

Status of the documentation:
20.04.2022

Gira S1

Order No. 2089 00



Gira S1 (Fig. 1:1)

GIRA

Contents

1. Configuration of the Gira S1 at a glance	4
1.1. Installation (see Chapter 7)	4
1.2. Configuration in the ETS (see Chapter 8)	4
1.3. Configuration in the Gira Device portal (see Chapter 10)	4
1.4. Configuration of access to the application (see Chapter 10.7)	4
2. Product description	5
2.1. Functions	5
2.2. KNX Secure	6
2.3. Functional description	6
2.4. Gira Device portal	7
2.5. Client software (Gira S1 Windows client)	8
3. Application scenarios	9
3.1. Access to the Gira X1	9
3.2. Configuration and control of the Gira HomeServer	10
3.3. Connecting Gira S1 with Gira HomeServer via KNX Secure Tunneling	11
3.4. Access to KNX installations	17
3.5. Access to websites on the remote network	18
3.6. Access via other TCP protocols	19
3.7. User rights and user groups	19
4. Time server	20
5. Data logger	21
5.1. Access to the data logger archive	22
6. VPN	23
6.1. Prerequisite for the VPN setup	23
6.2. VPN setup	23
7. Installation	24
7.1. Device design	24
7.2. Installation and electrical connection	24
8. Configuration in the ETS	26
8.1. Creating Gira S1 as a device in the ETS	26
8.2. Assigning physical addresses	27
8.3. Setting the IP address, subnet mask and address of the default gateway	28
8.4. Transferring application programs and configuration data	29
8.5. Parameters	30
8.6. Object table	34
9. Displays and operation	40
9.1. LED status displays	40
9.2. Factory reset	41
9.3. Firmware update of the device	42

GIRA

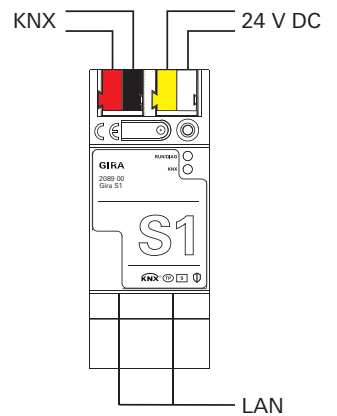
10. Using the Gira Device portal	43
10.1. Start page.....	43
10.2. Device overview	44
10.3. Registering a Gira S1	45
10.4. Links	46
10.5. Notifications	47
10.6. Device data	48
10.7. Access to applications	49
10.8. Configuring notifications	51
10.9. Portal user administration	54
10.10. Setting up VPN access	57
10.11. FAQs	58
11. Gira S1 Windows client	59
11.1. Installation.....	59
11.2. Connecting to the Gira Device portal	60
11.3. Configuring the access options of a Gira S1	62
11.4. Ending a remote access connection	69
12. Technical data	70
12.1. Accessories	70
13. Frequently asked questions (FAQs)	71
14. Troubleshooting and support	73
15. Gira S1 device website	74
16. License agreement	75

1. Configuration of the Gira S1 at a glance

This page displays the configuration process at a glance. You can find more detailed instructions for start-up in the chapters that are indicated below in the respective steps.

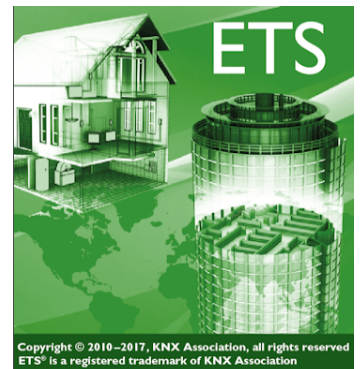
1.1. Installation (see Chapter 7)

- Mount the Gira S1.
- Connect the power supply,
- the KNX connection and
- the network connection.



1.2. Configuration in the ETS (see Chapter 8)

- Create the Gira S1 as a device in the ETS.
- Assign the physical addresses for the Gira S1.
- Assign the required group addresses.
- Transfer the application program and configuration.



1.3. Configuration in the Gira Device portal (see Chapter 10)

- Register the Gira S1.
- Create the users.
- Transfer device ownership, if necessary.
- Optionally, you can set up notifications, for example.

GIRA Device portal

Home Registration My devices My data Help

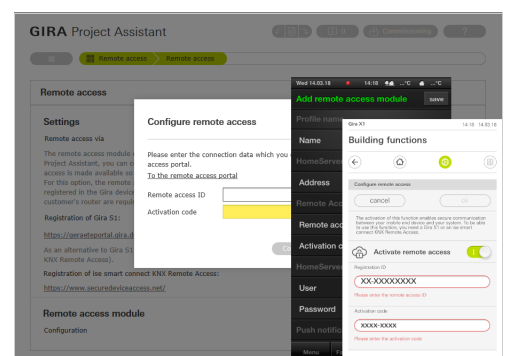
Registration

Take the time to register your Gira devices and benefit from a range of advanced downloads, updates and free supplementary modules such as the Gira Dynam forecast.

1. Serial number

1.4. Configuration of access to the application (see Chapter 10.7)

- First generate the activation codes in the Gira Device portal.
- Then enter the codes in the corresponding input screen of the relevant application (e.g. Gira Smart Home app, Gira Home-Server app, Gira S1 Windows client or Gira Project Assistant).



2. Product description

2.1. Functions

- Secure remote access to your smart home with KNX using the Gira HomeServer or Gira Smart Home app.
- Secure remote access to web-based visualisations.
- Secure remote maintenance and remote programming of the Gira HomeServer, Gira G1, Gira X1, Gira L1, and Gira KNX IP router.
- Secure remote programming via the Gira HomeServer Expert.
- Secure remote programming via the Gira Project Assistant (GPA).
- Secure remote maintenance and remote programming of KNX projects using ETS4 or ETS5 in conjunction with the Gira Project Assistant or the Gira S1 Windows client. The programming and diagnosis is supported via a group and bus monitor.
- Secure remote access to HTML pages (e.g. camera, NAS, router or switch) in the smart home network (depending on the technical implementation of the respective device website).
- Secure data transfer courtesy of SSL/TLS encryption.
- Portal server is located in Germany and is subject to German laws on data.
- Independence from internet provider and routers used. Secure remote access even with IPv6 Dual Stack Lite - (e.g. with Unitymedia), LTE, or UMTS connections.
- Management of access to the secure connections via KNX communication objects, Gira Smart Home app, Gira HomeServer app, and QuadClient.
- Status signalling of the secure connections via KNX communication objects.
- Send KNX status messages via e-mail. An attachment can be added to the e-mail, as an option.
- Send KNX status messages by SMS or voice call via the chargeable, additional service sms77 or MessageBird.
- Optimised KNX IP communication, for mobile or very slow connections.
- Supports the accelerated transfer of the ETS to KNXnet/IP devices via a direct KNX IP connection.
- An integrated Ethernet switch (two RJ45 connections) simplifies the connection of multiple IP devices. This enables multiple Gira S1 or other IP devices in the distribution to be connected without the aid of other active components.
- The Gira S1 can be used as a data logger. It incorporates a card reader for microSDHC cards up to 32 GB. The KNX EIB telegrams in an ETS4-compliant format can be recorded to the card for analysis purposes. The card memory can be used as a ring memory or as a ROM.
- As a clock, the Gira S1 can send the time and date to the bus at configurable intervals. It is possible to trigger the sending of the current time and the current date via a trigger.
- VPN network coupling enables access to KNX installations, visualisation interfaces and files in the home network, and much more. Uncomplicated access to the KNX system and other applications is also guaranteed for smartphone apps. VPN access can be controlled and monitored via KNX communication objects.
- Full support for KNX Secure.
- Sending push notifications to the Gira Smart Home app.
- Support of a secure tunnelling connection between Gira HomeServer and Gira S1.

2.2. KNX Secure

Gira S1 is compatible with KNX Secure. The required KNX Secure certificate or FDSK (Factory Default Setup Key) this contains is located on the side of the device as a sticker and is also enclosed with the device.

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



You cannot restore the FDSK yourself.

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

2.3. Functional description

The Gira S1 is installed in the customer's home network and prepares the home network for secure access via the Internet.

The Gira S1 is connected to the home network via Ethernet. It connects to the Gira Device portal automatically using the existing Internet access. Communication between the Gira S1 and the Gira Device portal is encrypted using AES and secured with digital certificates (for details, see chapter 2.4.1 "HTTPS proxy `httpaccess.net`").

You can already access almost all network devices using the Internet.

The Gira Smart Home app and the GPA can communicate directly with the Gira S1 via the Gira Device portal. With other Windows applications, such as ETS or Gira Expert, access is via the Gira S1 Windows client (see chapter 2.5 "Client software (Gira S1 Windows client)").

If you have a KNX installation in your house, you can connect it to the Gira S1 using the KNX connection if desired. As a result, the KNX devices can be accessed from anywhere, e.g. with the ETS.

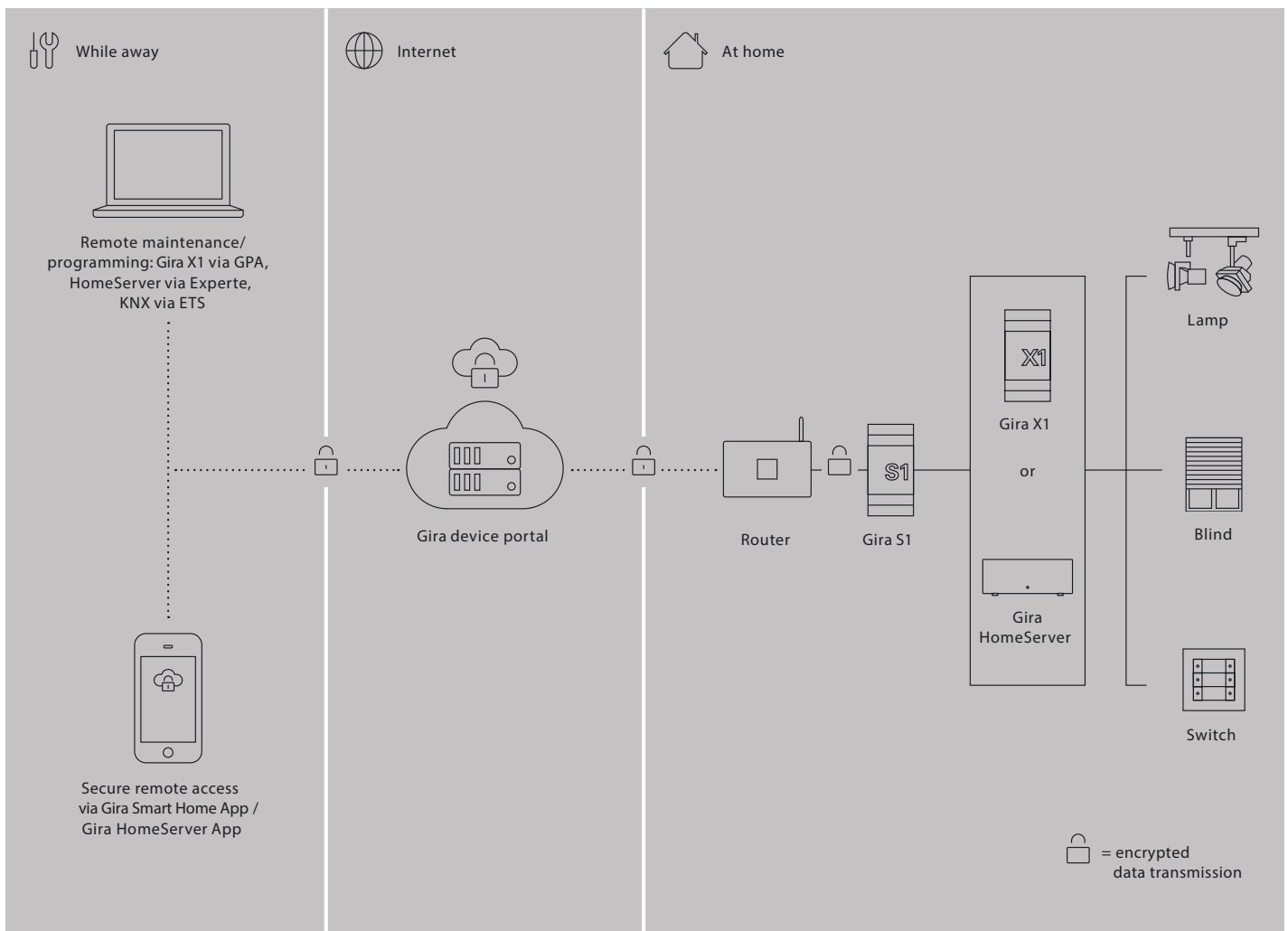


Figure 1: Overview of secure remote access using the Gira S1

2.4. Gira Device portal

You manage your Gira S1 using the Gira Device portal (<https://geraeteportal.gira.de>). Through the Gira Device portal, you can also provide other users with access to your Gira S1 and hence to the KNX and network devices in your home network.

You can assign any number of Gira S1 devices to one account on the Gira Device portal. If you or persons authorised by you wish to access end devices in your home network, the Gira Device portal always plays the part of the intermediary. The Gira Device portal does not store the data transferred, but only forwards it on.

The server for the Gira Device portal is operated in Germany in compliance with the German data protection guidelines.

Note

For technical reasons, the use of the Gira Device portal requires the use of cookies in the web browser.

2.4.1. HTTPS proxy httpaccess.net

Most network devices today, such as cameras or network printers, have an integrated web server for access with a web browser. Access via the Gira Device portal is especially easy in such cases. Each network device that can be accessed via a Gira S1 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.

All communication via the Internet is also encrypted, and user authentication occurs according to the access authorisation set on the Gira Device portal for the Gira S1.

To save you from having to remember links, the Gira Device portal manages a list of links of the end devices, which you can access at httpaccess.net. If the network device supports UPnP, the Gira Device portal can enter it automatically in the list of links. You can also enter devices in the list manually if they are not added automatically.

2.4.2. Communication – Secure, reliable and easy to handle

For communication with the portal server, the Gira S1 uses the standard protocols HTTPS, TLS/SSL and WebSockets. All data is encrypted using AES.

Gira S1 and the Gira Device portal authenticate each other with digital certificates and RSA key pairs. The certificates are issued by our own certification office.

Through the use of standard protocols and because the Gira S1 actively connects to the Gira Device portal, we achieve the best possible compatibility with the existing infrastructure. For your Internet router, the Gira S1 communication is no different from the encrypted connection of your web browser, e.g. for online banking or Google searches.

The advantage for you is that the Gira S1 works without requiring any complex configuration. This is a major advantage compared to other approaches to secure remote access, such as VPN or SSH tunnelling.

In contrast to other solutions, remote access even works via a mobile phone or IPv6 connection, even if it doesn't have a unique IP address that can be accessed externally.

2.4.3. Gira S1 notifications

KNX group objects and system events such as the logging in/logging out of a Gira S1 to/from the portal can be used to generate notifications in the portal server. In addition to static texts, they may also contain values from the KNX or even an attachment, such as a camera image.

These notifications can be configured for forwarding via e-mail, push messages, telephone or SMS - as configured by the user. Sending SMS or voice calls is done via the chargeable additional service sms77 or MessageBird.

In addition, forwarding of IFTTT triggers is possible.

2.5. Client software (Gira S1 Windows client)

You install the Gira S1 Windows client on a Windows computer. Through the Gira S1 Windows client, other applications running on your computer are given access to your devices without having to support the remote access function themselves.

The Gira S1 Windows client establishes an encrypted connection to the Gira S1 via the Gira Device portal. 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:

- You can configure KNX devices via KNXnet/IP using the ETS.
- You can configure a HomeServer using the Gira HomeServer Expert.
- 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.
- Many other use cases are supported via freely configurable TCP port forwarding.

3. Application scenarios

3.1. Access to the Gira X1

In conjunction with the Gira X1, the building functions can be controlled using secure remote access with the Gira Smart Home App.

The programming or maintenance of the Gira X1 using the Gira Project Assistant (GPA) can also be carried out via the secure remote access.

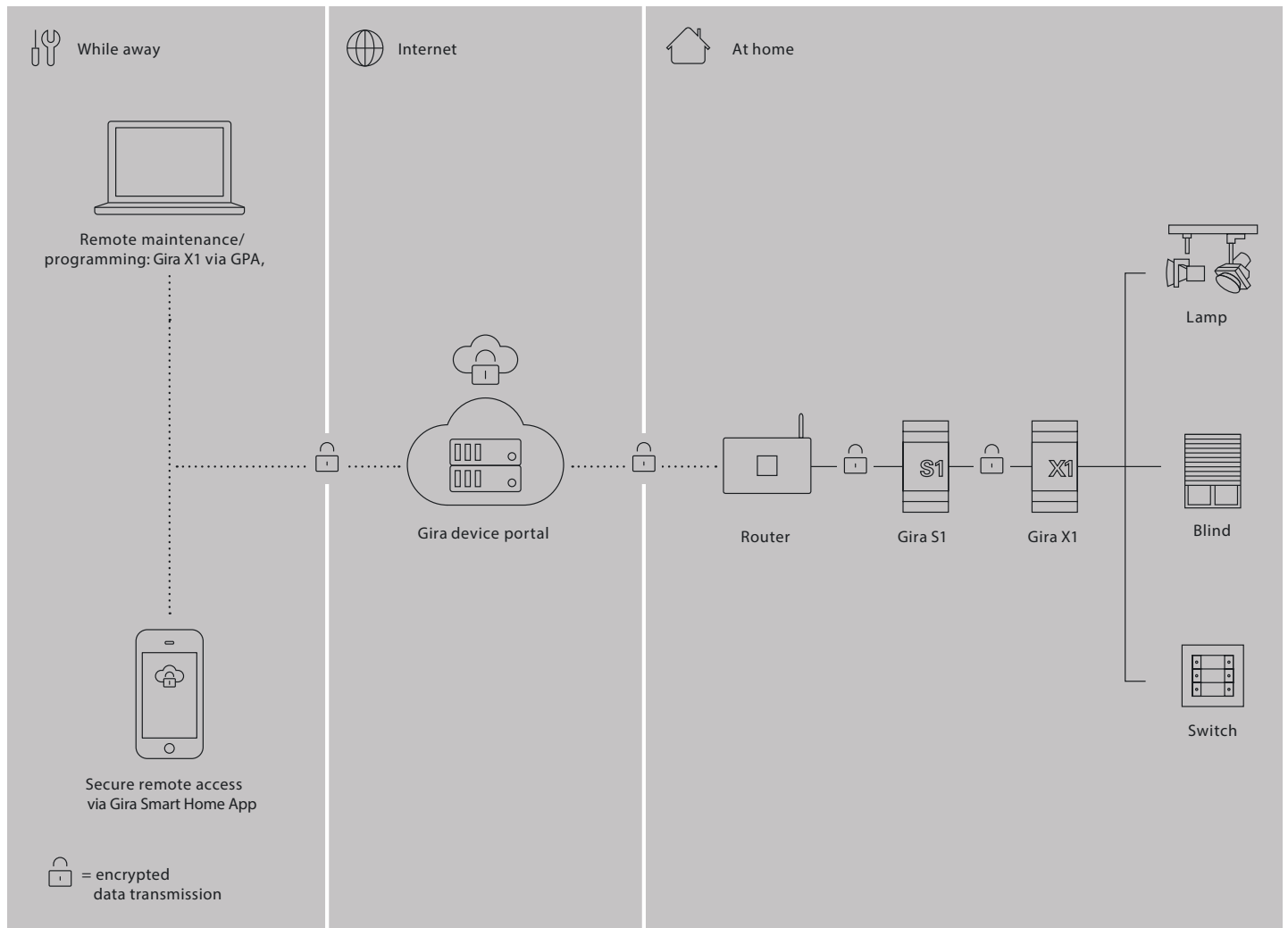


Figure 2: Configuration and operation of the Gira X1

3.2. Configuration and control of the Gira HomeServer

Access to the Gira HomeServer works in a similar way to access to the KNX installation. On the one hand, the KNX installation is accessed via the Gira HomeServer using the Eiblib/IP protocol, while on the other hand, the configuration is supported with the Expert. In addition, you can access the KNX installation directly via the interface function of the Gira S1. Here too, all data transmitted via the Internet is encrypted.

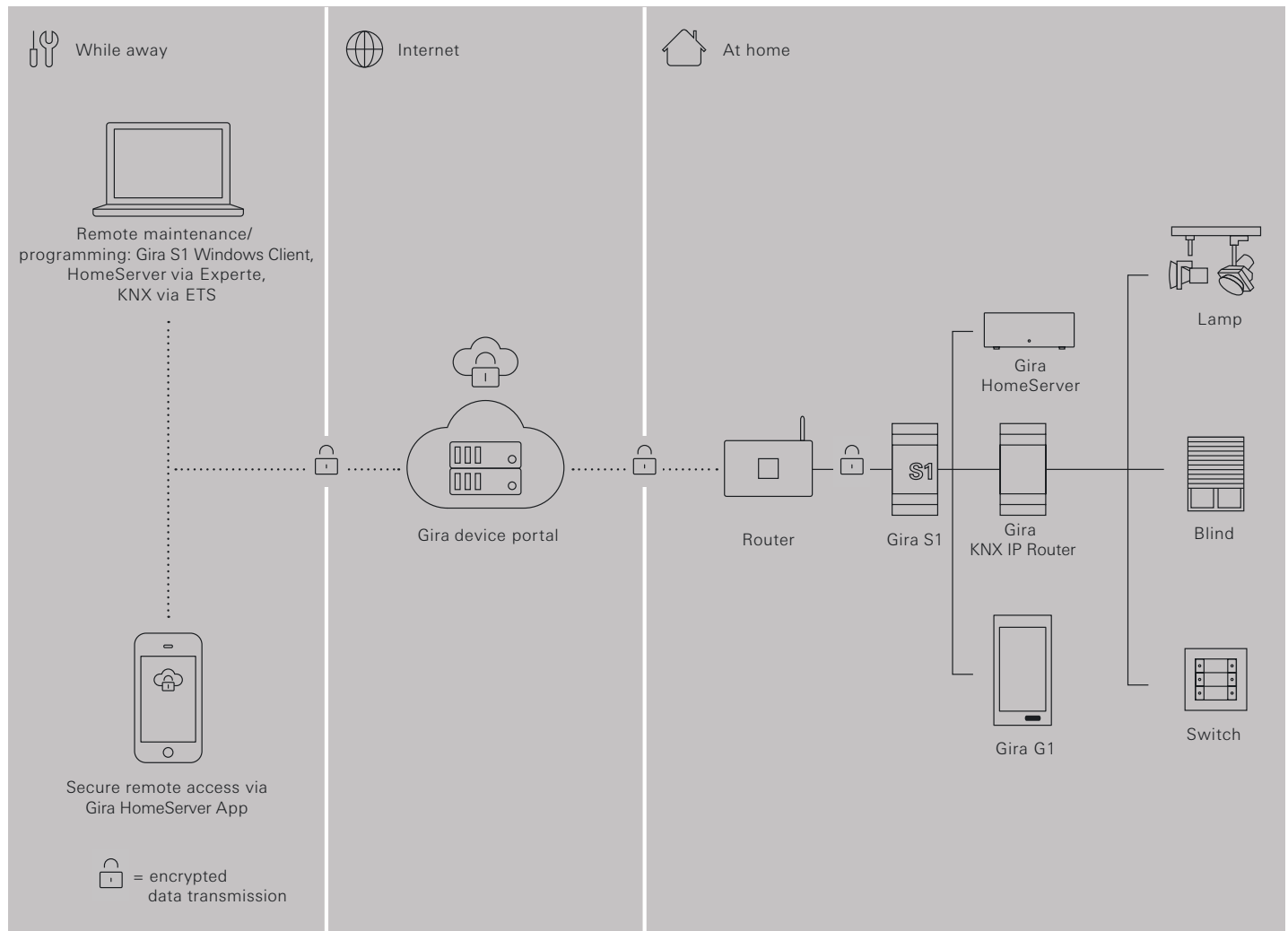


Figure 3: Secure configuration of the Gira HomeServer with the Gira S1.

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 remote access: The Gira S1 Windows client makes protocol transmission available locally via the IP address 127.0.0.1. In other words, if an Eiblib/IP connection is configured in the ETS, for example, 127.0.0.1 must be entered for the IP address for use via remote access (instead of the IP address of the Gira HomeServer on the remote network). The same applies for downloading with the Expert. For more information, see chapter 11.3.2 "Configuring the Gira HomeServer remotely and using the Eiblib/IP".

3.3. Connecting Gira S1 with Gira HomeServer via KNX Secure Tunneling

Gira HomeServer can be connected directly to the KNX bus via Gira S1.

To do this proceed as follows:

3.3.1. Settings in the ETS

- Select Gira S1.
- Activate Secure Commissioning.
- Activate Secure Tunneling.

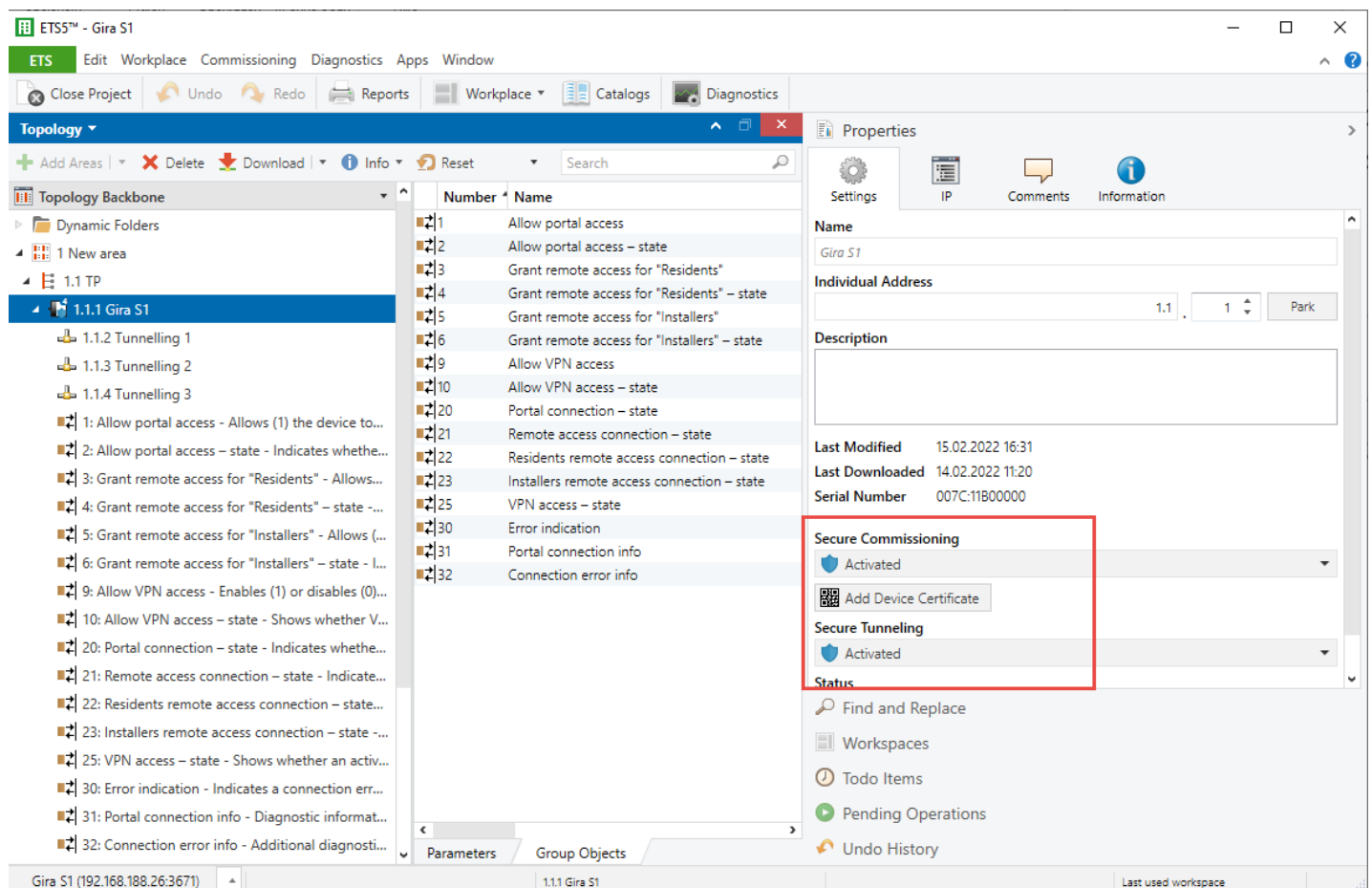


Figure 4: Activate secure commissioning and secure tunnelling

One of the existing tunneling connections is required for Gira HomeServer:

- Select a tunneling connection.
- Note the physical address of that tunneling connection.

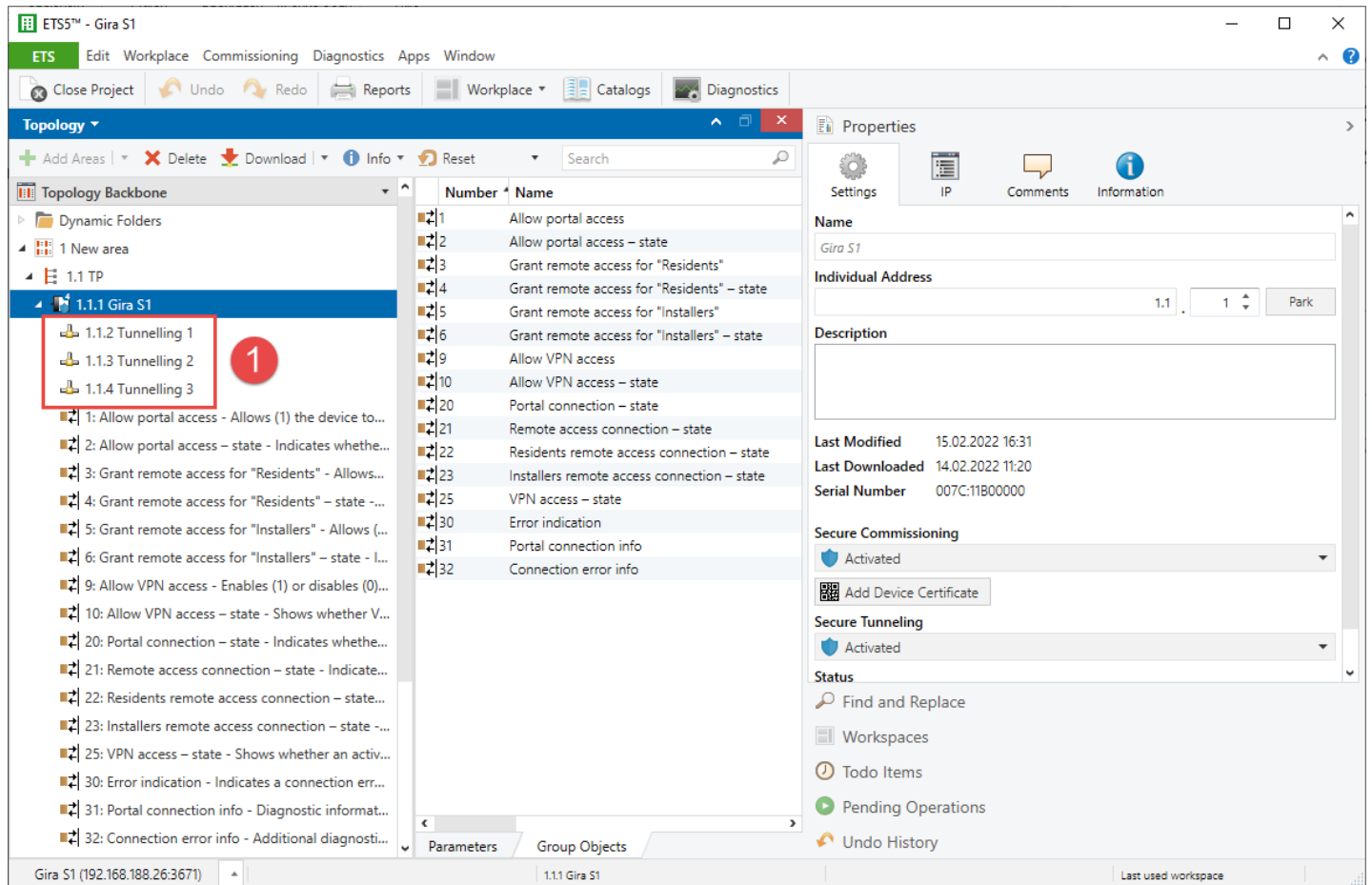


Figure 5: Physical address of the tunneling connection

- Switch to the "Bus" tab.
- Make a note of the IP address of Gira S1

The screenshot shows the ETS5 Professional software interface for a Gira S1 device. The 'Bus' tab is selected in the top navigation bar. The left sidebar contains a tree view with 'Interfaces' expanded. The main area displays 'Current Interface' as '1.1.1 Gira S1' with 'Individual Address: 1.1.2'. Below this, there are sections for 'Configured Interfaces' and 'Discovered Interfaces'. The 'Discovered Interfaces' section contains a table with two entries. The first entry, '1.1.1 Gira S1', is highlighted with a red box and a red circle with the number '2' next to it. The second entry is '15.15.255 Gira X1'. To the right of the table is the 'IP Tunneling' configuration panel, which shows the 'IP Address' as '192.168.188.26'.

Discovered Interfaces			
1.1.1 Gira S1	192.168.188.26:3671	00:0A:B3:28:07:46	
15.15.255 Gira X1	192.168.188.35:3671	00:0A:B3:29:0A:E0	

IP Tunneling configuration:

- Name: Gira S1
- Host Individual Address: 1.1.1
- Individual Address: 1.1.2 (Address free?)
- IP Address: 192.168.188.26
- Port: 3671
- MAC Address: 00:0A:B3:28:07:46

Figure 6: IP address of Gira S1

- Select Gira S1 and switch to the "IP" tab.
- Make a note of the commissioning password and authentication code.

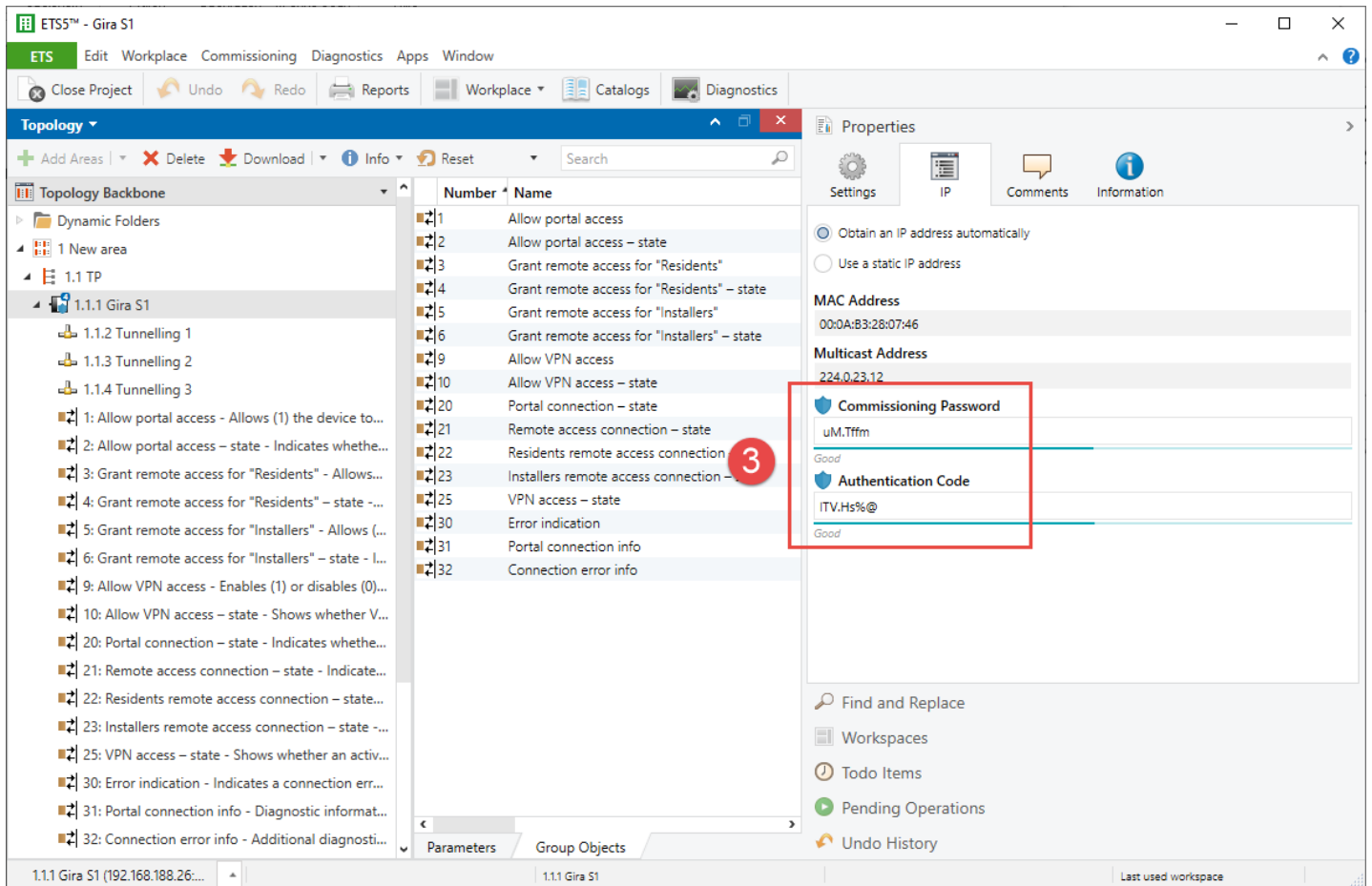


Figure 7: Gira S1 passwords

3.3.2. Settings in Gira HomeServer Expert

- In Gira HomeServer Expert navigate to "Project settings" and open the "KNX & iETS" tab.
- Enter the previously noted parameters in the corresponding fields:

Parameter	Entry
Interface:	KNXnet/IP tunneling (with KNX Secure support)
Physical address:	Physical address of the desired tunneling interface (1)
IP adress:	IP address of Gira S1 (2)
Port:	3671
Activate IP Secure:	Yes
Start-up password:	Start-up password of Gira S1 (3)
Authentication code:	Authentication code of Gira S1 (3)

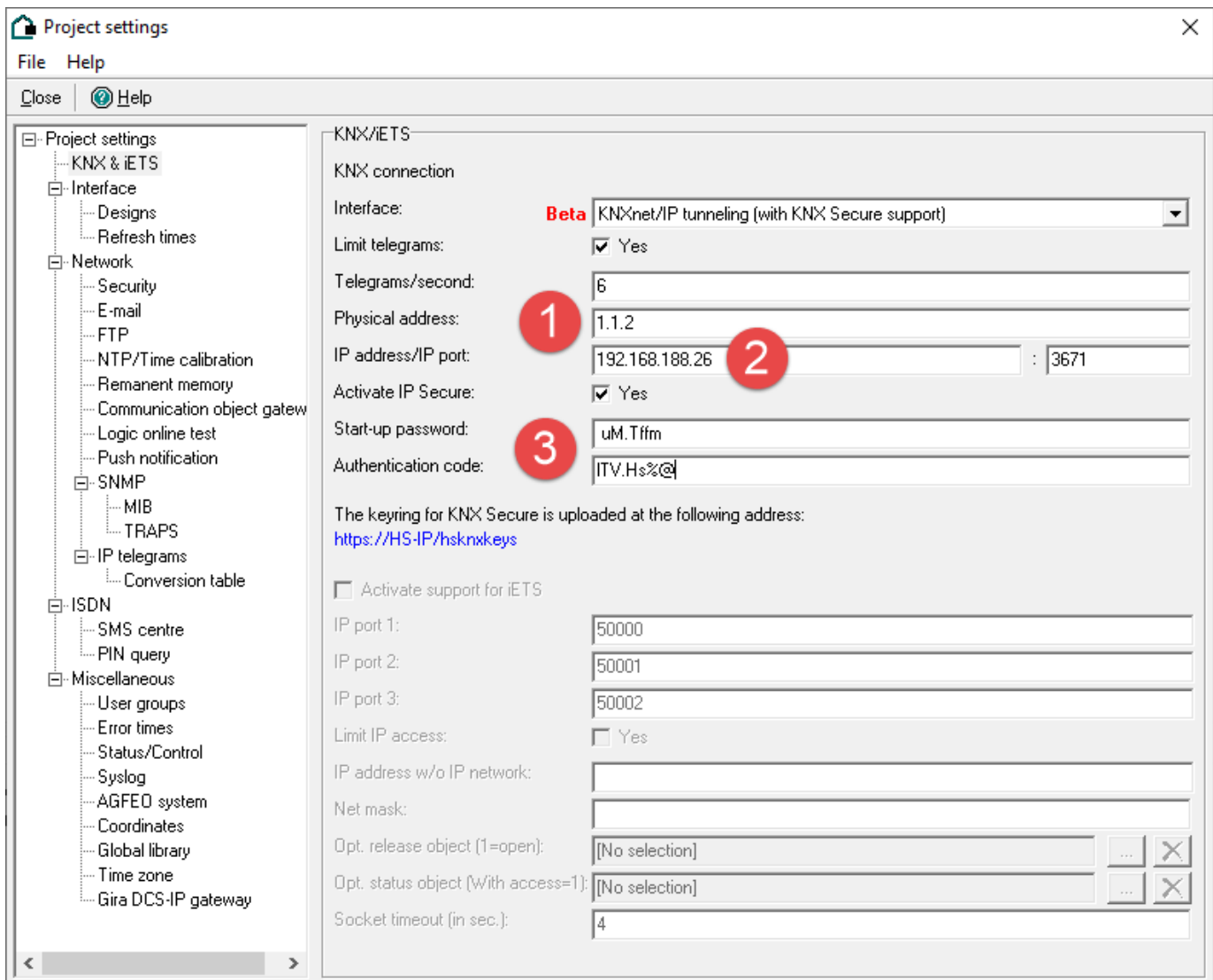


Figure 8: Gira HomeServer Expert – Settings

3.3.3. Transmit group addresses "Data Secure" (recommended)

Settings in the ETS

- Enter all used group addresses in the association table of the selected tunneling connection.

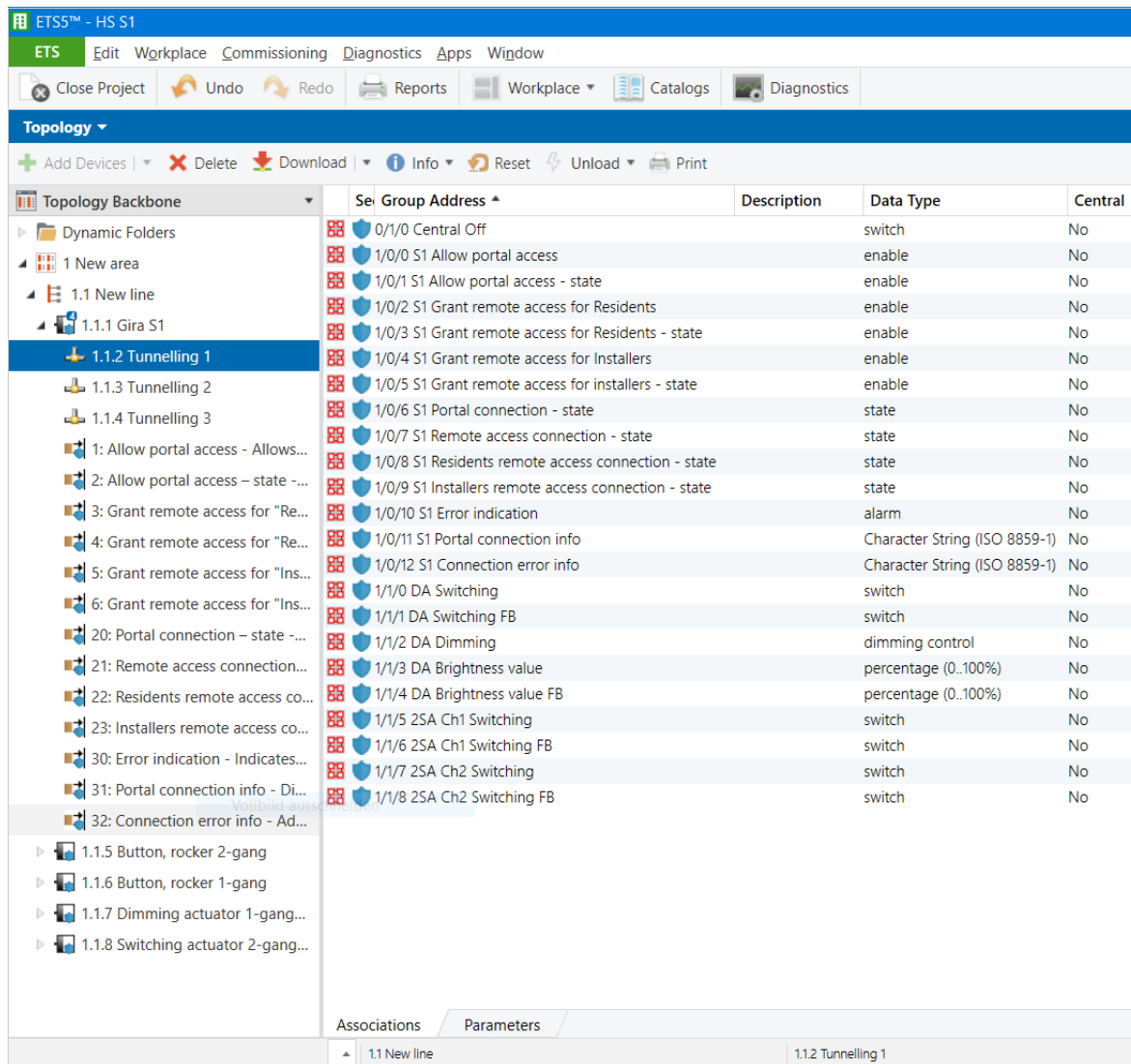


Figure 9: Associations of the tunneling connection

- Click on "Export key ring" in the ETS under "Security".
- Select the desired tunneling connection.

Settings in Gira HomeServer Expert

- Transfer the Gira HomeServer project with Gira HomeServer Expert.

Settings on the start page of the Gira HomeServer (<https://HS-IP/>)

- Go to the web page for uploading the KNX key bundle file.
- Select the exported key bundle file and enter the password.
- Authenticate the process and click on "Upload".

3.4. Access to KNX installations

The Gira S1 Windows client enables secure access to KNX installations via the Internet. For this purpose, the Gira S1 Windows client is installed on the computer and started in parallel to the ETS. Since the KNX/IP protocol is completely unprotected today, the Gira S1 transfers all KNX/IP data encrypted with SSL/TLS to the Gira Device portal while the portal, in turn, exchanges this data encrypted with SSL/TLS with the Gira S1 Windows client. The Gira S1 Windows client then provides the KNX/IP data for the ETS unencrypted locally on the computer using the ETS so that the ETS can be used completely transparently in the usual way.

The Gira Project Assistant (GPA) constitutes an alternative to the Gira S1 Windows Client. To use this option, you must create a GPA project, activate the "Remote maintenance" option in the project scope, and select "Gira S1 remote access module" as the remote access method. Then, enter your remote access ID and authentication key in the "Configure remote access" area. You only need to set this up once. Now click on "Connect" (top right). The GPA will establish the connection to the Gira S1. You can now start the ETS and see the remote system's ETS interfaces in the "Bus" area. The interfaces found have the prefix "GPA".

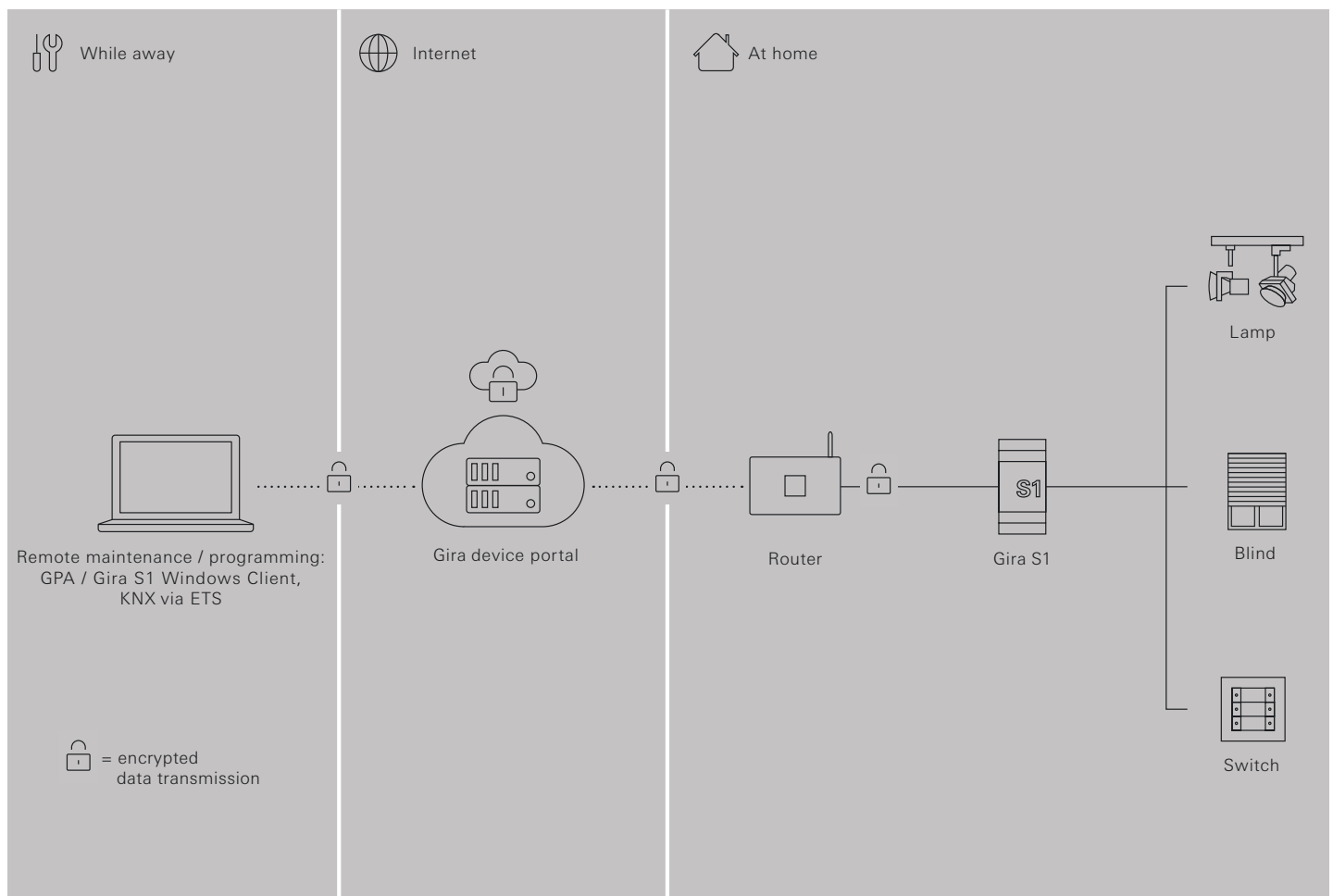


Figure 10: Secure remote access to the KNX installation with the Gira S1.

Once a connection to a specific Gira S1 has been established using the Gira S1 Windows client (see chapter 11.2 "Connecting to the Gira Device portal"), the KNX/IP interfaces available on the remote network appear in the ETS as if the ETS itself were on the remote network. To avoid confusion with other devices on your own network, it is possible to append a text to the device name normally displayed in the ETS. In addition, it is also possible to make only the KNX/IP interface of the Gira S1 available for the sake of simplicity. In addition to the KNX/IP interfaces, all devices that can be loaded directly via IP (see chapter "Accelerate transfer: Select transfer path IP") are made known to the ETS so that these accelerated downloads also work via remote access. For more information, see chapter 11.3 "Configuring the access options of a Gira S1".

3.4.1. Limitations and authorisation of access rights via KNX communication objects

If the Gira S1 is added to an ETS project, its communication objects can be used to prohibit or allow access options via KNX, even at runtime. The access rights limitations defined via the KNX in the remote installation always take precedence over the definitions in the portal. In this way, remote access can be deactivated completely, regardless of the settings in the Gira Device portal, through the use of group telegrams.

3.5. Access to websites on the remote network

Remote access via the Gira S1 enables secure access to websites on the remote network. For this purpose, the unencrypted (HTTP) data on the remote network (see Figure 11) is transported to the Gira Device portal server via an encrypted SSL/TLS connection and then to the web browser via an HTTPS connection.

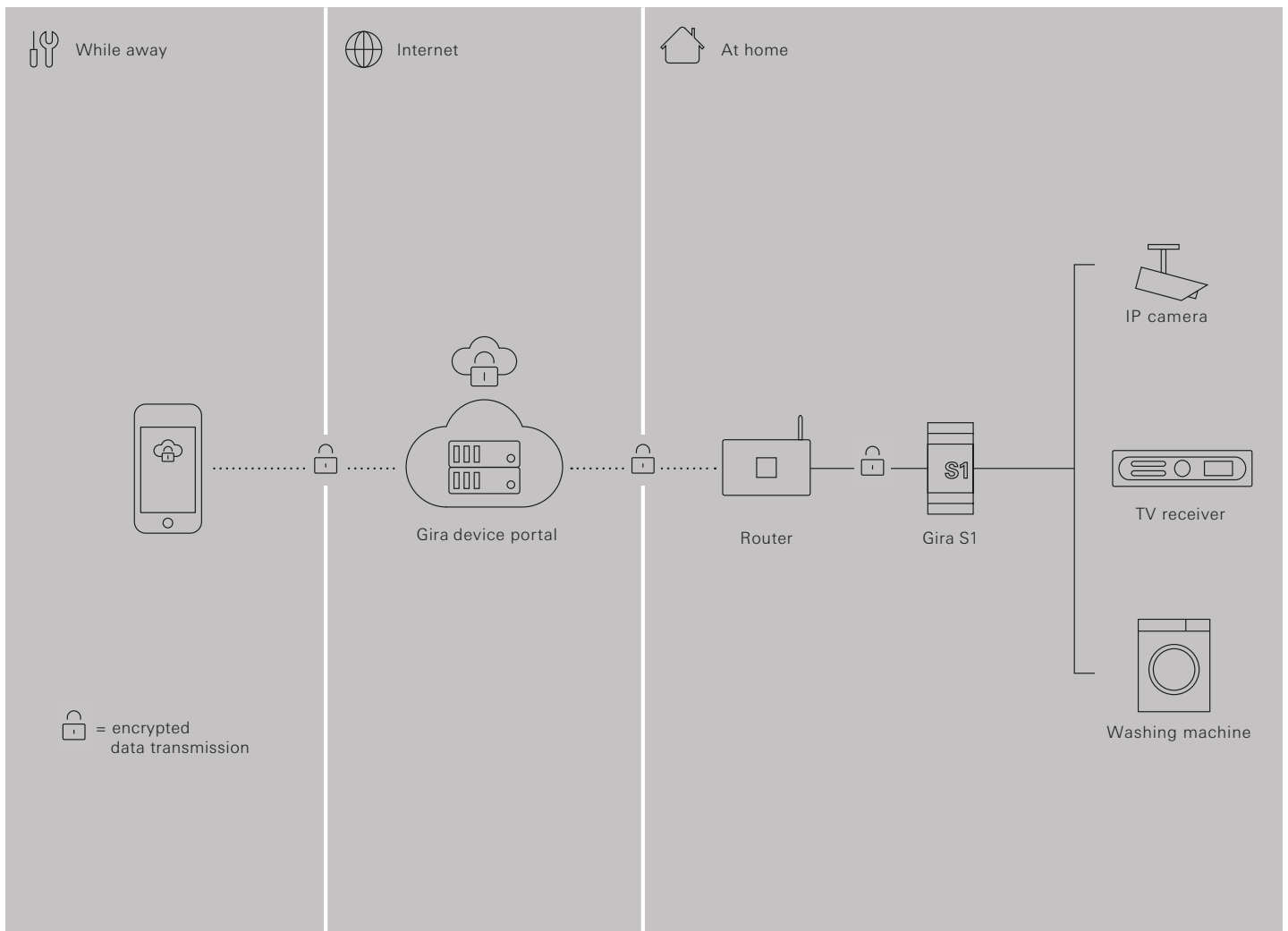


Figure 11: Secure access to websites via remote access.

The easiest way to access websites on the remote network via HTTP is through the Gira Device portal. Access via the Gira Device portal is quick to configure. For a description on this, see chapter 10.4 "Links".

3.6. Access via other TCP protocols

Using the Gira S1, it is possible to use nearly all TCP-based protocols securely over the Internet. The Remote Desktop Protocol (RDP), which Microsoft has defined for remote access to Windows computers, is widely used, among others. Together with the Gira S1 Windows client, you can easily configure access. For more information, see chapter 11.3.3 "Using other TCP protocols via remote access".

3.7. User rights and user groups

Irrespective of the type of access (e.g. websites, KNX, HomeServer, remote desktop connection), access rights for the predefined user groups "residents" and "installer" can be configured for each relationship between the Gira S1 and portal user and controlled dynamically using KNX communication objects.

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

- With the Gira S1, one or more portal users of the electrical trade company/system integrator are linked in the role of the "installer" for maintenance purposes.
- With the Gira S1, one or more portal users are linked in the role of "resident", typically all family members, for visualisation on a smartphone and website access.
- The Gira S1 is configured using the parameters in the ETS in such a way that the users with the "residents" user group always have access; in addition, the users in the "installer" user group have access by default.
- 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 grants the installer access by selecting an option in his/her visualisation or using the corresponding communication object. Automatic deactivation of access after a certain period of time is also easy to arrange using logic or a timer.
- For security-sensitive residents, it is also possible to deactivate remote access completely using a button or visualisation. In this case, the Gira S1 no longer reports to the portal, and remote access is impossible.
- The Gira S1 indicates that a connection has been established via remote access using KNX communication objects, thereby making suitable processing in a visualisation/logic (e.g. e-mail when someone connects) easily possible.

In addition, software access, such as visualisations, can be controlled using activation codes. Each user can create any number of codes on each Gira S1 to which he/she has access, e.g. for visualisation (see chapter 10.7 "Access to applications").

4. Time server

As a time server, the Gira S1 can send the current time to the KNX bus at configurable intervals. For this, first you activate the "Time server" parameter in the "General" parameter view so that the parameter page "Time server" becomes visible (see chapter 8.5 "Parameters"). You configure then the respective desired interval with the "Send time" and "Send date" parameters. The time sent is obtained from the system time. This is synchronised with a NTP server which can be configured via device website. The interval for sending the communication object 52 "Date and time" to the KNX bus is the shorter one of the parameters "Send time" (communication object 50) and "Send date" (communication object 51) if they differ.

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

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

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

With the time server function, a communication object is provided with which the sending of the time/date can be triggered (trigger). For more details, see chapter 8.6 "Object table".

The time server function is deactivated at delivery.

5. Data logger

The Gira S1 can be used as a data logger. The data logger functionality is controlled via the "Data logger" parameter in the "General" parameter view (see chapter 8.5 "Parameters"). If it is set to "Yes", the data logger functionality is always activated. If a microSD card is inserted into the device or if there is already a microSD card in the device, logging begins automatically if it is not deactivated via the "Activate data logger" communication object.

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

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

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

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

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

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

Naming and saving the log files on the microSD card is in accordance with the following scheme: 2010_01_06_TP1.trx (Year_Month_Day).

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

The Gira S1 supports SDHC cards up to a maximum of 32 GB. The cards must be formatted with FAT32.



Important note

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

Various communication objects are available for monitoring the memory status. The current card status and the occupancy level are queried via these communication objects. For more details, see chapter 8.6 "Object table".

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

5.1. Access to the data logger archive

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

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

GIRA Gira S1

Device status Data logger Network settings Download logfile Reboot Factory reset

Firmware update Diagnostics page

Data logger

Note: You can configure the data logger with the ETS. Further information can be found in the manual.

SD card status: (using 0 of 1910 MB)

Content

- **2019**
 - 2019-07 9.7 kB
 - 2019_07_11_TP1.xml 9.7 kB

© Copyright 2011-2019 Gira, Giersiepen GmbH & Co. KG V5.0.714.0 English ▼

Figure 12: Data logger archive

The number next to a month or a single file indicates the file size in bytes. Push the download symbol to start the download of a xml-file.

6. VPN

To access your home network via VPN, you need an OpenVPN client.

Download the OpenVPN software from <https://openvpn.net/community-downloads/> and install it on your PC.

The compatibility of version 2.5.0 with the VPN function of Gira S1 has been ensured.

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

6.1. Prerequisite for the VPN setup

- A user account has been created at <https://geraeteportal.gira.de>.
- Gira S1 is connected to the Internet.
- Gira S1 is registered in the Gira Device Portal.
- A published version (released) of the OpenVPN client has been downloaded and installed on the PC or smartphone.

6.2. VPN setup

1. Log in to the Gira Device Portal.
2. Click on "VPN access" in the function overview.
3. Click on the "Set up VPN access" button.
4. Wait until the configuration file has been created and download the file.
5. Open the OpenVPN client and import the configuration file.
6. Activate the VPN connection in the OpenVPN client.

If you want to create the VPN access for several users, each user needs their own user account in the Gira Device Portal. Repeat steps 4 to 6 for each user.



Note

First test whether the configuration you have made works before you set up VPN access for additional users.

7. Installation

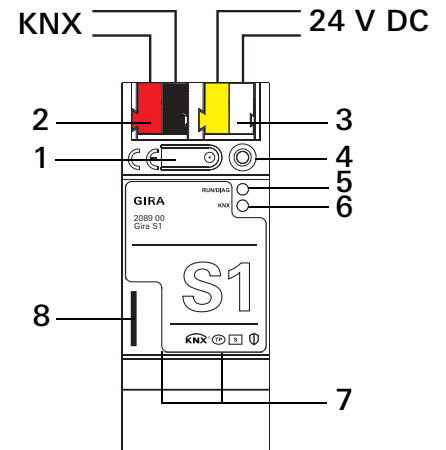


Safety note

Electrical devices may only be installed and connected by a qualified electrician. Failure to observe the instructions can result in damage to the device, fire or other dangers.

7.1. Device design

1. Programming button
2. KNX connection
3. External power supply connection
4. Programming LED (red):
on = programming mode active
5. Operating LED (green):
on = Gira S1 ready for operation
flashing slowly = Gira S1 not yet parametrised or parametrised incorrectly
flashing quickly = internal device error
6. KNX-LED (yellow)
on = connection to KNX system
off = no connection to KNX system
flashing = KNX data transfer
7. Network connection with LED (green/orange)
green on = data transfer rate 100 Mbit/s
green off = data transfer rate 10 Mbit/s
orange on = connection to IP network
flashing orange = no connection to IP network, no data being received from IP network
8. microSD card (up to 32 GB (SDHC))
A microSD card must be inserted for the data logger to be able to record telegrams.



7.2. Installation and electrical connection



Danger

There is a danger of electric shock if live parts are touched in the installation area. Electric shock may lead to death. Isolate before working on the device and cover up live parts in the vicinity!

7.2.1. Mounting the device

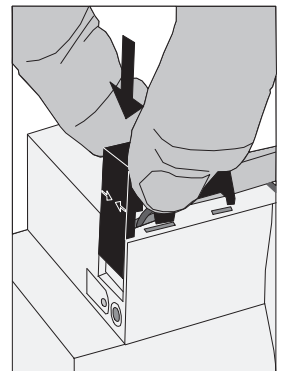
Observe the ambient temperature. Ensure sufficient cooling.

- Snap the device onto a top-hat rail according to DIN EN 60715. See figure 1 for installation position.
- Connect the external power supply to the connection terminal (3). Recommendation: Use white-yellow connection terminal.
- Connect KNX line with red-black bus terminal (2).
- Attach cover cap over the KNX/external power supply connection.
- Establish network connection by plugging RJ45 plug into RJ pin jack (7).

7.2.2. Attaching the cover cap

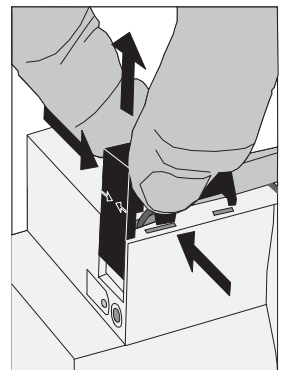
A cover cap must be attached to protect the bus connection from dangerous voltages in the connection area.

- Guide bus line to the rear.
- Attach cover cap over the bus terminal until it engages.



7.2.3. Removing the cover cap

- Press cover cap on the sides and remove.



8. Configuration in the ETS

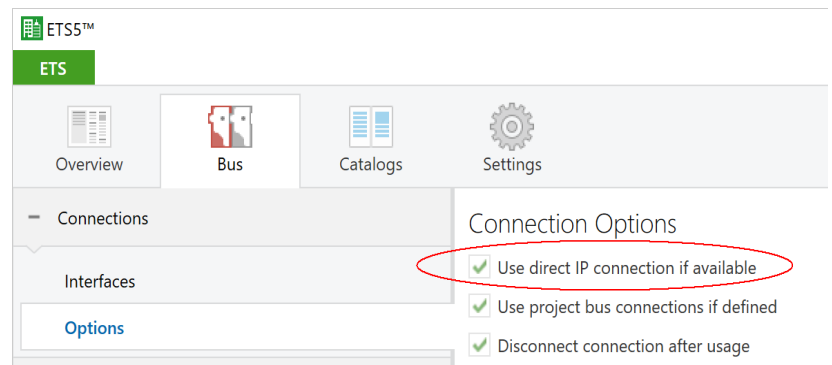
Configuration of the Gira S1 in the ETS is divided into the following steps:

1. Create the Gira S1 as a device in the ETS (Chapter 8.1).
2. Assign the physical address for the device as well as up to three physical addresses for the interface (Chapter 8.2).
3. Set the IP address, IP subnet mask and default gateway address of the Gira S1 or select "Obtain an IP address automatically" (from a DHCP server) (Chapter 8.3).
4. Set general parameters for the Gira S1, including a DNS server, if applicable (for information on the parameters, see Chapter 8.5).
5. Connect group addresses to group objects (for information on the object table, see Chapter 8.6).
6. Program the physical addresses (Chapter 8.3.1).
7. Transfer the application program and configuration (Chapter 8.4).

Accelerate transfer: Select transfer path IP

Programming (transfer from the ETS to the device) occurs in the ETS. No additional KNX data interface is required for the 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 via the IP side of the device is recommended. You can select this option on the ETS start page in the "Bus" - "Connections" - "Options" view: To transfer the ETS via the IP side, select the "Use direct KNX IP connection if available" option.



8.1. Creating Gira S1 as a device in the ETS

If you have not already done so, perform a one-time import of the ETS device application for the Gira S1 to the device catalogue of your ETS. You can download the ETS application free of charge at www.downloads.gira.de.

Product catalogue

Product name: Gira S1

Design: DRA (series installation)

Order No.: 2089 00

State of delivery

Upon delivery or after a factory reset, the Gira S1 is configured as follows before it is loaded with ETS for the first time:

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

If you already have an ETS project with a previous database entry, you can also update the application program. To do so, drag the new database entry into the project and then select the device with the old database entry. Now select "Information" in the device "Properties" and select the "Application" (ETS4.2) or "Application program" tab (ETS5). You can now replace the old database entry by clicking the "Update application program" (ETS4.2) or "Update" button (ETS5). Existing links to group addresses are not lost. You can now delete the newly added device. In ETS4.2, you require a special license for this. From ETS5 and higher, this is possible with any license.

8.2. Assigning physical addresses

The Gira S1 has three tunnelling servers (KNX/IP interfaces). These interfaces can be used for downloading and in the group and bus monitor modes. In addition to the device's physical address, the device also has (up to) three additional physical interfaces. You can configure these, as with many products today, using the interface settings after opening the KNX/IP connection in the ETS. In this case, you must take special care to ensure that the addresses are not already used elsewhere. From ETS4 and higher, it is possible to specify the number of additional addresses for products to ensure that these can be configured in the ETS. A list containing the additional addresses appears for this purpose below the input box for the physical address in the device properties in the ETS. In this case, the ETS ensures that the addresses are unique in the project and automatically loads three addresses to the device 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-assigns the additional addresses automatically.

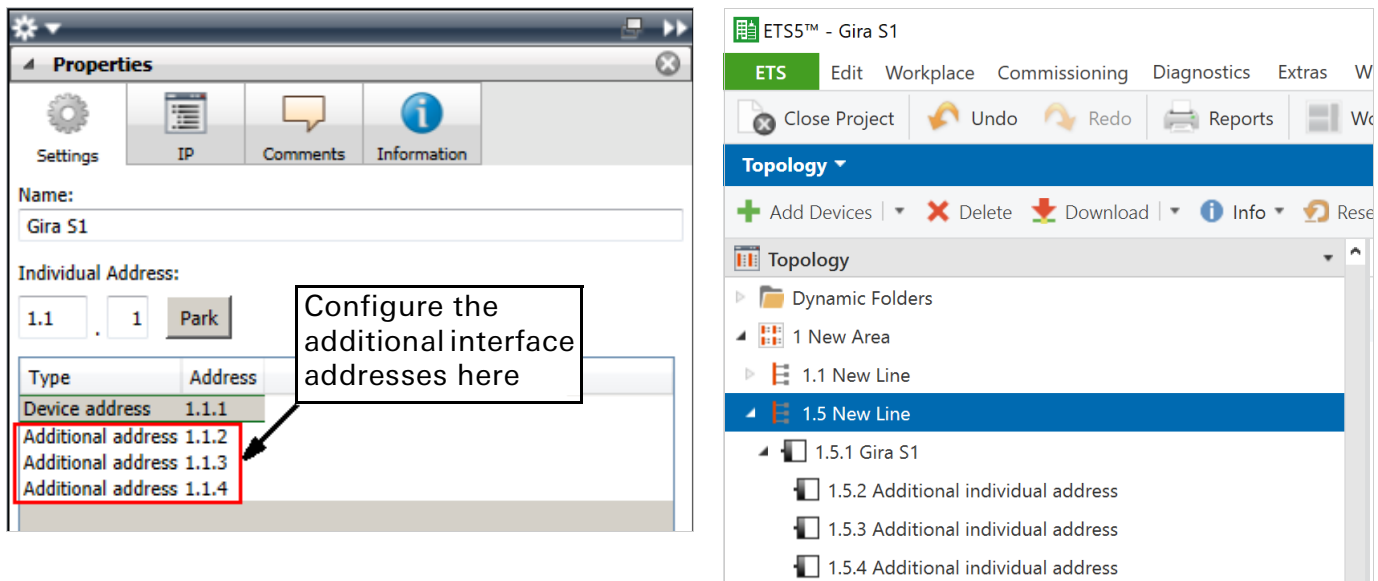


Figure 13: Additional physical addresses in ETS4 (left) and ETS5 (right)

8.3. Setting the IP address, subnet mask and address of the default gateway

In addition to the physical address on the KNX network, the Gira S1 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

Proceed as follows:

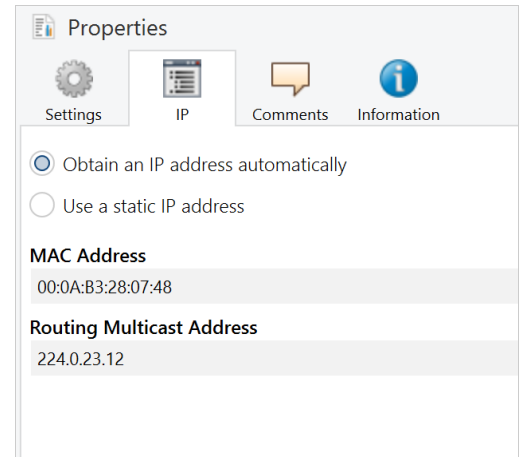
1. Select the Gira S1 in the ETS.
2. Display the properties of the Gira S1 in the properties column of the ETS.
3. Select the "IP" tab.

Then select either

- "Obtain an IP address automatically" (default)
The address data is obtained automatically from a DHCP server on the data network.

or

- "Use a static IP address"
and enter the data manually.
You can usually obtain the permissible IP address range, as well as 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 device parameters (see chapter 8.5 "Parameters")!

If the "Obtain an IP address automatically" setting is used, a DHCP server must issue the Gira S1 a valid IP address. If no DHCP server is available for this setting, the device starts up with an auto IP address after a certain waiting period (address range from 169.254.1.0 to 169.254.254.255). As soon as a DHCP server is available, the device is automatically assigned a new IP address.

8.3.1. Programming the physical address of the device

1. Ensure that the device and bus voltage are switched on.
2. Ensure that the programming LED (4) is not illuminated.
3. Briefly press programming button (1) – programming LED (4) lights up red.
4. Program the physical address using the ETS.

When the programming process is completed successfully,

- LED (4) goes out.
- the ETS displays the completed transfer marked in green under History in the properties column (normally at the far right of the window).
- the ETS sets the start-up checkmark on the device for "Adr" and "Cfg".

You can now make a note of the physical address on the device.



Note

The additional addresses of the tunnelling server, which the Gira S1 provides and which supports up to three connections, are also configured via the ETS in the device properties.

8.4. Transferring application programs and configuration data

Once you have programmed the physical address, you can transfer the application program, parameter settings and group address connections to the device. You can create the connection to the device via IP or KNX.

- To do so, select “Download Application”. The download takes approx. 15 seconds for a direct IP connection or approx. 2 minutes if using TP.
- Wait for approx. 15 seconds after the download while the device copies the data and initialises the application.
- Start-up is complete.

8.5. Parameters

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

8.5.1. General

Parameters	Entry / Selection	Remarks
DNS server (if not using DHCP)	Default gateway	The IP address of the default gateway is used (see chapter 8.3 "Setting the IP address, subnet mask and address of the default gateway").
	Individual DNS server IP address	This parameter enables you to set up an individual IP address for the DNS server.
	0.0.0.0	The individual DNS server IP address. If 0.0.0.0 is used, the default gateway is used.
Controlling VPN access via KNX	No Yes	This parameter provides the communication objects for VPN access and its status when activated.
Time server	No Yes	The device works as a time server and sends the current time and date to the KNX bus at configurable intervals.
Data logger	No Yes	This parameter determines whether the data logger function is activated. The corresponding communication objects are only available when it is activated.
Time zone	(UTC+01:00) Europe/Berlin Other UTC time zones	The time zone to be used is selected here. There are several time zones with identical UTC deviations. In some of these time zones, summer/winter time switchover is at a different time. One of the "Generic Time Zone w/o DST" time zones must be selected so that no automatic time changeovers are carried out. Important note: If this setting is changed, the Gira S1 will restart directly after the application has been programmed! Important note: The option to disable NTP via the device website has been deactivated since firmware version 5.0. If you have disabled NTP, an NTP server from ntp.org is automatically used as the default NTP server.
General remote access after restart	as before restart	After a restart, the general remote access status is set to the last known value before the restart. For example, if the general remote access status is activated before the restart, the remote access status is also activated after a restart.
	activated	Enables the device to establish a connection to the portal server after each restart.
	deactivated	Prohibits the device from establishing a connection to the portal server after each restart.

Parameters	Entry / Selection	Remarks
Remote access for the "residents" or "installer" groups after restart	as before restart	After a restart, the remote access status of the respective group is set to the last known value before the restart. For example, if the remote access status is activated before the restart, the remote access status is also activated after a restart.
	activated	Enables remote access for the respective group after each restart.
	deactivated	Prohibits remote access for the respective group after each restart.
Number of notification objects	0...50	Specify the number of notification objects here (max. 50). The "101 ff." group objects are visible according to your selection.
Separator for floating point numbers	. ,	

8.5.2. Parameter page Time server

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

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

8.5.3. Parameter page Data logger

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

Parameters	Entry / Selection	Remarks
Format		This parameter determines which format the data should be logged in on the microSD card.
	ETS4/ETS5	The data is stored in an ETS4-compliant format (.xml) which is also readable by the ETS5.
	ETS3	The data is stored in an ETS3-compliant format (.trx).
Memory type	cyclic buffer static buffer	This parameter specifies how the microSD card memory is to be used.
Memory status type		Only visible when "Memory type" is set to "static buffer". This parameter specifies what type the status object of the card occupancy level should be.
	binary	A 1-bit object is used. The value "1" means that the microSD card is full, "0" means that there is still space on the microSD card for logging
	value (0-255)	A 1-byte object is used. The value range is between 0 – 255. The value "255" corresponds to a card occupancy level of 100%.

8.5.4. Notifications

According to the number of notifications selected above, you can now specify the DP types and other parameters for the respective notification (notification no. 1 = group object 101, notification no. 2 = group object 102...).

Parameters	Entry / Selection	Remarks
Data type	Bool (1 bit, DPT 1.001) Percent (1 byte, DPT 5.001) Counter (1 byte, DPT 5.010) Floating point (2 bytes, DPT 9.*) Text (14 bytes, DPT 16.001)	You can select the required data type of the respective notification.
Notification only in case of value change	Checkbox (inactive)	
Threshold	0-1000 Specification as an integer	Suppress notifications. Only send a notification again once the threshold value is exceeded. The threshold value is the deviation from the last value (as an absolute number) that a notification generated. 0: not a threshold value. You will receive a notification for each change.


Parameters	Entry / Selection	Remarks
Basis of threshold value	Value per dropdown list	Factor by which the threshold value will be multiplied, if required. 1: not a factor.
Filter	<p>Always generate notification</p> <p>Generate notification for 1 (true) only</p> <p>Generate notification for 0 (false) only</p> <p>Text</p>	<p>For the Bool (DPT 1.001) data type, the filter is possible via a selection list.</p> <p>For all other data types, the filter can comprise a fixed value or up to two conditions. For a description, see parameter dialog.</p>
Priority	Low High Alarm	
Category	Text	Can be used to filter the notifications and their forwarded messages on the portal.
Subject	Text	For a description, see parameter dialog. Used as the "Subject" when sending e-mails.
Text	Text	For a description, see parameter dialog. Used as the "Text" when sending e-mails.
Add attachment	Checkbox (inactive)	
URL of the attachment	Text	Only http requests are supported. Observe the maximum permissible file size of 250 kB.


8.6. Object table



Note for all group objects that signal an active connection



When using HTTP access, i.e. without a Gira S1 Windows 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 Gira Device portal. HTTP connections may require up to five minutes to close. This means that the corresponding group objects that signal an active connection also do not signal closing until this point in time. In contrast, if using the Gira S1 Windows client, the connection is closed synchronously.

The following group objects are available for the connection of group addresses at the Gira S1:

Object	Name	Direction	Data width	DP type	Flags (CRWTU)
 1	Allow portal access	Write	1 bit	1.003	C-W--
Category:	Remote access	Data type:	Enable		
Function:	Allows the device to establish a connection to the portal server or prohibits it from establishing one.				
Description:	1 = Allow, 0 = Prohibit				

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

Object	Name	Direction	Data width	DP type	Flags (CRWTU)
 3 (Residents)  5 (Installer)	Grant remote access	Write	1 bit	1.003	C-W--
Category:	Remote access	Data type:	Enable		
Function:	Allows or prohibits remote access for members of the group				
Description:	1 = Allow, 0 = Prohibit				

Object	Name	Direction	Data width	DP type	Flags (CRWTU)
 4 (Residents)  6 (Installer)	Grant remote access – state	Read	1 bit	1.003	CR-T-
Category:	Remote access	Data type:	Enable		
Function:	Indicates whether remote access is allowed for members of the group.				
Description:	1 = Allowed, 0 = Prohibited				

Object	Name	Direction	Data width	DP type	Flags (CRWTU)
■ 9	Allow VPN access	Write	1 bit	1.003	C-W--
Category:	VPN access	Data type:	Enable		
Function:	Enables or disables VPN access for all users approved for the VPN on the Gira Device Portal.				
Description:	1 = Allow, 0 = Prohibit				
Object	Name	Direction	Data width	DP type	Flags (CRWTU)
■ 10	Allow VPN access – state	Read	1 bit	1.011	CR-T-
Category:	VPN access	Data type:	State		
Function:	Indicates whether VPN access is allowed.				
Description:	1 = Allowed, 0 = Prohibited				
Object	Name	Direction	Data width	DP type	Flags (CRWTU)
■ 20	Portal connection – state	Read	1 bit	1.011	CR-T-
Category:	Remote access	Data type:	State		
Function:	Indicates whether connection to portal is established. Group object 31 provides more detailed information.				
Description:	1 = Connected, 0= Disconnected				
Object	Name	Direction	Data width	DP type	Flags (CRWTU)
■ 21	Remote access connection – state	Read	1 bit	1.011	CR-T-
Category:	Remote access connection	Data type:	State		
Function:	Indicates whether at least one remote access 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)	Remote access connection – state	Read	1 bit	1.011	CR-T-
■ 23 (Installer)					
Category:	Remote access connection	Data type:	State		
Function:	Indicates whether a remote access connection is active for members o the group. An active connection is signalled for another group if applicable if access was granted to a member of this group based on membership in another group.				
Description:	1 = Active, 0 = Not active				
Object	Name	Direction	Data width	DP type	Flags (CRWTU)
■ 25	VPN access – state	Read	1 bit	1.011	CR-T-
Category:	VPN access	Data type:	State		
Function:	Shows wether an active VPN connection currently exists.				
Description:	1 = Active, 0 = Not active				

Object	Name	Direction	Data width	DP type	Flags (CRWTU)
■ 30	Error display	Read	1 bit	1.005	CR-T-
Category:	Connection error	Data type:	Alarm		
Function:	Indicates a connection error, which is described by group object 32. Further details can be found on the diagnostic page of the Gira S1.				
Description:	1 = Alarm, 0 = No alarm				
Object	Name	Direction	Data width	DP type	Flags (CRWTU)
■ 31	Portal connection info	Read	14 bytes	16.001	CR-T-
Category:	Connection error	Data type:	Character (ISO 8859-1)		
Function:	Diagnostic information about the portal connection				
Description:	Supplies more precise information on the portal connection status displayed by group object 20.				
Object	Name	Direction	Data width	DP type	Flags (CRWTU)
■ 32	Connection error info	Read	14 bytes	16.001	CR-T-
Category:	Connection error	Data type:	Character (ISO 8859-1)		
Function:	Additional diagnostic information in case of a portal connection error.				
Description:	Supplies more precise information on the connection error displayed by group object 30.				
Object	Name	Direction	Data width	DP type	Flags (CRWTU)
■ 50	Time	Read	3 bytes	10.001	CR-T-
Category:	Time server	Data type:	Time of day		
Function:	Sends cyclically and on request the current time.				
Description:	3 byte object for sending the current time. The interval can be parameterised (see chapter 8.5.2 "Parameter page Time server"). If you read this object explicitly before a valid NTP time could be obtained, the current system time is returned which can differ from the correct time.				
Object	Name	Direction	Data width	DP type	Flags (CRWTU)
■ 51	Datum	Read	3 bytes	11.001	CR-T-
Category:	Time server	Data type:	Date		
Function:	Sends cyclically and on request the current date.				
Description:	3 byte object for sending the current date. The interval can be parameterised (see chapter 8.5.2 "Parameter page Time server"). If you read this object explicitly before a valid NTP time could be obtained, the current system date is returned which can differ from the correct date.				

Object	Name	Direction	Data width	DP type	Flags (CRWTU)
■ 52	Date and time	Read	8 bytes	19.001	CR-T-
Category:	Time server	Data type:	Date/Time		
Function:	Sends cyclically and on request current date and time.				
Description:	8 byte object for sending the current date and time. The interval is determined by the shorter interval of the parameters for the communication objects 50 "Time" and 51 "Date" (see chapter 8.5.2 "Parameter page Time server"). If you read this object explicitly before a valid NTP time could be obtained, the current system time and date is returned which can differ from the correct time and date.				

Object	Name	Direction	Data width	DP type	Flags (CRWTU)
■ 53	Trigger send date/time	Write	1 bit	1.007	C-W--
Category:	Time server	Data type:	Trigger		
Function:	Triggers the sending of date and time.				
Description:	1-bit object for triggering the sending of the current time/date if the object has been assigned any desired value. If no NTP query has been successful yet, no values will be sent.				

Object	Name	Direction	Data width	DP type	Flags (CRWTU)
■ 54	NTP query – state	Read	1 bit	1.002	CR-T-
Category:	Time server	Data type:	Boolean		
Function:	Indicates whether a valid time could be requested by the NTP server.				
Description:	1-bit object for display of the status of the last NTP query. If the NTP query was successful and the system time has been reset as a result or if there was an error during the previous query, the object is assigned a "1". If the last NTP query was not successful, the object is assigned a "0".				

Object	Name	Direction	Data width	DP type	Flags (CRWTU)
■ 55	SD card error	Read	1 bit	1.002	CR-T-
Category:	Data logger	Data type:	Boolean		
Function:	Indicates whether there is currently an error with the SD card.				
Description:	1-bit object for signalling an SD card error. When a "1" is assigned to the object, an SD card error has occurred.				

Object	Name	Direction	Data width	DP type	Flags (CRWTU)
■ 56	SD error code	Read	1 byte	20.*	CR-T-
Category:	Data logger	Data type:	-		
Function:	Indicates the current error code (0 = no error).				
Description:	1-byte object for signalling a microSD card error. 0 = microSD card OK 1 = microSD card full 2 = microSD card not inserted 4 = Fault has occurred in microSD card (e.g. incorrectly formatted)				

Object	Name	Direction	Data width	DP type	Flags (CRWTU)
■ 57	Activate data logger	Write	1 bit	1.001	CRW--
Category:	Data logger	Data type:	Switch		
Function:	Activates (1 = default) or deactivates (0) the logging and indicates the status on request.				
Description:	1-bit object to activate the data logger. When a "1" is assigned to the object, the data logger is active. If a "0" is assigned to it, it is deactivated.				
Object	Name	Direction	Data width	DP type	Flags (CRWTU)
■ 58	Data logger – state	Read	1 bit	1.002	CR-T-
Category:	Data logger	Data type:	Boolean		
Function:	Indicates whether the data logger is currently recording data.				
Description:	1-bit object which reflects the state of the data logger. If the object has a value of "1", the data logger is active. A "0" means that the data logger is inactive.				
Object	Name	Direction	Data width	DP type	Flags (CRWTU)
■ 59	SD card – memory state	Read	1 bit	1.002	CR-T-
Category:	Data logger	Data type:	Boolesch		
Function:	Indicates if the SD card memory is exhausted (1 = full).				
Description:	1-bit object for display of the occupancy level of the SD card. When a "1" is assigned to the object, the SD card is full. If it is assigned a "0", then there is still space for logging on the SD card.				
Object	Name	Direction	Data width	DP type	Flags (CRWTU)
■ 60	SD card – filled memory capacity	Read	1 byte	5.001	CR-T-
Category:	Data logger	Data type:	Percentage (0..100%)		
Function:	Shows how many % of the SD card memory is occupied.				
Description:	1-byte object for displaying the memory occupancy of the SD card. The value range is 0-255 (equivalent to 0-100%).				
Object	Name	Direction	Data width	DP type	Flags (CRWTU)
■ 101 - 150	Notification	Write	1 bit	1.001	C-W--
Category:	Switching	Data type:	On/Off		
Function:	Sends a notification to the portal server.				
Description:	This is one of five possible DP types for the 50 group objects "101 to 150". The DP type is specified by selecting the corresponding data in the general parameters (see chapter 8.5 "Parameters").				
Object	Name	Direction	Data width	DP type	Flags (CRWTU)
■ 101 - 150	Notification	Write	1 byte	5.001	C-W--
Category:	Percent	Data type:	Percent (0 to 100%)		
Function:	Sends a notification to the portal server.				
Description:	This is one of five possible DP types for the 50 group objects "101 to 150". The DP type is specified by selecting the corresponding data in the general parameters (see chapter 8.5 "Parameters").				

Object	Name	Direction	Data width	DP type	Flags (CRWTU)
■ 101 - 150	Notification	Write	1 byte	5.010	C-W--
Category:	Counter	Data type:			
Function:	Sends a notification to the portal server.				
Description:	This is one of five possible DP types for the 50 group objects "101 to 150". The DP type is specified by selecting the corresponding data in the general parameters (see chapter 8.5 "Parameters").				
Object	Name	Direction	Data width	DP type	Flags (CRWTU)
■ 101 - 150	Notification	Write	2 bytes	9.*	C-W--
Category:	Floating point	Data type:	KNX floating point		
Function:	Sends a notification to the portal server.				
Description:	This is one of five possible DP types for the 50 group objects "101 to 150". The DP type is specified by selecting the corresponding data in the general parameters (see chapter 8.5 "Parameters").				
Object	Name	Direction	Data width	DP type	Flags (CRWTU)
■ 101 - 150	Notification	Write	14 bytes	16.001	C-W--
Category:	Text	Data type:	Character (ISO 8859-1)		
Function:	Sends a notification to the portal server.				
Description:	This is one of five possible DP types for the 50 group objects "101 to 150". The DP type is specified by selecting the corresponding data in the general parameters (see chapter 8.5 "Parameters").				

9. Displays and operation

9.1. LED status displays

The device features three status LEDs on the top of the housing and four status LEDs at the network connections.

The LED displays have different meanings

- during device start-up and
- during operation.

9.1.1. LED status display during device start-up

After switching on the power supply (DC 24 V at the yellow-white connection terminal) or after power is restored, the device displays the status with the following combinations of LEDs:

“RUN/DIAG” LED (green)	“KNX” LED (yellow)	Meaning
off	off	Error: No power supply. Please check connections and power supply.
off	on	Device is starting up
flashes slowly	on	The device is completely powered up but not yet parametrised. A ETS download is necessary.
flashes quickly	off	Error: Please contact support. The firmware cannot be started
alternating slow flashing of LEDs		Error: Please contact support. The newly loaded firmware cannot be started. The system is trying to activate the previous firmware (invalid firmware).

9.1.2. LED status display during operation

Once the device has started up, the meaning of the LEDs is as follows:

“RUN/DIAG” LED (green)	Meaning
on	Normal operation: Remote access is generally allowed and the device connects to the portal server, but no remote access is currently active.
off	Device in the starting process or out of operation. Wait until the starting process has completed or check the power supply.
flashes slowly at 2 s intervals	Note: No remote access allowed. The device does not connect to the Gira Device portal; remote access is technically impossible.
flashes slowly three times at 2 s intervals	Note: Remote access is allowed for at least one group and there is at least one active connection. Remote access is therefore in use.

“KNX” LED (yellow)	Meaning
on	Normal operation: KNX connection is established; no KNX telegram traffic.
flashes quickly	Normal operation: KNX connection is established; KNX telegram traffic.
off	Error: Connection to KNX is interrupted. Check the bus connection.

9.2. Factory reset

Following a factory reset, the device behaves as it did on delivery. The device is not configured. This can be seen after the device starts up by the slowly flashing green LED (5).

The following physical KNX address is factory preset:15.15.255

9.2.1. Factory reset using the Gira Project Assistant

You can carry out a factory reset using the Gira Project Assistant as follows:

- Start the Gira Project Assistant and click the "Action Center" tile.
- The view that opens lists all the devices found on your network.
- Select the Gira S1 that you want to reset to the factory settings.
- Click the gear symbol in the selected line and select the "Factory reset" entry in the menu that opens.
- In the dialog that opens, enter the device password of the Gira S1. You can find the password on a sticker on the device.
- The factory reset is carried out.

9.2.2. Factory reset using the programming button on the device

You can carry out a factory reset on the device via a sequence during start-up:

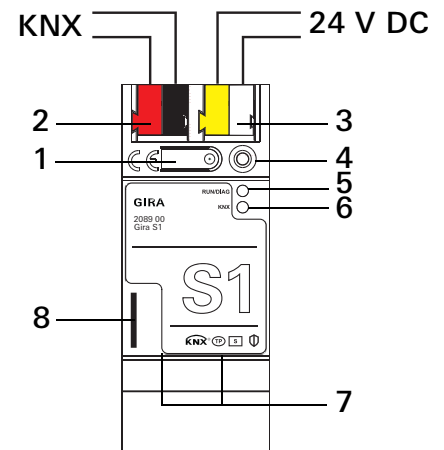
- Make sure that the device is switched off (pull out the white-yellow connection terminal).
- Press and hold the programming button (1) and switch on the device (plug in the white-yellow connection terminal).
- Press and hold the programming button until the programming LED (4), the operation indication 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 operation indication LED (5) and the KNX LED (6) flash quickly simultaneously.
- The factory reset is carried out.
- Release the programming button.
- The device does not need to be restarted following a factory reset.

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

9.2.3. Factory reset using the device's diagnostic page

You can also trigger the factory reset using the device's diagnostic page.

- Call up the device's diagnostic page:
To do so, open the Windows Explorer and click "Network".
The Gira S1 is displayed in the "Other Devices" area.
Double-click the Gira S1 symbol.
Alternatively, you can enter the IP address of the device in your browser.
- On the website that opens, enter the registration ID of the Gira S1 as the password. You can find the registration ID on a sticker on the device.
- Click "Factory reset" in the menu bar at the top.
- Confirm the security check.
- The next page displays the factory reset being carried out. As soon as it has finished, the start page is reloaded.



9.3. Firmware update of the device

9.3.1. Firmware update using the Gira Project Assistant

You can carry out a firmware update using the Gira Project Assistant as follows:

- Start the Gira Project Assistant and click the “Action Center” tile.
- The view that opens lists all the devices found on your network.
- Select the Gira S1 that you want to update.
- Click the gear symbol in the selected line and select the “Select firmware” entry in the menu that opens.
- Select the required firmware and click “Start update”.
- In the dialog that opens, enter the device password of the Gira S1.
- The firmware is updated. This may take several minutes. Do not disconnect the device from the network during this time.

9.3.2. Firmware update using the device website

The Gira S1 provides an option for installing firmware updates using the device website. To do so, click “Update firmware” on the device website. The Gira S1 now searches the update server automatically for a newer version and displays the current firmware version as well as the version of any available updates.

If the new firmware is not compatible with the configuration of the previous firmware, a corresponding message is displayed. A distinction is made between the following instances:

1. The new version provides new functionality. The device works with the same range of functions after the update. New functions cannot be used by a newer catalogue entry until after an ETS download.
2. The new version is completely incompatible with the parametrisation of the version currently used. An ETS download is absolutely essential. It is recommended to unload the ETS application program prior to the update and to configure the device with the new catalogue entry after the update.

You can start the update by clicking the “Update firmware” button. If there is any potential incompatibility, you must confirm the update again to ensure that it is compatible.

9.3.3. Local firmware update with no Internet access

In addition to an online update, you can also carry out a local update without Internet access. You can select the firmware file by clicking the “Select file” button and then start the update by clicking the “Update firmware” button. In this case, the user is responsible for ensuring that the update is compatible (see chapter 9.3.4 “Compatibility between ETS catalogue entry and firmware”). It is not possible to downgrade to an older version using this procedure.

9.3.4. Compatibility between ETS catalogue entry and firmware

The version numbers of the ETS catalogue entry and the firmware are structured according to the X.Y schema. The main number X of the respective version indicates whether the catalogue entry and firmware are compatible. This is the case if both main numbers are identical. The second part of the version number, Y, has no relevance for compatibility. It simply indicates updates within the version.

If new firmware has a higher main number, it is not guaranteed that this version is compatible with an old ETS catalogue entry. It is therefore recommended to unload the application program of the device before updating the firmware and to only use the new catalogue entry afterwards.

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

10. Using the Gira Device portal

To use the remote access functions, you must register the Gira S1 in the Gira Device portal.

You can access the Gira Device portal at the following secure address: <https://geraeteportal.gira.de>.

10.1. Start page

On the start page of the Gira Device portal, you must first log in with your user data to obtain corresponding access to configuration settings.

Before using the Gira Device portal for the first time, you must register as a user. To do so, click "Register".

Registration is carried out using the currently common standard of e-mail address verification. Specify your e-mail address during registration. An e-mail will automatically be sent to this e-mail address for verification purposes. It is essential to confirm the link contained in this e-mail. This ensures that login with a different e-mail address is not possible.

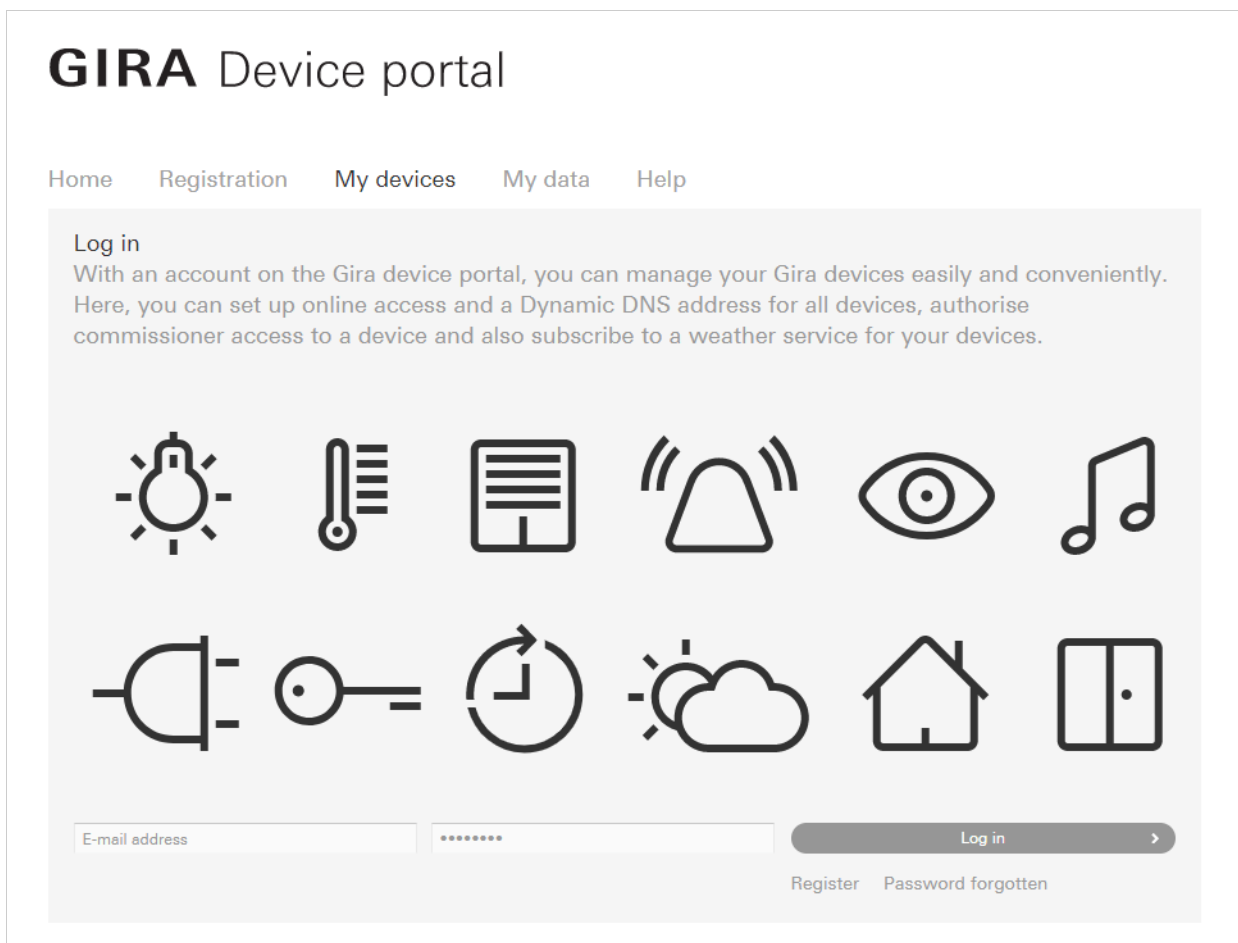


Figure 14: Gira Device portal – Start page

10.2. Device overview

Once you have logged in to the Gira Device portal, you see a list of all the devices linked to your user account. When you log in for the first time, this list is usually empty.

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

1. You add a new Gira S1 to your list of devices by registering the device and thus becoming the owner (see chapter 10.3 “Registering a Gira S1”).
2. Another user gives you access rights to a Gira S1, which is managed by the other user.
3. Another user transfers ownership to you (see chapter 10.9.3 “Transferring device ownership - Handing over the keys”).

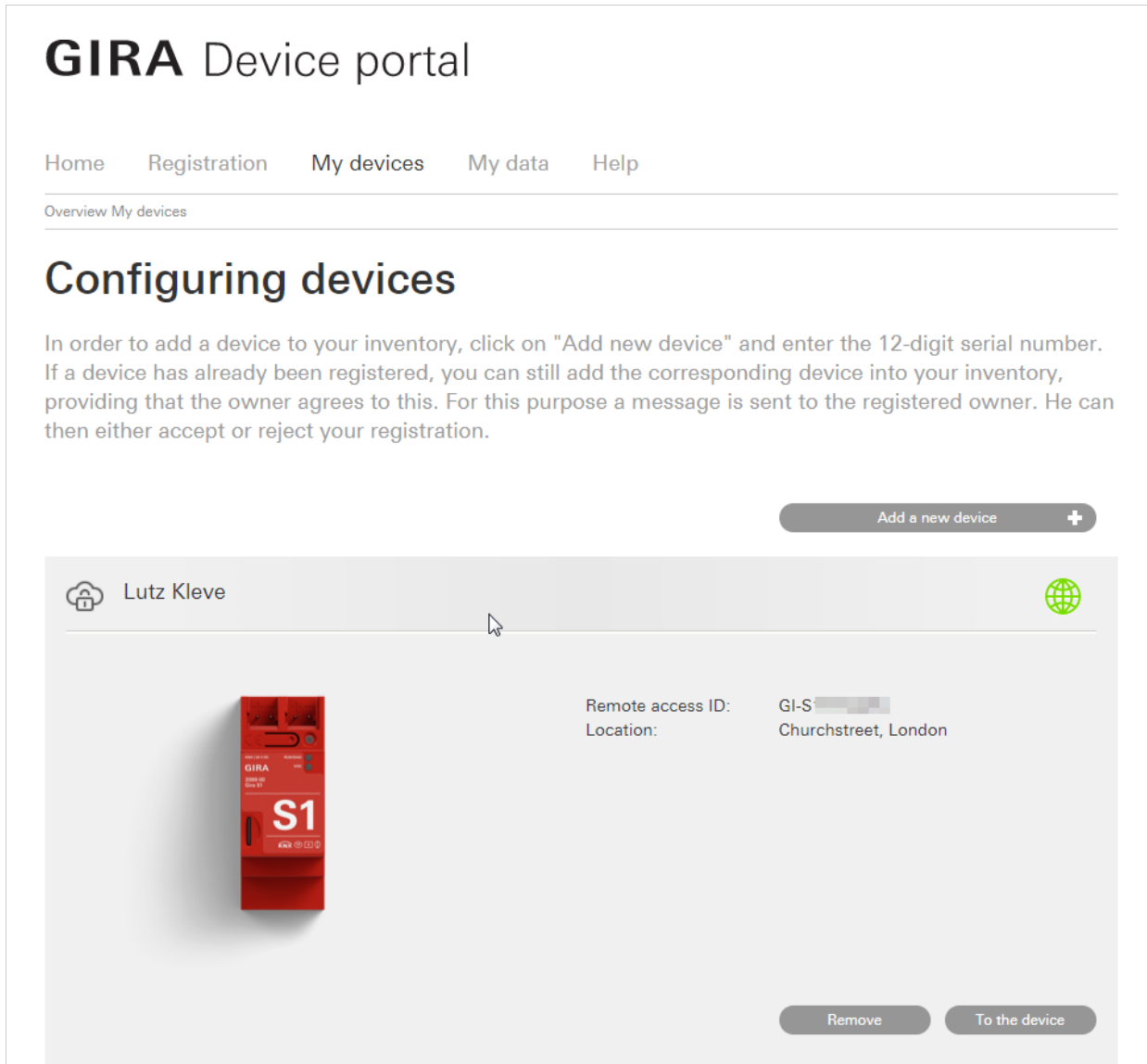


Figure 15: Gira Device portal – Devices belonging to the user currently logged in

10.3. Registering a Gira S1

To register a Gira S1, proceed as follows:

1. Log in to the Gira Device portal with your user ID.
2. Click "Registration" in the device portal.
3. Select the Gira S1 as the device.
4. Enter the registration ID of your device.
You can find the registration ID on a sticker on the device.
5. Give your device a name and enter a location.
6. Click "Next" and accept the terms of use.
7. Once you have successfully registered your Gira S1, the overview page for the Gira S1 opens. The following options are available here:
 - Links (see Chapter 10.4)
 - Notifications (see Chapter 10.5)
 - Device data (see Chapter 10.6)
 - Access to applications (see Chapter 10.7)
 - Receiving notifications (see Chapter 10.8)
 - Portal user (see Chapter 10.9)
 - VPN access (see Chapter 10.10)
 - FAQs (see Chapter 10.11)

10.4. Links

The “Links” view lists the websites of the devices on the network. This page stores the links for devices that have already been used in the past. In addition, by clicking the “Discover Devices” button, you can also search for devices on the remote network. A link is generated automatically for each device found. Most devices, such as printers, DSL routers or IP cameras are recorded in the process. From a technical perspective, the Simple Service Discover Protocol (or SSDP for short) is used here.

Using the “Manually add link” dialog, you can add links to devices that are not found automatically and save them to the list.

GIRA Device portal

Home Registration My devices My data Help

Overview My Devices › Lutz Kleve › Links

Gira S1 Lutz Kleve

Gira S1 is online

Links to the web interfaces of the devices

Here you can access the web interfaces of the devices in the network, e.g. to view log information. For security, the password must be entered again from the Gira device portal.

Description	URL/Address	Protocol	Options
KNX/IP-Router (192.168.137.10...	http://192.168.137.10:8080/discovery/presentation	HTTP	Edit Delete
Gira S1 (192.168.137.167...	http://192.168.137.167	HTTP	Edit Delete
Gira X1 (192.168.137.189...	https://192.168.137.189:4433/discovery/presenta...	HTTP	Edit Delete

Figure 16: Gira Device portal – Access to HTTP websites

10.5. Notifications

The “Notifications” area displays all messages for a Gira S1 sorted in chronological order. You can open any attachments, such as camera images, directly using a link.

You can also forward these messages according to configurable rules (see chapter 10.8 “Configuring notifications”).

The screenshot shows the GIRA Device portal interface. At the top, there is a navigation menu with links for Home, Registration, My devices, My data, and Help. Below the navigation, a breadcrumb trail reads 'Overview My Devices > Lutz Kleve > Notifications'. The main heading is 'Gira S1 Lutz Kleve'. To the right of the heading is a red Gira S1 device. Below the heading, there is a green globe icon and the text 'Gira S1 is online'. A notification icon is shown below, followed by the heading 'Notifications' and the text 'Here you can see all messages that the device generates and receives.' A yellow hint box contains a lightbulb icon and the text: 'Hint: In the [Message Forwarding](#) section, you can specify which system messages are to be generated.' Below the hint, there are two input fields for 'From (mm/dd/yyyy)' and 'To (mm/dd/yyyy)', and a 'Filter' button. At the bottom, there is a table with the following data:

Created	Category	Subject	Content	Severity	Options
02/22/2018, 12:31:46 (Berlin)	SDA	SDA Connector GI-S1 [redacted] is online		⚡ System	🗑️ Delete
02/22/2018, 12:31:31 (Berlin)	SDA	SDA Connector GI-S1 [redacted] is offline		⚡ System	🗑️ Delete

Figure 17: Gira Device portal – Notifications

10.6. Device data

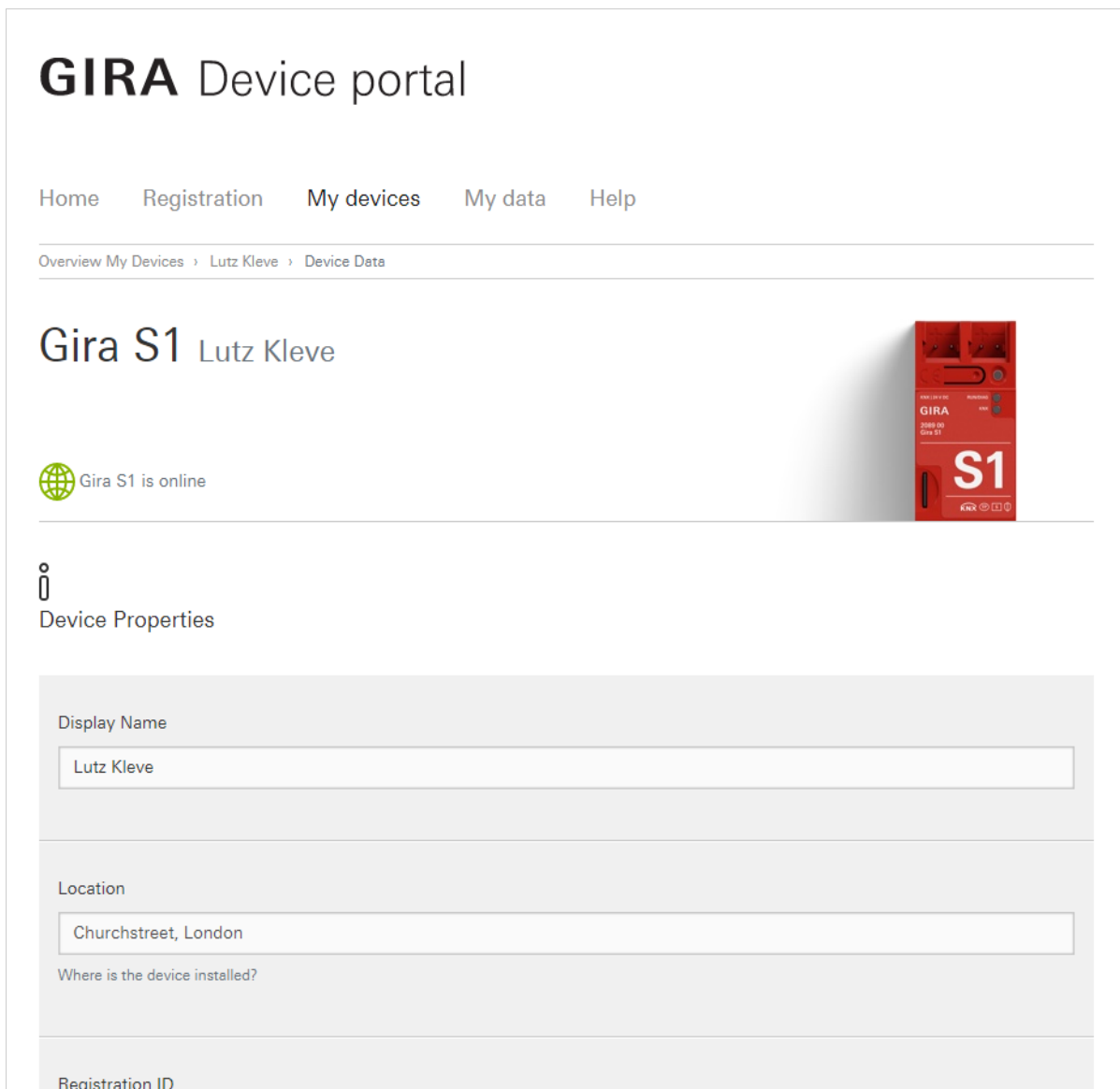
This page displays detailed information about the Gira S1. Using the “Display” button, you can view the complete registration ID, which you can then copy to the clipboard using the “Copy” button.

A text field appears in the “Location” line, which can be assigned by the user as desired. The location is a property on the Gira S1 and is therefore the same for all users. The description can be entered by any user linked to the Gira S1. This enables the installer, for example, to specify the address as the location after handing over the keys, while the home owner enters “At home” as the location.

Using “Delete device from portal”, you can delete the Gira S1 from the device portal. It only makes sense to use this function if the Gira S1 is sold, as all user authorisations and similar are deleted permanently.

The users for this device are also displayed. By clicking the “User administration” button, the “Portal user administration” page opens on which you can add or delete users, for example.

The “Data consumption” area displays information on the current connection status of the Gira S1. The time specifications are displayed according to the time zone settings of your user. In addition, the volume of data consumed until now is displayed for the current month and for the previous month. For information on the volume of data available and the terms of use, see chapter 16 “License agreement”.



The screenshot shows the GIRA Device portal interface. At the top, there is a navigation menu with links for Home, Registration, My devices, My data, and Help. Below the navigation, a breadcrumb trail reads "Overview My Devices > Lutz Kleve > Device Data". The main heading is "Gira S1 Lutz Kleve". To the right of the heading is a red Gira S1 device. Below the heading, there is a green globe icon and the text "Gira S1 is online". Underneath, there is an information icon and the text "Device Properties". The device properties are displayed in a light gray box with the following fields:

- Display Name: Lutz Kleve
- Location: Churchstreet, London
Where is the device installed?
- Registration ID: (partially visible)

Figure 18: Gira Device portal – Device data

10.7. Access to applications

Software access, such as visualisations, is controlled using activation codes. Each user can create any number of codes on each Gira S1 to which he/she has access, e.g. for visualisation.

For every activation code generated, a text field is available which describes the use of the code. You can delete the activation codes at any time (e.g. when a smartphone is lost). The same activation code is never generated twice, which means that a code which is lost as a result of deletion can never be recovered or reused.

To create a new activation code, click "Create new app access".

The following actions are available for created activation codes:

- Copy to the clipboard
- Delete the activation code

Home Registration My devices My data Help

Overview My Devices › S1 v2 › Remote Access

Gira S1 S1 v2

Gira S1 is offline

Remote access

Here you can set up accesses for apps that are allowed to control home automation. It will u. a. supports the following apps: Gira X1 app, Gira Project Assistant (GPA) and HomeServer app (iOS).

The rights of the access data created here are identical to the rights of the creator. If, for example, an installer creates access data, every app that uses this access data is identified by the Gira S1 as an 'installer' and may be rejected. Therefore, check which user group you belong to before creating a remote access. Remote accesses that are to be used by residents must also be created by a resident. If there is not yet a person in the 'Resident' user group, you can create one using the 'Add User' button in the Portal Users area.

1. Check whether you belong to the same user group as the users of the remote access to be created.
2. Create a new remote access.
3. Enter the created access data in the desired app(s).

Remote Access ID: GI- [redacted] [Copy ID](#)

Name	Activation Code	Options
Smart Home App	Activation Code: wr29-bsy3 Copy code Activation perform valid until: 02/16/2022, 12:40:23 (Europe/Berlin)	Edit Delete

Figure 19: Gira Device portal – Activation codes

Then enter the access data created in the required application.

10.7.1. Entering access data in the Gira Project Assistant (GPA)

1. Open the project in the GPA.
 2. The "Remote access" option must be enabled in the project scope.
 3. Click the "Remote access" tile in the project.
 4. Select the "Remote access via Gira S1" option in the view that opens.
 5. Click the "Configure remote access" button.
 6. Enter the remote access ID and the activation code and click "Connect".
-

Note

The connection provided via the Gira Project Assistant is available to all participants on the same network as the computer with the Gira Project Assistant. Therefore please do not use this function on public networks.

10.7.2. Entering access data in the Gira Smart Home app

1. Open the Gira Smart Home app on your smartphone.
2. Open the system menu in the app by tapping the gear symbol in the navigation bar.
3. Tap the "System" button in the system menu.
4. Tap "Connection to Gira device".
5. Tap "Configure remote access".
6. Activate remote access by moving the slider switch to the right.
7. Enter the remote access ID and the activation code and click "OK".

10.7.3. Entering access data in the Gira HomeServer app

1. Open the Gira HomeServer app on your smartphone.
2. Create a new profile.
3. Select the "Profile with remote access module" option in the dialog that opens.
4. Enter the remote access ID and the activation code in addition to the other data required for the profile, and click "Save".

10.8. Configuring notifications

In this area you can specify which notifications are to be generated and create forwarding rules.

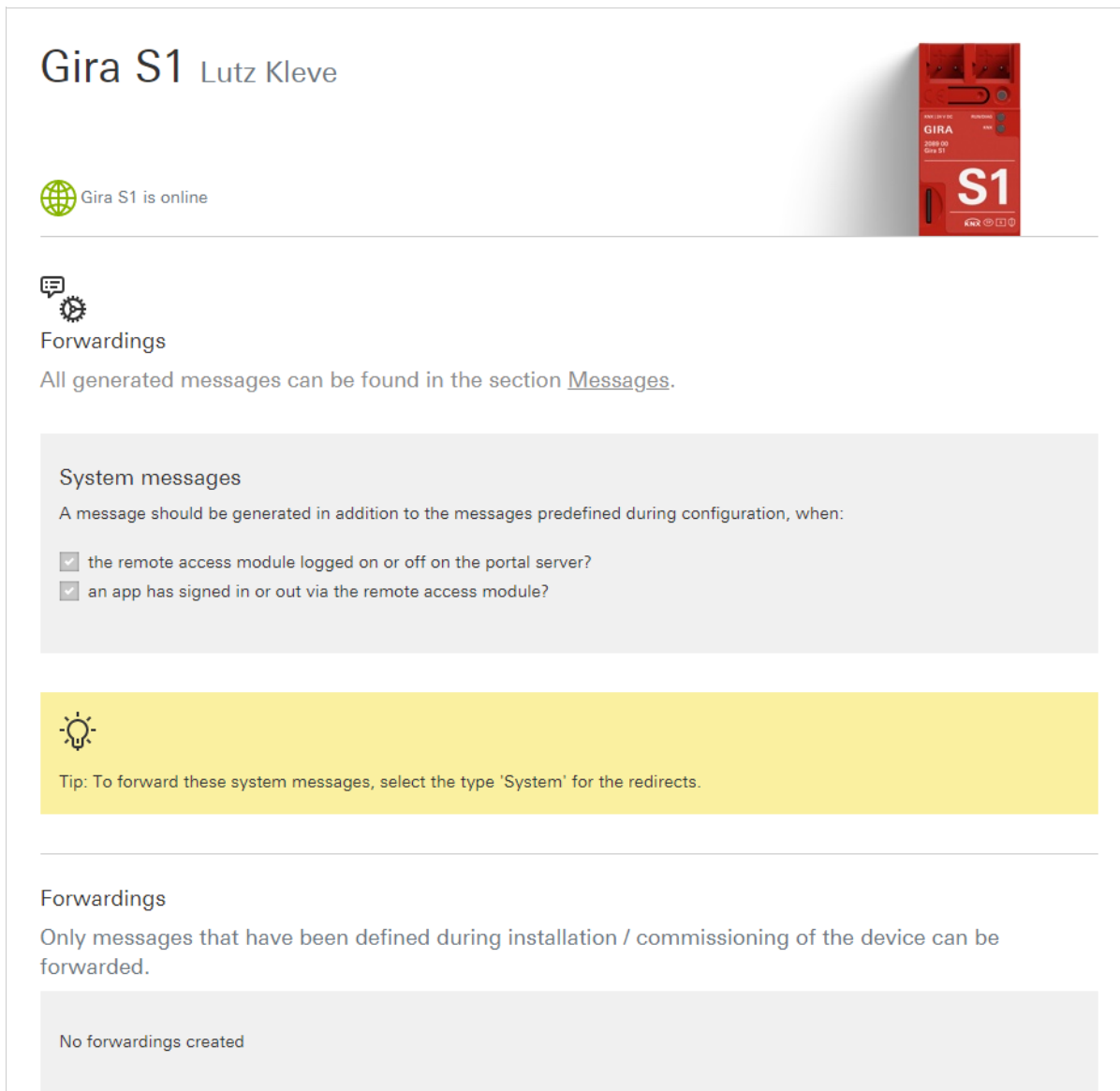


Figure 20: Gira Device portal – Receiving notifications

10.8.1. System messages

You can record system events such as the logging in/logging out of a Gira S1 to/from the portal and the access to the remote network via an app.

10.8.2. Notifications via KNX

The purpose of notifications is to save information from the installation, e.g. about KNX group objects, on the portal in a message database. 50 KNX communication objects are available for receiving values from the KNX and generating messages from them.

The following data types are supported:

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

In addition to selecting the data type, you can specify filters, e.g. limits or value ranges, in which messages are to be created.

Suppress notifications: If you don't wish to be notified of every change, you can specify a threshold value (as an absolute value). Changes will only then be reported once this threshold value is exceeded.

The two text properties, "Subject" and "Text", may comprise static texts in which the value received from the KNX can be used for each placeholder. In addition, you can specify a web address for loading an attachment from a web server (e.g. IP camera) and attaching it to a message.

You can find the actual descriptions of this function in the parameter dialog in the ETS.



Note

Es können maximal 120 Benachrichtigungen in zwei Minuten und 1000 Benachrichtigungen innerhalb von 24 Stunden versendet werden. Bei Überschreitung einer dieser Grenzen wird der Nachrichtenversand gesperrt. Eine Benachrichtigung mit dem Titel „Drop notification“ und dem Inhalt „Dropped excess notification(s)“ wird versendet. Die Sperre wird aufgehoben, sobald die Nachrichtengrenzen unterschritten werden.

10.8.3. Forwarding

Notifications are first displayed in the “Notifications” view of the device portal only. As an administrator, you can specify forwarding rules for notifications.

When notifications are created, they can be forwarded in different ways:

- E-mail (default is the user ID of the portal; multiple addresses can be specified)
- SMS (uses sms77.de or MessageBird as the provider; multiple addresses can be specified)
- Text-to-speech service (telephone voice call), which reads the notification aloud; available in many different languages (uses sms77.de or MessageBird as the provider)
- IFTTT (If-this-then-that, uses IFTTT.com, for experienced users only)



Note

To use the SMS, text-to-speech or IFTTT functions, which are based on the services of sms77.de, Messagebird.com or IFTTT, you must set up a separate account at sms77.de, Messagebird.com or ifttt.com. The corresponding access data must be stored in the “External Services” menu item in the “My data” view.

Each forwarding rule makes it possible to select and forward notifications according to their severity and/or category (text filter; if it contains at least one word, the filter condition is fulfilled). You can configure any number of forwarding rules, of which all the active ones can be evaluated upon receipt of a notification. The deactivation option enables you to create rules that are not always required, e.g. only when you are on holiday. Example: You want all notifications with the severity “System” to be forwarded to you via e-mail (including e.g. the online/offline notifications). For this purpose, proceed as follows:

- Click “Create new forwarding”.
- Deactivate all severity levels except “System”.
- Activate the “Forwarding via e-mail” option. Enter the e-mail address for receiving forwarded messages.
- Save the forwarding rule. It is activated automatically.



Note

The notifications generated by the system, e.g., for online/offline status of the Gira S1, are always generated with the “System” severity and “Remote access” category. All severities up to “System” and any categories can be used when notifications are used via KNX objects.

10.9. Portal user administration

The Gira Device portal enables differentiated configuration of access rights based on users for each Gira S1. You can define the following for each user:

- **Portal role:** The portal role exclusively defines the configuration rights of the Gira S1 in the Gira Device portal. Possible options here include "owner", "administrator" and "user", whereby the owner is an administrator with a special role, which is why only we only refer to administrators and users in the following.
- **Access group:** You can use the access group to control access to the remote network. Possible options here include "residents" and "installer", whereby a user can be assigned to neither group or to both groups.

Besides adding new users to a Gira S1, you can also further restrict user rights or delete the connection of a Gira S1 to a user.

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

Home Registration **My devices** My data Help

Overview My Devices > S1 v2 > Portal Users

Gira S1 S1 v2

Gira S1 is offline

Portal user administration

Here you can give other persons access to the portal functions of the device and define new device owners.

Lightbulb icon: The owner of the Gira S1 should be assigned the owner's portal role after commissioning. This has the following reasons, among others:

- An owner has full control over the device and over the users.
- In the event of any misuse, e.g. violation of data protection or personal rights through camera use, the owner is liable.
- If the property is sold, only the owner can transfer ownership of the Gira S1.

Name/Email	Description	Portal Role ⓘ	User Group/s ⓘ	Options
[Redacted]		Administrator	Resident, Installer	Edit Delete

Figure 21: Managing access rights for users

10.9.1. The portal role of a user on a Gira S1

The difference between an administrator and user lies in the rights to make configuration changes on the Gira Device portal. The owner of the device is also automatically the administrator. All administrators can manage all the properties and user rights for the Gira S1 (with the exception of ownership). The user can at most view the properties.



Note

The role of a user is based solely on the configuration options on the Gira Device portal and has nothing to do with the access rights to the remote network via remote access. Only the user groups are used for the latter.

10.9.2. The access group of a user on a Gira S1

Using the access groups, it is possible to grant access to the remote network permanently or even just temporarily based on groups. Using KNX communication objects, residents and installers can be activated or deactivated at any time for both groups.



Note

The access groups of a user are based solely on the rights to access the remote network via remote access, for example, to visit websites or to access the KNX installation using the ETS. If you want to change the configuration options on the Gira Device portal for a user, use portal roles for this purpose.

10.9.3. Transferring device ownership - Handing over the keys

From the moment a Gira S1 is registered in the Gira Device portal, the Gira S1 has an owner. From then onwards, there is only ever one owner.

The owner is the person who is legally responsible for the use of remote access. At the time of the installation or configuration, this is usually the electrician or system integrator. When the keys are handed over to the owner of the installation, ownership is usually transferred.

The owner of a Gira S1 can take away all rights of all other users at any time, including other administrators, whereas no one can deny him or her access.

In the event of misuse of the Gira S1 or remote access within the meaning of the license agreement or other legal regulations (violation of data protection or personal rights by cameras, or similar), the owner is liable in the first instance.

Ownership can be transferred in the Gira Device portal. For this purpose, the "Change owner" button is available on the "Portal user administration" page.

Ownership is transferred using a secure procedure:

1. The current owner clicks the "Change owner" button, enters the e-mail address of the intended new owner and submits the request.
2. The intended new owner receives an e-mail containing a link for accepting the transfer of ownership. For security purposes, the same applies to the current owner.

3. When both the new owner and the current owner have accepted the transfer, both receive a corresponding e-mail and ownership is transferred.

If the request is not confirmed by the new owner or the current owner, no transfer of ownership takes place.



Note

Please note that the previous owner is assigned the “administrator” user role as soon as the transfer of ownership is complete. If this is not desired, you can change this in the “Portal user” view.

10.10. Setting up VPN access

Under "VPN access" administrators can make the following settings:

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

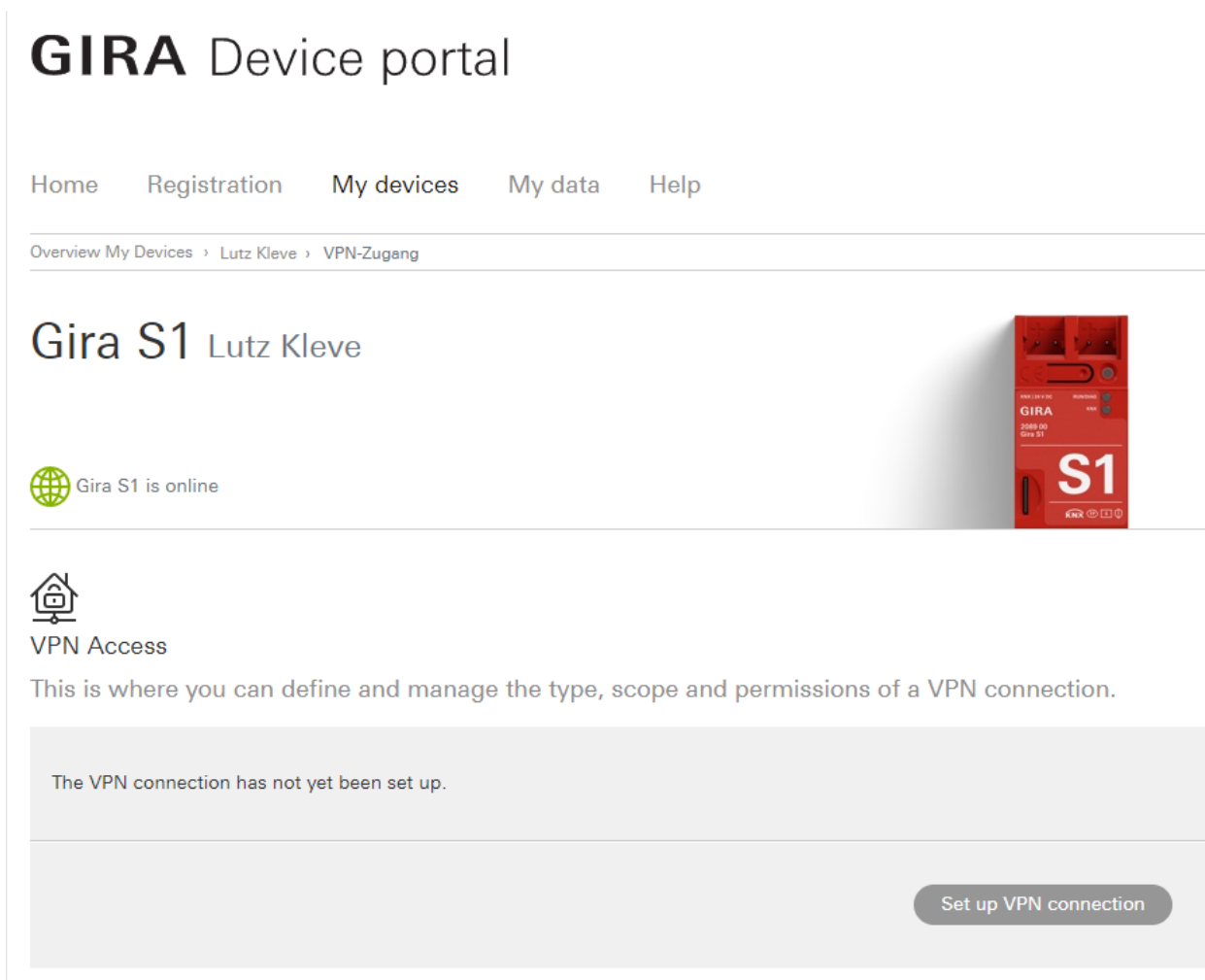


Figure 22: Gira Device Portal - Setting up VPN access

Note

If you change the properties under "VPN access", the current configuration files will be invalid. For each created user, a new configuration file is created, which you have to download and import into the OpenVPN client of the respective user.

10.11. FAQs

The most frequently asked questions about Gira S1 and its settings in the Gira Device Portal are answered in the "FAQs" view.

11. Gira S1 Windows client

The Gira S1 Windows client is an application that is installed on a computer, which can be used to access devices on the remote network securely over the Internet if the HTTP protocol is not used. The Gira S1 Windows client is not required for accessing websites on the remote network using a web browser, see chapter 3.5 “Access to websites on the remote network”.

The most typical use cases for the Gira S1 Windows client include:

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

In addition, the Gira S1 supports the use of many other TCP-based IP protocols such as Microsoft's Remote Desktop Protocol (RDP) for remote access to a Windows computer.

The Gira S1 Windows client is currently available for Microsoft Windows versions 7 and higher. You can find the current version at www.download.gira.de.

11.1. Installation

Start the installation of the Gira S1 Windows client by double-clicking the installation file. During the course of the installation, the following dialog appears:



Figure 23: Installation dialog

The “Add firewall exception” option must remain activated so that the Gira S1 Windows client works without errors.

11.2. Connecting to the Gira Device portal

Upon starting the Gira S1 Windows client, a login dialog appears.

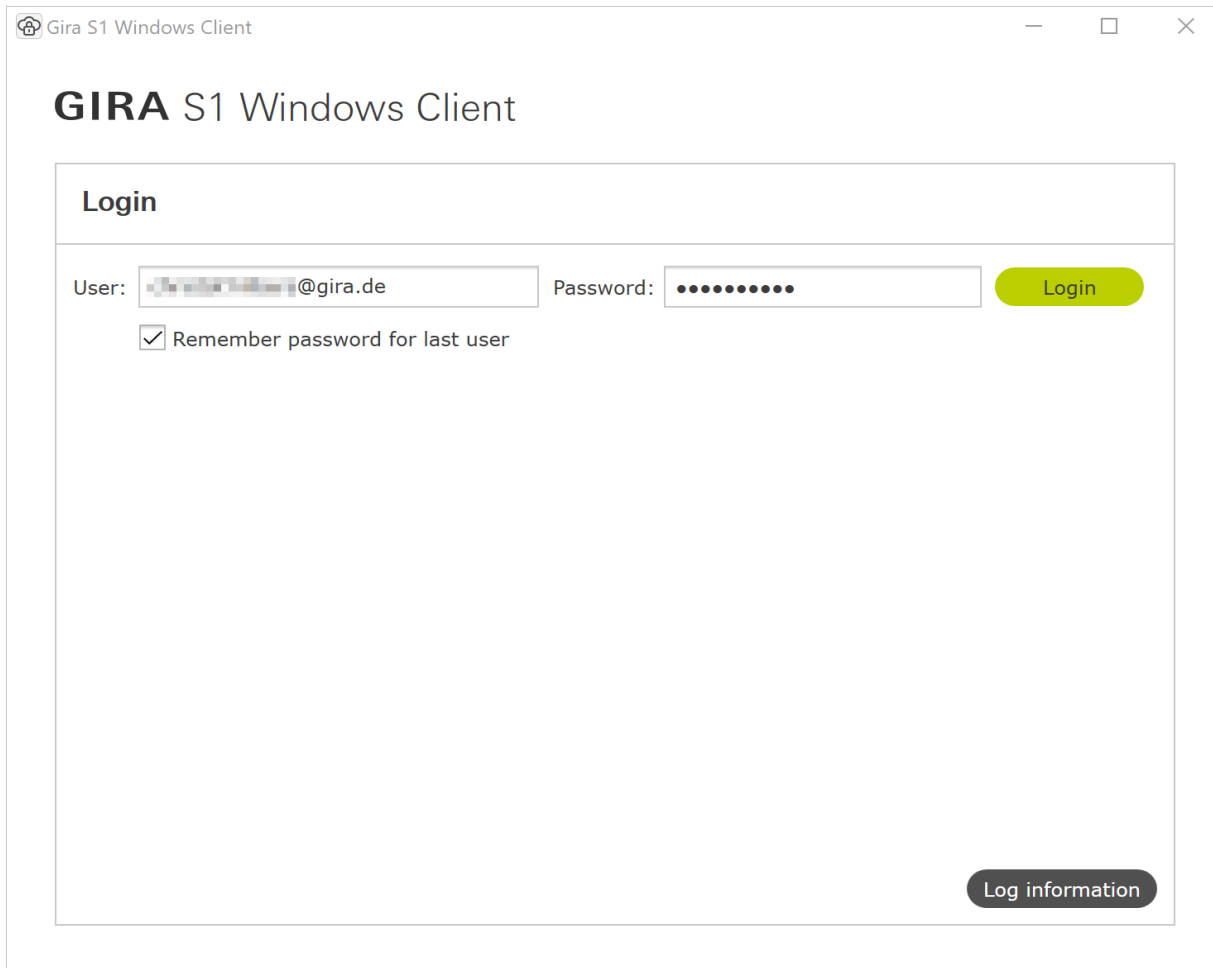


Figure 24: Gira S1 Windows client login

Log in here using the login data from the Gira Device portal. In other words, enter your portal user name (note: this is always an e-mail address) and the associated password, and click “Login”.

Remember password for last user

If you activate this option, the Gira S1 Windows client remembers the password so that you can simply click “Login” the next time you log in to the device portal.

Log information

By clicking the “Log information” button, a window opens in which you can view the log file previously recorded. By clicking “Delete log files when next closing”, all saved log information is deleted when the Gira S1 Windows client closes. If you click “Generate ZIP archive”, the log information is stored in a ZIP folder, which you can then attach to an e-mail to help with support cases, for example. You can activate “Advanced logging” for troubleshooting in the case of problems.

Once you have logged in to the Gira Device portal using the “Login” button, a list of all Gira S1 devices is displayed for which you have access rights.

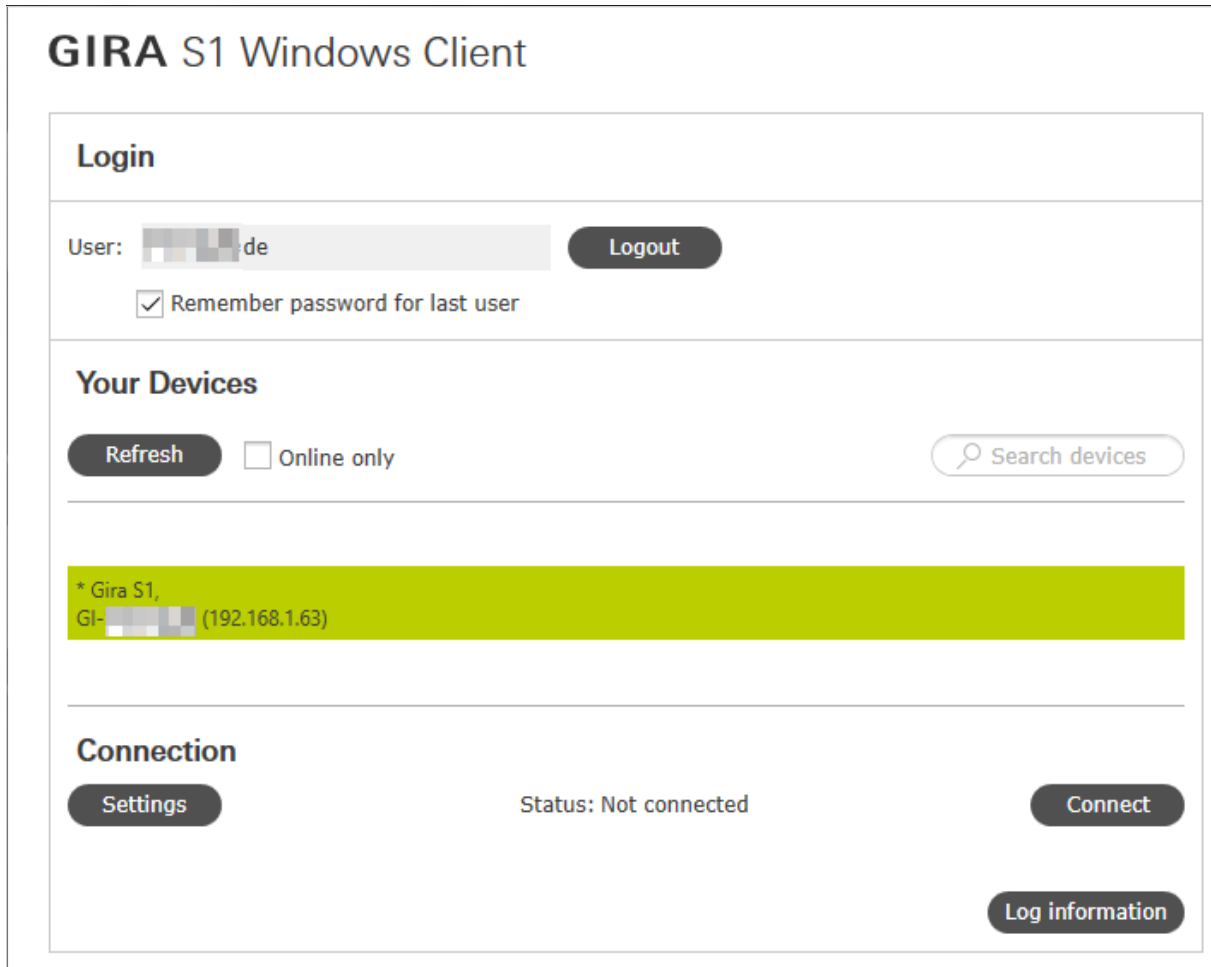


Figure 25: Displaying the available Gira S1 devices

Connecting to the Gira S1

If you select a Gira S1 in the list, you can either click “Connect” to connect to the Gira S1 or click “Configure” to change the configuration of the Gira S1.

If you are using the Gira S1 with this Gira S1 Windows client for the first time, a default configuration is created.

Once you have adapted the configuration on your applications, if applicable (see chapter 11.3 “Configuring the access options of a Gira S1” ff.), you can connect to the Gira S1 using the “Connect” button.

Note

The connection provided via the Gira S1 Windows client is available to all participants on the same network as the computer with the Gira S1 Windows client. Therefore please do not use the Gira S1 Windows client on public networks.

Online only

If you activate the “Online only” option, the list only displays the Gira S1 devices currently connected to the Internet, i.e. devices that are “online”.

11.3. Configuring the access options of a Gira S1

If you are connected to the Gira S1, you can click “Configure” to configure the access options. In addition to HTTP access, for which a Gira S1 Windows client is not required, the standard use of the Gira S1 is to access KNX installations remotely and securely using the KNX/IP protocol. The configuration for this service is therefore always visible and activated by default.

In addition to KNX/IP, the Gira S1 Windows client also offers easy access for secure remote configurations of the Gira HomeServer. Here, you can update a project using the HomeServer Expert or create a bus connection using 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 therefore also the configuration, of access to a Gira HomeServer or additional TCP connections is optional and can be activated or deactivated using the settings for the respective Gira S1 (see figure).

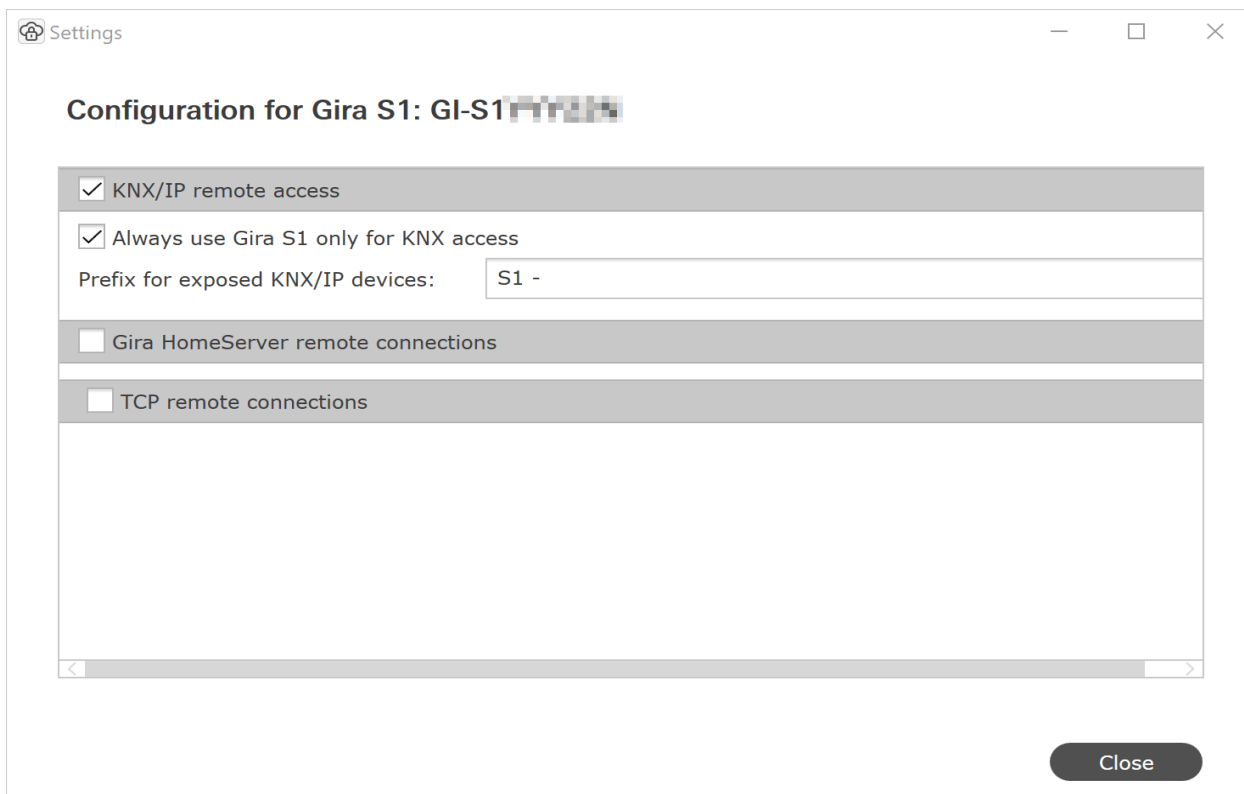


Figure 26: Gira S1 configuration options

Status display after starting the remote access connection

You start the secure connection to the Gira S1 using the “Connect” button. If an error occurs when the connection is being established, a corresponding error message is displayed.

If a connection is established successfully, the configuration options are deactivated, since it is not possible to modify an active connection. Nevertheless, you can click “Configure” to open the configuration dialog while a connection is active. In this case, a button with an information graphic is displayed in the configuration dialog for the three connection types (KNX/IP, Gira HomeServer and TCP). If errors occur with individual connections, e.g. if not a single KNX/IP device is found or a TCP connection could not be established, a button with a warning triangle also appears. The buttons all have tool tips and also display the text in an input field when you press them.

Important note: A frequently-occurring problem is a configuration that uses a local port which is already in use by another application. In this case, please select a different local port.

11.3.1. Accessing a KNX installation via KNX/IP

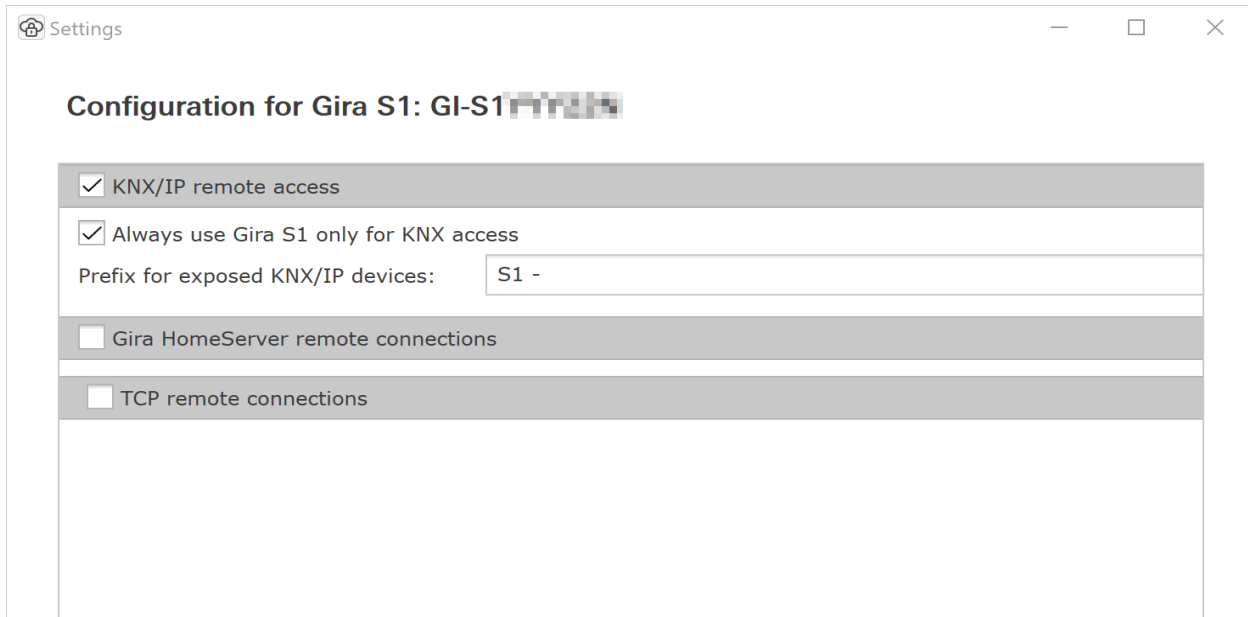


Figure 27: KNX/IP remote access configuration

The configuration for secure KNX/IP remote access comprises three options:

KNX/IP remote access

KNX/IP access can generally be deactivated, if you only need to quickly access a computer via Remote Desktop and do not need KNX/IP, for example.

Always use Gira S1 only for KNX access

If desired, you can also make only the tunnelling server of the Gira S1 accessible via remote access, e.g. because many devices are available on the remote network and you are in a hurry.

Prefix for exposed KNX/IP devices

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 by default so that they appear in the Connection Manager of the ETS. (Observe the note below on the user of ETS4 versions older than ETS4.2). To see at a glance which devices are connected via remote access, you can enter a prefix of your choice up to eight characters in length.

Important note:

When using ETS4 versions older than ETS4.2, problems may occur during automatic detection of the KNX/IP interfaces in the ETS4, which mean that they do not appear. In this case, you must configure the interfaces manually in the ETS4.

To do so, manually create a new connection in the ETS4, assign a name of your choice and copy the corresponding IP address and port from the Gira S1 Windows client to the input fields in the ETS4. The Gira S1 Windows client provides assistance here if a connection is open by offering buttons for copying the corresponding values to the clipboard.

Refer to the figure below for this.

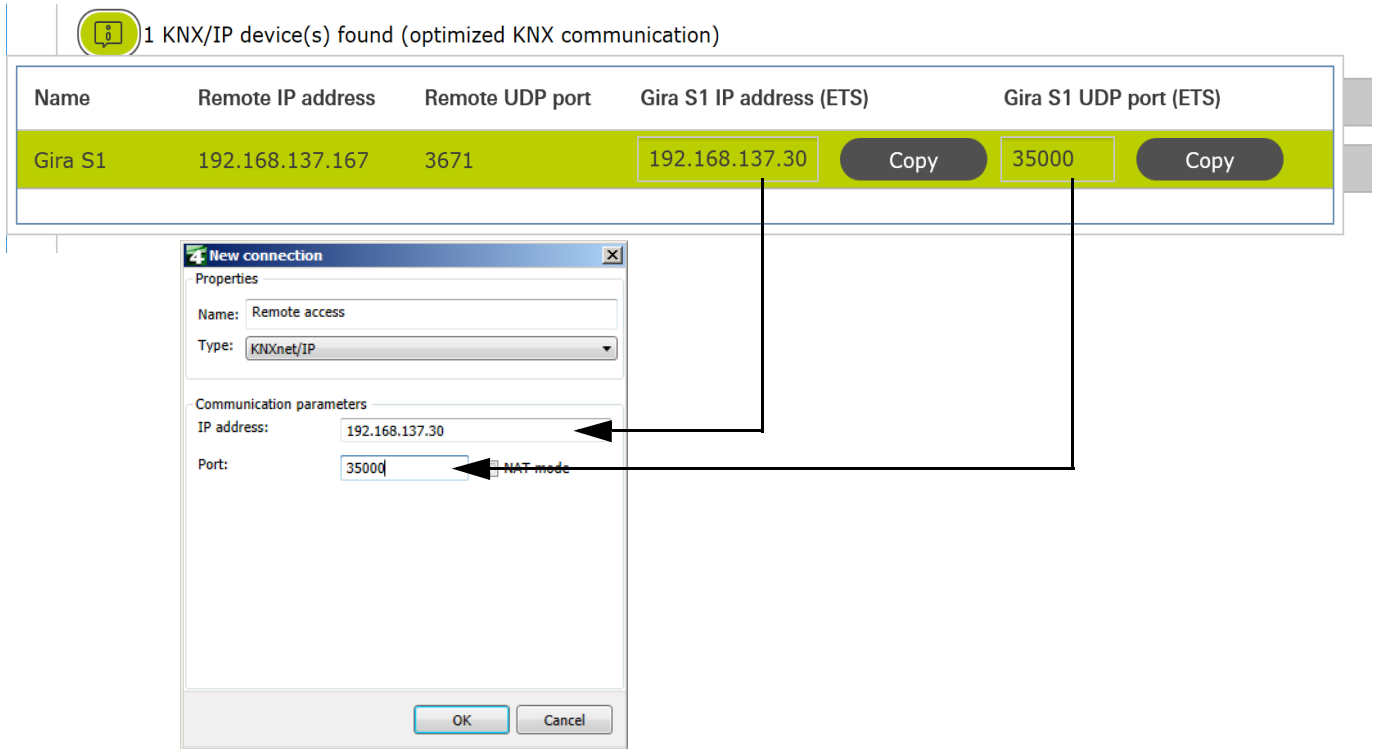


Figure 28: Manual KNX/IP interface configuration for ETS older than ETS4.2.

Note

The Gira S1 Windows client remembers the locally used port (starting with 35000) for each tunnelling server from the remote network so that the connections created manually remain valid later on for a new remote access connection to the same installation. Remote access communication is specially optimised for KNX communication so that it still works reliably even with slow Internet connections.

11.3.2. Configuring the Gira HomeServer remotely and using the Eiblib/IP

The screenshot shows the 'Settings' window for 'Gira S1: GI-S1111111111'. The configuration is organized into sections with expandable/collapsible headers:

- KNX/IP remote access**: This section is currently collapsed.
- Gira HomeServer remote connections**: This section is expanded.
 - Gira HomeServer: IP or DNS name: [Empty text field]
 - Gira Expert: Enable remote access on local port
 - HomeServer Expert port: [443]
 - Local Expert port: [8443]
 - Default values are:
 - 443 for the HomeServer Expert port
 - 8443 for the Local Expert port, as 80 is often already in use
- Eiblib/IP: Enable remote access**: This section is expanded.
 - Eiblib/IP: Enable remote access
 - HomeServer config port: [50000]
 - Local config port: [50000]
 - HomeServer read port: [50001]
 - Local read port: [50001]
 - HomeServer write port: [50002]
 - Local write port: [50002]
 - Default values are:
 - 50000 for the config ports
 - 50001 for the read ports
 - 50002 for the write ports
- TCP remote connections**: This section is currently collapsed.

At the bottom right of the window is a 'Close' button.

Figure 29: Gira HomeServer remote access configuration.

Gira HomeServer IP or DNS name

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

Gira Expert: Enable remote access on local port 8443

Use this option to enable remote access for the HomeServer Expert. We recommend using the standard port 8443. However, any other free port can also be used - although ports smaller than 1000 are not recommended.



Note

Gira HomeServers from version 4.7.0 use port 443 for the configuration; the port is set as the default value.

To load the Gira HomeServer on the remote network with the Expert via remote access, you must select the “Different address” option in the “Transfer project” dialog of the Expert with an active remote access connection; always enter 127.0.0.1 as the IP address, followed by the configuration port (default is 8443).

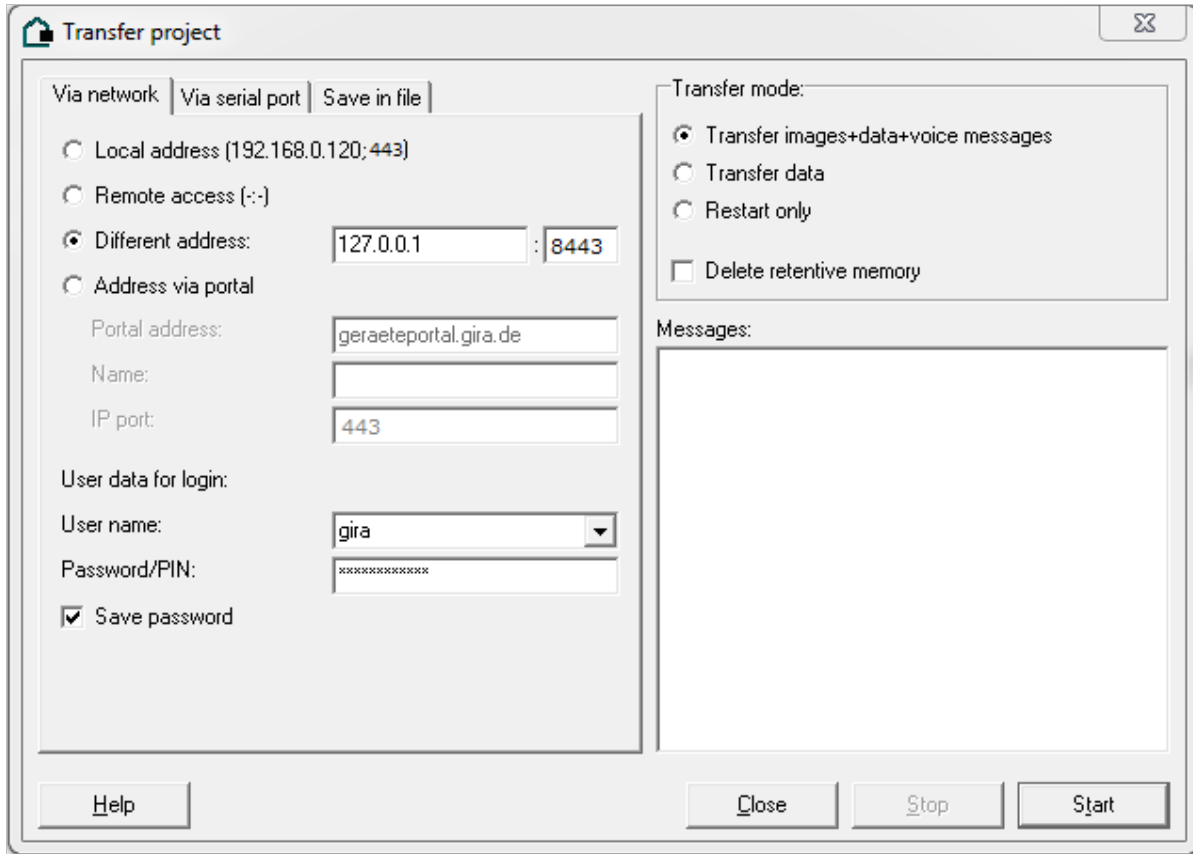


Figure 30: Transferring a project with the Expert via remote access.

Enable Eiblib/IP remote access

The ports 50000, 50001 and 50002, which are usually free on your local computer, are used for the Eiblib/IP protocol by default, which means that you do not generally have to make any changes here. To use Eiblib/IP with the Gira HomeServer, you must create a connection of the “Eiblib/IP” type in the ETS as before. As with the Expert, the server address 127.0.0.1 must always be entered here. The ports can usually retain their default values (50000, 50001 and 50002).

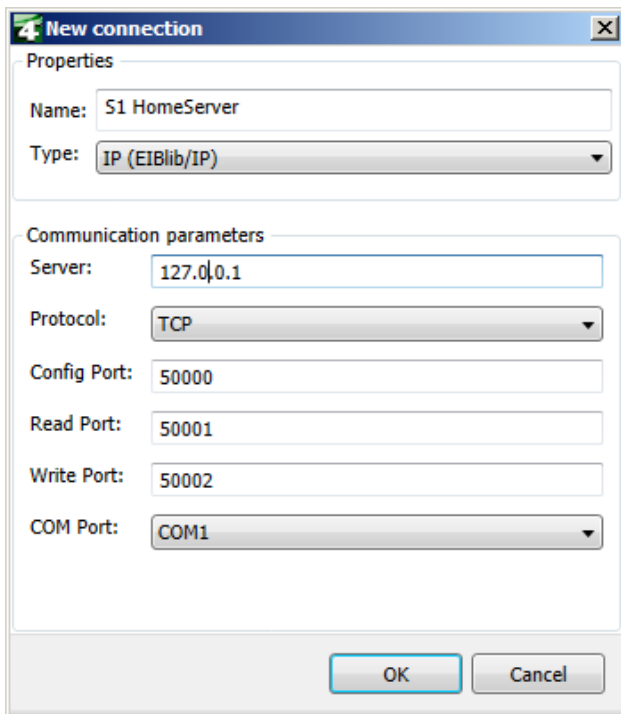


Figure 31: Using the Gira HomeServer with Eiblib/IP via remote access for KNX connection.

11.3.3. Using other TCP protocols via remote access

Using the settings in “TCP remote access connections”, you can use other TCP-based IP protocols via remote access. To do so, click “Add” and enter the corresponding values for the remote access. For example, the Microsoft Remote Desktop Protocol (RDP), which is used by the Microsoft Remote Desktop connection application, is wellknown. Here, too, the port is usually already used locally by the computer, which is why the translation to a port is required, as in the example in the figure below.

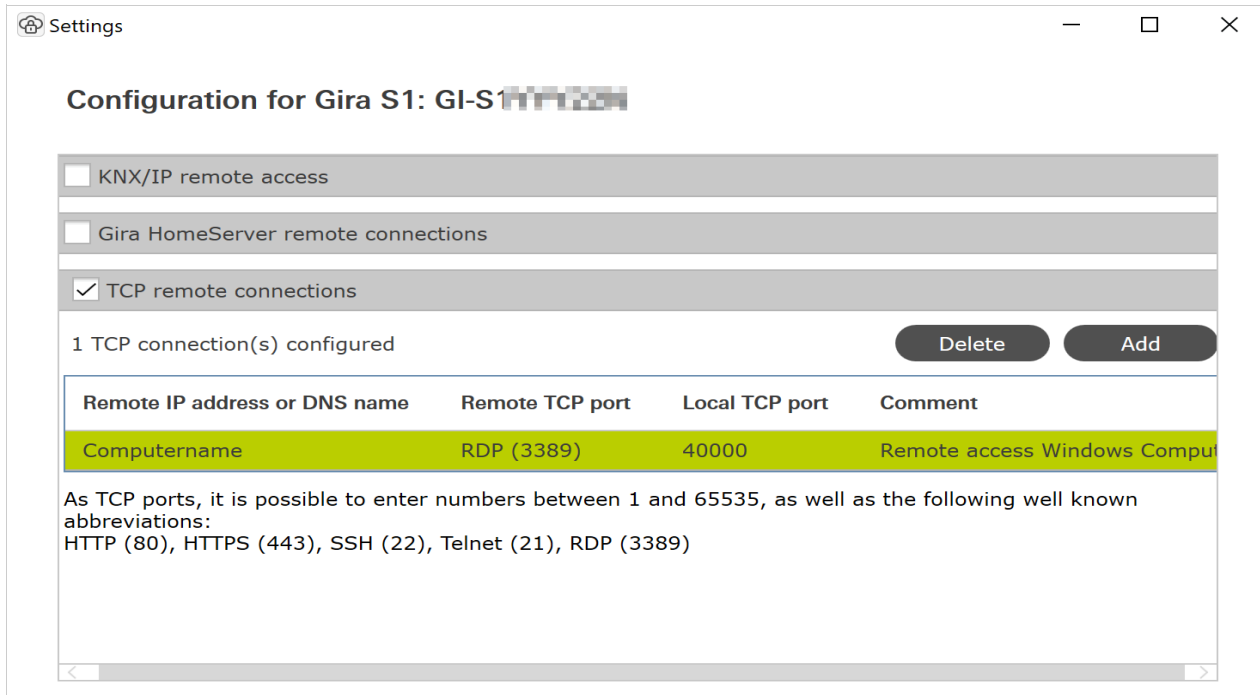


Figure 32: TCP remote access configuration.

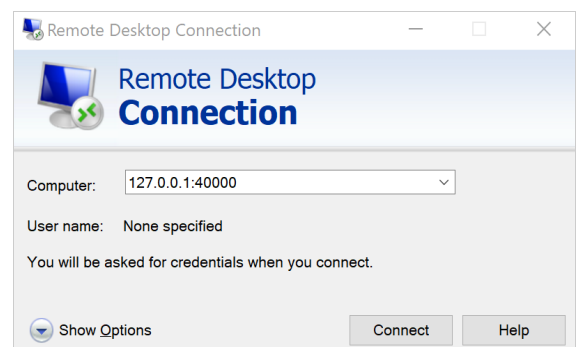
Note: Often, you can no longer use the TCP port which must be addressed on the device on the remote network (in this example, 3389, the default port for RDP) on your computer, for example, because you have installed software on your computer which is already using this port. In this case, you must find another available port. It can help to use ports starting with 40000 here (as in our example).

If you now want to establish a remote desktop connection to the target computer via remote access (in our example, “computername”), you still have to enter the port if it does not correspond to the default port.

In our example, the connection can be established as follows:

Note: It is common syntax for the explicit specification of a port to write the port with a preceding ":" directly after the host name (only required if it is 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.

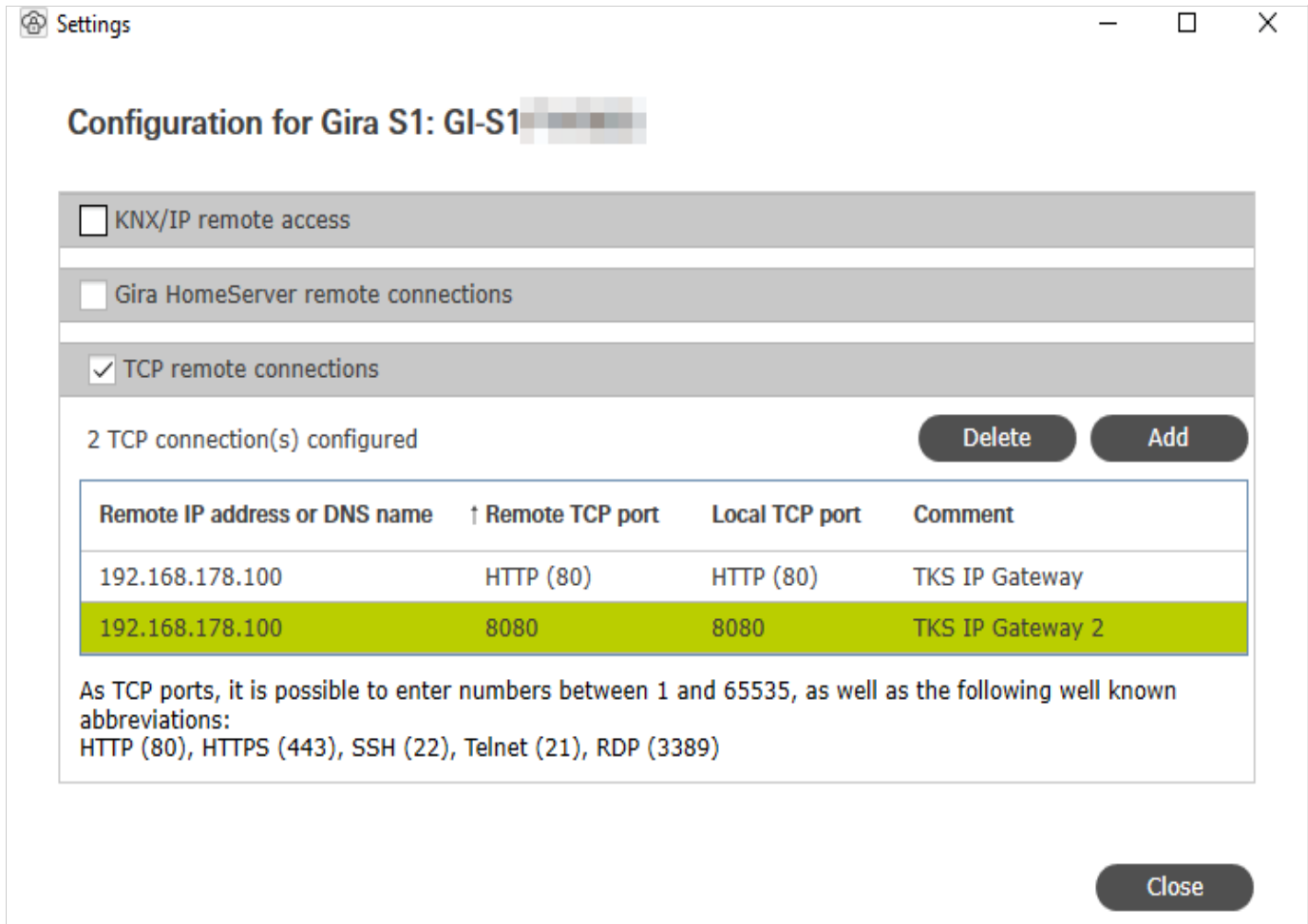


11.3.4. Configuring the Gira DCS-IP gateway

If you want to configure the Gira DCS-IP gateway via remote access, please use the “Activate TCP remote access connections” option.

Create two connections with the two ports, HTTP (80) and 8080. Enter the IP address of the corresponding DCS-IP gateway.

Once a remote access connection to Gira S1 has been established, you can call up the DCS-IP gateway assistant by entering the address `http://localhost:80` into the address line of your browser.



11.4. Ending a remote access connection

After successfully using a connection, you can terminate an active connection using the “Disconnect” button. The connection is also disconnected automatically if the Gira S1 Windows client is closed.

12. Technical data

KNX medium	TP1
Security	KNX Data Secure (X-Mode)
Start-up mode	S mode (ETS)
KNX supply	DC 21...30 V SELV
KNX current consumption	type 2.5 mA
KNX connection	Bus connection terminal
External supply	
Voltage	DC 24...30 V
Power consumption	2 W (at DC24 V)
Connection	Connection terminal
IP communication	Ethernet 10/100 BaseT (10/100 Mbit/s)
IP connection	RJ45 pin jack
Supported protocols	DHCP, AutoIP, TCP/IP, UDP/IP (Core, Routing, Tunnelling, Device Management), ARP, ICMP, IGMP
Ambient temperature	0 °C to +45 °C
Storage temperature	-25 °C to +70 °C
Installation width	36 mm (2 MW)
microSD card	up to 32 GB (SDHC)

12.1. Accessories

Additional power supply
Order No.: 1296 00
KNX power supply 320 mA
Order No.: 1086 00

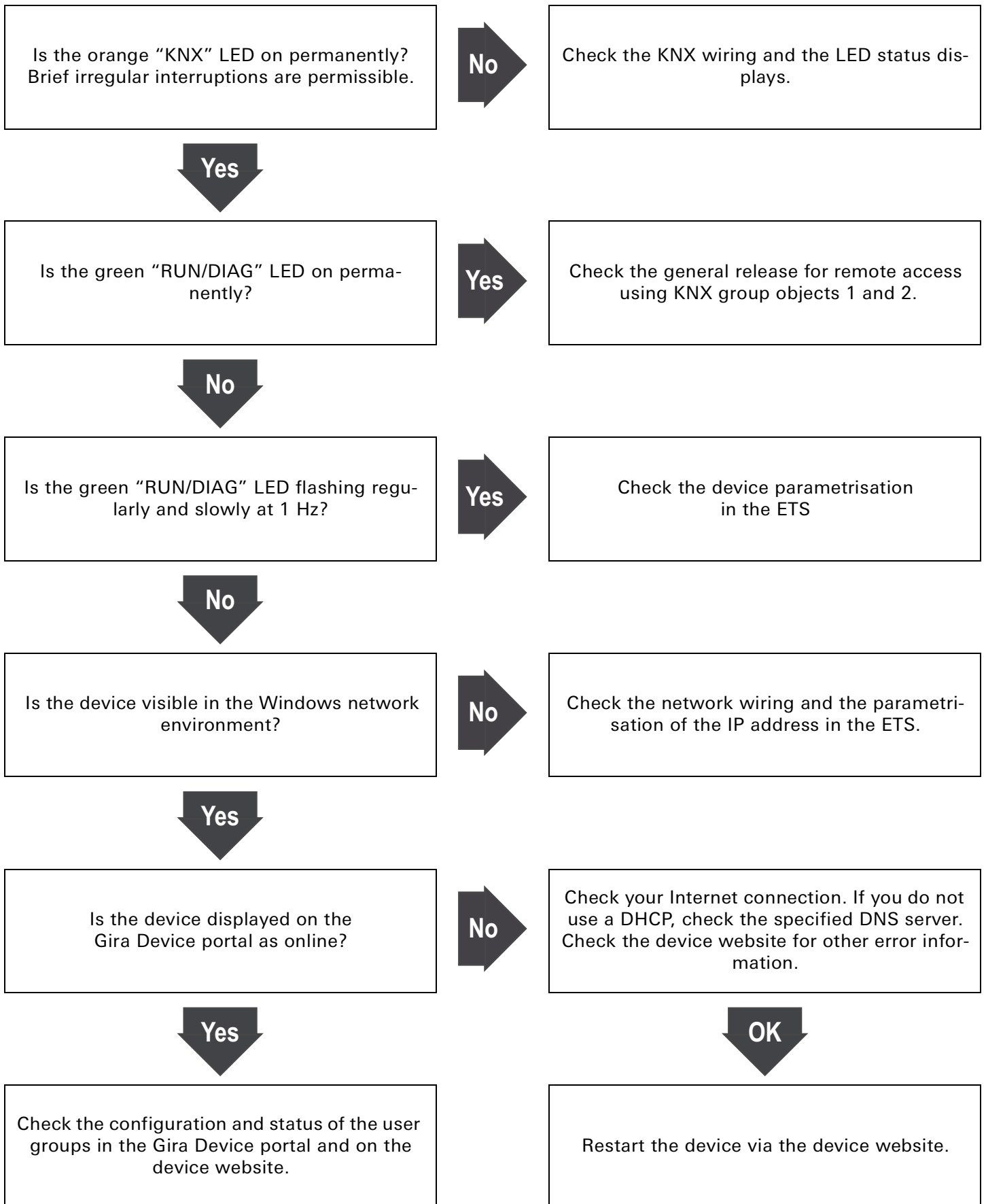
13. Frequently asked questions (FAQs)

- How do I find the IP address of my Gira S1?
Open Windows Explorer. The Gira S1 is displayed together with its IP address in the “Network” - “Other Devices” area.
- How much Internet data traffic is generated if the Gira S1 is connected to the portal?
To maintain the connection, approx. 400 bytes of data traffic/minute are generated. This corresponds to approx. 560kB/day or 16.5 MB/month. This data volume is not charged as user data by the Gira Device portal as laid down within the limitation of the data volume in the license agreement for the Gira S1.
- Which communication channel does the Gira S1 use for the Gira Device portal?
The Gira S1 communicates with the Gira Device portal exclusively via an HTTPS connection using the default port 443. All data is exchanged in both directions via this one connection, which means that it is not generally necessary to configure the firewall.
- Why do cookies need to be activated in order to use remote access?
Cookies are used to safeguard access. We use cookies exclusively to secure the connection. There is no tracking or exchange of data with third parties.
- Which protocols can be used to access devices in the remote network?
Without installing the Gira S1 Windows client, you can access devices in the remote network that can be reached via HTTP. This includes nearly all devices with a browser-based user interface. These devices are found automatically via UPnP.
Besides KNX/IP and the Gira HomeServer, all TCP-based protocols, e.g. Telnet, ssh, HTTPS, Windows Remote Desktop, ftp, etc., work with the Gira S1 Windows client.
- Why do the relevant group objects not immediately report that there is no longer a connection after closing the browser when using the HTTP access?
For a detailed description on this, see see chapter 8.6 “Object table”.
- In my ETS4, the KNX/IP interfaces that are published via the Gira S1 Windows client do not appear automatically. Why is that?
With ETS4 versions older than ETS4.2, this can lead to problems (see chapter 11.3.1 “Accessing a KNX installation via KNX/IP”).
- Can the three KNX/IP ETS interfaces be used for download, group and bus monitor?
Yes, the interfaces support all download operations as well as the group and bus monitor.
- Can the Gira S1 device website also be accessed securely via the Internet?
Yes, the status page for the device can be accessed securely via the Internet.
- When downloading the application program, why does ETS report the error that data cannot be written to a protected area?
Please make sure that your ETS version is up to date. Gira S1 requires ETS from version 4.2 or 5.0.2, or higher.
Also check whether the versions of the application program and the Gira S1 firmware match.
- Is the portal server really necessary?
Yes, only one server can provide remote access that almost always works and does not require extensive configuration.
- What data does the server store?
The server only stores data that is absolutely necessary for providing the service. Besides data entered during login and data that is visible via the user interface, this includes information on the quantity and time of the data volume transferred.
The server never stores any user data!

- Is operation of the servers guaranteed within Germany?
Yes. Operation of our portal and the data servers (for an even distribution of data traffic) is guaranteed in Germany. To ensure high availability, the servers are leased from reputable hosting providers as root servers to prevent unauthorised access to the servers and data by third parties. Due to the fact that server operation is in Germany, the German Data Protection Act applies, which is much more restrictive compared to other countries.
- Why does the license exclude continuous operation (24x7) and include a data volume restriction?
As all data must be routed through the portal server (see above), continuous operation, especially video streaming, for example, is extremely performance-intensive. To guarantee a generally high level of performance, certain restrictions are therefore necessary.
If you have use cases that exceed these limits, please get in touch with us. License models with an extended scope are not excluded for the future.
- When I access a website remotely, it does not work correctly, even though it works locally. Why is that?
Not all websites can be loaded from the remote network via remote access. More complex pages (e.g. with Flash or intensive Javascript use) in particular may not work.
- I have carried out a partial download using ETS4 and now the group communication does not work. Why?
There is an implementation error in ETS4 concerning the partial download, which has an impact on our product. Please never download the device as a partial download using ETS4. Instead, always carry out an application download. This problem does not exist in ETS5.
- After unloading the application on the device website of the Gira S1, why do I still see the previously configured physical address and IP address?
After unloading an application, the device website is not currently updated until the device has been restarted.

14. Troubleshooting and support

The following fault tree is intended to solve the most frequent problems.



15. Gira S1 device website

All settings and parameters can be seen at a glance on the Gira S1's device website. You can also change the network settings here, save a log file, which you can pass on to the Gira hotline in the event of a fault or servicing, trigger a restart and a factory reset as well as perform a firmware update. The device website is displayed in the Internet browser.

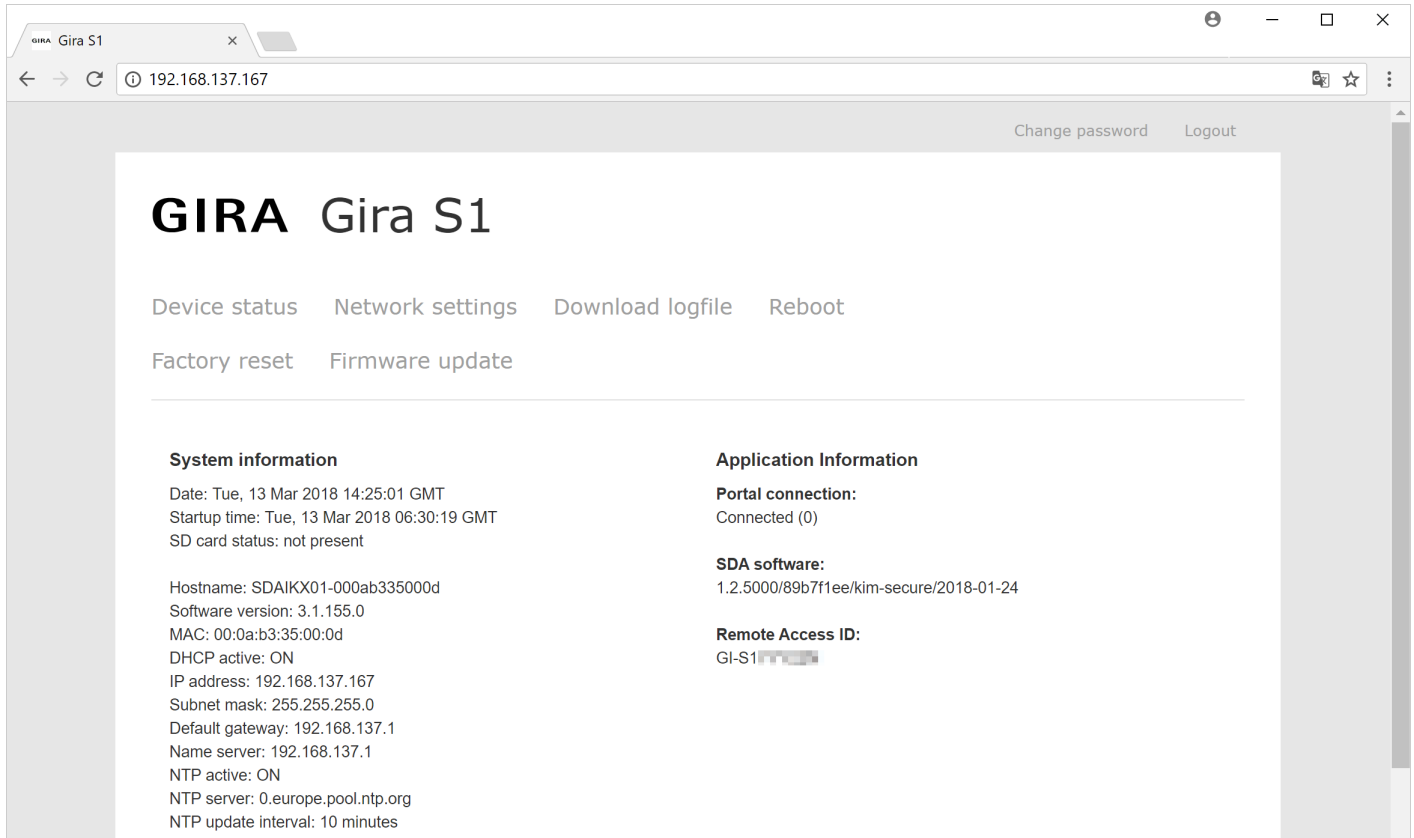


Figure 33: Gira S1 device website

Calling up the device website

If you know the IP address of the Gira S1, you can call up the device website by entering the IP address in the address line of a web browser (Chrome, Firefox...). To do this, the PC must be on the same network as the Gira S1.

If you do not know the IP address, open Windows Explorer and click "Network". The Gira S1 is displayed in the "Other Devices" area. Double-click the Gira S1 symbol to open a device website.

Entering a password

On the website that opens, enter the registration ID of the Gira S1 as the password. You can find the registration ID on a sticker on the device.

Access data for the diagnostic page

To open the diagnostics page of the Gira S1, please use the following access data:

User name: device

Password: GPA password (located on a sticker on the device)

16. License agreement

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

By accepting this agreement and installing the Gira S1 device software or putting a "Gira S1 device" into use, you conclude an agreement with Gira, Giersiepen GmbH & Co KG and agree to be legally bound by the terms of this agreement. This is exclusively a license agreement and does not constitute a product sales agreement.

1. Definitions

Licensor: Gira, Giersiepen GmbH & Co KG, Radevormwald, Germany

Licensee: The legal recipient of the Gira S1 device software.

Gira S1 devices: The term Gira S1 devices refers to the Gira S1 devices that each consist of a hardware device and the associated firmware.

Firmware: Software which is embedded on the Gira IP device and is conducive for the operation of the same.

Start-up software: The start-up software refers to the application program, which is provided for the planning and configuration of the Gira S1 devices.

Software from third parties: Third-party IP

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

The software packages used in this product - which are licensed within the mentioned framework - are described on the device website in the section "Licenses".

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

2. Licensed property

The subject matter of this agreement is the software provided on the Gira S1, as well as the corresponding documentation in written or electronic form.

3. Rights of use of the Gira S1 software

The licensor grants the licensee the non-exclusive, non-transferable right to use the firmware for an unlimited time in accordance with the conditions of this usage license on the Gira S1 device 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.

4. Restriction of rights of use, transfer to a third party

4.1. The licensee is not authorised to use, copy, process or transfer the Gira S1 software in whole or in part in any way other than as described herein. Excluded from this is one (1) copy, which shall be produced by the licensee exclusively for archiving and backup purposes.

4.2. The licensee is not authorised to apply reverse-engineering techniques to the Gira S1 software or to convert the Gira S1 software to another form. Such techniques particularly include 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).

4.3. The license for Gira S1 software is bound to the use of the Gira S1 device. It is only permitted to transfer the Gira S1 software to third parties or provide third parties with access to the software in conjunction with the transfer of the Gira S1 devices.

The licensee's right of use will expire upon the transfer to a third party.

The licensee is only permitted to transfer the software and all license keys required to use the software with the exception of specifically labelled software to third parties in the following instances:

4.3.1 The licensee removes any backup copies as well as the license keys required to use the software from his system by deleting and/or uninstalling them.

4.3.2 The third party gives a commitment to Gira prior to the transfer and use that it will comply with these Terms and Conditions of Use.

The licensee shall specifically point out these Terms and Conditions of Use to the third party prior to transferring the Gira S1 device.

4.4. The licensee is not authorised to rent or lease the Gira S1 software or grant sublicenses to the program.

4.5. The licensee requires written approval from the licensor to create and distribute software which is derived from the Gira S1 software.

4.6. The mechanisms of the licence management and copying protection of the Gira S1 software may not be analysed, published, circumvented or disabled.

5. Ownership, secrecy

5.1. The Gira S1 software and the documentation (which shall be provided in printed form or also as online help or online documentation), along with all changes made thereto, are and shall remain the property of the licensor. The licensor reserves all other rights and interests in the licensed property. The licensee shall observe these rights.

5.2. No part of the licensed property, that is not 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. The licensee pledges only to use the licensed property for the sole purpose of exercising rights under this usage license.

6. Changes

The licensor may expand, improve or otherwise modify the licensed property at any time without notice. The license terms shall continue to apply.

7. Warranty

The Gira S1 software shall be delivered together with software from third parties as listed in section 1. No warranty is provided for software from third parties.

With regard to the license terms for this software, please refer to the links (URLs) specified in Section 1. These terms are included in this agreement.

The licensor shall provide the licensee with the complete machine-readable source code for the third-party software (Open Source Software) listed under item 1 within 36 months after delivery of the software, upon request. The licensor shall charge the licensee the shipping costs for this.

7.1. The Gira S1 software and the documentation (which shall be provided in printed form or also as online help or online documentation) shall be provided to the licensee in the respective valid version. The warranty period for the Gira S1 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 runnable on the computer stations specified by the licensor.

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

7.2. Otherwise, no guarantee shall be provided for the freedom from faults of the Gira S1 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.

8. Liability

The licensor shall not be liable for damages due to loss of profit, data loss or any other financial loss resulting from the use of the Gira S1 software.

This limitation of liability is valid for all damage claims of the licensee, regardless of the legal basis. Liability is limited to the product purchase price.

The exclusion of liability does not apply to damage caused by premeditation or gross negligence on the part of the licensor. The exclusion of liability does not affect any licensee claims based on the legal provisions concerning product liability.

9. Data protection

By signing this license agreement, you agree to the validity of the GIRA data protection policy in its current version. See <http://www.gira.de/impressum/datenschutz.html>

10. Applicable law and jurisdiction

This agreement is governed by the law of the Federal Republic of Germany under express exclusion of the UN Convention on Contracts for the International Sale of Goods.

Jurisdiction is the court competent for the location of the licensor.

11. 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 Gira S1 software and the documentation submitted (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 Gira S1 software shall expire upon the termination of the agreement. In this case, the Gira S1 devices must be taken out of operation. Further use of the Gira S1 devices without a license is prohibited.

12. Subsidiary agreements and changes to the agreement

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

13. Exception

All rights not expressly mentioned in this agreement are reserved.