KNX
Product documentation

Status of the documentation:
06.10.2026

Gira F1
Order No. 2049 00



Gira F1 (Fig. 1:1)

Contents

1. Quick overview of the Gira F1 3
1.1. Installation (see Chapter 3) 3
1.2. Configure the KNX Bridge (see Chapter 4) 3
1.3. Configuring the SIP firewall (see Chapter 5) 3
1.4. Use in the IP door communication system 3

2. Product description 4
2.1. Functions 5
2.2. KNX Secure 5

3. Installation 6
3.1. Device design 6
3.2. Installation and electrical connection 7

4. Configuration of the KNX Bridge in the ETS 8
4.1. Setting up Gira F1 as a device in the ETS. 8
4.2. IP settings of the KNX Bridge (LAN 1) 9
4.3. Transferring application programs and configuration data 11
4.4. Parameters 12
4.5. Object table 13
4.6. Example: Application of the KNX Bridge 16
4.7. Example: Generating a message text on the Gira G1 17
4.8. Flag settings 18

5. Configuring the SIP firewall on the device website 19
5.1. Homepage 19
5.2. Device information 21
5.3. Network settings 22
5.4. SIP door communication 24
5.5. Diagnostics 30

6. Displays and operation 31
6.1. LED status displays 31
6.2. Device identification 31
6.3. Factory reset 32
6.4. Firmware update of the device 34

7. Technical data 35
7.1. Accessories 35

8. Frequently asked questions (FAQ) 36
8.1. General network and IP settings 36
8.2. When using the ETS 36
8.3. When using SIP door communication systems from other manufacturers 36

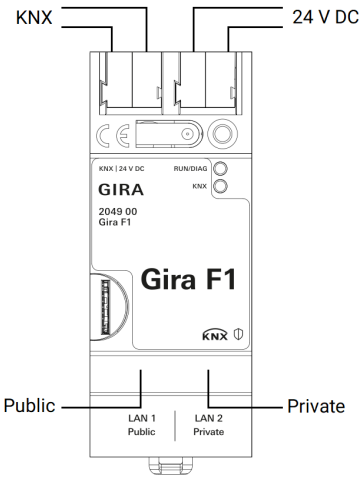
9. Licence Agreement 37

1. Quick overview of the Gira F1

This page shows the configuration process at a glance. Configuration of the Gira F1 is determined by its intended use. You can read a detailed guide to commissioning in the sections indicated in each step of the procedure.

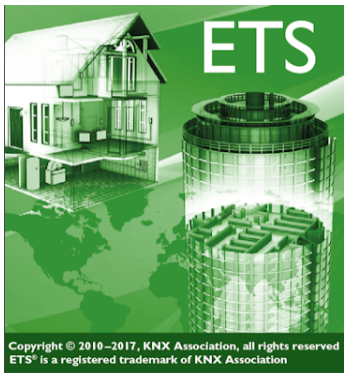
1.1. Installation (see Chapter 3)

- Mount the Gira F1.
- Connect the power supply,
- make the KNX connection (for the KNX Bridge) and
- the connection to the required networks, depending on the application.



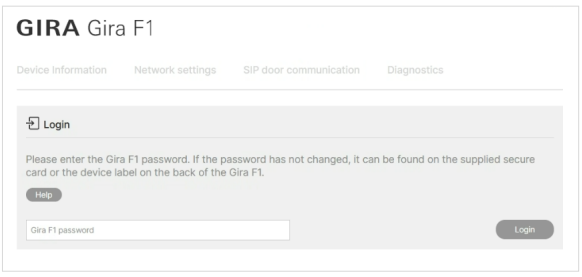
1.2. Configure the KNX Bridge (see Chapter 4)

- Select the right device application of the Gira F1 for the configuration step (KNX IP or KNX TP).
  Example:
  KNX IP application in the ETS project for the building.
  KNX TP application in the ETS project for the residential unit.
- Assign the individual address for the project.
- Assign the group addresses required for the connections between the projects. The KNX information is transferred between the two KNX projects through the connections.
- Transfer the application program.



1.3. Configuring the SIP firewall (see Chapter 5)

- Open the device website and log in.
- Configure the network settings for the public and private network.
- Configure the settings for SIP door communication.



1.4. Use in the IP door communication system

The settings are made via the Gira Project Assistant (GPA) and the Gira F1 device website. Information on needs-based parameterisation of the Gira F1 and other system components can be found in the system basics of the Gira IP door communication.

2. Product description

The Gira F1 is used to isolate two building networks securely. Only previously enabled functions and the associated data can cross the network boundaries. The functional scope of the Gira F1 includes KNX and SIP. This makes it possible to integrate network-based SIP door intercom systems made by other manufacturers.

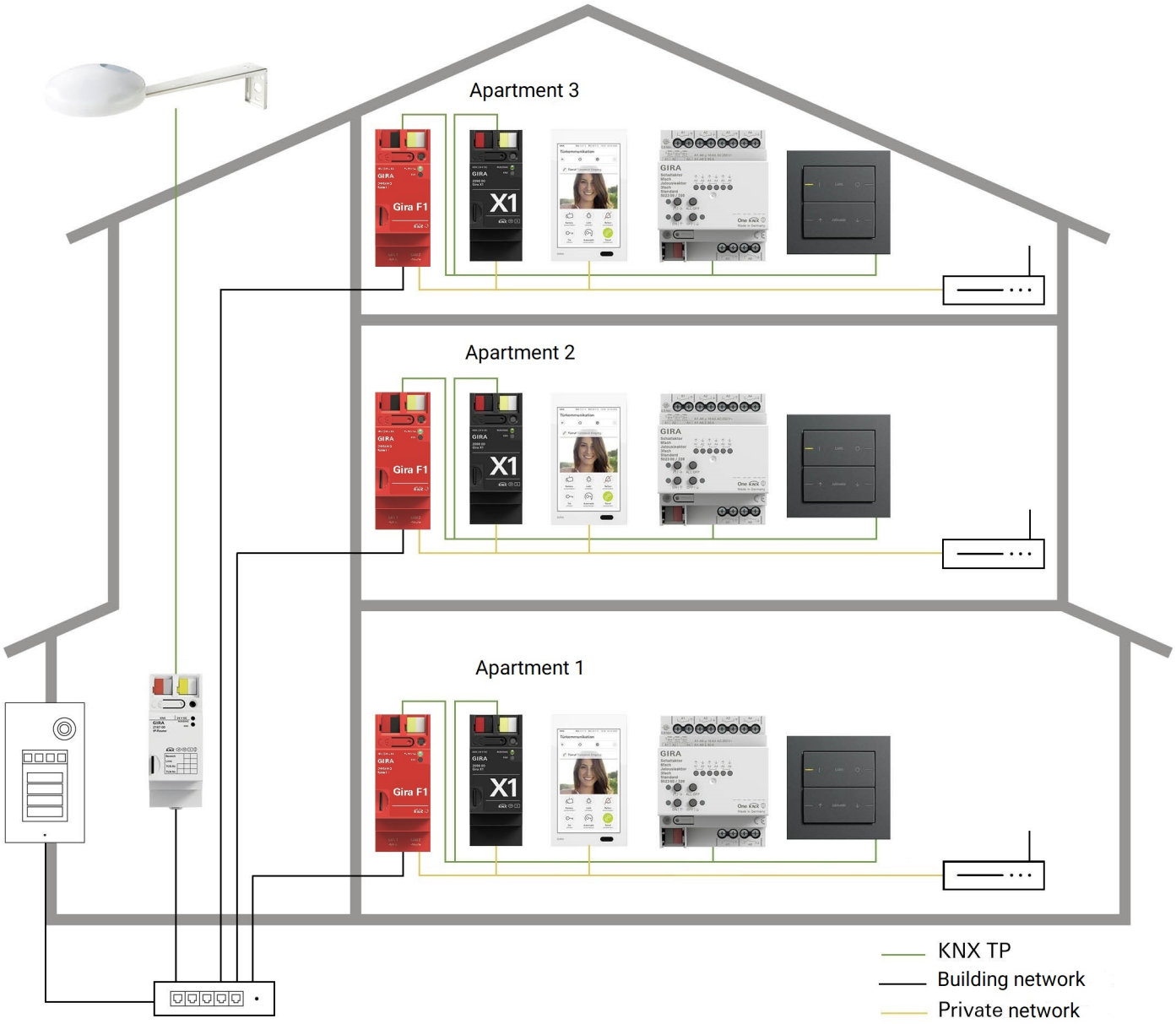


Figure 1: System overview

2.1. Functions

- SIP firewall
  In modern multistorey buildings, there are door stations which are intended to trigger door calls for the individual residential units (e.g. the Gira G1 as an SIP client).
  The network-based SIP protocol establishes the communication between the door station and the participants in the homes. As a firewall, the Gira F1 guarantees security of access to both the private and the public network.
  The Gira F1 makes it possible to ensure that only essential SIP protocols are allowed to pass through the firewall – thus, for example, the door call can be put through from the public network to the private network or the concierge can be called from the private network.
  The Gira F1 is set up as an SIP firewall on the device website (Chapter 5.4).

  Use in the IP door communication system
  In conjunction with the IP door communication system, the Gira F1 ensures separation between the private network (residential unit) and the public building network. The Gira F1 ensures that only necessary door communication protocols pass through the firewall. Information on needs-based parameterisation of the Gira F1 and other system components can be found in the system basics of the Gira IP door communication.
- KNX Bridge
  The Gira F1 can connect two independent KNX systems as a KNX Bridge. Configuration is carried out in the respective ETS projects. The Gira F1 has two ETS applications which map the two KNX systems (IP and TP). Communication between the KNX IP (building network) and the KNX TP (private network/home) takes place bidirectionally. Up to 1000 group objects are available to the two networks for this. Restriction of communication can be achieved with the flags in the ETS (Chapter 4.8).
- Combined operation
  The Gira F1 allows combined operation of the SIP firewall (Chapter 5.4) and KNX Bridge (Chapter 4) functions.

2.2. KNX Secure

The Gira F1 is compatible with KNX Secure. Each network area (KNX TP and KNX IP) has its own Secure certificate. The KNX Device Certificate can be found on a label on the side of the device and is also enclosed with the device.

For maximum security, we recommend removing the label from the device.

You cannot restore the KNX Device Certificate yourself.

Keep the KNX Device Certificate in a safe place. If you do, however, lose the KNX Device Certificate, contact our support team.

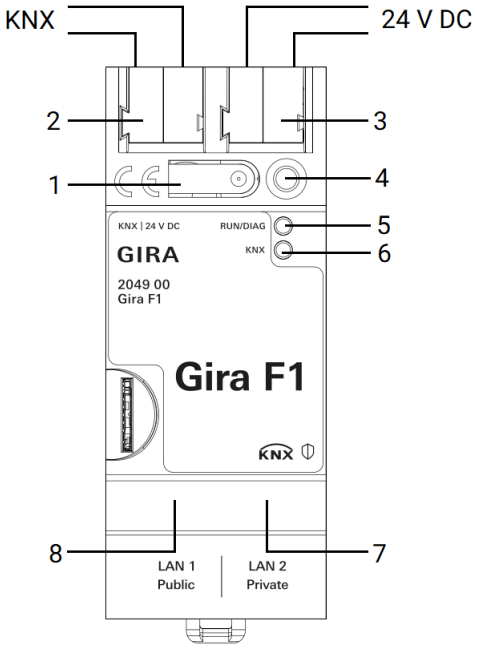
---

3. Installation

Safety instructions

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 hazards.

3.1. Device design



1. Programming button
2. KNX connection
3. External power supply connection
4. Programming LED (red/yellow):
   red = KNX Bridge TP – programming mode active
   red = IP door communication system –
   device identification
   yellow = KNX Bridge IP (LAN 1) – programming mode active
   orange = KNX Bridge (both sides) – programming mode active
5. Operating LED (green):
   on = Gira F1 ready for operation (TP side)
   flashing slowly = Gira F1 not yet configured
   flashing quickly = internal device error
   flashing at intervals = the two networks are in the same address range
6. KNX LED (yellow)
   on = connection to KNX TP system
   off = no connection to KNX TP system
   flashing = KNX data transfer
7. Network connection LAN 2 private with LED (green/orange)
   green on = data transmission rate 100 Mbit/s
   green off = data transmission rate 10 Mbit/s
   orange on = connection to IP network
   orange flashing = no connection to IP network, no data reception from IP network
8. Network connection LAN 1 public with LED (green/orange)
   green on = data transmission rate 100 Mbit/s
   green off = data transmission rate 10 Mbit/s
   orange on = connection to IP network
   orange flashing = no connection to IP network, no data reception from IP network

3.2. Installation and electrical connection

Danger

Electric shock if live parts are touched in the installation environment.
Electric shock may result in death.
Isolate and cover live parts in the vicinity before working on the device!

Selection of installation location

We recommend decentralised installation of the Gira F1 and the power supply in the sub-distribution box of each residential unit to ensure the security of the private network.
The Gira F1 and the devices connected to it on a network must be installed in the same earthing system.

3.2.1. Mounting the device

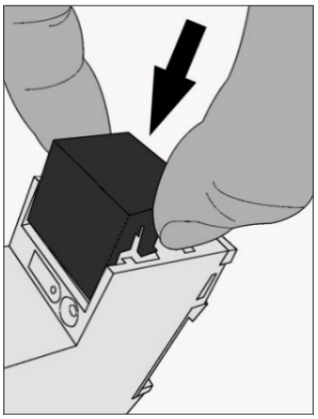
Observe the temperature range. Ensure sufficient cooling.

- Snap the device onto a top-hat rail according to DIN EN 60715. See Figure 1 for installation position.
- Connect the external power supply 24-30 V DC to the connection terminal (3).
  Recommendation: use white-yellow connection terminal.
- Connect the KNX line of the residential unit to the red-black bus terminal (2).
- Place the cover cap over the KNX/External power supply connection.
- Make the network connection by inserting the RJ45 plug into the RJ pin jack (7 and 8).

3.2.2. Attaching the cover cap

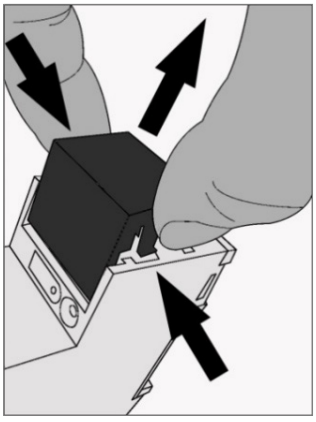
A cover cap must be attached to protect the bus connection from dangerous voltages in the connection area.

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



3.2.3. Removing the cover cap

- Press the cover cap on the sides and pull off.



4. Configuration of the KNX Bridge in the ETS

Transfer of the KNX information between the two KNX projects to be connected is carried out via the connectors on both sides, which are configured in the applications.

Configuration of the Gira F1 in the ETS can be broken down into the following steps:

1. Select the right device application of the Gira F1 for the use case (KNX IP or KNX TP) (Chapter 4.1).
   Example:
   KNX IP application in the ETS project for the building.
   KNX TP application in the ETS project for the residential unit.
2. Set the IP address, IP subnet mask and standard gateway address of the Gira F1 or select “Obtain IP address automatically (from a DHCP server)” (Chapter 4.2).
3. General parameters for setting the Gira F1 (parameters, see Chapter 4.4)
4. Connect group addresses to group objects (object table, see Chapter 4.5).
5. Assign individual addresses (Chapter 4.2.1).
6. Transfer application program (Chapter 4.3).

4.1. Setting up Gira F1 as a device in the ETS.

If you have not done so already, import the ETS device application required for your use case once into the device catalogue of the ETS.
Two applications (KNX Bridge TP and KNX Bridge IP) are available for the Gira F1.
Alternatively, you can also download the ETS applications from www.downloads.gira.de free of charge.

Product catalogue
Product name: Gira F1
Design: DRA (series installation), 2 MW
Order no.: 2049 00

Delivery condition

In its delivery condition or after a factory reset and before it is loaded with an ETS for the first time, the Gira F1 is configured as follows:
The individual address for the Gira F1 KNX Bridge TP and the Gira F1 KNX Bridge IP (LAN 1) is 15.15.255.

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 select the device with the old database entry. Now select “Information” under the “Properties” of the device and then the “Application program” tab. You can then replace the old database entry using the “Update” button. Existing links with group addresses will not be lost. The newly added device can then be deleted again.

Note: Do not use “Change application program”

Please do **not** use the “Change application program” dropdown menu, as the entire configuration of the Gira F1 will be lost if you use this function.

4.2. IP settings of the KNX Bridge (LAN 1)

In addition to the individual addresses in the KNX network, the Gira F1 must be assigned to an address in the IP data network. The following information is required for this:

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

You can configure the DNS server on the device website (see chapter 5.3 “Network settings”)

Note: IP settings via ETS or device website

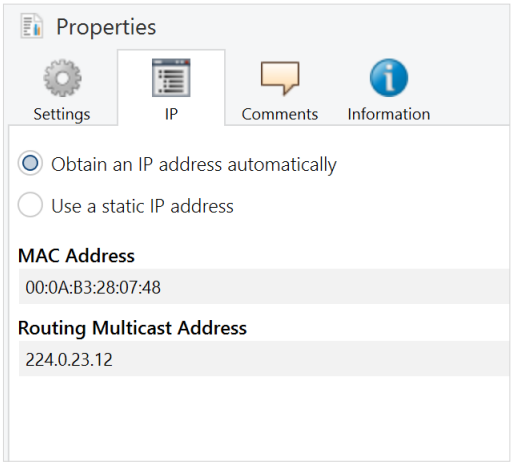
If both network connections are being used, the IP addresses must be assigned to different networks.
Example: 192.168.2.120 for public and 192.168.2.122 for private is **not permitted**, even if there are two separate networks with two separate routers.
With a subnet mask of 255.255.255.0, the correct setting is e.g.:
192.168.**2**.123 for public and 192.168.**1**.123 for private
or with a subnet mask of 255.255.0.0 e.g.:
192.**168**.2.123 for public and 192.**178**.2.123 for private.
Incorrect configuration of the network settings is indicated by the operating LED flashing green at intervals.

The IP connection LAN 1 (Public) must be set up to use the KNX Bridge function.
Proceed as follows:

1. Select the Gira F1 KNX Bridge IP (LAN 1) in the ETS.
2. Display the properties of the Gira F1 in the Properties column of the ETS.
3. Select the “IP” tab.
   Now select either
   - “Obtain IP address automatically” (default)
     The address details are obtained automatically from a DHCP server on the data network.

or

- “Use fixed IP address”
  and enter the details manually.
  You will usually find the permitted IP address range and the subnet mask and standard gateway in the interface for the router configuration.



Note: IP settings via ETS or device website

The IP settings of the Gira F1 can be configured via ETS **and** via the device website.
The settings configured most recently on the device take effect.
Use identical IP settings in the ETS and on the device website.

Note: Program both applications

Ensure that you have assigned an individual address for both the applications “Gira F1 KNX Bridge TP” and “Gira F1 KNX Bridge IP (LAN 1)“, you program them both and transfer the application programs and configuration data.

Transfer of IP settings
Simply transferring the application program is **not** sufficient to apply the IP settings from the ETS. This can only be done by downloading the individual address.

Programming mode
Briefly press programming button (1) (< 4 seconds) – programming LED (4) turns red.
Press and hold programming button (1) (> 4 seconds) – programming LED (4) turns yellow.
You have the option to set both bridges to programming mode:
First press and release programming button (1) and then press and hold it – programming LED (4) turns orange.

If the Gira F1 is connected via IP, you can also put the device into programming mode via the “Diagnostics” tab on the device website (Chapter 5.5).

4.2.1. Programming the individual address of the KNX Bridge TP

1. Ensure that the device and bus voltage are switched on.
2. Ensure that the programming LED (4) is not on.
3. Briefly press programming button (1) (< 4 seconds) – programming LED (4) turns red.
4. Alternatively, programming mode can be activated on the device website.
5. Program the individual address using the ETS.

When the programming process has been completed successfully,

- the LED (4) goes out.
- the ETS shows the completed transfer highlighted in green under History in the Properties column (usually on the right of the screen).
- the ETS ticks the commissioning boxes on the device for “Adr” and “Cfg”.

4.2.2. Programming the individual address of the KNX Bridge IP (LAN 1)

Selecting the IP transfer path

The Gira F1 is a KNX IP multicast device. No additional KNX data interface is required for transfer via IP. You can select this option in the ETS project in the “Bus interface” - “Settings” view.
For transfer of the ETS via the IP page, select the setting “Use direct KNX-IP connection if supported by target device”.



1. Ensure that the device and bus voltage are switched on.
2. Ensure that the programming LED (4) is not on. If it is red, briefly press the programming button (1) (< 4 s) to deactivate it.
3. Press and hold programming button (1) (> 4 seconds) – programming LED (4) turns yellow.
4. Alternatively, programming mode can be activated on the device website.
5. Program the individual address using the ETS.

When the programming process has been completed successfully,

- the LED (4) goes out.
- the ETS shows the completed transfer highlighted in green under History in the Properties column (usually on the right of the screen).
- the ETS ticks the commissioning boxes on the device for “Adr” and “Cfg”.

4.3. Transferring application programs and configuration data

Following programming of the individual address, application programs, parameter settings and group address connections can be transferred to the “Gira F1 KNX Bridge TP” and “Gira F1 KNX Bridge IP (LAN 1)” devices.

- Select “Program application program” for this.
- After the download, wait approx. 15 seconds while the device applies the data and initialises the applications.
- Commissioning is complete.

4.4. Parameters

The Gira F1 is divided into two devices each with their own parameters in the ETS. The parameters for the public and private networks do not differ.

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

4.4.1. General

Parameter	Entry / selection	Comments
Show restart	Checkbox **(inactive)**	If this parameter is activated, the device can be restarted via a group object.
Show KNX statuses	Checkbox **(inactive)**	If this parameter is activated, the group objects for programming mode, their status and the bus voltage if present are enabled.

4.4.2. Connections

Connections are the bridge between the two KNX projects to be connected.

Max. 1000 objects (group addresses) can be connected.

As soon as connections and corresponding object sizes have been selected, the corresponding group objects are ready for connection.

Note: Same object size for same object number

In order to facilitate forwarding between public and private networks, connections with the same number must also contain the same object sizes (DPT).

Parameter	Entry / selection	Comments
Connection	**Use no connection**	If “Use no connection” is selected, there are no connections available in the form of group objects in the ETS.
	Use up to 20 connections	If “Use up to 20 connections” is selected, connections one to twenty are available in the form of group objects in the ETS.
	…	…
	Use up to 1000 connections	If “Use up to 1000 connections” is selected, connections one to one thousand are available in the form of group objects in the ETS.
Connection 1…1000	**Not selected** 1 bit 4 bit 1 byte 2 byte 4 byte 8 byte 14 byte	The selected object size should correspond to the data point types to be connected. **Example:** If the command to switch on a light is to be forwarded, select “1 bit” to allow DPT 1.001 Switch to be received and sent.

4.5. Object table

The following group objects for connection of group addresses are available in both devices of the Gira F1:

Object	Function	Name	Length	DPT		Flags (KLSÜA)
1	Ready	Gira F1 KNX Bridge	1 bit	1.011	Status	KL-Ü-

Description: Object that represents the status of the device.
1 = ready for operation, 0 = not ready for operation

Object	Function	Name	Length	DPT		Flags (KLSÜA)
2	Status	Gira F1 KNX Bridge	1 byte	5.010	Count impulses (0…255)	KL-Ü-

Description: Object for transmitting the current device status.

00h	Ready	Gira F1 has started up and is ready for operation.

Object	Function	Name	Length	DPT		Flags (KLSÜA)
3	Restart	Gira F1 KNX Bridge	1 bit	1.015	Reset	K-S--

Description: Object for receiving the restart prompt.
1 = restart

Object	Function	Name	Length	DPT		Flags (KLSÜA)
8	Runtime (s)	Gira F1 KNX Bridge	3 byte	13.100	Time difference (s)	KL---

Description: Object for reading the operating time in seconds. Time since last restart.

Object	Function	Name	Length	DPT		Flags (KLSÜA)
50	Programming mode	Gira F1 KNX Bridge	1 bit	1.001	Switch	K-S--

Description: Object for receiving programming mode.
1 = switch on, 0 = switch off

Object	Function	Name	Length	DPT		Flags (KLSÜA)
51	Status Programming mode	Gira F1 KNX Bridge	1 bit	1.001	Switch	KL-Ü-

Description: Object for transmitting programming mode.
1 = switched on, 0 = switched off

Object	Function	Name	Length	DPT		Flags (KLSÜA)
60	Bus voltage present	Gira F1 KNX Bridge	1 bit	1.011	Status	KL-Ü-

Description: Object for checking the bus status.
1 = device has bus access, 0 = device has no bus access
Note: The object does not transmit the status on restart of the device.

Object	Function	Name	Length	DPT	Flags (KLSÜA)
100 - 1099	Connector LAN1/TP	No. / 1 bit	1 bit	-	K-SÜ-

Description: This is one of 7 possible DP types for the 1000 group objects “100 to 1099”.
The definition of the DP type is set by selecting “Connections” on the parameters page.

Object	Function	Name	Length	DPT	Flags (KLSÜA)
100 - 1099	Connector LAN1/TP	No. / 4 bit	4 bit	-	K-SÜ-

Description: This is one of 7 possible DP types for the 1000 group objects “100 to 1099”.
The definition of the DP type is set by selecting “Connections” on the parameters page.

Object	Function	Name	Length	DP type	Flags (KLSÜA)
100 - 1099	Connector LAN1/TP	No. / 1 byte	1 byte	-	K-SÜ-

Description: This is one of 7 possible DP types for the 1000 group objects “100 to 1099”.
The definition of the DP type is set by selecting “Connections” on the parameters page.

Object	Function	Name	Length	DP type	Flags (KLSÜA)
100 - 1099	Connector LAN1/TP	No. / 2 byte	2 byte	-	K-SÜ-

Description: This is one of 7 possible DP types for the 1000 group objects “100 to 1099”.
The definition of the DP type is set by selecting “Connections” on the parameters page.

Object	Function	Name	Length	DP type	Flags (KLSÜA)
100 - 1099	Connector LAN1/TP	No. / 4 byte	4 byte	-	K-SÜ-

Description: This is one of 7 possible DP types for the 1000 group objects “100 to 1099”.
The definition of the DP type is set by selecting “Connections” on the parameters page.

Object	Function	Name	Length	DP type	Flags (KLSÜA)
100 - 1099	Connector LAN1/TP	No. / 8 byte	8 byte	-	K-SÜ-

Description: This is one of 7 possible DP types for the 1000 group objects “100 to 1099”.
The definition of the DP type is set by selecting “Connections” on the parameters page.

Object	Function	Name	Length	DP type	Flags (KLSÜA)
100 - 1099	Connector LAN1/TP	No. / 14 byte	14 byte	-	K-SÜ-

Description: This is one of 7 possible DP types for the 1000 group objects “100 to 1099”.
The definition of the DP type is set by selecting “Connections” on the parameters page.

Note on configuration

Every connection in the private KNX TP system has a counterpart connection in the public KNX IP network. A group object is provided for each configured connection in the respective network.
The KNX Bridge function works in both directions. The connections are therefore bidirectional and, among other things, allow transmission and reception of telegrams.
A telegram from a residential unit can also trigger a telegram in the KNX system of the building, e.g. switching on the light in the stairwell.
By default, the flags K, S and Ü of this group object are activated.
Deactivate individual flags to increase security and prevent unwanted functions.

Practical tip: Transfer of configuration

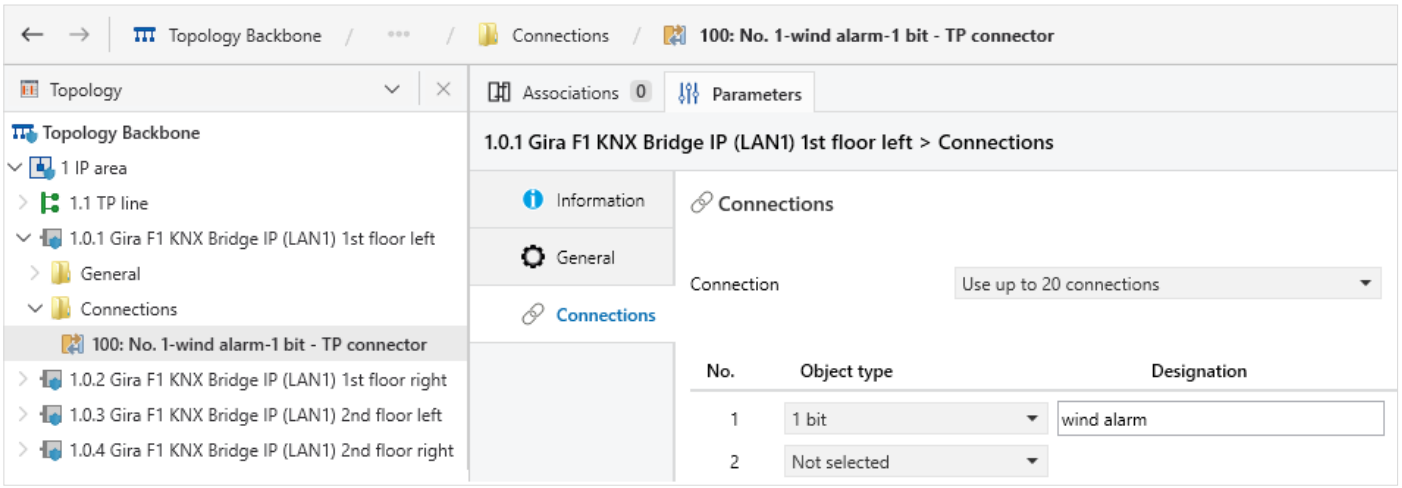
If the configuration on the TP side and the IP side is carried out by different people, information about the configured connections (connection number and data point type) and their function must be passed on.

4.6. Example: Application of the KNX Bridge

Transfer of a wind alarm from a KNX weather station to the residential unit.

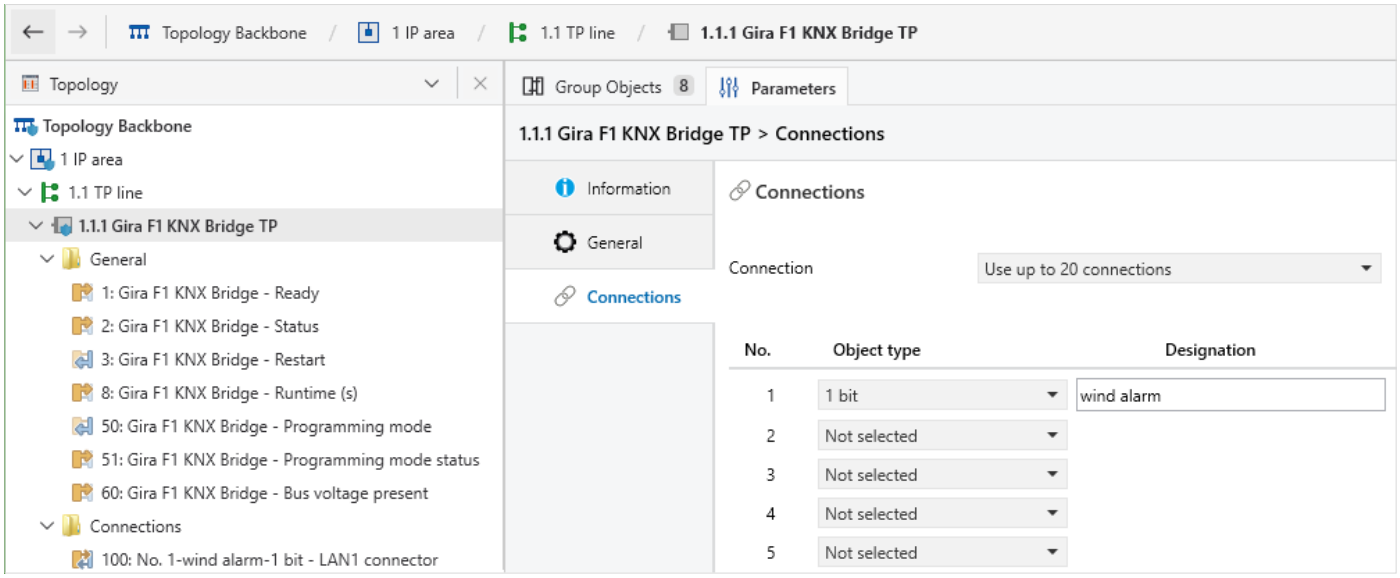
The KNX weather station, usually a KNX TP product, first requires a change of media from KNX TP to KNX IP. This can be done using a Gira IP router or another Gira F1.

- Create Gira F1 with the application Gira F1 KNX Bridge IP (LAN 1) in the IP line.
- Open IP application of the KNX Bridge.
- Set group address Wind alarm 1/1/10 as a DPT 1 bit object and give connection no. 1 a unique name. This generates group object 100 automatically.
- Assign group address of the wind alarm to group object 100.



The Gira F1 is now prepared on the IP side and receives the status of the wind alarm.
Proceed as follows to configure the TP side:

- Set up Gira F1 with the application Gira F1 KNX Bridge TP in the KNX project for the residential unit.
- Create the same connection with the same DPT for the wind alarm.
- The wind alarm can now be assigned to any group address.



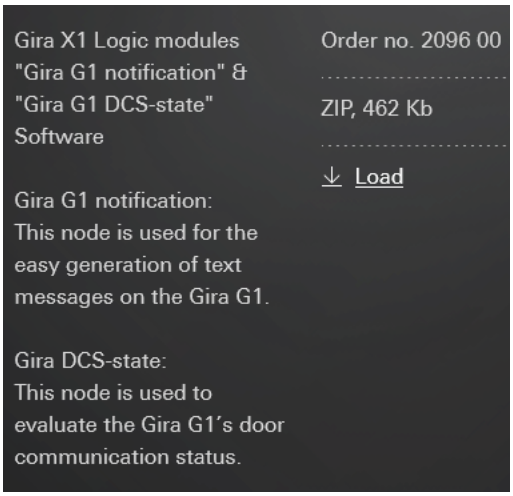
4.7. Example: Generating a message text on the Gira G1

The Gira G1 provides the option of displaying information to residents on a message page.
A Gira G1 and a Gira X1 are required for this.

In the example, a 1 bit KNX telegram is sent from the building to all Gira F1s.
The telegram contains the function of moving all blinds to their top end position and locking them for window cleaning.
The residents are to be sent a message about why the blinds cannot be moved.
The message is displayed in the residential units on the Gira G1.

Procedure:

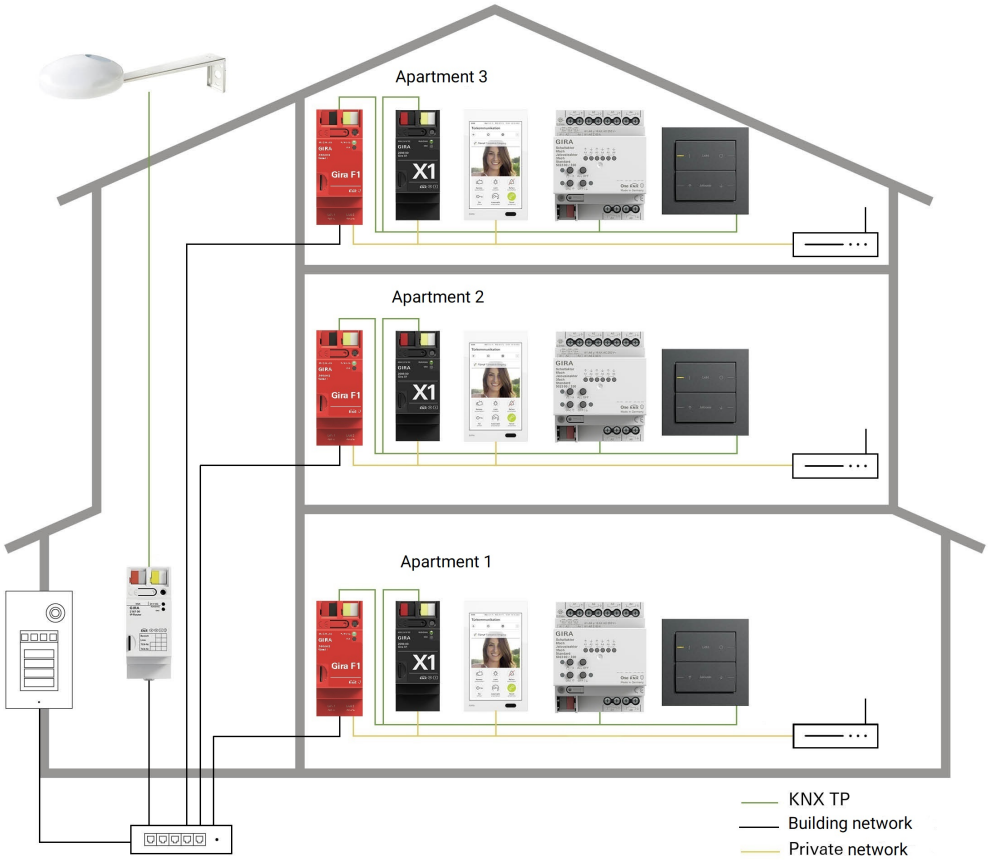
- In the KNX TP application of the Gira F1, set up a connection with the object type “1 bit”.
- Assign a clear name to the connection, such as “Window cleaning lock”.
- Import the “Gira G1 notifications” logic node into the X1 of the residential unit.
  You will find the logic node in the download area of the Gira X1 on the Gira website.
- Attach a group address to the connection created and the logic of the Gira X1.
- The logic node is triggered by the 1 bit telegram “Window cleaning lock”.
- The configured message text is transferred by means of an internal Gira data point via IP from the Gira X1 to the Gira G1.



4.8. Flag settings

Fundamentally, only the flags K, S and Ü of the connectors are set on delivery.
A read request is forwarded in the Gira F1 via the connection created when the L flag is activated.

Example



The following statuses are to be made available:

- The weather station sends events (a wind alarm, for example) to the residential unit.
- From the residential unit, a server (a Gira HomeServer, for example, or a Gira X1) triggers a read request to check the current weather status.
- After a restart of the Gira F1, a read request is sent to the weather station.

The following event is to be avoided:

- A wind alarm sent from the residential unit is not forwarded to the public area.

For this, you need to set the following flags:

Flags	TP	IP
K (communication)	active	active
L (read)	active	N/A
S (write)	N/A	active
Ü (transfer)	active	active
A (update)	N/A	N/A
I (read on init)	N/A	active

5. Configuring the SIP firewall on the device website

On the device website of the Gira F1, information about devices and diagnostics is displayed at a glance. Here you can also configure the network and door communication settings.
The device website is displayed in the internet browser.

Note: Difference between configuring for Gira devices and third-party devices

This chapter describes the configuration of the SIP firewall in relation with SIP door communication systems from other manufacturers. Configuration within the scope of the IP door communication system is described in the system basics of the Gira IP door communication.

5.1. Homepage

Accessing the device website

Note: Accessing the device website with HTTPS

We recommend that you use HTTPS to access the device website for security reasons. Enter https:// before the IP address and click on “Advanced...”. Then click on “Accept risk and continue”.

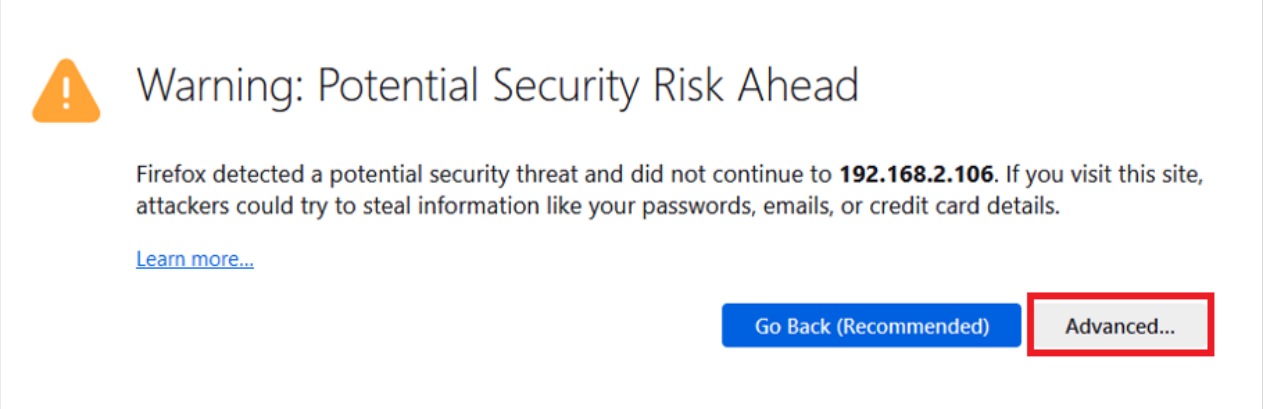


Figure 2: HTTPS input

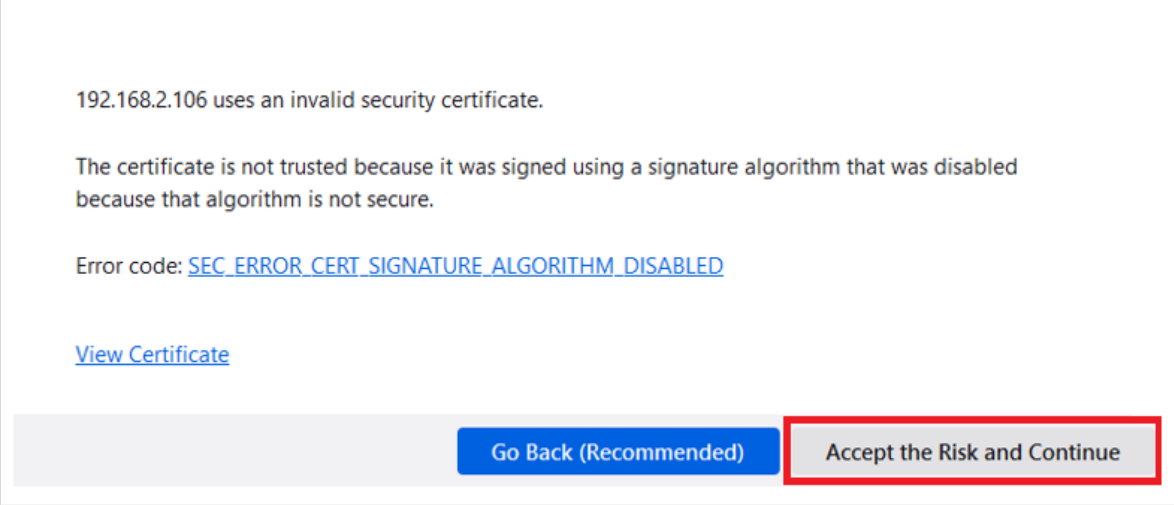


Figure 3: HTTPS confirmation

If you know an IP address of the Gira F1, you can open the device website by entering the IP address in the address line of an internet browser (Chrome, Firefox, ...). The PC must be on the same network as the Gira F1 for this to work. Access is possible from both the public IP side and the private IP side.
If you do not know the IP address, open Windows Explorer and click on “Network”. The Gira F1 is displayed under “Other devices”. Double-click the Gira F1 symbol to open the device website. Alternatively, the IP address of the Gira F1 is also displayed in the Gira Project Assistant (GPA).

Another option is to enter “https://” in conjunction with the host name. The host name is composed of “FIREKX03-” and the MAC address of the LAN 2 connection.
Example: FIREKX03-000ab3280908. You will find the MAC address on a label on the side of the device.

Entering the password
On the website that then opens, enter the GPA Initial Device Password for the Gira F1.
This password can be found on a label on the side of the device and on the accompanying Secure Card.
The password can only be changed in the GPA.

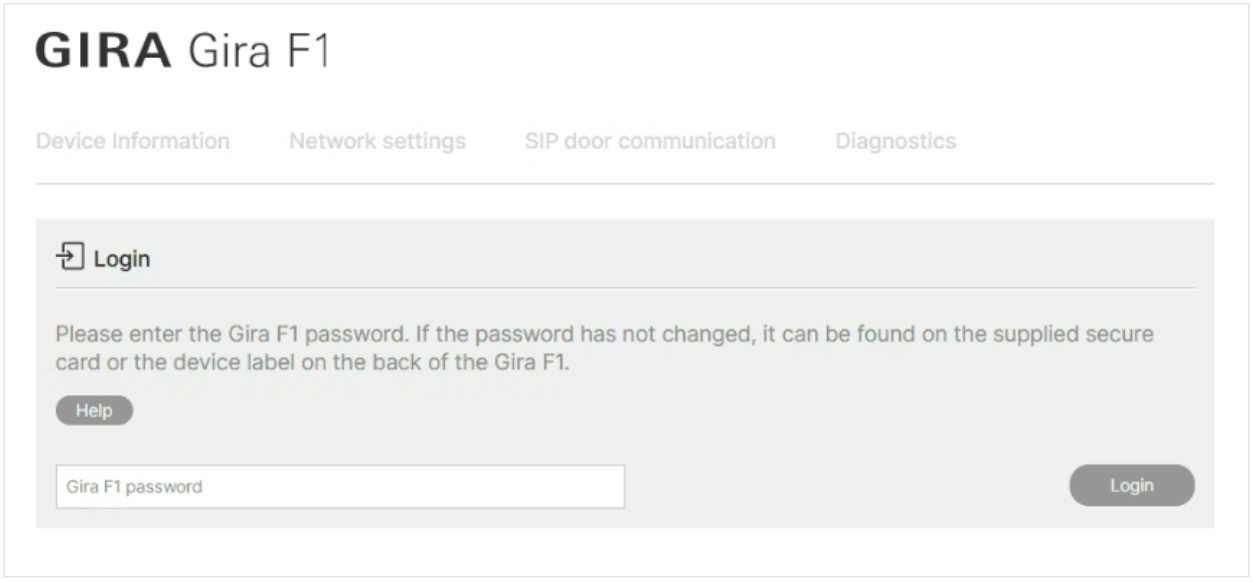


Figure 4: Device website – Login

5.2. Device information

The “Device information” tab provides basic information about the Gira F1. Among other things, it shows the MAC addresses of the public network (LAN 1) and the private network (LAN 2).

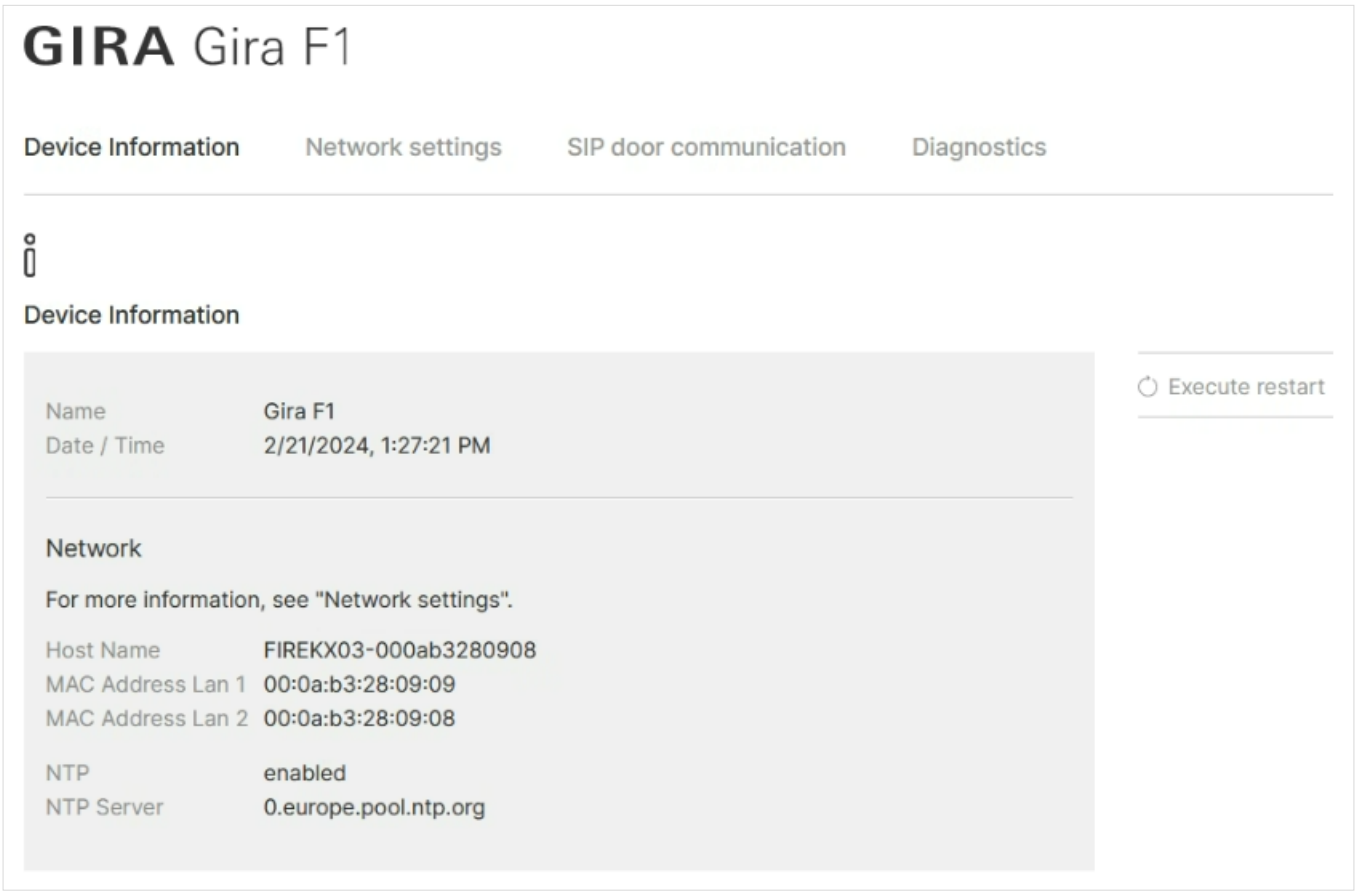


Figure 5: Device website – Device information

5.3. Network settings

If you wish to assign the IP address, the network mask and the gateway address yourself, you have the option to deactivate DHCP.

Note: IP settings via ETS or device website

If both network connections are being used, the IP addresses must be assigned to different networks. Example: 192.168.2.120 for public and 192.168.2.122 for private is **not permitted**, even if there are two separate networks with two separate routers.
With a subnet mask of 255.255.255.0, the correct setting is e.g.:
192.168.**2**.123 for public and 192.168.**1**.123 for private
or with a subnet mask of 255.255.0.0 e.g.:
192.**168**.2.123 for public and 192.**178**.2.123 for private.
Incorrect configuration of the network settings is indicated by the operating LED flashing green at intervals.

In addition, you can prioritise the addresses for the gateway and DNS of a network.
This can be useful if you use an NTP server on that network to provide the time. The current time of the Gira F1 is required for SIPS operation.

If you want to use a specific DNS server, you can set up the IP address of a primary and secondary server (server which is accessible as an alternative).

Settings for the public network

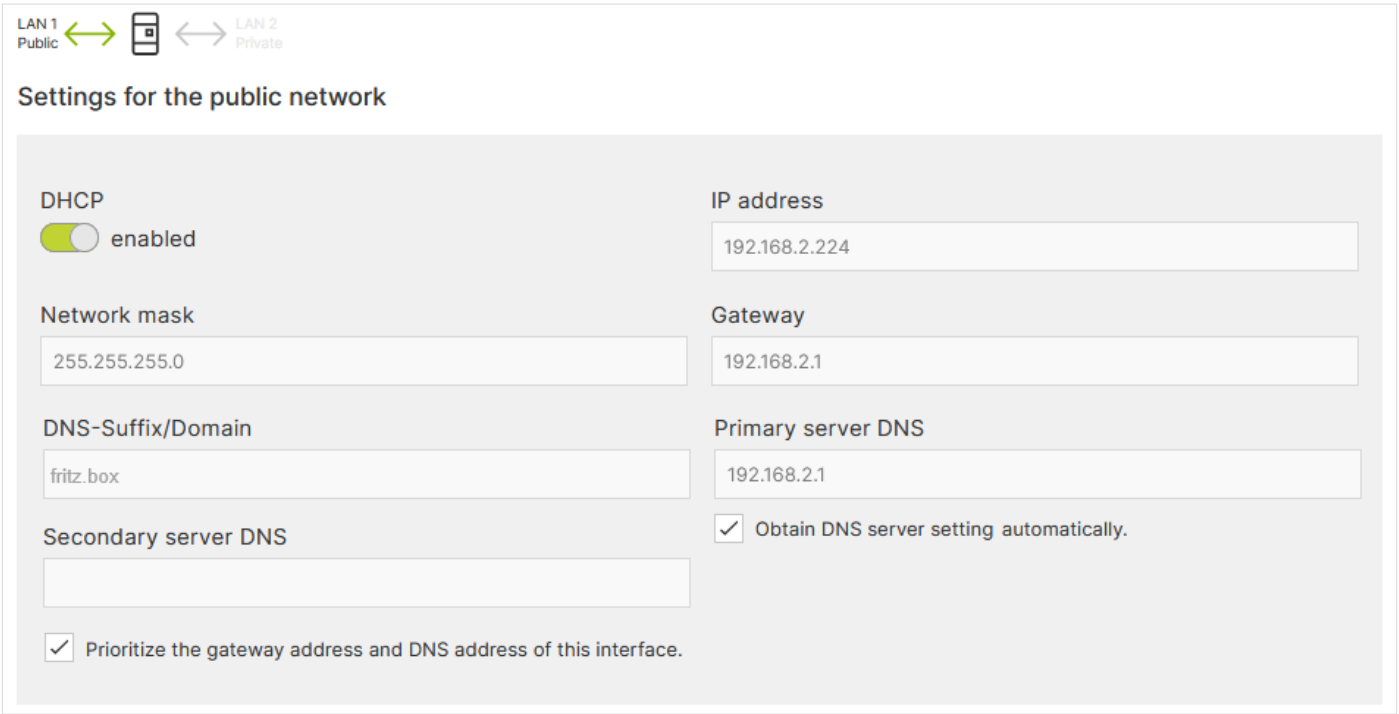


Figure 6: Device website – Settings for the public network

Settings of the private network

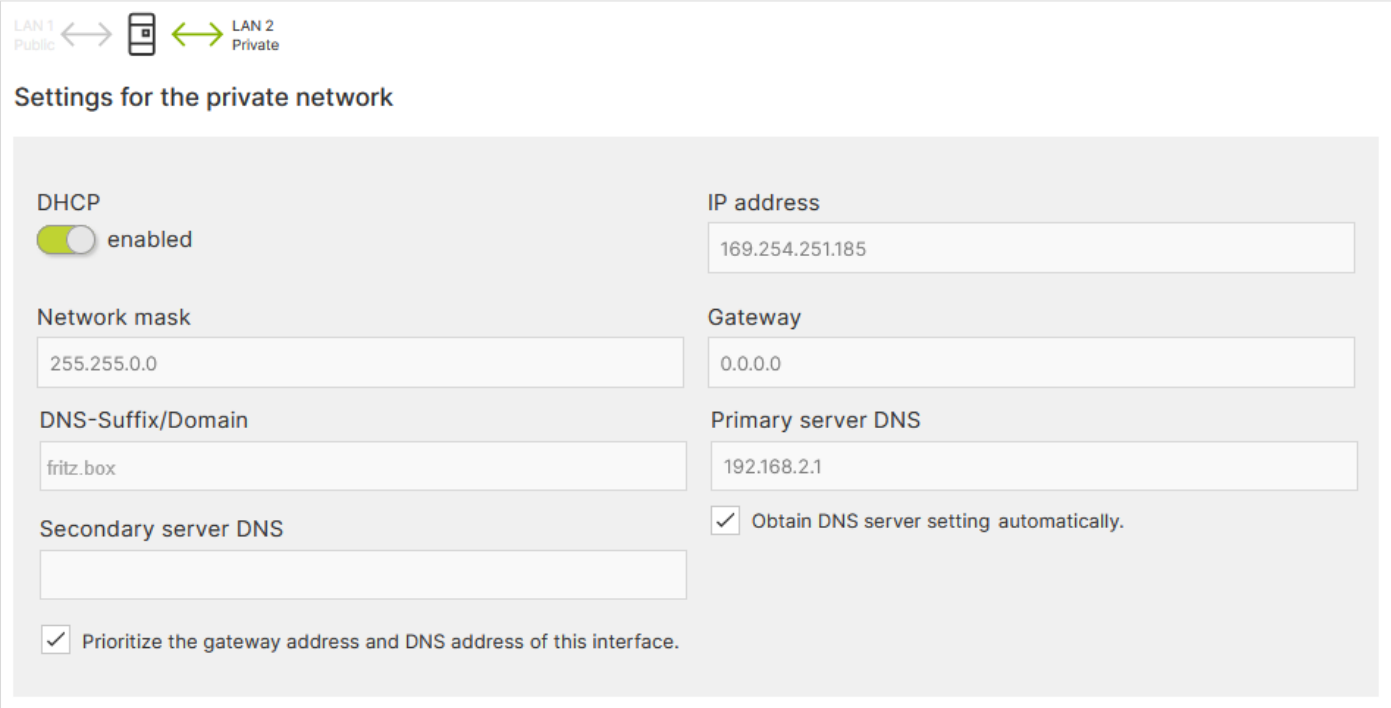


Figure 7: Device website – Settings for the private network

5.4. SIP door communication

The “SIP door communication” tab is used to register IP door stations from the public network and home stations as well as telephone systems on the private network.

In addition, you have the option to export or import the registration data to facilitate set-up of several Gira F1s. The export function can also be used for data backup.

5.4.1. Settings for the public network (LAN 1)

At least one port must be enabled (status “open”) for communication between an IP door station and the Gira F1. Set the status of both ports to “open” if you want to use both encrypted and unencrypted devices.

Security risk

Unencrypted communication on the public network represents a security risk.

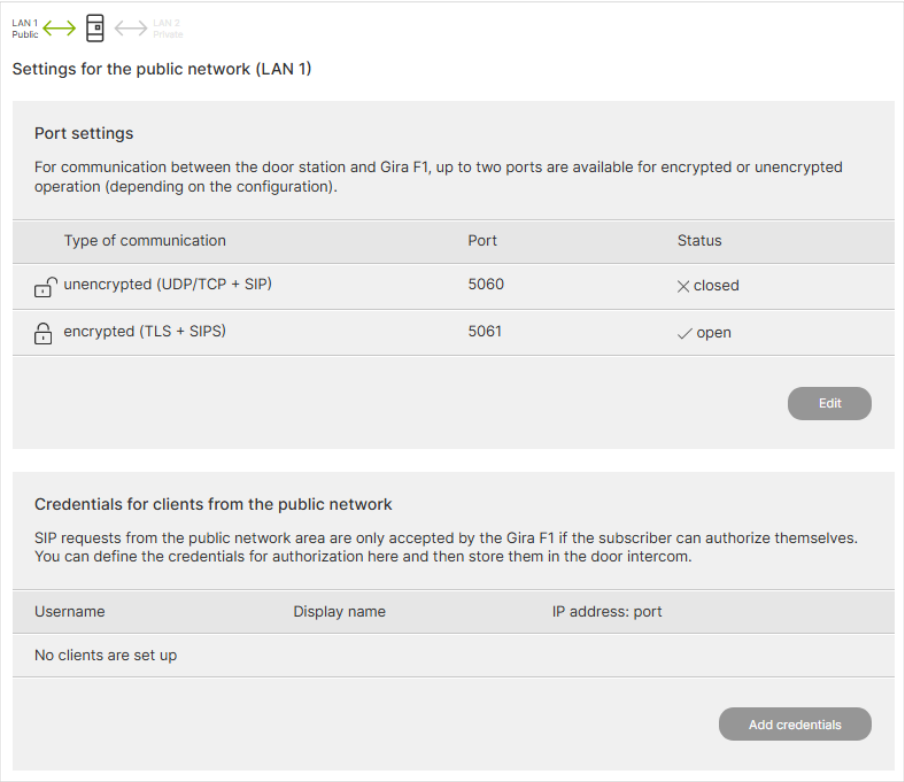


Figure 8: Device website – SIP door communication on the public network

After successful registration of the door station on the Gira F1, the call buttons of the door station must be configured in such a way that a direct call is triggered in the required slot.

Example:

SIP:slot-1@192.168.1.123:5060 (unencrypted)

SIP:slot-2@192.168.1.456:5061 (encrypted)

The door call is forwarded from the slot in the public network to the slot in the private network.

5.4.2. Settings for the private network (LAN 2)

The SIP server of the Gira F1 can be used in two different ways:

1. As a registrar/main station, the Gira F1 communicates with SIP-compatible home stations such as the Gira G1. If registration details for the home stations (connections in the private network) have been set up, they must match the registration details on the device website for the home station.
2. As a SIP client/extension, to integrate a door communication system into a telephone system via the Gira F1.

The mode of use is selected under “Connections in the private network” when configuring the respective slot.

Port settings

At least one port must be enabled (status “open”) for communication between an SIP-compatible home station and the Gira F1. Set the status of both ports to “open” if you want to use both encrypted and unencrypted devices.

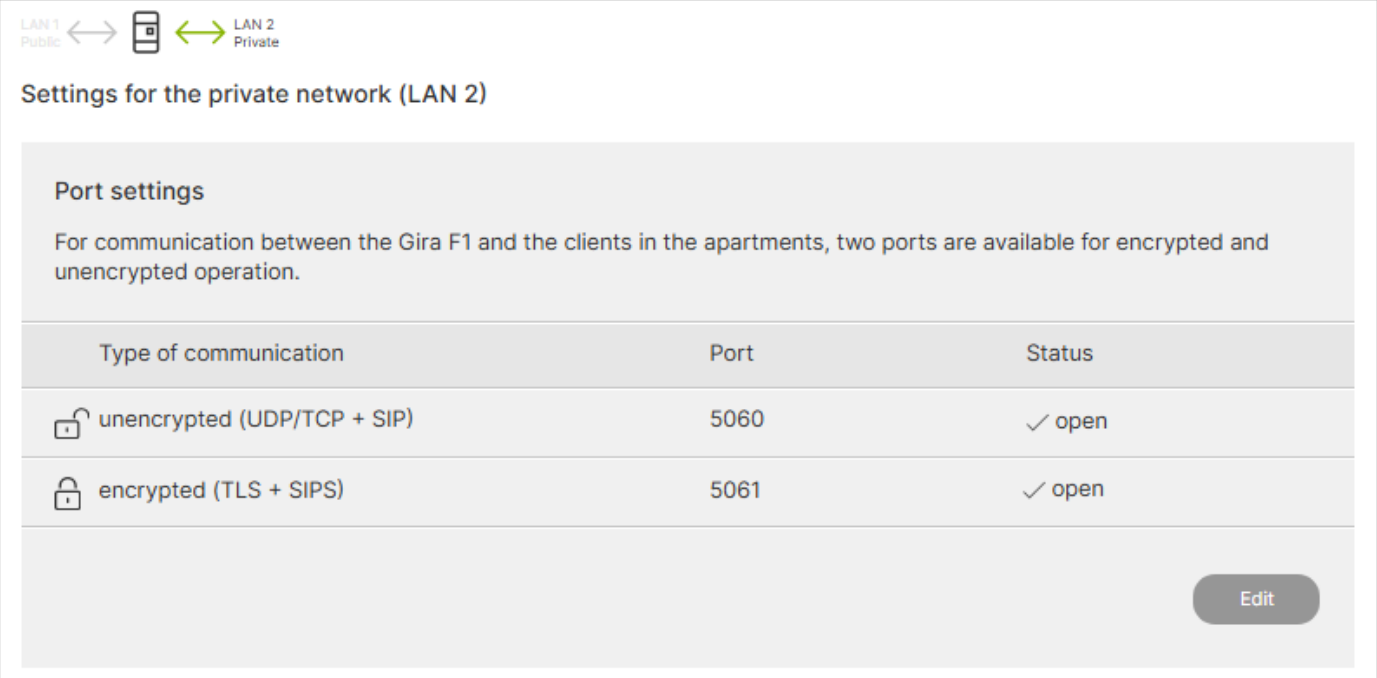


Figure 9: Device website – SIP door communication in the private network

Connections in the private network

Click on the edit symbol to configure the registration details.
The registration details can be exported as a PDF if required.

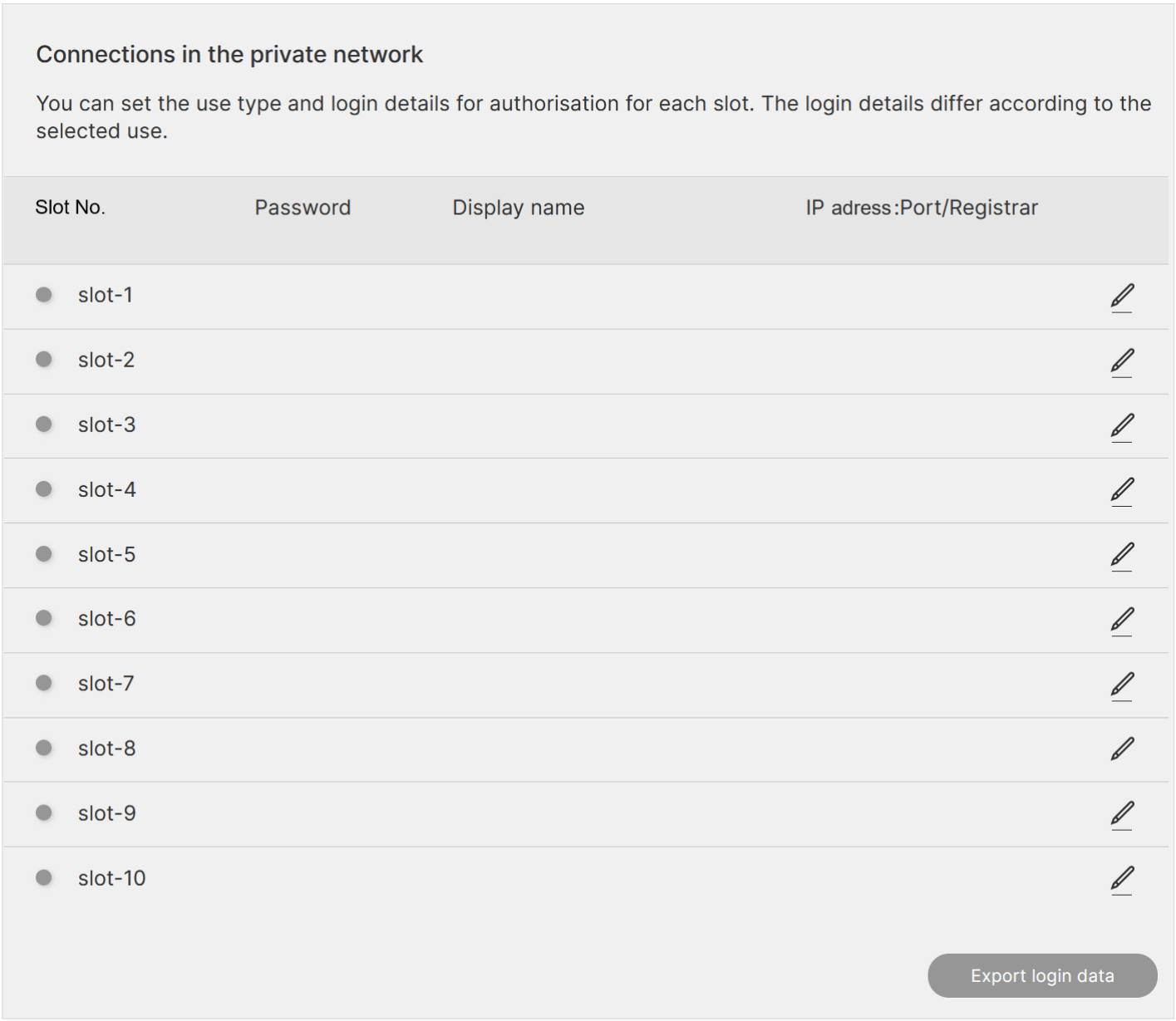


Figure 10: Device website – Connections in the private network

Meaning of the indicators:

Grey = no connection settings configured

Red = connection settings have been configured, but a connection cannot be established (e.g. server unreachable, incorrect registration details or no internet connection).

Yellow = connection settings have been configured but no device is registered.

Green = SIP participant (e.g. Gira G1) has successfully registered with the Gira F1.

The indicators are updated depending on the registration interval of the client. An intact connection may be displayed even though the connection has been disconnected in the meantime.

This can occur when power is restored after a power failure or after changing the port settings.

5.4.3. Use as a registrar/main station

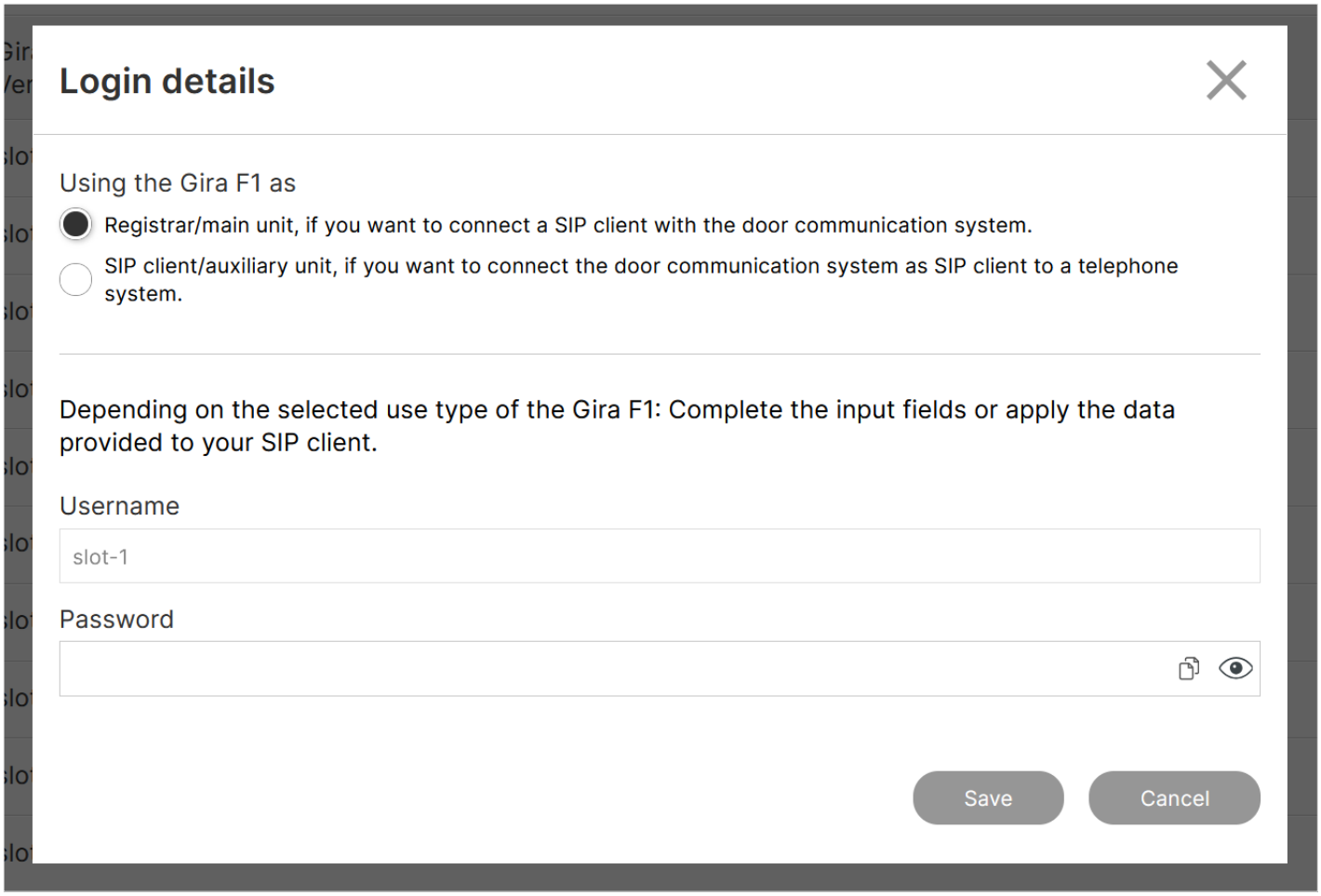


Figure 11: Use as a registrar/main station

Example: Setting up SIP door communication with Gira G1

- Go to the device website of the Gira F1 and log in.
- Open the “Network settings” tab.
- Under “Settings for the public network”, enter an IP address or activate DHCP.
- Under “Settings for the private network”, enter an IP address or activate DHCP.
- Open the “SIP door communication” tab.
- Enter the port settings under “Settings for the private network” and make a note of the number of the open port.
- Under “Connections in the private network”, select an available slot number and click on the edit symbol.
- Select “Registrar/main station” as the mode of use, enter a password and make a note of the user-name (slot-1 to slot-10) and the password. The username cannot be changed.

- Switch to the device website of the Gira G1 and log in.
- Open the “SIP door communication” tab.
- Under “Type of SIP calls”, select “Registrar”.
- Enter a name for the SIP participant in the “Display name” box. This is displayed by the participants that are called by the Gira G1 subsequently (internal call).
- In the “Address of the SIP server” box, enter the IP address from the “Settings for the private network” of the Gira F1. The Gira F1 now acts as the SIP server or registrar.
- In the “Port of the SIP server” box, enter the port number you noted for the private network of the Gira F1.
- In the “Username” box, enter the username you noted (slot-1 to slot-10).
- In the “Password” box, enter the password you noted.

- Switch back to the device website of the Gira F1 and go to the “SIP door communication” tab.
- Under “Registration details for clients from the public network”, add the registration details of the SIP door station and make a note of them.

- Switch to the set-up page for the SIP door station.
- Enter the registration details for the door station there (client on the public network).

Changing the port settings

If the port settings are subsequently changed, the SIP door station must be registered again.

5.4.4. Use as a SIP client/extension

To forward door calls from a door communication system to a telephone system, you must enter the registration details for the telephone system in the Gira F1. Please note that the registrar entry must begin with “SIP:” (see Figure 12, “Registrar” field).

If the SIP domain (Remote Domain) differs from the registrar address, enter the SIP ID in the format “username@domain” (see Figure 12, “SIP-ID” field).

If you want to secure communication using certificates, tick “Use secure communication”. Then select the procedure appropriate for your telephone system.

Connecting to cloud telephone systems

If the Gira F1 is to be connected to a cloud telephone system as an extension on the private network, please note the following:

- The private network must have internet access.
- On the private network, the Gira F1 must be assigned to the same subnet as the DNS server or the router with an integrated DNS server.

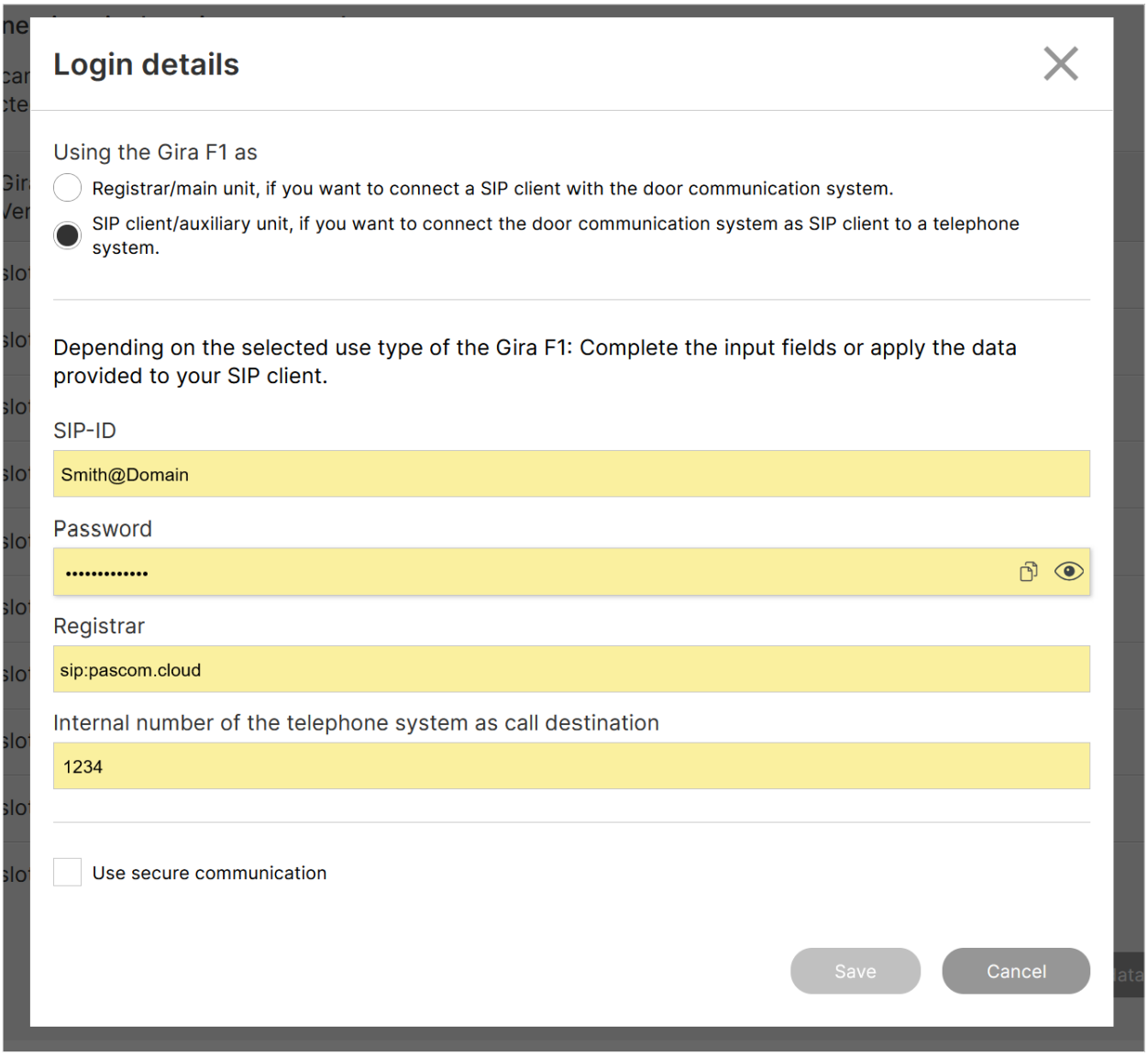


Figure 12: Use as a SIP client/extension (Sample data)

5.5. Diagnostics

On the diagnostics page of the Gira F1, you will find the following options:

- view information about memory use, the file system and processes that are running;
- carry out a restart;
- reset the device to its factory settings (KNX TP, KNX IP and SIP);
- activate programming mode for the Gira F1 KNX Bridge TP;
- activate programming mode for the Gira F1 KNX Bridge IP (LAN 1);
- in the event of an error or service request, download a log file that you can forward to the Gira hotline.

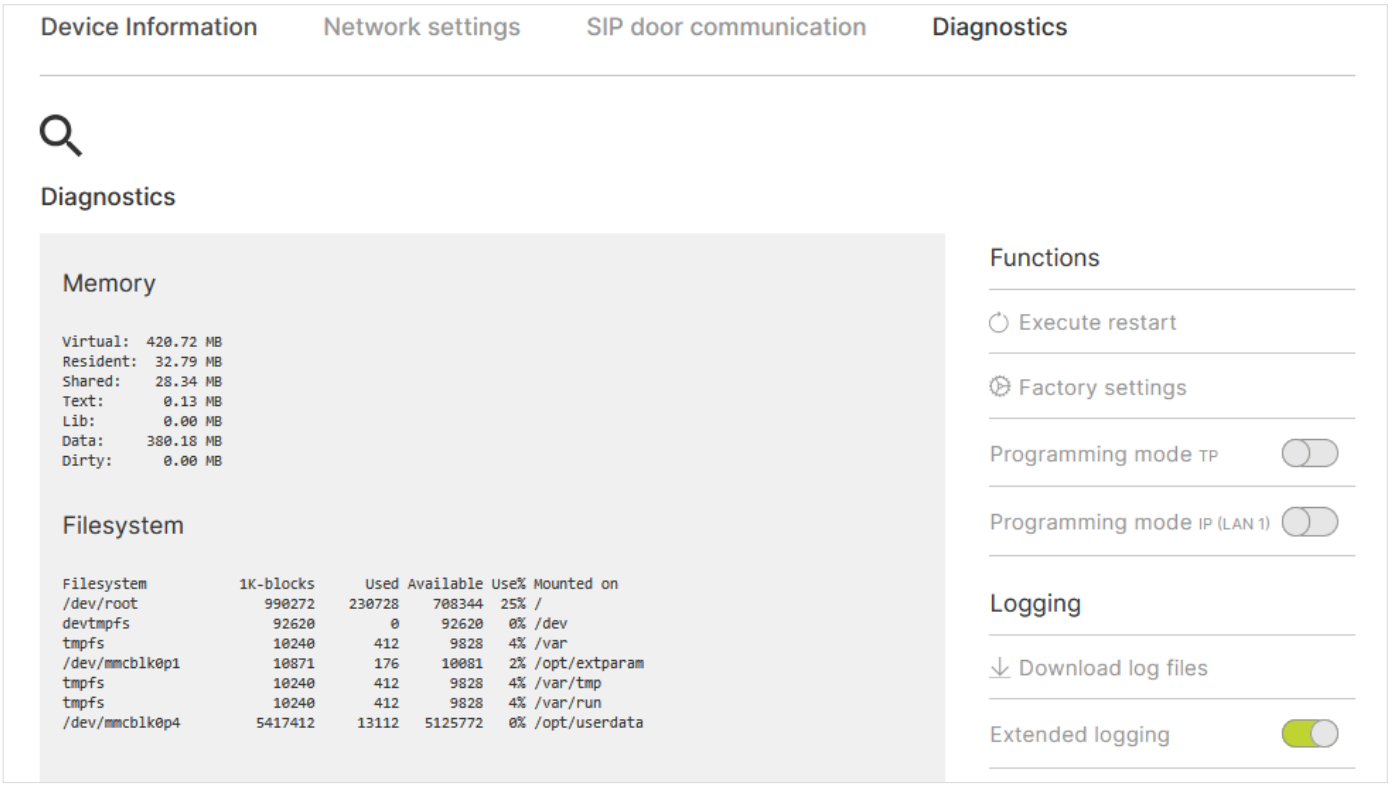


Figure 13: Device website – Diagnostics

6. Displays and operation

6.1. LED status displays

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

The LED displays have different meanings

- when the device is starting up and
- in operation.

6.1.1. LED status display when starting the device

After switching on the power supply (DC 24 V on the white-yellow connection terminal) or after the power is restored, the device shows its status with the following LED combinations:

"RUN/DIAG" LED (green)	"KNX" LED (yellow)	Meaning
off	off	Error: No supply voltage. Please check connections and power supply.
off	on	Device is starting
flashing slowly	on	The device is fully booted but not yet configured. An ETS download is required
flashing quickly	off	Error: Please contact support. The firmware cannot be started.
Both LEDs slowly flashing alternately		Error: Please contact support. The reloaded firmware cannot be started. The system is trying to activate the previous firmware (invalid firmware).

6.1.2. LED status display in operation

Once the start-up of the device is complete, the LEDs have the following meanings:

"RUN/DIAG" LED (green)	"KNX" LED (yellow)	Meaning
on	on	Normal operation: KNX TP connection has been established, no KNX telegram traffic.
on	flashing quickly	Normal operation: KNX TP connection has been established, KNX telegram traffic.
on	off	Error: Connection to KNX TP has been interrupted. Check the bus connection.
Flashing at intervals	n. a.	Network error, both networks in the same address range.

6.2. Device identification

In conjunction with the IP door communication system, the programming LED of the Gira F1 can be triggered via the device website of the commissioning door station. The programming LED lights up red until identification on the device website of the door station is complete.

Conversely, a signal can be sent to the device website of the door station by briefly pressing the programming button. Pressing the button again ends the device identification.

6.3. Factory reset

After a factory reset, the device behaves as it did when delivered. The device is not configured. This can be seen from the slowly flashing green LED (5) when the device is started up.

The following individual KNX addresses are pre-set in the factory: 15.15.255.

After a factory reset, both networks are set to DHCP.

6.3.1. Factory reset using the Gira Project Assistant

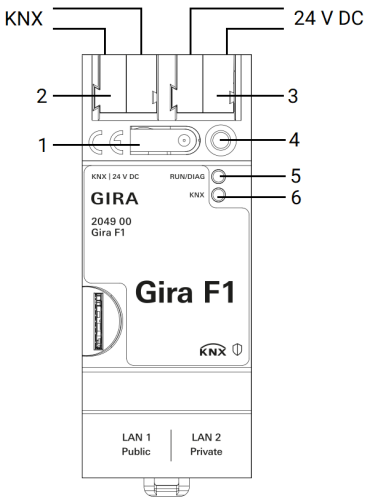
A factory reset can be carried out using the Gira Project Assistant as follows:

- Start the Gira Project Assistant and click on the “Devices on the network” tile.
- All devices located on your network are shown in this view.
- Select the Gira F1 which you want to reset to its factory settings.
- On the highlighted row, click on the gear symbol and select “Factory reset” from the menu that then opens.
- Enter the device password for the Gira F1 in the dialog box that pops up. This password can be found on a label on the device.
- The factory reset is then carried out.

6.3.2. Factory reset via the programming button on the device

The device can be reset to its factory settings by following a sequence as it starts up:

- Ensure that the device is switched off (pull out the white-yellow connection terminal).
- Press and hold the programming button (1) and switch the device on (plug in the white-yellow connection terminal)
- Continue to hold down the programming button until the programming LED (4), the operating LED (5) and the KNX LED (6) start flashing slowly at the same time.
- Release the programming button (1) for a moment, press and hold it again until the programming LED (4), the operating LED (5) and the KNX LED (6) start flashing quickly at the same time.
- The factory reset is then carried out.
- Release the programming button.
- The device does not need to be restarted after a factory reset.



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

6.3.3. Factory reset via the diagnostics page of the device

A factory reset can also be triggered via the diagnostics page of the device.

- Go to the device website of the Gira F1:
  To do so, open Windows Explorer and click on “Network”.
  The Gira F1 is displayed under “Other devices”.
  Double-click the Gira F1 symbol.
  Alternatively, you can also enter the IP address of the device in your browser.
- On the website that then opens, enter the device password for the Gira F1, which can be found on a label on the device.
- Click on Diagnostics on the top menu bar.
- On the right of the Diagnostics page, click on “Factory settings”.
- Confirm the security prompt.
- The next page displayed shows the factory reset running. As soon as it is complete, the homepage is reloaded.

6.4. Firmware update of the device

6.4.1. Firmware update via the Gira Project Assistant

A firmware update can be carried out via the Gira Project Assistant as follows:

- Start the Gira Project Assistant and click on the “Devices on the network” tile.
- All devices located on your network are shown in this view.
- Select the Gira F1 which you want to update.
- On the highlighted row, click on the gear symbol and select the item “Select firmware” from the menu that then opens.
- Select the firmware you want and click on “Start update”.
- Enter the device password for the Gira F1 in the dialog box that pops up.
- The firmware is then updated. This can take several minutes. Do not disconnect the device from the network during this time.

6.4.2. Local firmware update without internet access

In addition to an online update, a local update without internet access is possible. The firmware file can be selected using the “Select file” button and then started by means of the “Update firmware” button. In this case, the user is responsible for ensuring that the update is compatible (See section 6.4.3 “Compatibility of ETS catalogue entry and firmware”). A downgrade to an older version is not possible with this process.

6.4.3. Compatibility of ETS catalogue entry and firmware

The version numbers of the ETS catalogue entry and the firmware are structured according to the pattern X.Y. The main number X of the version in question indicates whether the catalogue entry and firmware are compatible. This is the case if the two main numbers are identical. The second part of the version number Y has no significance for compatibility. It simply indicates updates within the version.

If new firmware has a higher main number, there is no guarantee that that version is compatible with an old ETS catalogue entry. It is therefore advisable always to remove the application program from the device before an update and only to use the new catalogue entry following it.

If the main numbers are the same, it may be necessary to use a new ETS catalogue entry to enable full functionality. This is not necessarily the case, however, if the new functions are not used in your project.

7. Technical data

KNX TP Medium	TP1
Security	KNX Data Secure (X-Mode)
Commissioning mode	S mode (ETS)
KNX supply	21...30 V DC SELV
Current consumption KNX	typ. 2.5 mA
KNX connection	Bus connection terminal
External supply	
Voltage	24...30 V DC
Power consumption	2 W (at 24 V DC)
Connection	Connection terminal
IP communication	Ethernet 10/100 BaseT (10/100 Mbit/s)
IP connection	2× RJ45 jack (public/private)
Ambient temperature	0 °C to +45 °C
Storage temperature	-25 °C to +70 °C
Installation width	36 mm (2 MW)

7.1. Accessories

Additional power supply
Order No.: 1296 00

KNX power supply 320 mA
Order No.: 2122 00

8. Frequently asked questions (FAQ)

8.1. General network and IP settings

What do I have to consider before changing the router in the private network?

If DHCP has been selected in the IP settings of the connected devices, those devices (e.g. Gira F1, Gira X1, Gira G1) will be given new IP addresses as a result of the change of router. Access of the Gira G1 SIP client to the registrar of the Gira F1 (e.g. slot-1) is therefore no longer possible. The new IP addresses must be entered on the device websites for the Gira F1 and Gira G1 so that the door calls can be forwarded correctly again.

If a Gira G1 and a Gira X1 are used, their IP addresses must also be updated for a properly functioning client connection.

8.2. When using the ETS

Why is the IP address entered in the ETS not transferred to the device?

The IP address can only be transferred to the device if the individual address has been programmed.

Why is the IP address entered on the device website not used by Gira F1?

Remember that the IP address can be entered on both the device website and in the ETS. If you have first entered the IP address on the device website and then programmed the device in the ETS, the IP address used there will be used. If “Obtain IP address automatically” is selected in the IP settings of the ETS, the IP address entered on the device website can be overwritten.

If the Gira F1 is accessible via an IP site, the IP address of that other site is shown on the device website.

8.3. When using SIP door communication systems from other manufacturers

What do I have to consider before changing devices?

If the Gira F1 has to be replaced for servicing, the IP settings of LAN 1 and LAN 2 must be configured again. The system documentation must be followed for this. When using DHCP, check that the Gira F1 has received the same IP addresses.

If a door station is used and/or a Gira G1 as a home station, the IP addresses of the call button and registrar (Gira F1) must be adapted.

The SIP settings can be re-imported with the previously exported and saved json file.

In the ETS project of the building, the IP side (LAN 1) must be loaded with the individual address and the application of the Gira F1.

In the ETS project of the home, the TP side must be loaded with the individual address and the application of the Gira F1.

How do I back up the data configured on the device website?

Use the export function on the “SIP door communication” tab to back up the settings of the various networks.

9. Licence Agreement

The contractual conditions for your use of the software as the “Licensee” are specified below.

By accepting this Agreement and installing the Gira F1 device software or using a “Gira F1 device”, you are concluding a contract with the company Gira, Giersiepen GmbH & Co KG and declaring that you are bound by the provisions of this Agreement. This is exclusively a licence agreement and not an agreement for the sale of goods.

1. Definitions

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

Licensee: The lawful recipient of the Gira F1 device software.

Gira F1 devices: The term Gira F1 devices means the Gira F1 devices consisting of a hardware device and the associated firmware.

Firmware: Software embedded in the Gira IP device and used to operate it.

Commissioning software: The commissioning software refers to the application program provided to set up and configure the Gira F1 devices.

Third-party software: Third-party IP

This product uses software from third-party sources in the context of the GNU General Public License (GPL) and Lesser GNU General Public License LGPL and of the Berkeley Software Distribution (BSD) and MIT licence.

The software packages used in this product and licensed as indicated above are described on the device website under the heading “Licences”.

The licence texts of the GPL and LGPL are available on the following website: http://www.gnu.org/licenses/licenses.html

2. Subject of the licence

The subject of this Agreement is the software provided on the Gira F1 and the associated documentation in written or electronic form.

3. Rights of use for the Gira F1 software

The Licensor grants the Licensee a non-exclusive, indefinite, non-transferrable right that cannot be sub-licensed to use the firmware in accordance with the business conditions of this user licence on the Gira F1 device for the purposes and areas of application specified in the applicable version of the documentation (which is provided in printed form and also as online help or online documentation).

The Licensee undertakes to ensure that anyone who uses the program does so only within the framework of this Licence Agreement and observes this Licence Agreement.

4. Restrictions to the rights of use, transfer to third parties

4.1. The Licensee is not entitled to use the Gira F1 software in any way other than that described here or to copy, edit or transfer it in whole or in part. Excepted from this is one (1) copy that is prepared by the Licensee exclusively for archiving and backup purposes.

4.2. The Licensee is not entitled to apply reverse engineering techniques to the Gira F1 software or to convert the Gira F1 software into another form. Such techniques include, in particular, disassembly (conversion of binary encoded machine commands of an executable program into an assembly language that can be read by humans) and decompilation (conversion of binary encoded machine commands or assembly commands into source code in the form of high-level commands).

4.3 The licence for the Gira F1 software is bound to the use of the Gira F1 device. Transfer of the Gira F1 software to third parties or making the software accessible to third parties is permissible only in conjunction with transfer of the Gira F1 devices.

On transfer to third parties, the rights of use of the Licensee shall expire.

The Licensee may transfer the software and all of the licence keys required to use the software, with the exception of software marked accordingly, to third parties only if

4.3.1 the Licensee removes all backup copies and licence keys required to use the software from its system by deletion and/or deinstallation.

4.3.2 the third party undertakes to comply with these terms of use vis-à-vis Gira before transfer and use.

The Licensee shall expressly draw the attention of the third party to these terms of use before passing on the Gira F1 device.

4.4. The Licensee is not entitled to rent or lease the Gira F1 software or to issue sub-licences to the program.

4.5. The Licensee requires the written consent of the Licensor to create and distribute software that is derived from the Gira F1 software.

4.6. The mechanisms of licence management and copying protection for the Gira F1 software may not be analysed, published, circumvented or disabled.

5. Ownership, confidentiality

5.1. The Gira F1 software and the documentation (which is provided in printed form and also as online help or online documentation) and any changes to it are and shall remain the property of the Licensor. The Licensor also reserves all further rights to and shares in the subject of the Licence. The Licensee shall respect those rights.

5.2. The subject of the licence, i.e. the software and the documentation (which is provided in printed form and also as online help or online documentation) may not be passed on to third parties, either in whole or in part, whether in return for payment or not. The Licensee agrees to use the licence exclusively for the purpose of exercising its rights under this licence for use.

6. Alterations

The Licensor may extend, improve or otherwise alter the subject of the licence at any time without notice. The terms of the licence shall continue to apply.

7. Warranty

The Gira F1 software is supplied with the third-party software listed in Section 1. No warranty is provided for the third-party software.

As far as the licence terms for that software are concerned, please see the links (URLs) specified in Section 1. The terms are included in this Agreement.

The Licensor shall make the complete, machine-readable source code of the third-party software listed under Section 1 (open source software) available to the Licensee on request within 36 months of delivery of the software. The Licensor shall charge the Licensee the shipping costs for this.

7.1 The Gira F1 software and the documentation (which is provided in printed form and also as online help or online documentation) shall be made available to the Licensee in the latest applicable version. The warranty period for the Gira F1 software is 24 months. During this time, the Licensor shall guarantee the following:

- The software is free of material and manufacturing defects on handover.
- The software works according to the documentation provided in its latest applicable version.
- The software is capable of running on the computer stations specified by the Licensor.

Fulfilment of the warranty shall take place exclusively by replacement delivery.

7.2 Otherwise no warranty is provided for the absence of defects in the Gira F1 software and its data structures. The warranty also does not cover defects that result from improper handling or other causes outside the sphere of influence of the Licensor. Further warranty claims are therefore excluded.

8. Liability

The Licensor is not liable for damages for loss of earnings, loss of data or other financial losses that come about in the context of use of the Gira F1 software.

This limitation of liability applies to all compensation claims of the Licensee, whatever the legal grounds. The amount of liability is limited to the purchase price of the product.

The exclusion of liability shall not apply to damage caused by malicious intent or gross negligence on the part of the Licensor. Claims of the Licensee based on the statutory regulations regarding product liability are also unaffected by the exclusion of liability.

9. Privacy

By concluding this Licence Agreement, you are accepting the latest applicable version of the GIRA privacy policy. See http://www.gira.de/impressum/datenschutz.html

10. Applicable law and court of jurisdiction

This Agreement is governed by the law of the Federal Republic of Germany, with the express exception of the UN Convention on the International Sale of Goods.

The place of jurisdiction is the court responsible for the registered office of the Licensor.

11. Termination

This Agreement and the rights granted in it shall end if the Licensee fails to fulfil one or more provisions of the Agreement or terminates the Agreement in writing. In this case, the Gira F1 software and the documentation (which is provided in printed form and also as online help or online documentation) supplied, including all copies, shall be returned in full promptly and without request. Any claim to reimbursement of the price paid is excluded in this case.

When the Agreement comes to an end, the licence for use of the Gira F1 software shall expire. In this case, the Gira F1 devices shall be taken out of operation. Further use of the Gira F1 devices without a licence is excluded.

12. Ancillary agreements and amendments to the Agreement

Ancillary agreements and amendments to the Agreement shall take written form to become valid.

13. Exception

All rights not expressly mentioned in this Agreement are reserved.