Status of the documentation:
14.07.2015
Printing date: 23.07.2015

Product Manual

ise smart connect KNX Secure

Order No. 1-0003-004

Valid for Application Software version 2.1, Firmware version 2.2 and SDA Client v1.1

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 applications using freely configurable TCP port forwarding through the SDA client for Windows
- KNX/TP connection with integrated IP interface (tunnelling server) for KNX access using the ETS or other software, max. three simultaneous connections, to be used for download and group as well as bus monitoring
- Status signalling and access management of the secured connections through KNX group 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 Secures 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 Secure or other KNXnet/IP devices using the direct KNX-IP connection.
- Configuration of the ise smart connect KNX Secure is carried out using the latest version of ETS4 or ETS 5. The application accesses ETS functions not supported by earlier ETS versions. This is why previous versions of ETS cannot be used for configuration.

1.2 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.

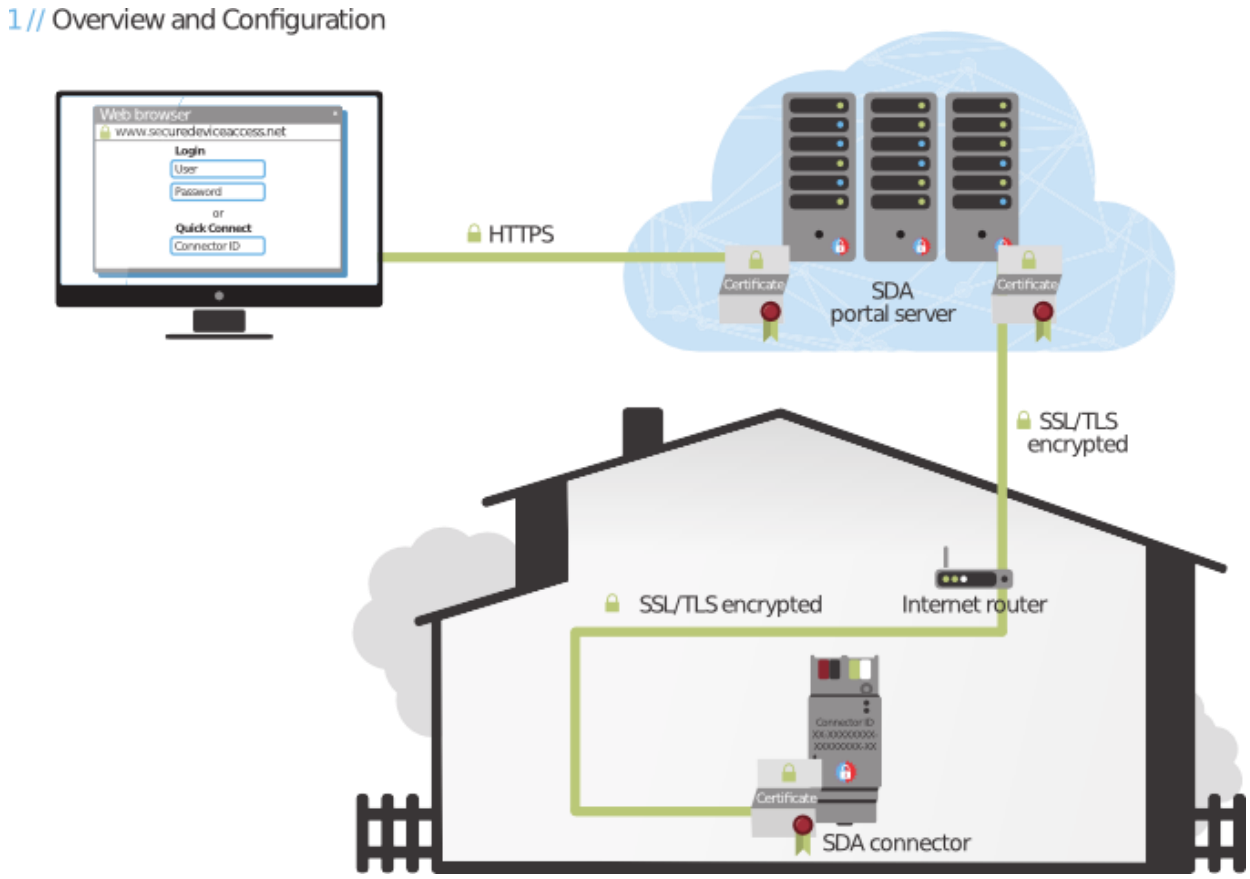


Figure 1 – Overview of secure access with "Secure Device Access"

1.2.1 ise smart connect KNX Secure, "SDA connector" in general

The ise smart connect KNX Secure (referred to as the "SDA connector" in the following) is the device for which you are currently reading the instructions. It 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 1.2.4).
Using the Ethernet connection to the home network, you can now access almost all network devices using the Internet. 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 different platforms (see 1.2.6).
If you have a KNX installation in your house, you can connect it to the ise smart connect KNX Secure 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.

1.2.2 Quick Connect

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

Using the connector ID, you can access your end devices immediately after unpacking and connecting them without any additional logging in.
Part of the connector ID is randomly generated and therefore cannot be guessed. Whoever knows the connector 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. Access is then no longer possible via "Quick Connect" unless you enable this explicitly again.

SDA portal server

1.2.3 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.

HTTPS proxy httpaccess.net

1.2.4 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 SDA 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.

Communication – Secure, reliable and easy-to-handle

1.2.5 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.
Through the use of standard protocols and due to the fact that the SDA connector actively connects to the SDA portal server, we achieve optimum 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.

Client software (SDA client)

1.2.6 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. 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 applications are supported.

1.3 Definitions and explanation of terms

- Secure Device Access, or SDA
  Designates the entire system which provides secure access to your home over the Internet. See 1.2.
- 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 1.2.3.
- SDA connector, ise smart connect KNX secure
  The SDA connector is a small electronic device which is connected to your home network and which links it to the portal server. See 1.2.1.
- Connector ID
  Each SDA connector has a unique ID which is printed on the device. This 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 connector ID is random and cannot be guessed.
- Quick Connect
  Access to devices behind an SDA connector without having to log in to a portal by simply entering the connector ID. See 1.2.2. Quick Connect is the counterpart of Portal Connect
- Portal Connect
  Access to devices behind an SDA connector after logging in to a portal. See 1.2.3. Portal Connect is the counterpart of Quick Connect.
- SDA client
  Computer software which enables other applications to communicate via SDA without them having to know anything about SDA.
- Device, network device
  A device with a network connection or KNX connection installed in your home which is to be accessible via SDA.
- 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.
- Installers
  Access group for external service providers. Access is blocked from this group as standard.

- Residents
  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 the SDA portal server. 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."
- 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

Quick Connect vs. SDA portal

2.1.1

The easiest and quickest usage type is Quick Connect. With Quick Connect, remote access of the installation occurs solely by entering the connector ID (see also 1.2.2) which is printed on the device. This has the advantage of not having to log a user into the portal. An example application would be an ise smart connect KNX Secure at a construction site in connection with a UMTS/LTE router which is 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.

Limitations and authorisation of access rights via KNX group objects

2.1.2

If the ise smart connect KNX Secure is added in an ETS project, its group 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.

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) are transported to the SDA portal server via an encrypted SSL/TLS connection and then to the web browser via an HTTPS connection.

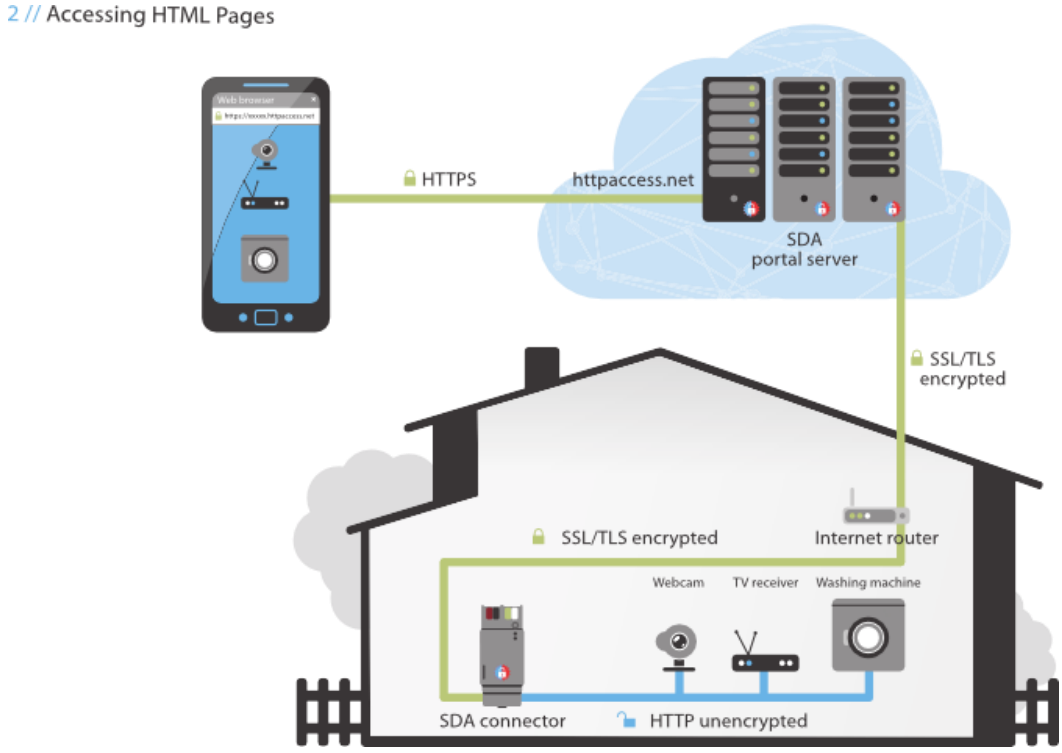


Figure 2 – Secure access to websites via "Secure Device Access"

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.

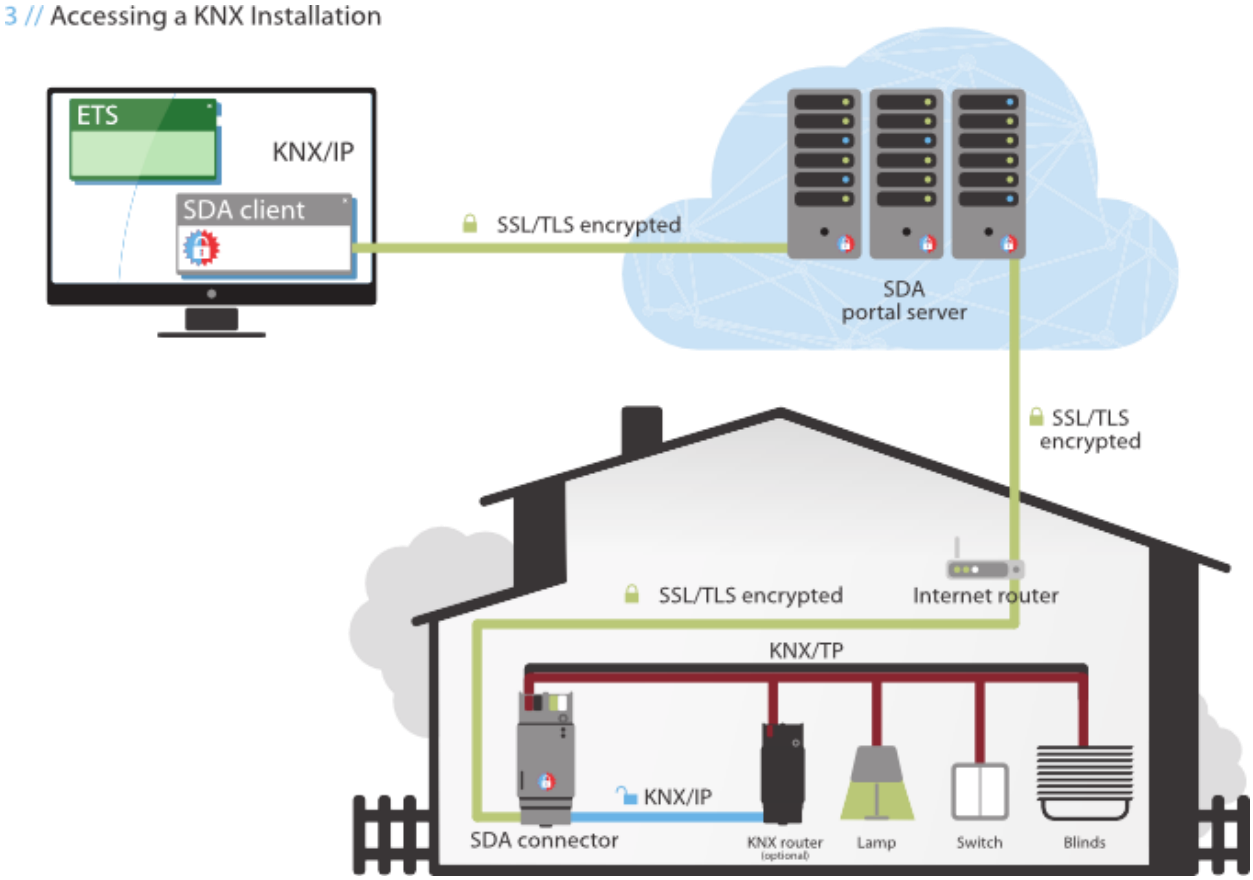


Figure 3 – Secure access to the KNX installation with "Secure Device Access"

Once a connection to a specific SDA connector has been established with the SDA client (see Section 4.2), the KNX/IP interfaces 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 7.3) 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.

2.4 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. On the other, the configuration is supported with the Expert. All data are also encrypted upon transmission over the Internet here.

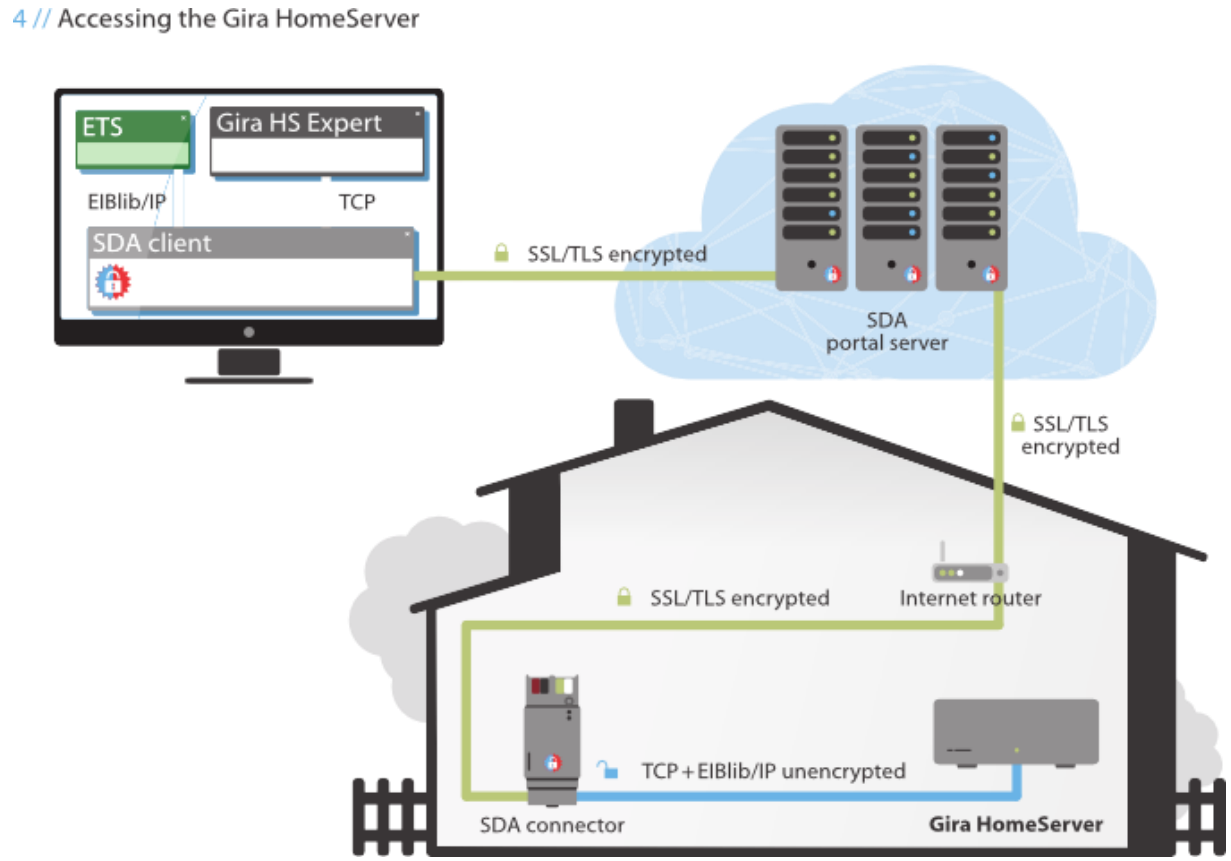
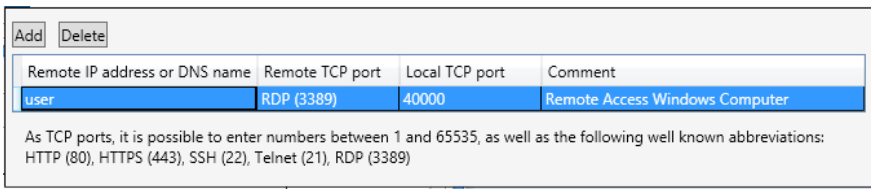


Figure 4 – Secure configuration of the Gira HomeServer with "Secure Device Access"

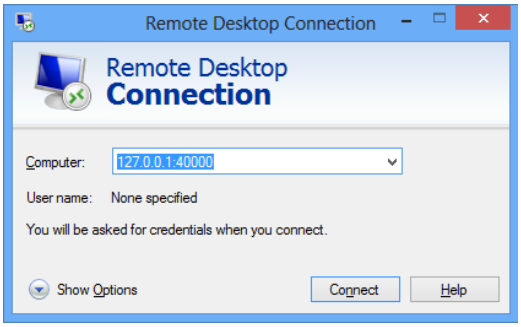
Note: Since automatic detection is not possible for the Eiblib/IP and the HomeServer configuration protocol, the following must be observed for the use of these protocols via SDA: The SDA client makes available protocol transmission locally over IP address 127.0.0.1, i.e. if an Eiblib/IP connection is 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.

2.5 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. Access is made possible by a single TCP connection configuration:



Note the following here: 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 ("csd-i7" in our example), you will have to enter the port if it does not correspond to the default port. In our example, the connection can be established as follows.



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.

Additional information can be found in Section 4.3.4.
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.

2.6 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 group 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 the "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 group 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 group objects to make appropriate processing in a visualisation/logic (e.g. e-mail when someone connects) easily possible.

3 Use 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 web-sites on the remote network by entering a user or 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 connector ID printed on the device

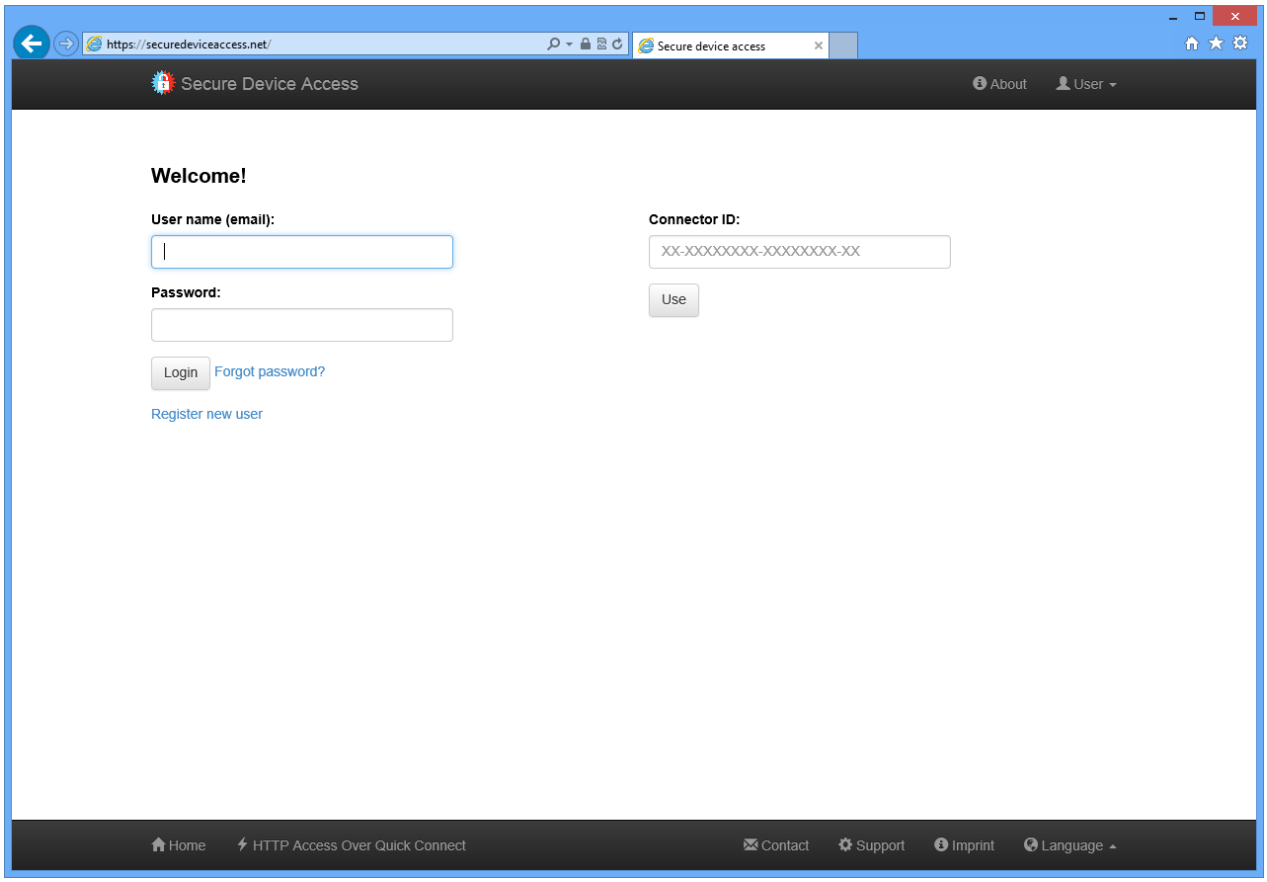


Figure 5 - SDA portal – Start page

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 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.

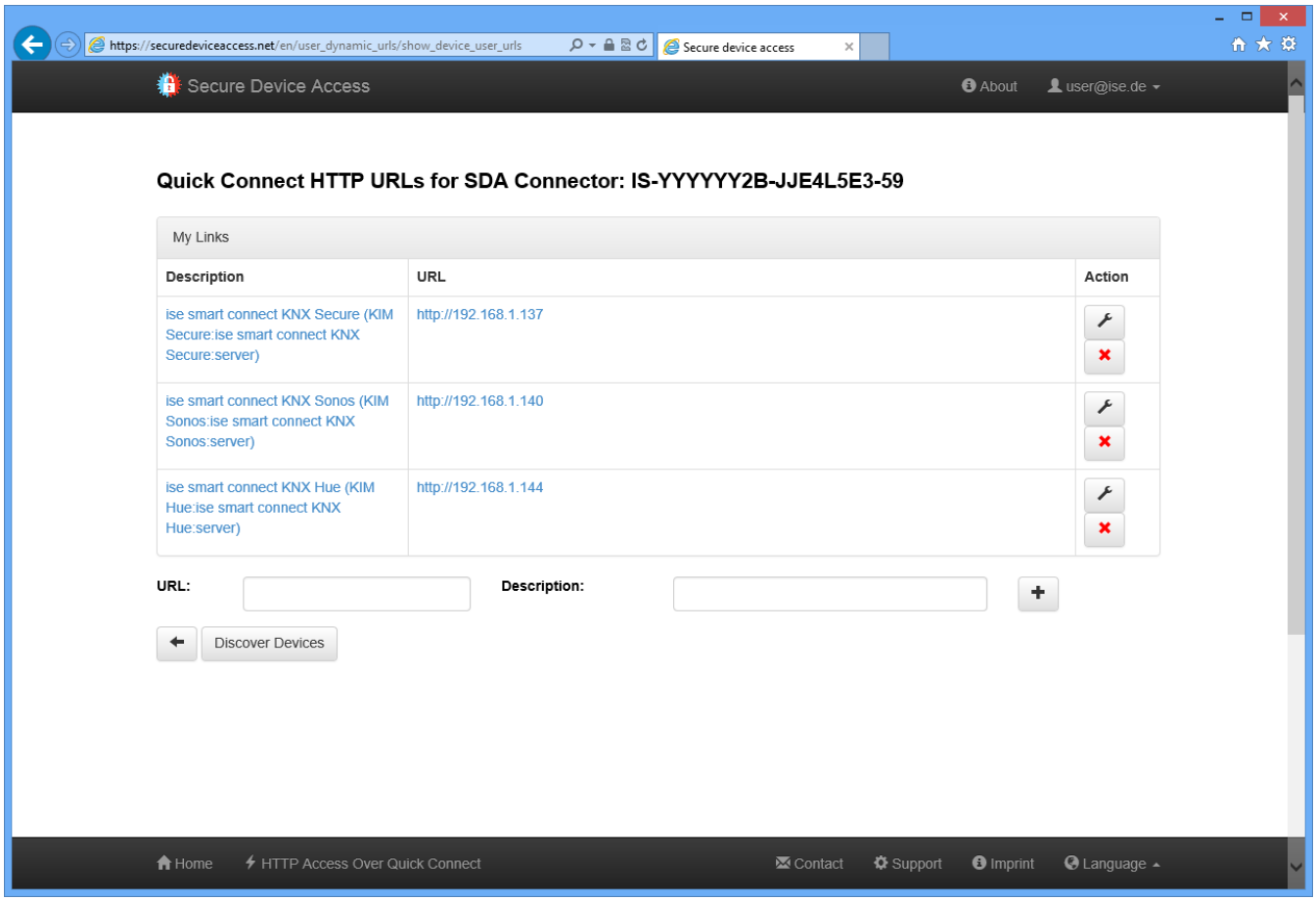


Figure 6 - Access to HTTP websites via Quick Connect

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.

Important note: 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 10) with a precise description of the product, screen shots and a brief error description.

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 Secure 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 connector ID and thus become the owner (for an important note, see Section 3.9)

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 an important note, see Section 3.9)

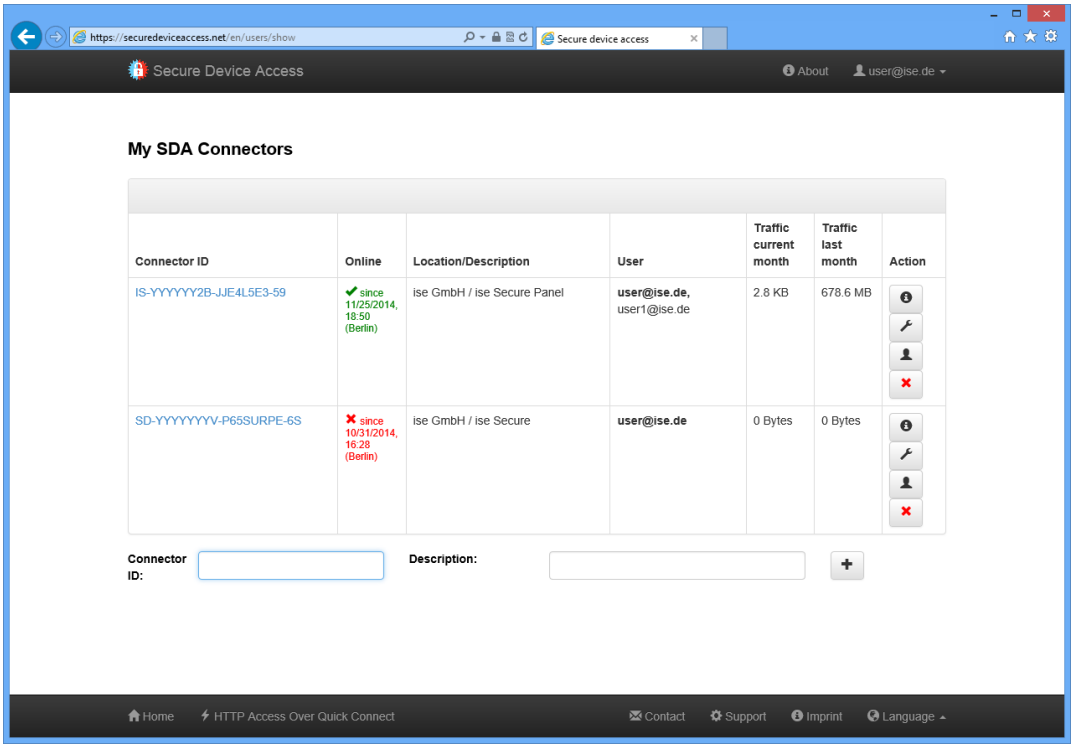


Figure 7 – SDA connectors of the logged in user

In the list of SDA connectors linked to your user, you can access websites on the remote network using the corresponding SDA connector via the "Connector 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 3.9). 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 11.
Up to four actions can be available (depending on the user rights):

- Display of expanded information on an SDA connector (see Section 3.6)
- Display and change properties of an SDA connector (see Section 3.7)
- Manage access rights for other users (see Section 3.8)
- Delete connection with SDA connector (Note: this is not possible as long as you are the owner of the SDA connector! See also Section 3.9)

3.5 HTTP access via Portal Connect

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

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 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 firmware version) currently running on the SDA connector

3.7 Displaying and changing properties of an SDA connector

This page enables the description and access groups applicable for the logged in user to be changed. The location and Quick Access can also be changed for the SDA connector if the logged in user has access rights for this.

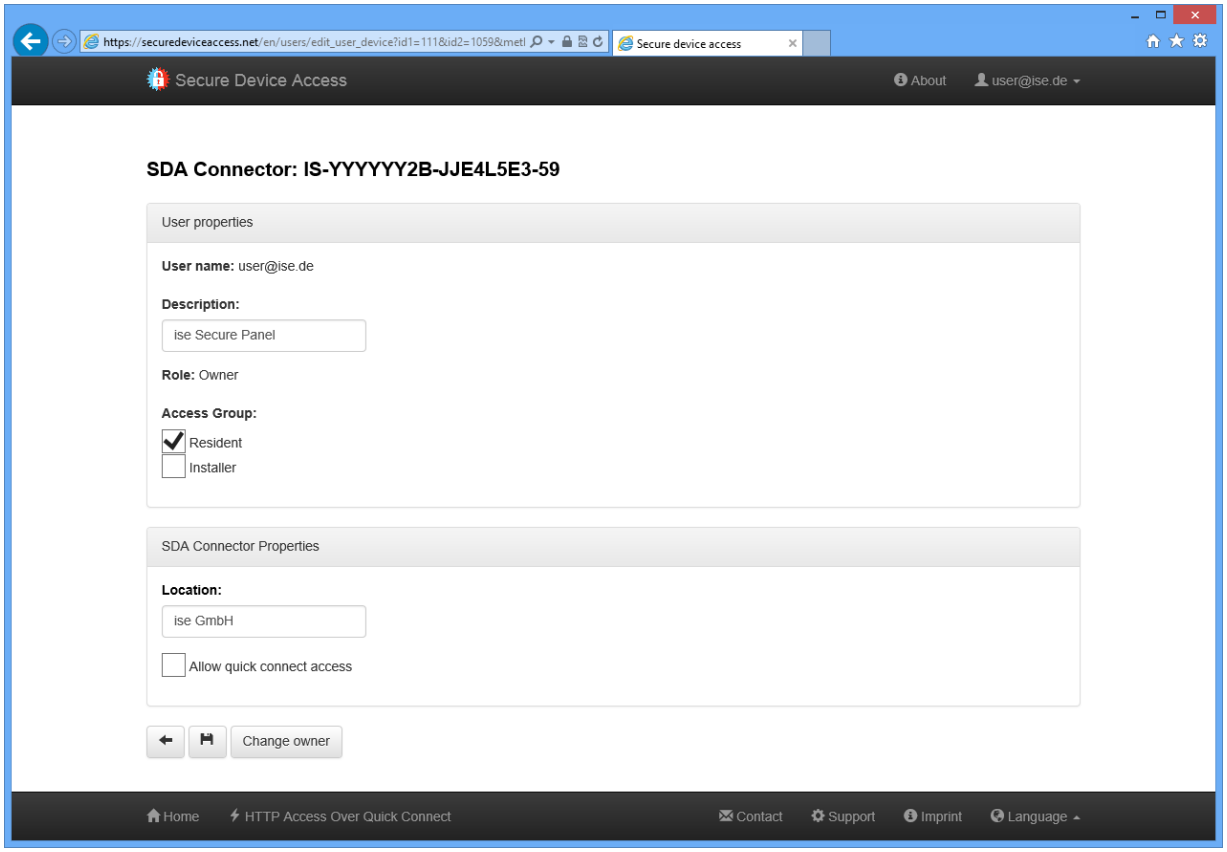


Figure 8 – Displaying and changing properties of an SDA connector

3.8 Managing access rights for users

Secure Device Access enables different configuration of access rights on a user-by-user basis.
The following can be defined for each user (if the currently logged in user possesses the corresponding rights):

- Role: Possible options here include "owner", "administrator" and "user", whereby the owner is an administrator with a special position (see Section 3.9), 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.

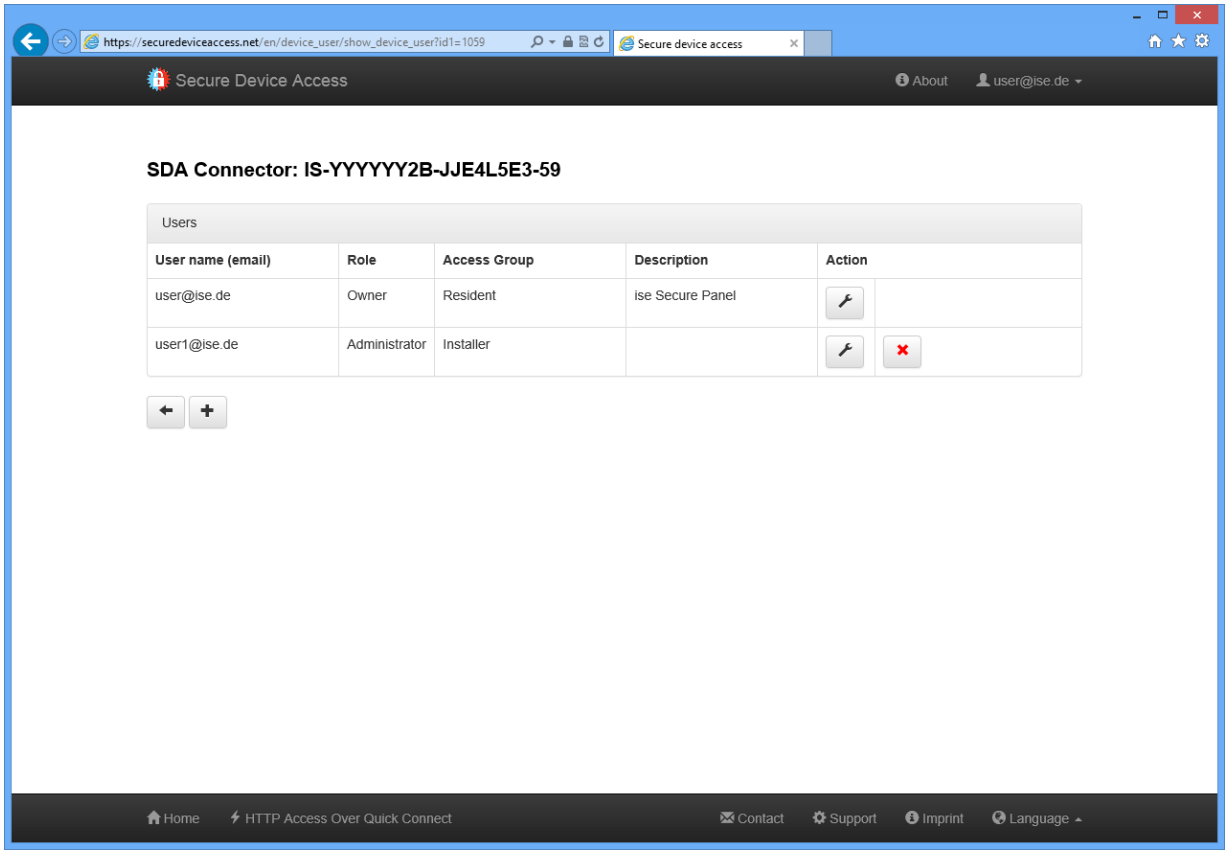


Figure 9 – Managing access rights for other users

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.

Important: 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 3.8.2)!

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 group 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 Section **Fehler! Verweisquelle konnte nicht gefunden werden.**.

Important: 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 3.8.1)!

3.9 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 (see 3.7). 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 an Internet browser. See Section 2.2. 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 http://www.securedeviceaccess.net under Service/Downloads.

4.1 General settings

Using the button for general settings on the top right-hand side (see figure), you can enable extended logging for problem analysis and you can create a ZIP archive with the log files for an e-mail to support, or you can clear the logfiles.
Furthermore, you can specify whether the SDA client should remember the last password used and whether you would like to have Gira HomeServer support activated 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.
In addition, you can configure the connection timeout for the connection to the SDA portal. 3 seconds is a good value for 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, it can easily be done by increasing the timeout.
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 for this purpose.

Figure 10 – General settings in the SDA client

4.2 Connecting to an SDA connection using the SDA client

As described above, there are two options for establishing a connection to an SDA connector: Quick Connect and Portal Connect.
For this reason, you first select the connection type after starting the SDA client.

Establishing a connection via Quick Connect

Select "Quick Connect" as the connection type (see figure). Then enter the connector ID in the field next to it. 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.

4.2.1

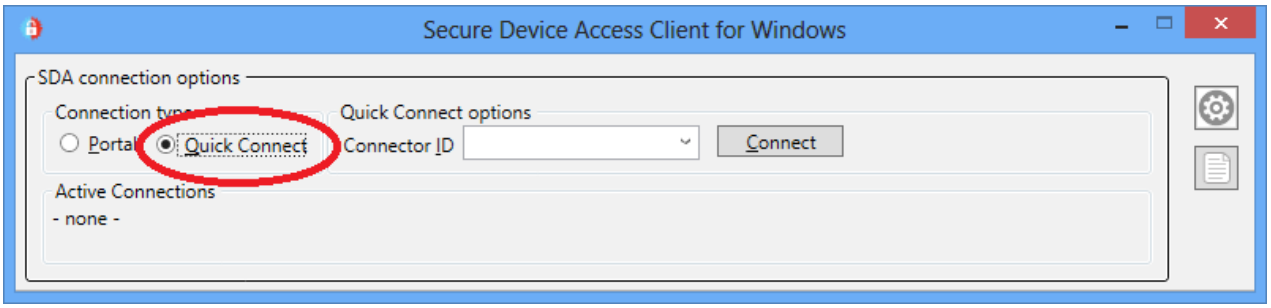


Figure 11 – Connecting SDA connector via Quick Connect

After entering a valid SDA connector 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 ff.), you can establish the connection using the "Connect" button.

Establishing a connection via Portal Connect

4.2.2

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

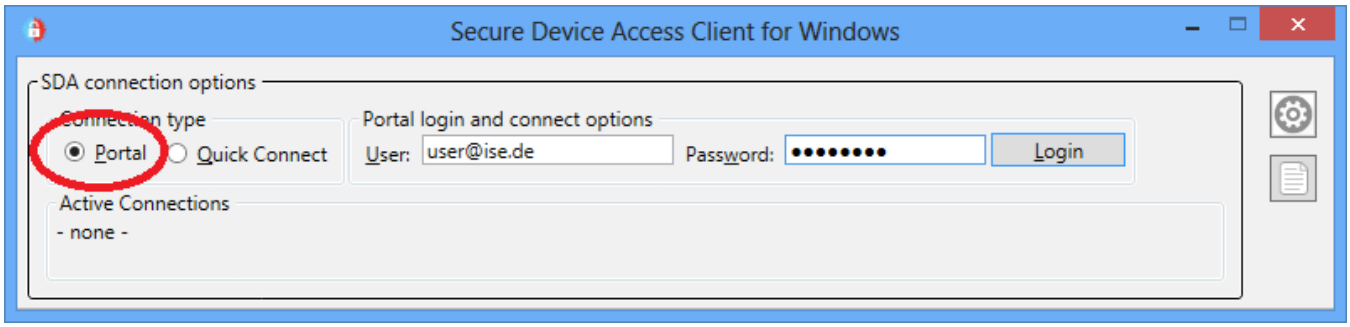


Figure 12 – Logging in to the SDA portal server

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.

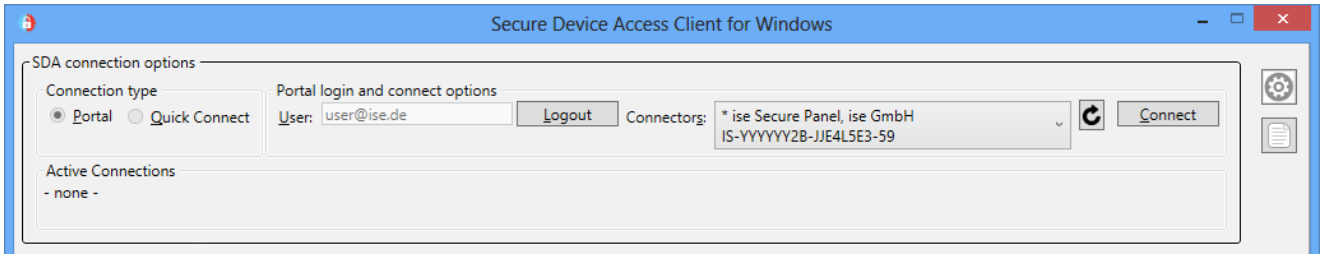


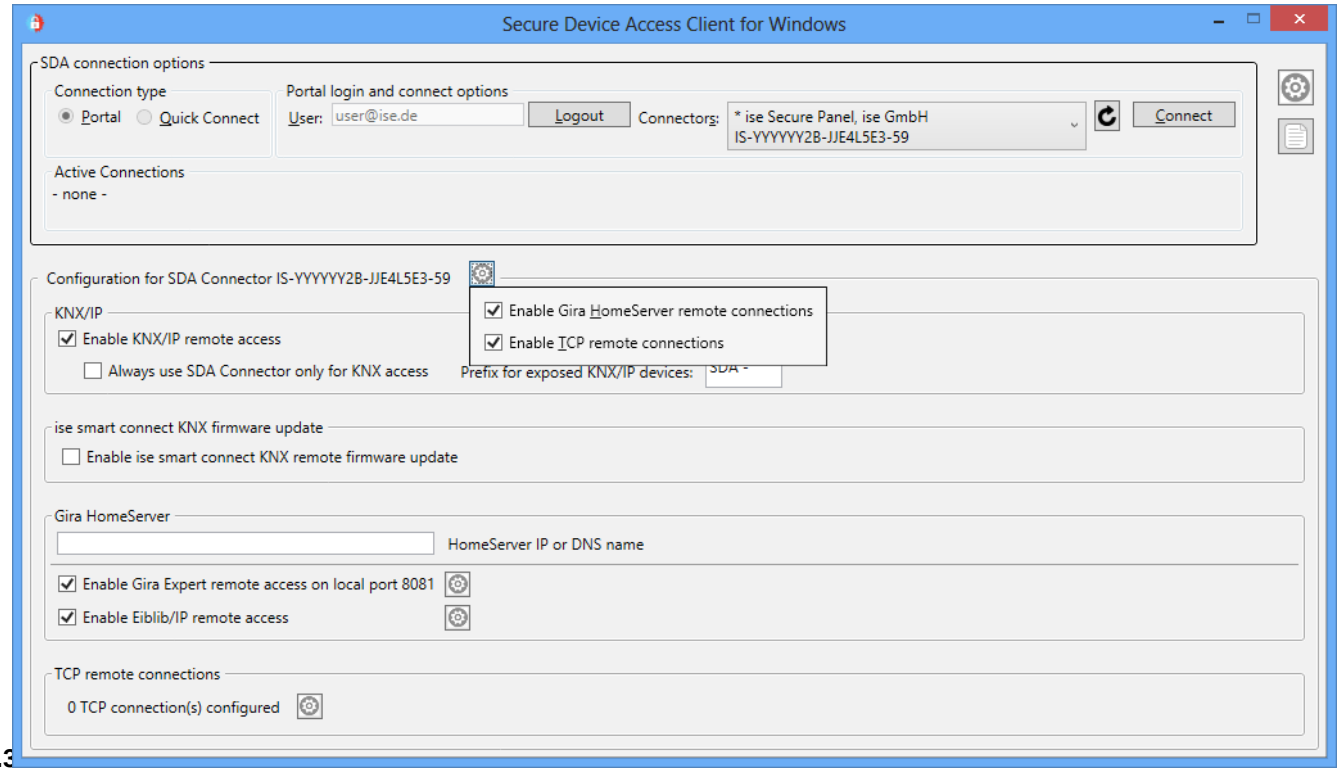
Figure 13 – Using SDA connector via Portal Connect

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 ff.), you can establish the connection using the "Connect" button.

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 Secure 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, the software of ise smart connect devices can also be updated remotely if necessary with the ise Update Tool using SDA.
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).



4.3

Figure 14 – SDA connector configuration options

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 (see ETS options) 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 Secure accessible via SDA, e.g. because there are many devices on the remote network and you are in a hurry.

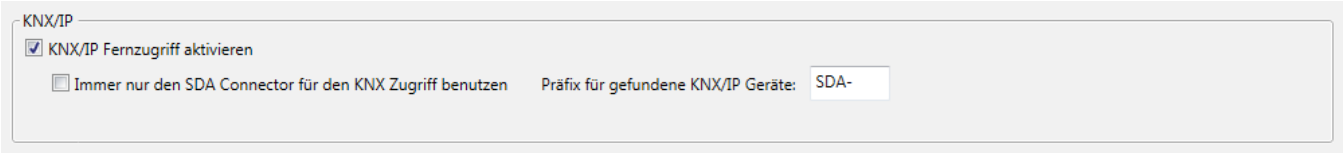


Figure 15 – KNX/IP remote access configuration

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.

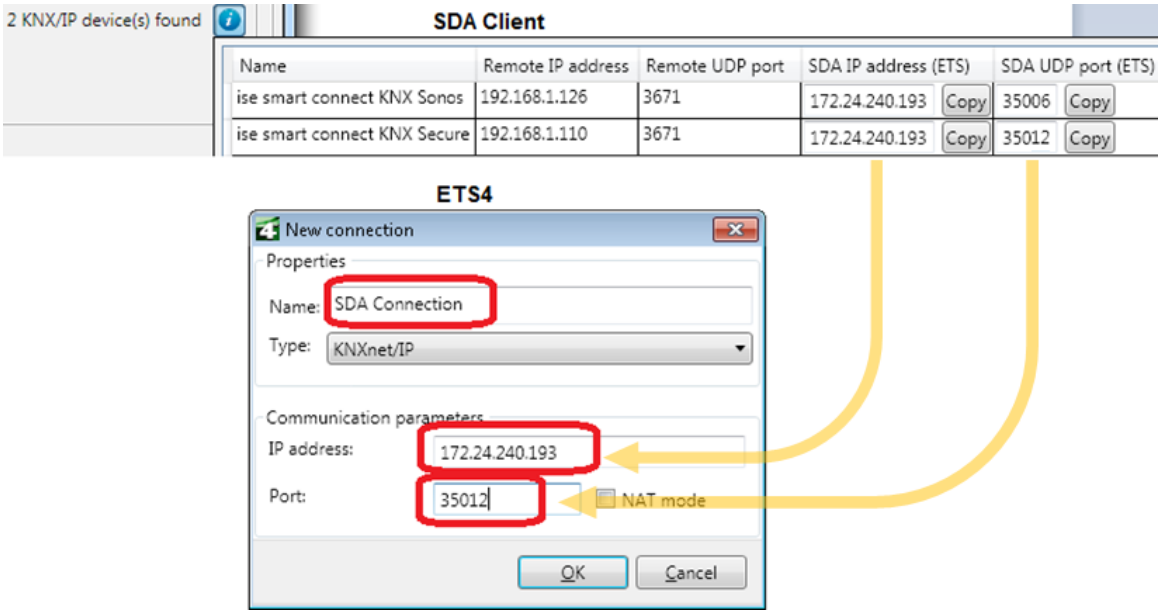


Figure 16 – Manual KNX/IP interface configuration for ETS prior to ETS4.2

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.

4.3.2 Updating the software of ise smart connect devices

Note: The SDA communication is specifically optimized for the KNX protocol. Hence, the KNX communication is stable also via slow Internet connections.

The ise Update Tool is available for updating the device software (firmware) of ise smart connect devices should this be required. If you activate the option for the firmware update in the SDA client, you can then also update the software remotely using the ise Update Tool.
Please note here, that the SDA connection must already have been established by the time the ise Update Tool is started.
A description of the update procedure with the ise Update Tool is provided with the tool.

Important note: Searching for and querying devices for the firmware update noticeably delays establishment of the SDA connection. Please only activate this option if you want to perform a firmware update.

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

4.3.3

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.
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.

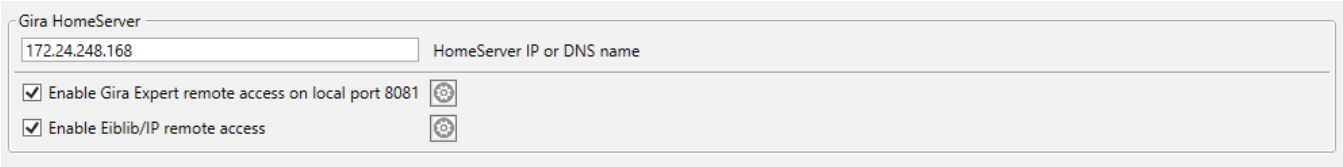


Figure 17 – Gira HomeServer remote access configuration

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).

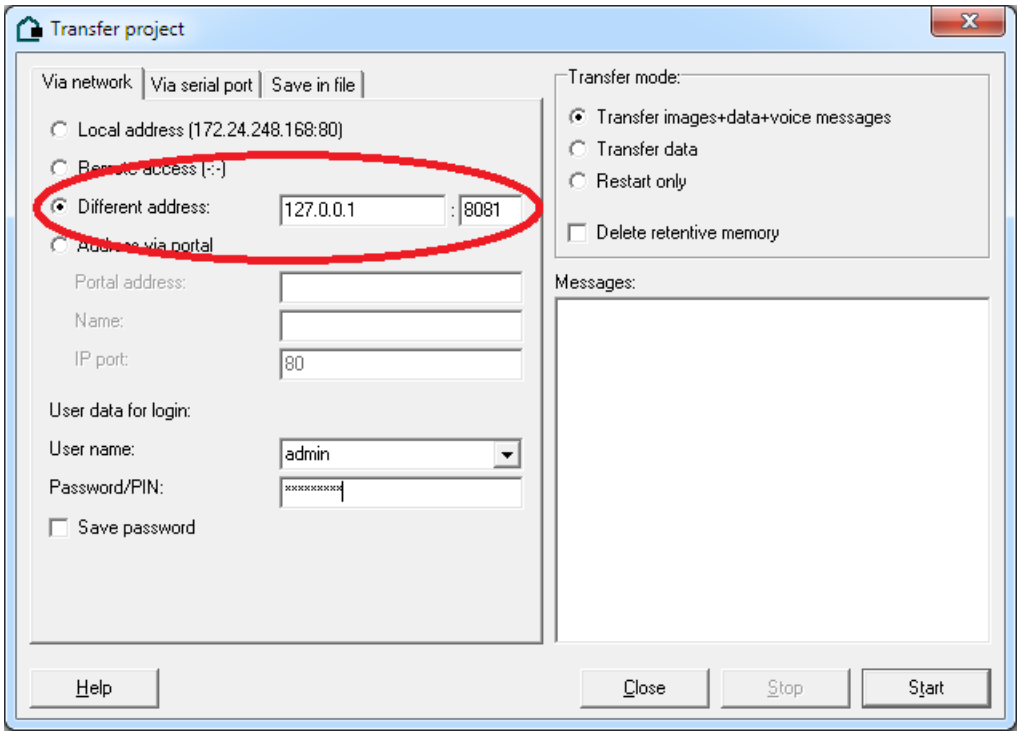


Figure 18 – Transferring a project with the Expert via SDA

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).

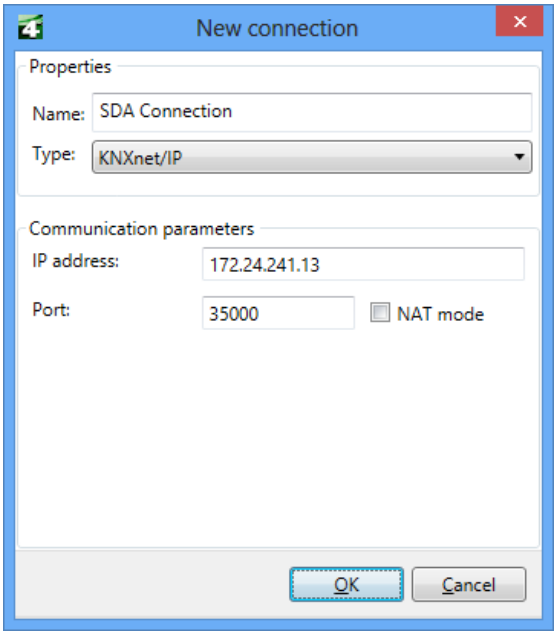


Figure 19 – Using the HomeServer with Eiblib/IP via SDA for KNX connection

4.3.4 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).

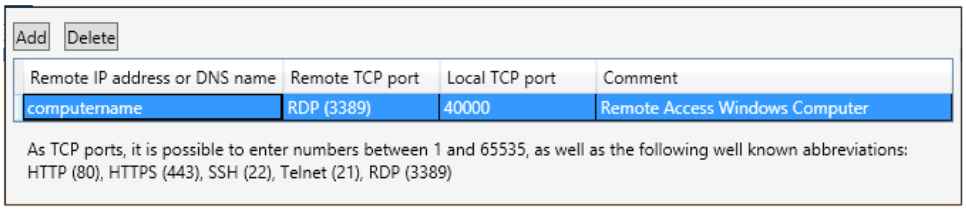


Figure 20 – TCP remote access configuration

Please also read Section 2.5 for this purpose.

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.

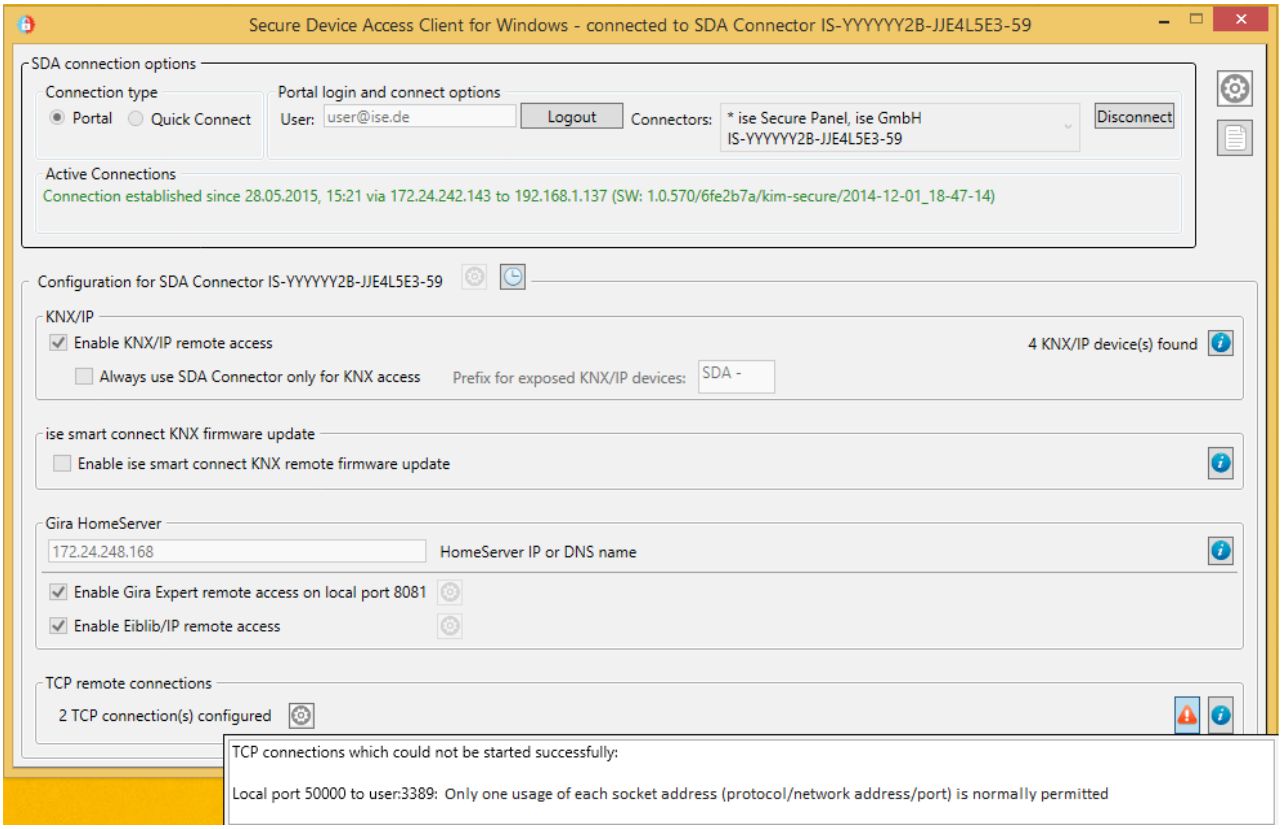


Figure 21 – Status information in the SDA client after connection establishment

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: Below the button for the general settings at the top right there is a button with a symbol resembling a piece of paper which has been written on. It provides detailed connection information to experts in a log book window.

4.5 Measuring the communication performance

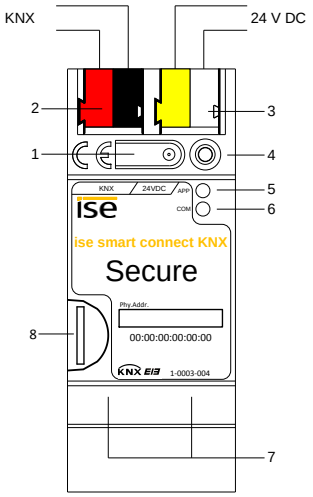
By using the button with the stop watch symbol right to the configuration button, it is possible to perform a communication performance measurement when having a connection etsablished successfully. The roundtrip time (the time span beginning with sending q request to the remote SDA Connector and receiving the reply from the SDA Connector) is between 30-40 milliseconds for fast Internet connections and can go up to seconds using very slow connections.
Important note: Having a roundtrip duration above five seconds in average will cause problems with the KNX communication.

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 Installation, electrical connection and operation

5.1 Device design



Dimensions:

Width (W):
36 mm (2 HP)

Height (H):
90 mm

Depth (D):
74 mm

Figure 22: ise smart connect KNX Secure

1	Programming button for KNX	Switches the device to the ETS programming mode or vice versa.
2	KNX connection (twisted pair)	On left: (+ / red) On right: (– / black)
3	Connection for power supply	DC 24–30 V, 2 W (at 24 V) On left: (+ / yellow) On right: (– / white)
4	KNX programming LED (red)	Red: Device is in ETS programming mode Yellow: For start or diagnosis code, see 7.2.1 / 7.2.2
5	LED *APP* (green)	Green: Normal operation Off/ Flashing: For start or diagnosis code, see 7.2.1 / 7.2.2
6	LED *COM* (yellow)	Yellow: Normal operation (brief dark phases indicate KNX tele-gram traffic) Off/ Flashing: For start or diagnosis codes, see 7.2.1 / 7.2.2
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 Flashing: Data reception on IP
8	MicroSD card holder	The SD card is not used in the current device software. Media size: Up to 32 GB microSDHC Formatting: FAT32

5.2 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.

5.3 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 it audibly engages (comp. Configuration A).
- Removing the cover cap: The cover cap is removed by pressing it in slightly on the side and pulling it off to the front (comp ConfigurationB).

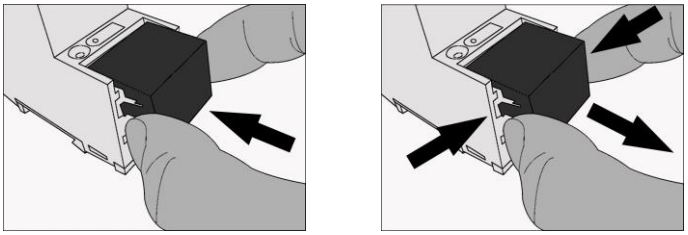


Figure 23: Mounting/removing a cover cap.

6 Configuration in the ETS

Note: Upon delivery and also after a factory reset, the ise smart connect KNX Secure 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 Secure is divided into the following steps:

Preparations:		**For explanations, see**
1	Mount device and connect it to KNX bus connection and auxiliary voltage.	→ Chapter 5
2	Install the ise smart connect KNX Secure 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 Secure as a device in the ETS.	→ Section 6.1
2	Assign the physical address of the device and the maximum three physical addresses of the interface as usual according to the KNX topology. **Important note:** As one of the first devices on the market to do so, the ise smart connect KNX Secure 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 6.2
3	Set IP address, IP subnet mask and default gateway address of the ise smart connect KNX Secure or select "Obtain an IP address automatically (from a DHCP server)".	→ Section 6.3
4	Set general parameters, incl. DNS server for the ise smart connect KNX Secure.	→ Section 6.4.1
5	Connect group addresses to group objects as usual.	→ Section 6.5
6	The ise smart connect KNX Secure is now ready for commissioning via "*Program ETS*" and for testing of the functions.	

6.1 Configuration step 1 − Create ise smart connect KNX Secure as device in the ETS

If it has not yet been done, import the ETS device application to the ise smart connect KNX Secure 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.

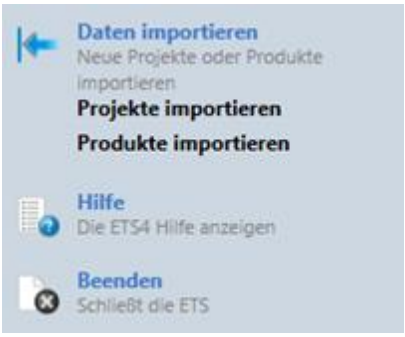


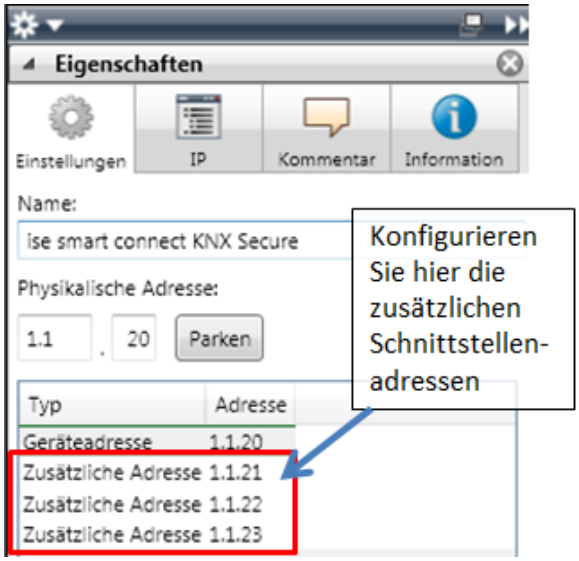
Figure 24: Product import via the ETS4 start page.

The other explanations in this document refer to

Hardware		Application software	
Device:	**ise smart connect KNX Secure**	Application:	ise smart connect KNX Secure
Manufacturer:	**ise GmbH**	Version**:**	**V2.1**
Order No.	**1-0003-004**		
Version:	**V1.0**		
Design:	**DRA (series installation)**		

6.2 Configuration step 2 – Assigning physical addresses

The ise smart connect KNX Secure has access to three tunnelling servers (KNX/IP interfaces). In addition to the physical address of the device, the device also has (up to) three additional physical interfaces. These interfaces can be used for download and group as well as bus monitoring.
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.



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.

6.3 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 Secure must also be assigned an address on the IP data network. This includes the following information:

- IP address
- Subnet mask
- Address of the default gateway

- DNS server

This can occur in two ways, either

- automatically by obtaining the data from a DHCP server (e.g. integrated in the router of the data network) or
- via manual setting in the ETS.

Proceed as follows for this purpose:

1. Select the device in the ETS.

2. Display the properties of the device in the sidebar of the ETS as shown in Figure 25.

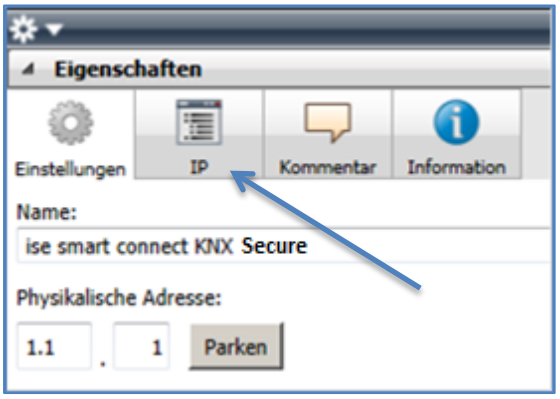


Figure 25: Device properties dialog of the ETS

3. Select the "IP" tab as per Figure 26. Then select either

   ⊙*Obtain an IP address automatically (default)*

   The address data are obtained automatically from a DHCP server on the data network.

   or

   ⊙ *Use the following IP address*

   Here, you 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 6.4)!

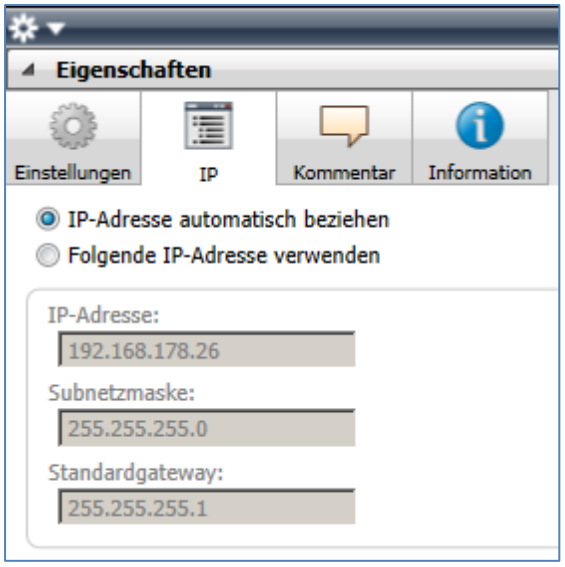


Figure 26: Setting of the IP address data of the device on the "IP" tab in the sidebar of the ETS

If the ⊙ *Obtain an IP address automatically* setting is used, a DHCP server must issue the ise smart connect KNX Secure 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.

6.4 Setting general parameters.

Parameter page *General*

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

Parameter	Entry/Selection	Remarks
6.4.1 DNS server (if not using DHCP)	**Default gateway**	The IP address of the default gateway is used (see Section 6.3 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 the default gateway is used, then 0.0.0.0 is used.
Remote access in general	**as before restart**	After a restart, the general remote access status is set to the last known value before the restart. If the general remote access status is enabled before the restart, for example, the remote 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.
	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.

6.5 Connect group addresses to group objects.

The following group objects are available for the connection of group addresses at the ise smart connect KNX Secure.

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 remote 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 remote 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 probably also signalled for another group 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 Secure device.

Description: 1 = Alarm, 0 = No alarm

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

Rubric: Connection error
Data type: Character (ISO 8859-1)
Function: Diagnostic information about the portal connection
Description: Supplies precise information on the portal connection status which is displayed by group object 20.

Object	Name	Direction	Data width	DP type	Flags (CRWTU)
32	Connection error info	Read	14 byte	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 precise information on the connection error which is displayed by group object 30.

7 Commissioning

7.1 Operation

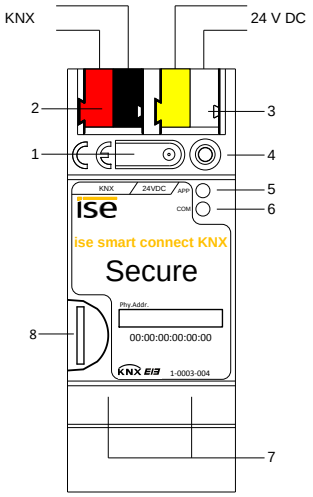


Figure 27: ise smart connect KNX Secure.

1	Programming button for KNX	Switches the device to the ETS programming mode or vice versa.
2	KNX connection (twisted pair)	On left: (+ / red) On right: (– / black)
3	Connection for power supply	DC 24–30 V, 2 W (at 24 V) On left: (+ / yellow) On right: (– / white)
4	KNX programming LED (red)	Red: Device is in ETS programming mode Yellow: For start or diagnosis code, see 7.2.1 / 7.2.2
5	LED *APP* (green)	Green: Normal operation Off/ Flashing: For start or diagnosis code, see 7.2.1 / 7.2.2
6	LED *COM* (yellow)	Yellow: Normal operation (brief dark phases indicate KNX telegram traffic) Off/ Flashing: For start or diagnosis codes, see 7.2.1 / 7.2.2
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 Flashing: Data reception on IP
8	MicroSD card holder	As Media size: Up to 32 GB microSDHC Formatting: FAT32

7.2 LED status displays

The devices 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.

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:

7.2.1

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 in an alternating fashion (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).	✘

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: Remote access is generally granted, the device is connecting to the SDA portal server, however remote access is not currently active.
○ 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: Remote access not allowed. 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

7.3 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 side and the KNX-TP side.

Due to considerably shorter transfer times, download through the IP side of the device is recommended.

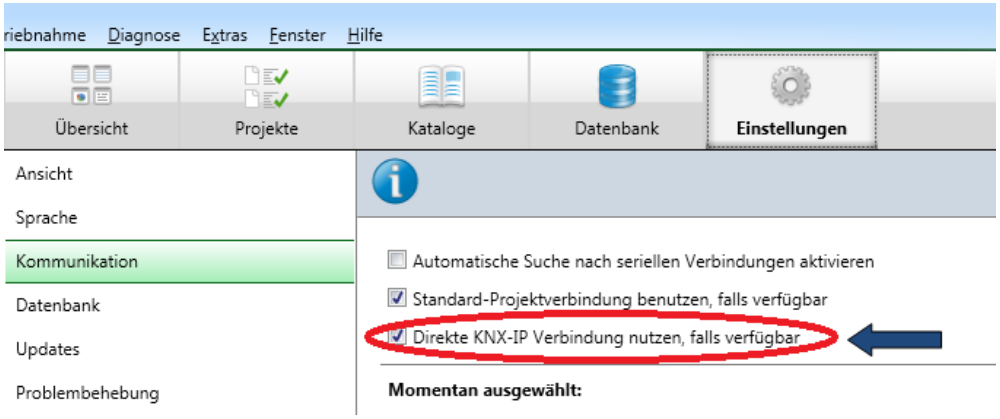


Figure 28: The "*Use direct KNX-IP connection if available*" setting accelerates the transfer from the ETS to the device.

For transfer of the ETS over the IP side, set the setting

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

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

7.4 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 Secure brings along and which supports up to three connections, are also configured via the ETS in the properties of the device.

7.5 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.

- 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.
- After the download, please wait approx. 15 seconds while the device copies the data and installs the application.
- Commissioning is complete.

7.6 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 is unconfigured. This can be recognized after starting up the device from the slowly flashing green APP LED (5).

7.6.1 Using the programming button on the device

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

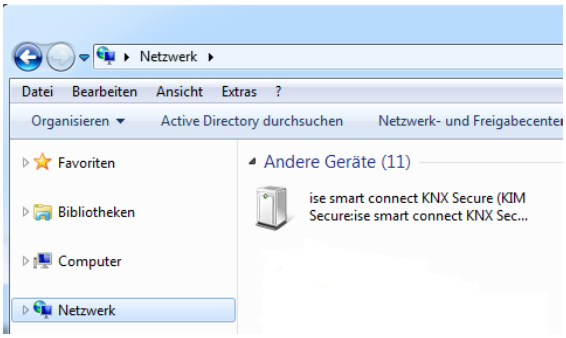
- Make sure that the device is switched off.
- Press and hold programming button (1) and switch on the device.
- Press and hold programming button (1) until the programming LED (4), the RUN LED (5) and the KNX LED (6) flash slowly simultaneously.
- Briefly release the programming button (1), then press 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.

7.6.2 Using the website of the device

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

- Call up the website of the device. For this purpose, double-click the icon of the device in the *Other Devices* area in the network environment.



- Alternatively, you can also enter the IP address of the device in your browser.
- 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.

7.7 Displaying information over the website

Calling up the website is described in Section 7.6.2 – *Using the website of the* device.

The start page of the device shows the system information, system configuration and application information

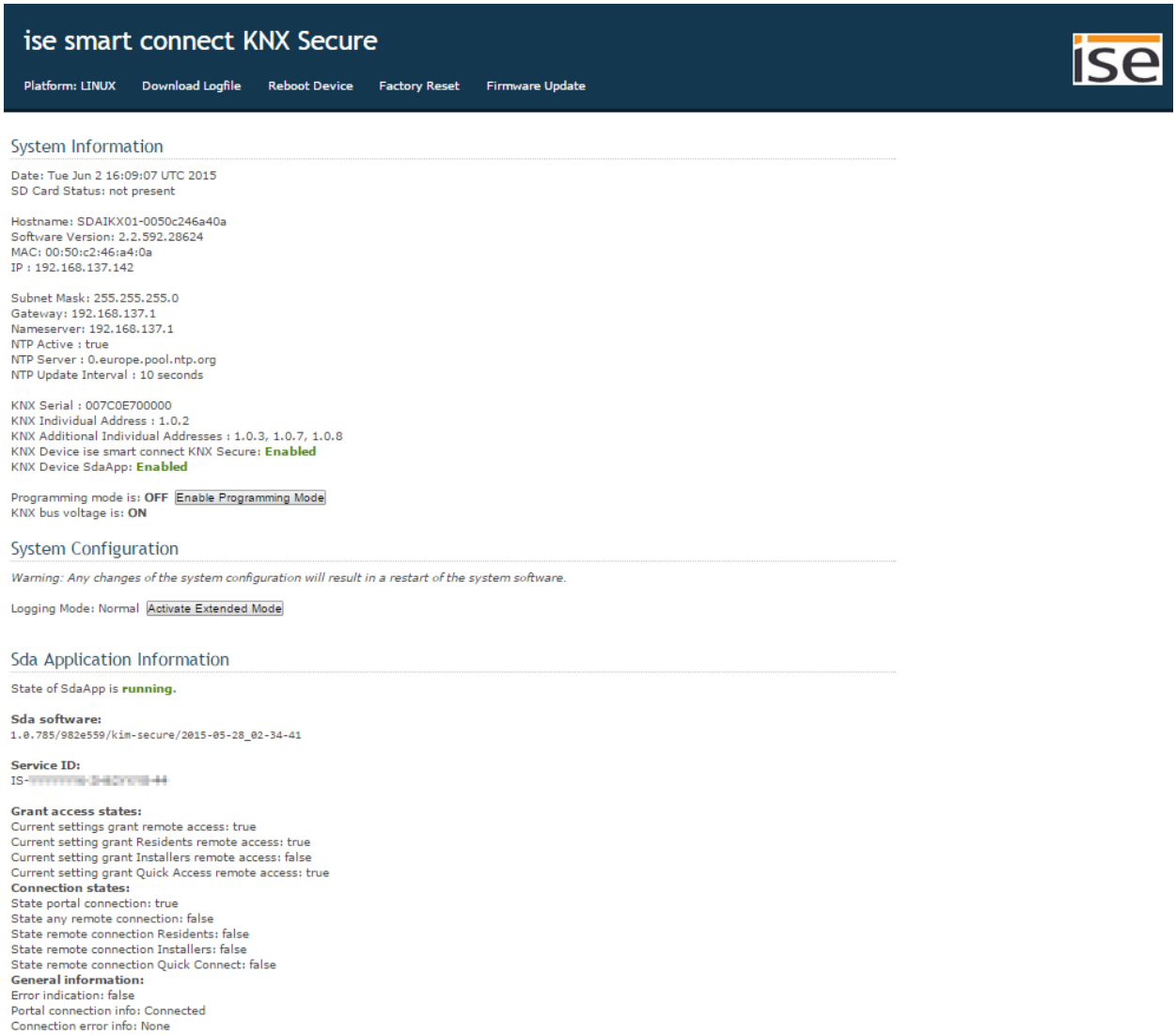


Figure 29: Device website for the system information, system configuration and application information

Important note: If the ise smart connect KNX secure device 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.

8 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

9 Frequently asked questions (FAQ)

- **How do I find out the IP address of my ise smart connect KNX Secure?**
  Please read about this in Section 7.6.2 – *Using the website of the* device.

- **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 Secure?**
  At present, the website is not updated after unloading until the device is restarted.

- **Are there software updates for my ise smart connect KNX Secure device?**
  Available software updates can be found on the firmware website. For more information, please visit the product area of www.ise.de.

- **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 6.5 – *Connect 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 6.2 – *Configuration step 2 – Assigning physical addresses*.

- **Can I use the KNX/IP ETS interfaces for download and monitoring in ETS?**
  Yes, absolutely. You may use them for all kinds of downloads, group and bus monitoring.

- **Can the website of my ise smart connect KNX Secure also be reached over the Internet?**
  Yes, the status page of the device can be called up securely over the Internet.

- **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 Secure 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!

- **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. To always guarantee good performance, certain limitations are necessary.
  Should you have applications which go beyond these conditions, please contact us. License models with expanded scope have not been ruled out for the future.

- **Is the operation of the servers in Germany guaranteed?**
  Yes. Our portal as well as the data server (for uniform distribution of traffic), are all guaranteed operating in Germany. The servers are hired as so called root servers from reputable hosting providers to ensure high-availability and so that no third party has access to the server and the data. By operating in Germany the much more restrictive German Data Protection Act is in place in comparison to other countries.

- **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 10) 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 blocked access for a group (e.g. installers), but the corresponding group object signals to me that there is an active remote access connection. Why?**
  The group object for active remote access of a group indicates that a member of the corresponding group is connected with the SDA connector. It does not matter why access was granted.
  Example: Access for installers is blocked, but access via "Quick Connect" is active. A member of the "Installer" group connects, and the connection is permitted based on the authorisation of "Quick Connect". In this case, both group objects "Quick Connect remote access connection status" and "Installer remote access connection status") signal the existence of a remote access connection.

10 Troubleshooting and support

If you have a problem with your ise smart connect KNX Secure 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 Secure, please refer to Section 10.1 – *Downloading log files if a problem* occurs.

10.1 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 7.6.2). To do so, proceed as follows:

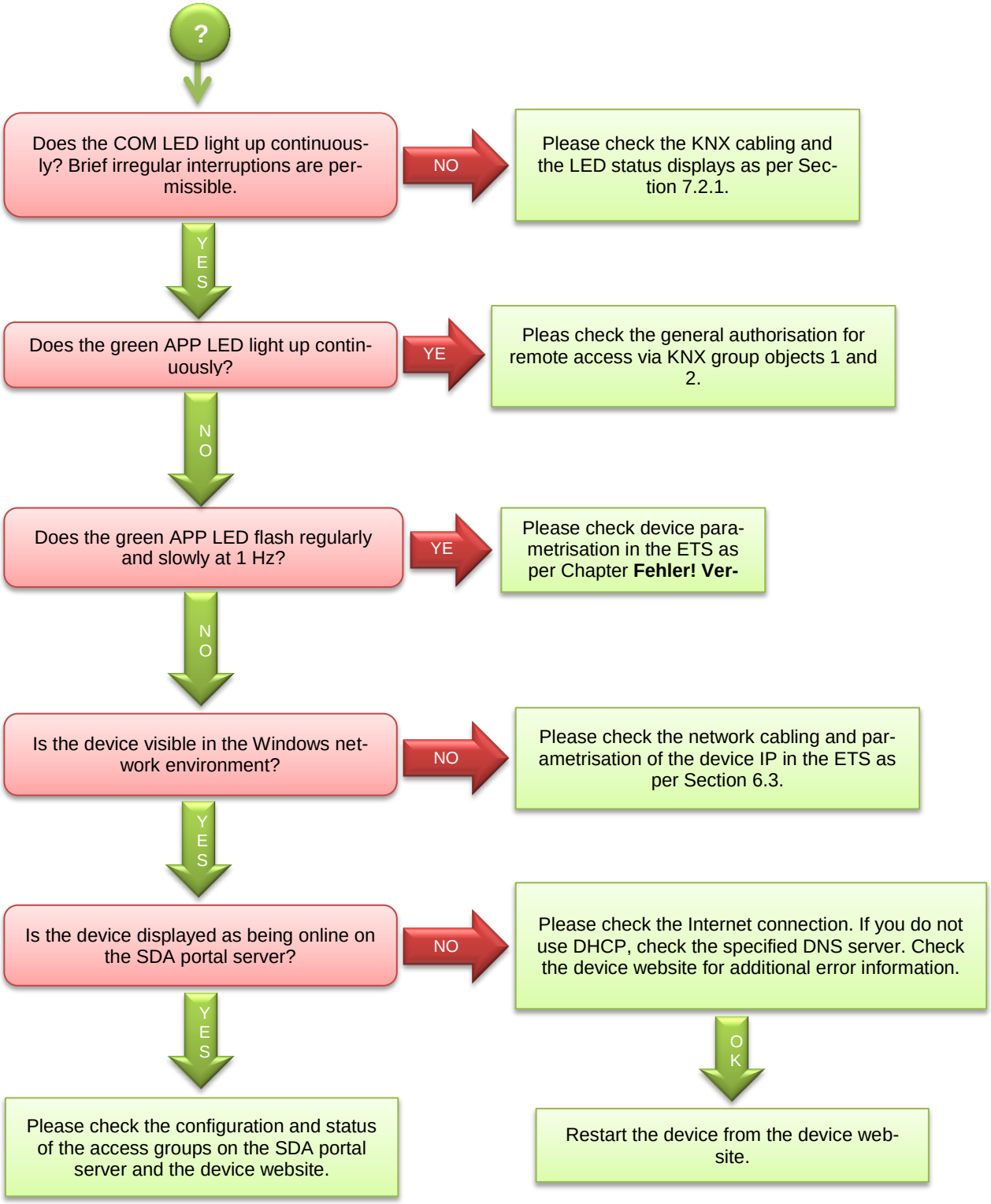
- Call up the website of the device. For this purpose, double-click the icon of the device in the *Multimedia* area in the network environment.
- Select *Device Status* in the upper menu bar on the website.
- Select *Download Log File* in the upper menu bar on the status page.
- The page which opens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

10.2 Status page of the ise smart connect KNX Secure

You can call up the device status on the website of the ise smart connect KNX Secure (see Section 7.6.2). 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 Secure. Should an error occur, please send us a screen shot of the status page.

10.3 The ise smart connect KNX Secure 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 the approaches above nor Chapter 9 provide a solution, please load the log files from the device (if possible) and send them together with an error description containing as many details as possible to support@ise.de.

11 ise smart connect KNX Secure software licence agreement

Hereinafter are the contract terms for your use of the software as the "Licensee".
By accepting this agreement and installing the ise smart connect KNX Secure software or putting the ise smart connect KNX Secure into use, you conclude an agreement with ise Individuelle Software-Entwicklung GmbH and agree to be legally bound to the terms of this agreement.

11.1 Definitions

Licensor: ise Individuelle Software-Entwicklung GmbH, Oldenburg, Kaiserstraße 14, Germany.
Licensee: The legal recipient of the ise smart connect KNX Secure software.
Firmware: Software which is embedded on the ise smart connect KNX Secure hardware and enables operation of the ise smart connect KNX Secure.
ise smart connect KNX Secure software: The ise smart connect KNX Secure software designates all of the software provided for the ise smart connect KNX Secure 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.

11.2 Object of the agreement

The object of this agreement is the ise smart connect KNX Secure 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.

11.3 Rights of use of the ise smart connect KNX Secure software

11.3.1 Firmware and SDA client

The Licensor grants the Licensee the non-exclusive, non-transferable right to use the ise smart connect KNX Secure 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.

11.3.2 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 securedeviceaccess.net GbR. 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.

11.4 Restriction of rights of use

11.4.1 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 500 MB per month per SDA connector.
We reserve the right to implement the usage limits named above using technical measures.

11.4.2 Copying, modification and transmission

The Licensee is not authorised to use, copy, modify or transfer the ise smart connect KNX Secure 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.

Reverse engineering and conversion technologies

The Licensee is not authorised to apply reverse-engineering techniques to the ise smart connect KNX Secure software or to convert the ise smart connect KNX Secure software to another form. 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).

11.4.3

Firmware and hardware

The firmware may only be installed and used on the hardware (ise smart connect KNX Secure) approved by the Licensor.

11.4.4

Transfer to a third party

The ise smart connect KNX Secure software may not be passed on to third parties, nor may it be made accessible to third parties.

11.4.5

Renting out, leasing out and sub-licensing

11.4.6 The Licensee is not authorised to rent or lease the ise smart connect KNX Secure software or grant sub-licenses to the program.

Software creation

11.4.7 The Licensee requires written approval from the Licensor to create and distribute software which is derived from the ise smart connect KNX Secure software.

11.4.8

The mechanisms of license management and copy protection

The mechanisms of the license management and copying protection of the ise smart connect KNX Secure software may not be analysed, published, circumvented or disabled.

11.5 Ownership, confidentiality

11.5.1

Documentation

The ise smart connect KNX Secure 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.

11.5.2

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.

11.6 Changes, additional deliveries

The ise smart connect KNX Secure 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.

11.7

11.7 Warranty

The ise smart connect KNX Secure software shall be delivered together with software from third parties as listed in Chapter 12 – *Open Source Software*. No warranty is provided for software from third parties.

Software and documentation

The ise smart connect KNX Secure 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 re-

spective valid version. The warranty period for the ise smart connect KNX Secure software is twenty-four (24) months. During this time, the licensor shall provide the following warranty:

- 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.

Limitation of warranty

11.7.2 Otherwise, no warranty shall be provided for the freedom from faults of the ise smart connect KNX Secure 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.

11.8 Liability

The Licensor shall not be liable for damages due to loss of profit, data loss or any other financial loss resulting as part of the use of the ise smart connect KNX Secure software, even if the Licensor is aware of the possibility of damage of that type.
This limitation of liability is valid for all damage claims of the Licensee, 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.

11.9 Applicable law

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

11.10 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 ise smart connect KNX Secure software and the documentation turned over (which is provided in printed form or also as online help or online documentation) including all copies shall in this case be returned immediately and without being requested to do so. No claim to reimbursement of the price paid shall be accepted in this case.
The license for use of the ise smart connect KNX Secure software shall expire upon termination of the agreement. In this case, the ise smart connect KNX Secure product must be taken out of operation. Further use of the ise smart connect KNX Secure 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.

11.11 Subsidiary agreements and changes to the agreement

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

11.12 Exception

All rights not expressly mentioned in this agreement are reserved.

12 Open Source Software

This product uses software from third-party sources used within the scope of the GNU General Public License (GPL) or Lesser GNU General Public License LGPL and within the scope of the Berkeley Software Distribution (BSD) and the MIT license.

The software packages used in this product which are licensed within the scope stated here are described in the following.

Software package	U-Boot
Version of the software	2.012.07
Source	http://www.denx.de/wiki/U-Boot/WebHome
License	GNU GPL, Version 2, June 1991
Copyright notice	Copyright © 2000-2012 by Wolfgang Denk et al.

Software package	GNU/Linux
Version of the software	03/02/2020
Source	http://kernel.org
License	GNU GPL, Version 2, June 1991
Copyright notice	Copyright © 1992-2013 by Linus Torvalds et al.

Software package	Buildroot
Version of the software	2.012.11
Source	http://buildroot.org
License	GNU GPL, Version 2, June 1991
Copyright notice	Copyright © 1999-2005 Erik Andersen, 2006-2012 The Buildroot developers

Software package	GNU C Library (GLIBC)
Version of the software	2.30.3
Source	http://www.gnu.org/s/libc/
License	GNU LGPL, Version 2.1, February 1999
Copyright notice	Copyright © 1996-2012 by Roland McGrath et al.

Software package	Boost C++ Libraries
Version of the software	1.49.0 (firmware) and 1.55.0 (SDA client)
Source	http://www.boost.org
License	Boost Software Licence, version 1.0
Copyright notice	Copyright 2012 Boost.org

Software package	libupnp
Version of the software	01/06/2017
Source	http://sourceforge.net/projects/pupnp/files/pupnp/
License	BSD
Copyright notice	Copyright (c) 2000-2003, Intel Corporation. All rights reserved.

Software package	Websocketpp
Version of the software	0.3.x
Source	http://www.zaphoyd.com/websocketpp
License	BSD
Copyright notice	Copyright (c) 2013, Peter Thorson. All rights reserved.

Software package	jQuery
Version of the software	1.11.1
Source	https://jquery.org
License	MIT Licence
Copyright notice	Copyright 2014 The jQuery Foundation

Software package	openssl
Version of the software	1.0.0 (firmware) and 1.0.1 (SDA client)
Source	https://www.openssl.org
License	OpenSSL license and SSLeay license
Copyright notice	Copyright (c) 1998-2011 The OpenSSL Project. All rights reserved. Copyright (C) 1995-1998 Eric Young (eay@cryptsoft.com)

The license texts of the GPL and LGPL are available via the following web page:
http://www.gnu.org/licenses/licenses.html

The source code for this software can be obtained via the e-mail address info@ise.de.

This offer is valid for 3 years after the discontinuation of the service for this product.

13 GNU GENERAL PUBLIC LICENSE

Version 2, June 1991

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users. This General Public License applies to most of the Free Software Foundation's software and to any other program whose authors commit to using it. (Some other Free Software Foundation software is covered by the GNU Lesser General Public License instead.) You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid anyone to deny you these rights or to ask you to surrender the rights. These restrictions translate to certain responsibilities for you if you distribute copies of the software, or if you modify it.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must give the recipients all the rights that you have. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

We protect your rights with two steps: (1) copyright the software, and (2) offer you this license which gives you legal permission to copy, distribute and/or modify the software.

Also, for each author's protection and ours, we want to make certain that everyone understands that there is no warranty for this free software. If the software is modified by someone else and passed on, we want its recipients to know that what they have is not the original, so that any problems introduced by others will not reflect on the original authors' reputations.

Finally, any free program is threatened constantly by software patents. We wish to avoid the danger that redistributors of a free program will individually obtain patent licenses, in effect making the program proprietary. To prevent this, we have made it clear that any patent must be licensed for everyone's free use or not licensed at all.

The precise terms and conditions for copying, distribution and modification follow.

TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License applies to any program or other work which contains a notice placed by the copyright holder saying it may be distributed under the terms of this General Public License. The "Program", below, refers to any such program or work, and a "work based on the Program" means either the Program or any derivative work under copyright law: that is to say, a work containing the Program or a portion of it, either verbatim or with modifications and/or translated into another language. (Hereinafter, translation is included without limitation in the term "modification".) Each licensee is addressed as "you".

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running the Program is not restricted, and the output from the Program is covered only if its contents constitute a work based on the Program (independent of having been made by running the Program). Whether that is true depends on what the Program does.

1. You may copy and distribute verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and give any other recipients of the Program a copy of this License along with the Program.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Program or any portion of it, thus forming a work based on the Program, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

> **a)** You must cause the modified files to carry prominent notices stating that you changed the files and the date of any change.
> **b)** You must cause any work that you distribute or publish, that in whole or in part contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to all third parties under the terms of this License.
> **c)** If the modified program normally reads commands interactively when run, you must cause it, when started running for such interactive use in the most ordinary way, to print or display an announcement including an appropriate copyright notice and a notice that there is no warranty (or else, saying that you provide a warranty) and that users may redistribute the program under these conditions, and telling the user how to view a copy of this License. (Exception: if the Program itself is interactive but does not normally print such an announcement, your work based on the Program is not required to print an announcement.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Program, and can be reasona-

bly considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Program, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Program.

In addition, mere aggregation of another work not based on the Program with the Program (or with a work based on the Program) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may copy and distribute the Program (or a work based on it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you also do one of the following:

> **a)** Accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,
> **b)** Accompany it with a written offer, valid for at least three years, to give any third party, for a charge no more than your cost of physically performing source distribution, a complete machine-readable copy of the corresponding source code, to be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,
> **c)** Accompany it with the information you received as to the offer to distribute corresponding source code. (This alternative is allowed only for noncommercial distribution and only if you received the program in object code or executable form with such an offer, in accord with Subsection b above.)

The source code for a work means the preferred form of the work for making modifications to it. For an executable work, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the executable. However, as a special exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

If distribution of executable or object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place counts as distribution of the source code, even though third parties are not compelled to copy the source along with the object code.

4. You may not copy, modify, sublicense, or distribute the Program except as expressly provided under this License. Any attempt otherwise to copy, modi-

fy, sublicense or distribute the Program is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

5. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Program or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Program (or any work based on the Program), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Program or works based on it.

6. Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.

7. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Program at all. For example, if a patent license would not permit royalty-free redistribution of the Program by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Program.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system, which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

8. If the distribution and/or use of the Program is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Program under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such

case, this License incorporates the limitation as if written in the body of this License.

9. The Free Software Foundation may publish revised and/or new versions of the General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Program specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of this License, you may choose any version ever published by the Free Software Foundation.

10. If you wish to incorporate parts of the Program into other free programs whose distribution conditions are different, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

11. BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

12. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

14 OpenSSL Lizenzen

```
LICENSE ISSUES
==============

The OpenSSL toolkit stays under a dual license, i.e. both the conditions of
the OpenSSL License and the original SSLeay license apply to the toolkit.
See below for the actual license texts. Actually both licenses are BSD-style
Open Source licenses. In case of any license issues related to OpenSSL
please contact openssl-core@openssl.org.
```

14.1 OpenSSL License

```
/* ====================================================================
 * Copyright (c) 1998-2011 The OpenSSL Project.  All rights reserved.
 *
 * Redistribution and use in source and binary forms, with or without
 * modification, are permitted provided that the following conditions
 * are met:
 *
 * 1. Redistributions of source code must retain the above copyright
 *    notice, this list of conditions and the following disclaimer.
 *
 * 2. Redistributions in binary form must reproduce the above copyright
 *    notice, this list of conditions and the following disclaimer in
 *    the documentation and/or other materials provided with the
 *    distribution.
 *
 * 3. All advertising materials mentioning features or use of this
 *    software must display the following acknowledgment:
 *    "This product includes software developed by the OpenSSL Project
 *    for use in the OpenSSL Toolkit. (http://www.openssl.org/)"
 *
 * 4. The names "OpenSSL Toolkit" and "OpenSSL Project" must not be used to
 *    endorse or promote products derived from this software without
 *    prior written permission. For written permission, please contact
 *    openssl-core@openssl.org.
 *
 * 5. Products derived from this software may not be called "OpenSSL"
 *    nor may "OpenSSL" appear in their names without prior written
 *    permission of the OpenSSL Project.
 *
 * 6. Redistributions of any form whatsoever must retain the following
 *    acknowledgment:
 *    "This product includes software developed by the OpenSSL Project
 *    for use in the OpenSSL Toolkit (http://www.openssl.org/)"
 *
 * THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT ``AS IS'' AND ANY
 * EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE
 * IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR
 * PURPOSE ARE DISCLAIMED.  IN NO EVENT SHALL THE OpenSSL PROJECT OR
 * ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL,
 * SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT
 * NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES;
 * LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION)
 * HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT,
 * STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE)
 * ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED
 * OF THE POSSIBILITY OF SUCH DAMAGE.
 * ====================================================================
 *
```

```
 * This product includes cryptographic software written by Eric Young
 * (eay@cryptsoft.com).  This product includes software written by Tim
 * Hudson (tjh@cryptsoft.com).
 *
 */
```

14.2 Original SSLeay License

```
/* Copyright (C) 1995-1998 Eric Young (eay@cryptsoft.com)
 * All rights reserved.
 *
 * This package is an SSL implementation written
 * by Eric Young (eay@cryptsoft.com).
 * The implementation was written so as to conform with Netscapes SSL.
 *
 * This library is free for commercial and non-commercial use as long as
 * the following conditions are aheared to.  The following conditions
 * apply to all code found in this distribution, be it the RC4, RSA,
 * lhash, DES, etc., code; not just the SSL code.  The SSL documentation
 * included with this distribution is covered by the same copyright terms
 * except that the holder is Tim Hudson (tjh@cryptsoft.com).
 *
 * Copyright remains Eric Young's, and as such any Copyright notices in
 * the code are not to be removed.
 * If this package is used in a product, Eric Young should be given attribution
 * as the author of the parts of the library used.
 * This can be in the form of a textual message at program startup or
 * in documentation (online or textual) provided with the package.
 *
 * Redistribution and use in source and binary forms, with or without
 * modification, are permitted provided that the following conditions
 * are met:
 * 1. Redistributions of source code must retain the copyright
 *    notice, this list of conditions and the following disclaimer.
 * 2. Redistributions in binary form must reproduce the above copyright
 *    notice, this list of conditions and the following disclaimer in the
 *    documentation and/or other materials provided with the distribution.
 * 3. All advertising materials mentioning features or use of this software
 *    must display the following acknowledgement:
 *    "This product includes cryptographic software written by
 *     Eric Young (eay@cryptsoft.com)"
 *    The word 'cryptographic' can be left out if the rouines from the library
 *    being used are not cryptographic related :-).
 * 4. If you include any Windows specific code (or a derivative thereof) from
 *    the apps directory (application code) you must include an acknowledgement:
 *    "This product includes software written by Tim Hudson (tjh@cryptsoft.com)"
 *
 * THIS SOFTWARE IS PROVIDED BY ERIC YOUNG ``AS IS'' AND
 * ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE
 * IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE
 * ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE
 * FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL
 * DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS
 * OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION)
 * HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT
 * LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY
 * OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF
 * SUCH DAMAGE.
 *
 * The licence and distribution terms for any publically available version or
 * derivative of this code cannot be changed. i.e. this code cannot simply be
 * copied and put under another distribution licence
```

```
* [including the GNU Public Licence.]
*/
```