The update can be started using the *Update Firmware* button. Should an incompatibility arise, the update must be confirmed again for security purposes.

9.9.2 Local firmware update without Internet access

In addition to online updates, it is possible to carry out local updates without an Internet connection. This is intended for devices which do not have an Internet connection at their installation site and are only accessible via the local network. The firmware file can be selected locally using the *Select File* button and then started using the *Update Firmware* button. In this case, the user is responsible for ensuring that the update is compatible (see Section 9.9.3 "Compatibility of catalogue entry with firmware"). A downgrade to an older version is not possible using this process.

Note: To install a firmware update on a device of version v1.X, please contact support@ise.de.

9.9.3 Compatibility of catalogue entry with firmware

The version numbers in the catalogue entry and the firmware use an X.Y format. The main number, X, of the respective version indicates whether the catalogue entry and firmware are compatible. This is the case if both main numbers are identical. The second part of the version number, Y, is not relevant for compatibility. It simply indicates updates within the version.

If new firmware has a higher main number, it cannot be guaranteed that this version is compatible with an old ETS catalogue entry. For this reason, we recommend always unloading the application program from the device before the update and to then only use the new catalogue entry after that.

If the main numbers are the same, it may be necessary to use a new ETS catalogue entry for full functionality. However, this is not absolutely necessary if the new functions are not used in your project.

10 Technical data

KNX medium	TP
Commissioning mode:	S mode (ETS)
KNX supply	DC 21 to 30 V SELV
KNX connection	Bus connection terminal
External supply	
Voltage	DC 24 to 30 V ±10%
Connection	Bus connection terminal, preferably yellow (+)/white (–)
Power consumption	Typically 2 W (at DC 24 V, two Ethernet lines connected)
IP communication	Ethernet 10/100 BaseT (10/100 Mbit/s)
IP connection	2 x RJ45
Supported protocols	ARP, ICMP, IGMP, UDP/IP, DHCP, AutoIP
	KNXnet/IP as per KNX system specification: Core, Device Management
microSD card	Max. 32 GB microSDHC
Ambient temperature	0 °C to +45 °C
Storage temperature	-25 °C to +70 °C
Installation width	36 mm (2 HP)
Installation height	90 mm
Installation depth	74 mm
Protection type	IP20 (compliant with EN60529)
Protection class	III (compliant with IEC 61140)
Test marks	KNX, CE

11 Frequently asked questions (FAQ)

How do I find out the IP address of my ISE SMART CONNECT KNX REMOTE ACCESS?

Please read about this in Section 9.6 "Logging in on device website".

How much Internet data traffic occurs if I have connected the SDA connector to the portal?

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. This data volume is *not* considered by the SDA portal as user data in the sense of limiting the data volume in the licence agreement for the ISE SMART CONNECT KNX REMOTE ACCESS.

Which communication channel does the SDA connector use for the portal?

The SDA connector communicates with the SDA portal solely using an HTTPS connection via default port 443. Using this one connection, all data are exchanged in both directions so that it is generally not necessary to make a configuration in the firewall. If necessary,*.securedeviceaccess.net should be entered as the URL.

Why do I need to activate cookies to use SDA?

Cookies are used to secure access and the connection to SecureDeviceAccess. No tracking occurs! An exchange with third parties takes place only when linking user accounts with third-party providers.

Are there software updates for my ISE SMART CONNECT KNX REMOTE ACCESS device?

Information on software updates can be found in Section 9.9 "Firmware update of the device".

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

Without installing the SDA client software, you can access devices on the remote network which are accessible via HTTP. This means almost all devices which have a browser-based user interface. These devices are found automatically via UPnP. With the SDA client, all TCP-based protocols, e.g. Telnet, SSH, HTTPS, Window Remote Desktop, FTP and lots more, work alongside KNX/IP and the Gira HomeServer.

When carrying out access via HTTP, why do the corresponding group objects not report that a connection is no longer available immediately after my browser is closed?

You can find a comprehensive description on this in Section 8.5 "Connecting group addresses to group objects".

The KNX/IP interfaces which are published using the SDA client do not appear automatically in my ETS4. Why?

This problem can occur with ETS4 versions prior to ETS4.2. For information on this, please read Section 4.3.1 "Access to a KNX installation via KNX-IP."

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

For information on this, please read Section 8.2 "Configuration step 2 – Assigning physical addresses."

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

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

Can the website of my ISE SMART CONNECT KNX REMOTE ACCESS also be reached over the Internet?

Yes, the status page of the device can be called up securely over the Internet.

Why is the device website of my ISE SMART CONNECT KNX REMOTE ACCESS not displayed?

The browser used is not supported or the particular browser version 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 this documentation status). For security reasons, keep your browser up to date.

Why does the ETS report the error that a protected area cannot be written to when downloading the application program?

Please ensure that your ETS version is up to date. The ISE SMART CONNECT KNX REMOTE ACCESS requires ETS version 4.2 or 5.0.2 or higher.

Is the portal server really necessary?

The straight answer is: Unfortunately, yes! It would also be easier for us if we didn't need to operate any servers. However, there is no neat and clean technical solution available today which fulfils our requirements on stability and security. Remote access which is essentially always functional and does not require laborious configuration is only possible using a server.

What kind of data does the server save?

The server only saves the data which are absolutely required for provision of 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 transferred data volume.
The server does not save user data at any time!

Is operation of the server within Germany guaranteed?

Yes. Our portal 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. Due to their operation in Germany, the more restrictive (in comparison to other countries) German Data Protection Act applies.

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

Since all data has to pass through the SDA server (see above), continuous use is very performance intensive, in particular in the case of video streaming, for example. To always guarantee good performance, certain limitations are necessary. Should you have use cases which go beyond these conditions, please contact us. License models with expanded scope have not been ruled out for the future.

If I call up a website using SDA, it no longer functions correctly, even though it functions locally. How can that be?

Not all websites can be loaded from the remote network via SDA. More complex sites, in particular, such as those with Java implementations, may not function. In such cases, we ask that you send an e-mail to our support team (see Chapter 12 "Troubleshooting and support") with a precise description of the product, screen shots and a brief error description. We try to support as many products as possible via secure SDA HTTP access.

I have carried out a partial download with the ETS4, and now group communication does not work. Why?

Unfortunately, there is an implementation error in ETS4 with regard to partial downloads which is noticeable with our product. Please **never load the device with a partial download with ETS4**; always carry out an application download instead. This problem has been eliminated in ETS5.

Why do I see the previously configured physical and IP address after unloading the application on the website of the ISE SMART CONNECT KNX REMOTE ACCESS?

At present, the website is not updated after unloading until the device is restarted.

12 Troubleshooting and support

If you have a problem with your ISE SMART CONNECT KNX REMOTE ACCESS and require support, please send an e-mail with a detailed error description and the log file created after the error occurred to support@ise.de. For information on how to download the log files from your ISE SMART CONNECT KNX REMOTE ACCESS, please refer to Section 12.1 "Downloading log files if a problem occurs."

12.1 Downloading log files if a problem occurs

If a problem occurs, the log files are required for providing support. They can be downloaded via the website of the device (see Section 9.7.2 "Using the website of the device"). To do so, proceed as follows:

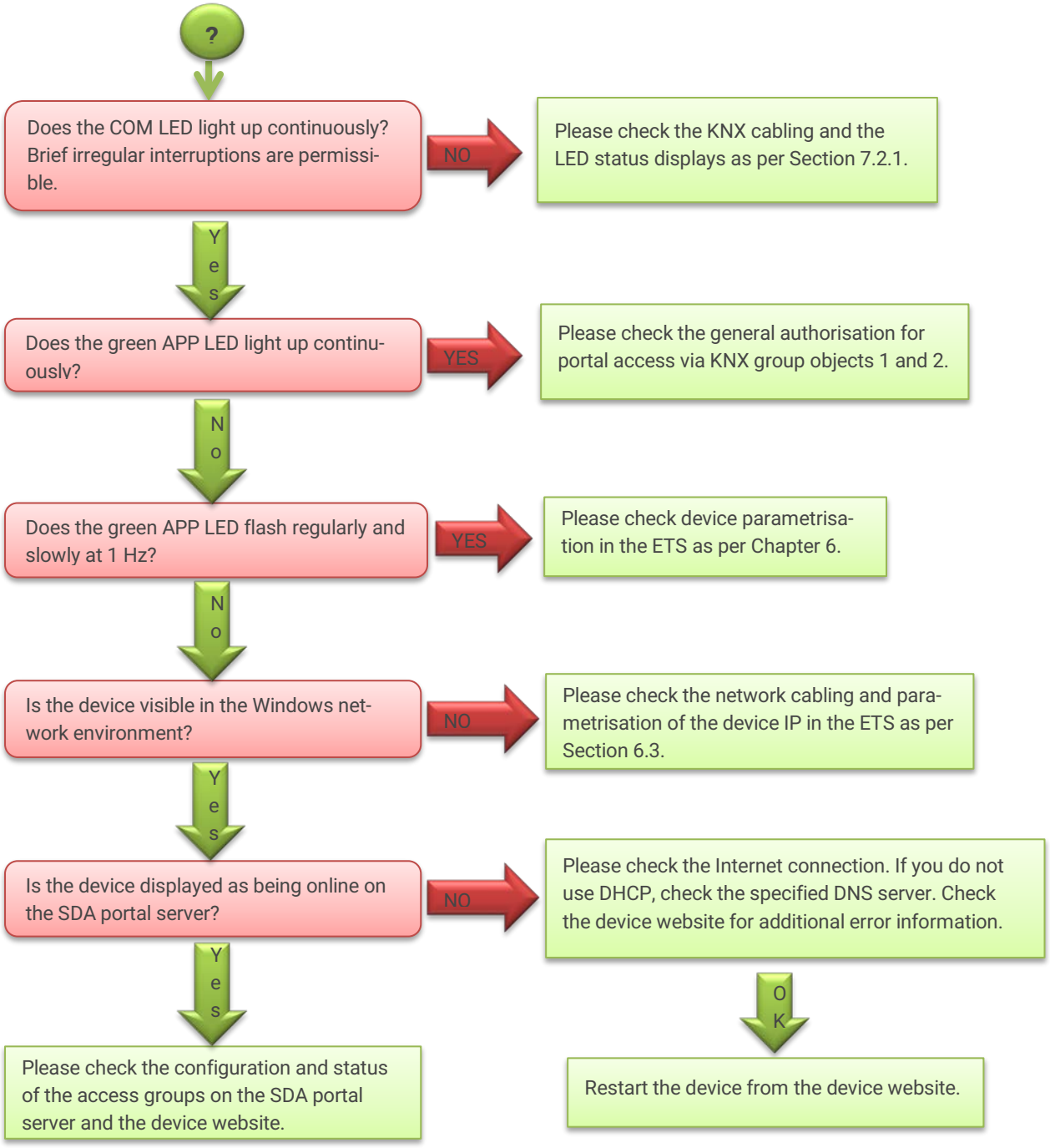
- Call up the website of the device. For this purpose, double-click the icon of the device in the *Multimedia* area in the network environment.
- Select *Device Status* in the upper menu bar on the website.
- Select *Download Log File* in the upper menu bar on the status page.
- The page which opens begins downloading the log files. If this does not occur, the provided link can be used.

12.2 Status page of the ISE SMART CONNECT KNX REMOTE ACCESS

You can call up the device status on the website of the ISE SMART CONNECT KNX REMOTE ACCESS (see Section 9.7.2 "Using the website of the device"). Among other things, it displays the installed software version and the configuration and connection status to the SDA portal server of the ISE SMART CONNECT KNX REMOTE ACCESS. Should an error occur, please send us a screen shot of the status page.

12.3 The ISE SMART CONNECT KNX REMOTE ACCESS does not work

The following error tree is intended to solve the most common problems. Should this be unsuccessful, please contact us at support@ise.de.



If neither of the above approaches of Chapter 9 provide a solution, please load the log files from the device (if possible) and send them together with an error description with as much detail as possible to support@ise.de.

13 ISE SMART CONNECT KNX REMOTE ACCESS software licence agreement

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

On accepting this agreement and installing the ISE SMART CONNECT KNX REMOTE ACCESS software or putting the ISE 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.

13.1 Definitions

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

Licensee: The legal recipient of the ISE SMART CONNECT KNX REMOTE ACCESS software.

Firmware: Software which is embedded on the ISE SMART CONNECT KNX REMOTE ACCESS hardware and enables operation of the ISE SMART CONNECT KNX REMOTE ACCESS.

ISE SMART CONNECT KNX REMOTE ACCESS software: The ISE SMART CONNECT KNX REMOTE ACCESS software designates all of the software provided for the ISE SMART CONNECT KNX REMOTE ACCESS product, including the operating data. This includes, in particular, the firmware and the product database. The SDA client software and SDA portal are also included.

13.2 Object of the agreement

The object of this agreement is the ISE SMART CONNECT KNX REMOTE ACCESS software provided on data media or through downloads, the SDA client software as well as the corresponding documentation in written and electronic form and the provision of the SDA portal.

13.3 Rights of use of the ISE SMART CONNECT KNX REMOTE ACCESS software

13.3.1 Firmware and SDA client

The Licensor grants the Licensee the non-exclusive, non-transferable right to use the ISE 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 form 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.

13.3.2 Secure Device Access portal

The Licensor provides the Licensee with a Secure Device Access portal server under https://securedeviceaccess.net for use with the firmware and SDA client. For this purpose, the Licensor currently utilises the service of ise Individuelle Software und Elektronik GmbH. The licensor can cancel operation of the SDA portal server with a notice period of 5 years for an important reason. In this case, the Licensor must make the SDA portal software available to the SDA Licensee as source code upon request to enable your own hosting of the server software and thus enable continuous use of SDA.

13.4 Restriction of rights of use

13.4.1 Maximum permissible transfer volume

The license rules out the use of continuous remote access, e.g. for visualisation or location networking. We consider repeated uninterrupted use for more than 12 hours at a time to be continuous use.

The transfer volume is limited to a maximum of 2 GB per month per SDA connector.

We reserve the right to implement the usage limits named above using technical measures.

13.4.2 Copying, modification and transmission

The Licensee is not authorised to use, copy, modify or transfer the ISE 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.

13.4.3 Reverse engineering and conversion technologies

The licensee is not authorised to apply reverse-engineering techniques to the ISE SMART CONNECT KNX REMOTE ACCESS software or to convert the ISE SMART CONNECT KNX REMOTE ACCESS software into another type. Such techniques include, in particular, disassembly (conversion of the binary-coded computer instructions of an executable program into an assembler language which can be read by humans) or decompilation (conversion of binary-coded computer instructions or assembler instructions into source code in the form of high-level language instructions).

13.4.4 Firmware and hardware

The firmware may only be installed and used on the hardware (ISE SMART CONNECT KNX REMOTE ACCESS) approved by the Licensor.

13.4.5 Transfer to a third party

The ISE SMART CONNECT KNX REMOTE ACCESS software may not be passed on to third parties, nor may it be made accessible to third parties.

13.4.6 Renting out, leasing out and sub-licensing

The Licensee is not authorised to rent or lease the ISE SMART CONNECT KNX REMOTE ACCESS software or grant sub-licenses to the program.

13.4.7 Software creation

The Licensee requires written approval from the Licensor to create and distribute software which is derived from the ISE SMART CONNECT KNX REMOTE ACCESS software.

13.4.8 The mechanisms of license management and copy protection

The mechanisms of the license management and copying protection of the ISE SMART CONNECT KNX REMOTE ACCESS software may not be analysed, published, circumvented or disabled.

13.5 Ownership, confidentiality

13.5.1 Documentation

The ISE SMART CONNECT KNX REMOTE ACCESS software and the documentation (which shall be provided in printed form 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.

13.5.2 Transfer to a third party

Neither the software nor the data backup copy nor the documentation (which shall be provided in printed form 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 charge or free of charge.

13.6 Changes, additional deliveries

The ISE 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 subject to possible changes by the licensor.

13.7 Warranty

The ISE SMART CONNECT KNX REMOTE ACCESS software shall be delivered together with software from third parties as listed in Chapter 14 – *Open Source Software*. No warranty is provided for software from third parties.

13.7.1 Software and documentation

The ISE 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 ISE SMART CONNECT KNX REMOTE ACCESS software is twenty-four (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 in accordance with the documentation included with it in the 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.

13.7.2 Limitation of warranty

Otherwise, no warranty shall be provided for the freedom from faults of the ISE SMART CONNECT KNX REMOTE ACCESS software and its data structures from defects. Nor does the warranty cover defects due to improper use or other causes outside the influence of the Licensor. Any additional warranty claims shall be excluded.

13.8 Liability

The Licensor shall not be liable for damages due to loss of profit, data loss or any other financial loss resulting from use of the ISE SMART CONNECT KNX REMOTE ACCESS software, even if the Licensor is aware of the possibility of such damage.

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 by premeditation or gross negligence on the part of the Licensor. Furthermore, claims based on the statutory regulations for product liability shall remain intact.

13.9 Applicable law

This agreement is subject to the laws of the Federal Republic of Germany.

The place of jurisdiction is Oldenburg (Oldb).

13.10 Termination

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

The license to use the ISE SMART CONNECT KNX REMOTE ACCESS software shall expire upon termination of the agreement. The ISE SMART CONNECT KNX REMOTE ACCESS product must be taken out of operation in such a case. Further use of the ISE SMART CONNECT KNX REMOTE ACCESS without a license is precluded.

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

13.11 Subsidiary agreements and changes to the agreement

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

13.12 Exception

All rights not expressly mentioned in this agreement are reserved.

14 Open Source Software

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

The individual software packages used, along with their licenses, are listed and described on the device website for this product under System / Licenses.

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

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