

Gira HomeServer/FacilityServer, Gira Giersiepen GmbH & Co KG

## Change Log v4.7.0

Status 16/07/2018

# GIRA

## System requirements

Operating system: Windows XP, Windows 7, Windows 8, Windows 10

Free hard drive space: at least 1 GB

RAM: at least 2 GB

Software platform: at least Microsoft .NET 4.5

## Supported devices

The Expert Software 4.7.0 is to be used in conjunction with the following end devices:

- HomeServer 4
- FacilityServer 4

## Devices not supported

The following device generations are no longer supported by the Expert software 4.7.0:

- HomeServer 3
- FacilityServer 3
- HomeServer 2

# GIRA

## Supported clients

The Expert Software 4.7.0 is only compatible with the following Gira clients:

- Gira QuadClient v4.7.0
- Gira HomeServer iOS-App v4.7.0
- Gira HomeServer Android-App v4.7.0 \*\*\*
- Gira G1 HS-Client v100.0.xxx \*\*\*
- Gira HS Client v4.7.0

\*\*\* This version is still under development, so a delivery date can not be named at this time.  
(As of 16.07.2018)

## Update information

It is only possible to update to firmware version 4.7.0 from the following versions:

- **4.5.0.160913R**
- **4.6.0.170320**

For more detailed information on the firmware update, see "Update and settings for HomeServer v4.7.0".

## What's new in Expert v4.7.0?



### Transport encryption

- Encrypted communication across all interfaces in accordance with the latest TLS 1.2 standards.
  - QC interface
  - HS Client
  - Communication object gateway
  - Analysis of websites/IP devices
  - Transfer of projects/firmware/retentive memory
  - Portal login
  - HS Monitor (HTML version)
- TLS v1.2 support (and TLS v1.0 for Gira Control devices with XP)
- The HomeServer/FacilityServer can create its own SSL certificates.
- Certificate management for certificates generated by third parties.
- Certificate management is not part of the Expert software. You can find all information on the current certificates at [https://HS\\_IP/hscert](https://HS_IP/hscert).  
This URL is also used to generate certificates from the HS/FS and/or to upload certificates onto the HS/FS.
- You can find the settings for these IP ports in Expert under *Master data -> Project -> Project settings -> Network -> Security*.
- For more information on this, see "**Manage certificates**" and "**Security**" in the Expert help.

# GIRA

Compatibility table			
Client / Tool	Version	Firmware 4.6.0	Firmware 4.7.0
QuadClient	4.5.0	✓	✗
QuadClient	4.7.0	✗	✓
HomeServer iOS app	up to 4.6.0	✓	✗
HomeServer iOS app	4.7.0	✓	✓
HomeServer Android app	up to 4.5.1	✓	✗
HomeServer Android app	4.7.0	✓	✓ ***
G1 HS-Client	100.0.153	✓	✗
G1 HS-Client	100.0.xxx	✓	✓ ***
Browser access (/hs /hslist etc.)	-	✓	✓ *
HS Client	up to 4.5.0	✓	✗
HS Client	from 4.7.0	✗	✓
Communication object gateway	from 4.7.0	✓	✗
Analysis of websites/IP devices	from 4.7.0	✓	✓
Transfer of projects, firmware and retentive memory	from 4.7.0	✓	✓
Portal login		✓	✓
HS Monitor	up to 1.0.130305	✓	✗
HS Monitor (html version)	from 4.7.0	✗	✓
Endpoints (https/http access)	from 4.7.0	✗	✓
Endpoints (WebSocket access)	from 4.7.0	✗	✓

# GIRA

Compatibility table			
Client / Tool	Version	Firmware 4.6.o	Firmware 4.7.o
S1 Windows client 32/64 bit	1.0.0.70		 **






\*\*\* This version is still under development, so a delivery date can not be named at this time.  
(As of 16.07.2018)

\*\* Access via http only (activation via Project settings/Security)

\* Yes, but the operating system and browser used must accept the certificate used by the HomeServer/FacilityServer. There are various options for this, which are described:

in the "Certificate management" chapter  
and

in the table below.


Information on calling HTTPS HomeServer/FacilityServer pages via a browser from version 4.7.0 or higher						
certificate used in the HS project	Browser	Version	Operating system	Version	Status	Status condition
Self-signed certificate	Google Chrome	66	Windows	<ul style="list-style-type: none"> <li>- 7</li> <li>- 8</li> <li>- 10</li> </ul>		The certificate must be ... <ul style="list-style-type: none"> <li>- temporarily accepted in the browser</li> </ul> <b>or</b> <ul style="list-style-type: none"> <li>- imported into the Windows certificate manager</li> </ul>
Official root certificate	Google Chrome	66	Windows	<ul style="list-style-type: none"> <li>- 7</li> <li>- 8</li> <li>- 10</li> </ul>		-
Self-signed certificate	Microsoft Internet Explorer	11	Windows	<ul style="list-style-type: none"> <li>- 7</li> <li>- 8</li> </ul>		The certificate must be ... <ul style="list-style-type: none"> <li>- temporarily accepted in the browser</li> </ul> <b>or</b> <ul style="list-style-type: none"> <li>- imported into the Windows certificate manager</li> </ul>
Official root certificate	Microsoft Internet Explorer	11	Windows	<ul style="list-style-type: none"> <li>- 7</li> <li>- 8</li> <li>- Embedded Standard 7</li> <li>- POSReady 7</li> </ul>		-
Self-signed certificate	Microsoft Edge	41	Windows	<ul style="list-style-type: none"> <li>- 10</li> </ul>		The certificate must be ... <ul style="list-style-type: none"> <li>- temporarily accepted in the browser</li> </ul> <b>or</b> <ul style="list-style-type: none"> <li>- imported into the Windows</li> </ul>

# GIRA

Information on calling HTTPS HomeServer/FacilityServer pages via a browser from version 4.7.0 or higher						
certificate used in the HS project	Browser	Version	Operating system	Version	Status	Status condition
						certificate manager
Official root certificate	Microsoft Edge	41	Windows	- 10	✓	-
Self-signed certificate	Mozilla Firefox	60	Windows	- 7 - 8 - 10	✓	The certificate must be ... - temporarily accepted in the browser <b>or</b> - imported into the Firefox certificate manager
Official root certificate	Mozilla Firefox	60	Windows	- 7 - 8 - 10	✓	-
Self-signed certificate	Apple Safari		iOS	- 10 - 11	✓	- The certificate must be ... - temporarily accepted in the browser or - imported into the iOS certificate manager
Official root certificate	Apple Safari		iOS	- 10 - 11	✓	-
Self-signed certificate	Google Chrome	64	Android	- 7 - 8	✓	The certificate must be ... - temporarily accepted in the browser or - imported into



# GIRA

Information on calling HTTPS HomeServer/FacilityServer pages via a browser from version 4.7.0 or higher						
certificate used in the HS project	Browser	Version	Operating system	Version	Status	Status condition
						the Android certificate manager
Official root certificate	Google Chrome	64	Android	- 7 - 8		-

## HTML-based HS Monitor

The HS Monitor has been completely revised and is available as an HTML version in the browser starting from this version.

The HS Monitor is called up in the Browser under the following URL:

`HTTPS://HS_IP/opt/hsmonitor/index.html`

or

`HTTPS://HS_IP/opt/hsmonitor/index.html#key=[Key]`

When the HS Monitor is started, the login mask appears. The key for the communication object gateway data connection defined in the Expert project can be entered here.

For more information on this, see "**HS Monitor - Use and operation**" in the Expert help.

# GIRA

## Syslog protocol function

Syslog is a standard when it comes to transferring log messages in an IP computer network.

The system messages created by the HS/FS can be transferred by Syslog protocol to other parties.

The last 100 messages received are displayed under the Syslog category on the Debug page.

For more information on this, see "**Syslog**" in the Expert help.

## New HTML help in the Expert software

The Expert help has been converted completely to HTML. All documents that were previously accessed via the Windows help, PDF or HTML are now available in HTML format.

You can access the HTML pages using any browser.

Note: Only the QC help is still available in PDF format.

## URL endpoints

The URL endpoints provide new possibilities for implementing free visualisations.

The URL endpoint function has been added to almost all HS objects for this purpose. This means that external access is permitted to all these HS objects directly via HTTPS or WebSocket. This provides greater freedom to design free visualisations through the use of the latest browser technologies: HTML5, JavaScript. These visualisations can also be implemented in modern web development tools outside the Expert software.

HomeServer objects (e.g. communication objects, scenes, sequences, etc., see documentation) can be retrieved or changed via a URL using an HTTPS call.

The HS objects are also available via a connection using WebSocket (WS) as an alternative to access via HTTPS.

For more information on this, see "**URL endpoints**" in the Expert help, as well as the Gira download area at [http://www.hs-help.net/hshelp/gira/other\\_documentation/Schnittstelleninformationen.zip](http://www.hs-help.net/hshelp/gira/other_documentation/Schnittstelleninformationen.zip)

# GIRA

## HSL 2.0: New logic module SDK

From firmware 4.7, there is a new approach to the development of logic modules with some additional options.

Several tools are provided for development. There is also a step-by-step "How To" for setting up your own development environment, in addition to the comprehensive documentation on the creation and function of these modules.

For more information on this, see "**Logic module SDK**" in the Expert help, as well as the Gira download area at [http://www.hs-help.net/hshelp/gira/other\\_documentation/Schnittstelleninformationen.zip](http://www.hs-help.net/hshelp/gira/other_documentation/Schnittstelleninformationen.zip)

## Free visualisation: New designs

Two new full-screen visualisation designs are available under Project settings interface/Designs:

- 1024x600 full-screen design (for Gira Control 9 Client 2)
- 1920x1080 full-screen design (for displays with full HD resolution)

## Errors fixed in Expert v4.7.0

- Fixed: telegram delay logic module – help adapted.
- Fixed: from Expert software 4.3.0 – internal communication object "Memory capacity assigned" is not described by the HomeServer/FacilityServer.

## What's new in QuadClient / QuadConfig v4.7.0?

### Transport encryption

- Encrypted communication between QuadClient and HomeServer/FacilityServer according to the latest TLS 1.2 standards.
- See also the help documentation.

### QuadClient Starter

- The QC Starter is a new Windows application which is installed on the client device, e.g. PC, Gira Control 19 Client 2.
- The QC Starter connects to the HomeServer/FacilityServer and then automatically downloads the Gira QuadClient application from the server if this not already installed on the client device.
- Following the one-time installation of the QuadClient Starter, the QuadClient no longer needs to be updated manually for future HS/FS updates on the end devices, such as Gira Control 19 Client 2 or Gira Control 9 Client 2, as the QuadClient Starter will always automatically download and install the latest QuadClient version from the HomeServer whenever a new version is available.
- For fast and easy access to the required HS/FS, you can create up to 20 HS/FS profiles in the QuadClient Starter. The number of profiles is unlimited in theory, but only a maximum of 20 profiles is assured.
- Functions:
  - Create / Delete HS/FS profiles
    - Profile name
    - IP/URL
    - Port
    - Start / Download QuadClient

# GIRA

- Define default profile
  - Kiosk mode
    - Activate / deactivate
    - Kiosk pin
    - Use PIN protection
  - Call the QuadClient Config Editor directly
- You can use the QC Starter from Expert version 4.7.0 and higher.
  - See also the help documentation.

## **User authorisations:**

You can now choose between four possible authorisations depending on the user.

Authorisations enable you to specify more specifically which system functions a user can use within the QuadClient.

The authorisations are guest user, group member, group administrator and system administrator. A project must contain at least one system administrator. When existing projects are handed over, at least one user must be appointed as the system administrator. The "system user" authorisation has been replaced by "group administrator". As a result, you no longer need to enter the system user password when logging onto the QuadClient for the first time.

System page redesign: The available configurations are offered according to the user currently logged in and his authorisations.

- See also the help documentation.

# GIRA

## **Change of user / user logoff**

- A user can be changed directly in the QuadClient at runtime in version 4.7.0 and higher. The QuadClient no longer requires a restart. As of this version, the "User list" option is available in the system settings for the QuadClient, where you can select the required user.
- In addition, you can trigger a change of user / user logoff using a communication object. To do this, each user is given a fixed ID which you can then select via the communication object.
- The communication object for the change of user / user logoff must be assigned to the required end device profile.
- You can also define what is to happen if the client device is idle for a certain amount of time. In this case, the user can be changed automatically, e.g. to the guest user, or the user can be logged off.
- See also the help documentation.

## **Save user password**

- The person performing the configuration can specify in the QuadConfig whether the user is allowed to save his password in the QuadClient.
- For users with guest user authorisation, this option is not available here.
- See also the help documentation.

# GIRA

## Locate end devices within a project

- End devices / client devices on which a QuadClient is running can now be located precisely within the building.
- This means that you can create end device profiles in the QuadConfig.
- You can assign additional information to each end device profile, including:
  - Designation
  - Device type
  - MAC address
  - Communication object for the indoor temperature
  - Communication object for the change of user
  - Button assignment for the user change rapid selection
  - Hold / do not hold door communication
- The assignment between the client device and end device profile can be defined directly both in the QuadConfig and in the QuadClient.
- See also the help documentation.

# GIRA

## Configurable button assignment/function buttons

- The four buttons in the navigation bar at the bottom of the QuadClient can now be freely configured.
- The buttons are configured directly in the QuadClient.
- The user performing the configuration in the QuadClient must have one of the following authorisations:
  - Group administrator
  - System administrator
- You can choose between the following functions:
  - Favourites
  - MyTouch
  - Direct function
  - Note
  - Change of user
  - Browser
  - not assigned
- See also the help documentation.



# GIRA

## Symbol selection dialog in the QuadConfig

- To allow quick and easy selection of the correct symbol, the following functions have been added to the symbol selection dialog:
  - View: Selection of different views for the symbol preview
  - Categories: Groups the symbols by topic in categories
  - Subcategory: Groups the symbols by topic in subcategories
  - Filter: Direct keyword search in the symbol preview
  - Window size: Changes the size of the dialog window variably
- Symbol preview in the properties area of the function templates and menu tiles.
- See also the help documentation.

## QuadClient Config Editor

- To allow quick and easy selection of the correct design, predefined display profiles have been added to the design settings for all Gira Control devices, thus reducing the amount of effort required to configure parameters.
  - Individual
  - Control 19 Client 1
  - Control 19 Client 2
  - Control 9 Client 1
  - Control 9 Client 2
  - Control 9 Client 1 (portrait format)
  - Control 9 Client 2 (portrait format)

# GIRA

## Project cache

- Project data is stored in the system throughout the lifetime of the project so that the QuadClient starts faster if the project has not changed, especially for remote connections using port forwarding.

## Plug-ins

- The new QC version is based on .NET 4.5.
- If plug-ins are used which are not included in the standard scope of delivery (e.g. Gira AppShop or 3rd party plug-ins), the plug-ins need to be updated.  
The easiest way to do this is by copying the updated plug-ins (hsp file) immediately after *completing* the installation of *HS Expert* and before importing the project into a "migration" folder. (Complete path: %Public%\Documents\Gira\HS+FS Experte 4.7.0\quad\plugins\migration\)
- Information for 3rd party developers: More information is available in the developer forum at: <http://www.entwicklerforum.gira.de>

## Errors fixed in the QuadClient / QuadConfig v4.7.0

- Fixed: from QuadClient 4.5.0 – the building structure sorting is not transferred.
- Fixed: from QuadClient 4.5.0 – when selecting design 2, is is not possible to call the plug-in via the menu button. One-quadrant view.
- Fixed: from QuadClient 4.5.0 – spelling mistake under scene function template.
- Fixed: from QuadClient 4.4.0 – when duplicating function templates, the settings in the original function template also change.
- Fixed: from QuadClient 4.4.0 – when using MyTouch with separate user groups, incorrect buttons are displayed to other users.
- Fixed: from QuadClient 4.4.0 – translation error in the timer of function template 1-118.
- Fixed: from QuadClient 4.4.0 – if an annually recurring date is selected in the timer for the year under the entry for \*\*, the date is not displayed in the timer overview.
- Fixed: from QuadClient 4.4.0 – open/close window status icons can be used in the "Switching plus 1-101" function template.

**Help documentation**

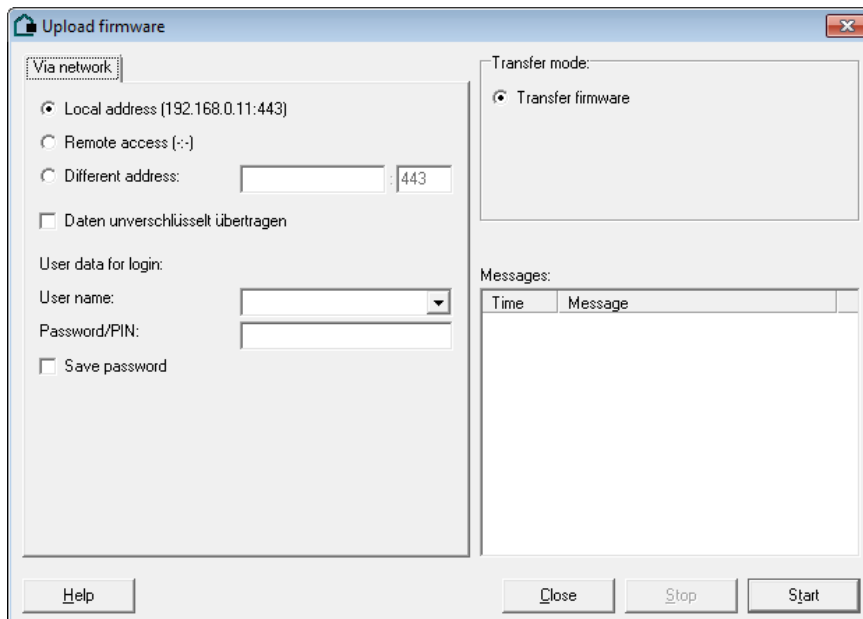
# GIRA

## Firmware update

### Update and settings for HomeServer v4.7.0

#### Upload firmware

Before you can transfer a project using Expert v4.7.0, you must update the firmware. A new transfer dialog is available in v4.7.0.



Note the following:

Back up your retentive data so that you can use it again if the update fails.

**A firmware update can only be carried out on HomeServers on which at least version 4.5.0.160913R or 4.6.0.170320 is installed.**

Please note that there is an "R" after the version number for a 4.5.0 version. This "R" means that the "recovery operation" has been successfully performed. The recovery operation reformats the firmware partition so that a renewed firmware transfer via the network does not fail. The recovery operation is implemented in Expert versions 4.1.0, 4.2.0, 4.2.1, 4.3.0, 4.4.0 and 4.5.0.

If you have a 4.5.0.160913 version on your HomeServer, in other words, without the recovery marking, you must perform a one-time transfer of the firmware via the network again using Expert v4.5.0. Afterwards, the firmware is displayed with the recovery marking.

If firmware 4.6.0 is already installed on the HomeServer, you can install firmware 4.7.0 directly via the network. Applicable from HomeServer index status 21 and FacilityServer index status 17.

# GIRA

The transfer must take place on the currently active port. This means that if the HomeServer is currently running with v4.5.0 and communicates on port 80 (http), firmware 4.7.0 must be transferred on port 80 (http).

If firmware 4.7.0 has been transferred successfully, port 443 (https) is activated. The http port also remains active until the first project is transferred.

When a project is transferred, both ports can be changed from the 4.7.0 version. The http port can also be activated/deactivated (see Project settings/Security).

**Once firmware version 4.7.0 has been transferred, an earlier version can no longer be transferred via the network (see Downgrade).**

# GIRA

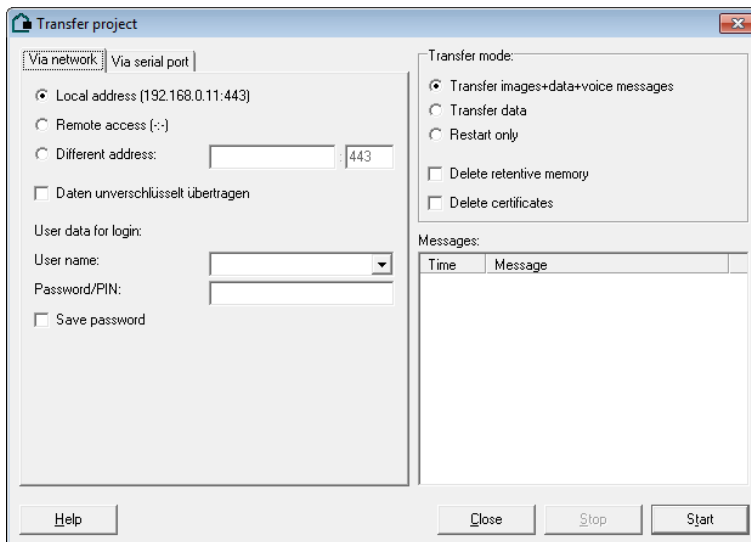
## Update via the router

In the case of a remote firmware update/project update via a router, pay attention to port forwarding. In other words, by deactivating the unencrypted port (http) and activating the encrypted port (https), it may no longer be possible to reach the HomeServer via port forwarding.

**In cases such as this, make sure that it is possible to access the router before updating the firmware/project in order to reconfigure port forwarding.**

## Transfer project

A new transfer dialog is available in version 4.7.0.



Note the following:

- The transfer is encrypted by default (TLS).
- By activating "Transfer data unencrypted", you can also transfer a project without TLS. To do so, the unencrypted port must be active (see Project settings/Security).
- It is no longer possible to calculate the transfer duration beforehand. As long as a transfer takes place, the progress bar pulsates.

## Downgrade

It is only possible to downgrade to an earlier version than 4.7.0 via serial transfer (RS232). Note the following:

- Use the serial firmware transfer tool from Expert 4.5.0 for the downgrade  
C:\Program Files\Gira\HS+FS\HS+FS Experte 4.5\firmware\fwupdate.exe

# GIRA

- For HomeServer index statuses <21 and FacilityServer index statuses <17, select firmware version 4.5.0 from the HS4 firmware folder.
  - For HomeServer index statuses >=21 and FacilityServer index statuses >=17, select firmware version 4.6.0.  
You can find this in the download area of the Gira homepage.
- **Once the firmware has been transferred, the HomeServer starts with no active port. It is essential to serially transfer a project.**  
If your project is very large and will therefore take a long time to transfer, select the "Transfer data" option as the transfer mode.  
You can select the "Transfer images+data+voice messages" option to transfer the required project again via the network.
  - Transfer the backed up retentive data.

---

## **Note: Downgrade**

The serial upgrade and downgrade via RS232 transfer has been tested in the Gira test laboratory with

- Windows Surface
  - Microsoft Windows 10 Professional
  - USB to Serial Adapter (manufacturer IGEL)
-

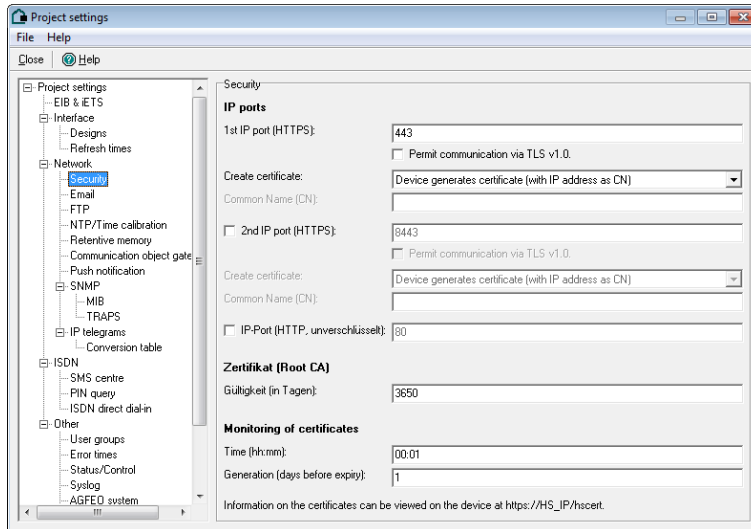


# GIRA

## Project settings

### Network

As of version 4.7.0, there is an additional "Security" page in the project settings. This is where port forwarding is configured.



# GIRA

## Security

### IP ports

The following interfaces are available for all ports for secure communication specified in the following:

Interface	Call
Lists	<HS IP address>/hslist
Visu / Menu / Query	<HS IP address>/hs
QuadClient / Apps	App
Certificate management	<HS IP address>/hscert
Communication object gateway	<HS IP address>/cogw
HSUpload area	<HS IP address>/opt

Two ports are available for secure communication (1st IP port (HTTPS) and 2nd IP port (HTTPS)). Only the 1st IP port (HTTPS) is active by default. The 2nd IP port (HTTPS) can be used for external communication, for example, if TLS v1.0 communication has been activated for the 1st IP port (HTTPS) and this is not to be open outside the network.

The HomeServer generally communicates via TLS v1.2. However, if you want the HomeServer to be accessed with a HomeServer client (HS client or QuadClient) that is installed on a Windows XP system, you must enable the "Permit communication via TLS v1.0" option, because operating systems based on Windows XP (Windows XP Embedded (Gira Control Client 9), Windows XP POSReady (Gira Control Client 19)) do not yet support the TLS v1.2 standard.

---

**Note:** If you are using a Gira Control 19 Client 2 and/or Gira Control 9 Client 2, the option must **not** be enabled, because Windows 7 is installed on these Control devices.

---

# GIRA

The "Create certificate" setting specifies whether the HomeServer creates its own certificate or whether a certificate can be loaded onto the HomeServer via the [https://\[HS IP\]/hscert](https://[HS IP]/hscert) page. If the HomeServer creates its own certificate, it is still possible to determine whether the certificate is based on the IP address of the HomeServer or a specific URL (called Common Name (CN), e.g. "homeserver.giradns.com"). If it is possible to use the HomeServer's "own" certificate, select the third option ("Load certificate onto the device"). Note that an updated certificate must be uploaded once the certificate has expired.

## Certificate

The following descriptions apply to certificates that were created by the HomeServer itself.

If the firmware of a HomeServer is updated to 4.7.0 for the first time, a root certificate (issuer's certificate) is created automatically. For example, for a HomeServer with IP address 192.168.0.11, a root certificate with the Common Name (CN) HS-192.168.0.11 is created. This root certificate has a validity of 10 years from its creation date, by default. Each HomeServer has its own root certificate.

For each active port, a subordinate certificate (applicant certificate) is created, which is valid for 90 days by default. Normally, a HomeServer automatically creates a new certificate one day before the subordinate certificate expires, which is also valid for 90 days. A browser only ever sees the subordinate certificate. The short validity period ensures that a "hacked" certificate cannot be misused for long.

The certificates created by the HomeServer are classified as not-trusted by current browsers, as browsers only ever trust certificates which were created by an official CA (Certificate Authority). An official CA can only be issued to a URL and not to an IP address. The owner of the URL must be verified by the CA.

See also Importing the HomeServer certificate into Windows, iOS and Android.

# GIRA

## **Certificate (Root CA)**

You can set the validity of the root certificate in days under "Certificate (Root CA)". 3650 days (=10 years) is set by default.

## **Monitoring of certificates**

The "Time (hh:mm)" setting defines the time when the validity of the certificate (or certificates, if using the 2nd IP port (HTTPS)) is checked while in operation. The default time is 00:30.

The value entered in "Generation (days before expiry)" specifies the number of days before the certificate expiry date that the HomeServer generates a new certificate. The default setting is one day before the existing certificate expires.

The "Time (hh:mm)" and "Generation (days before expiry)" settings apply to both certificates, if activated.

## **Certificate management**

### **Importing the HomeServer certificate into Windows**

The following steps explain how to integrate the HomeServer certificate in the Windows certificate manager. As a result, you avoid the browser security check on a client (Control 9 or Control 19). This is absolutely essential, for example, to enable a URL call in the QuadClient on a free visualisation page or to allow an Ajax visualisation to run in the browser without a security check.

If you are using the Microsoft Internet Explorer or Google Chrome browsers, for example, it is sufficient to import the certificate into the Windows certificate manager, because these browsers access this. If you are using a Mozilla-based browser, such as Firefox, the HomeServer certificate must also be imported into the browser's own certificate manager. Refer to the help of the respective browser for more information on how to do this.

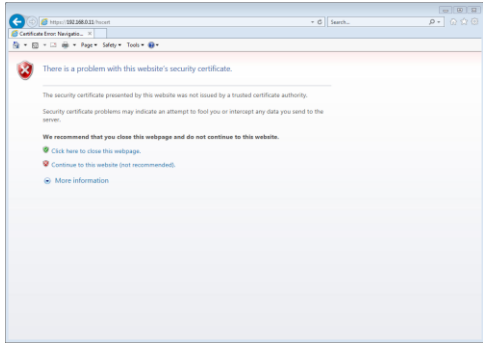
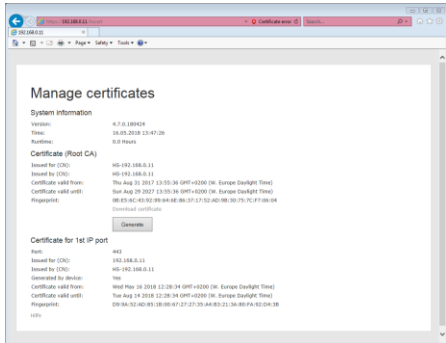
These instructions describe the steps for a Windows 7 system with Internet Explorer 11. The steps are basically the same for other Windows systems, but may vary slightly.

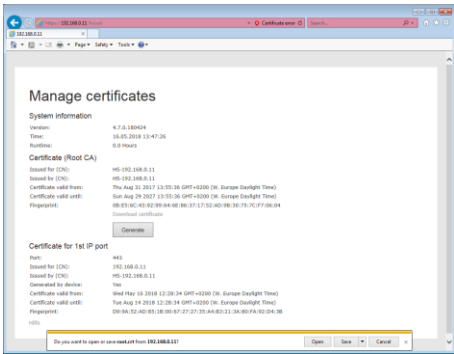
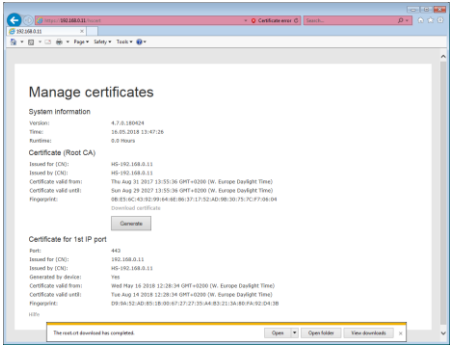
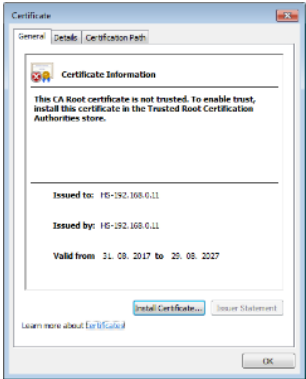
# GIRA

## Note: HomeServer certificates

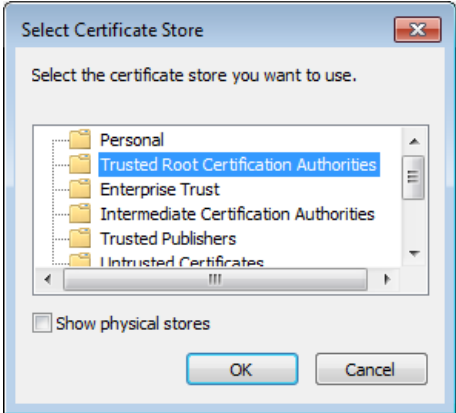
You only need to carry out the steps described once on the client devices, because the downloaded root certificate is valid for 10 years.

The validity period of the IP port certificates is limited to 90 days for security reasons. The certificates are automatically regenerated by the HomeServer and are thus valid again.

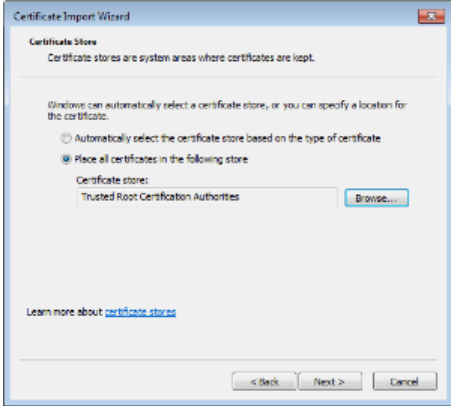
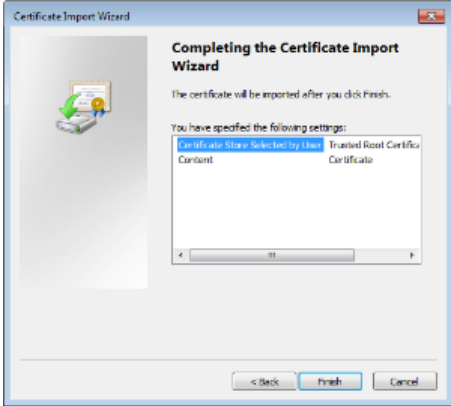
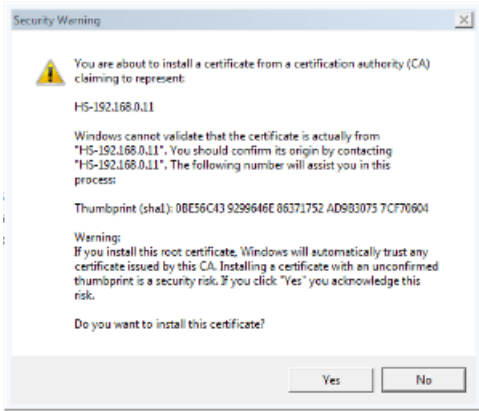
Steps	Figure
<p>Enter the following URL in Internet Explorer:</p> <p><code>https://&lt;HomeServer IP address&gt;/hscert</code></p> <p>A security warning appears, as Windows does not yet recognise the HomeServer certificate. Click "Continue to this website".</p>	
<p>The HomeServer certificate manager is then displayed. The red marking in the URL address bar indicates that the HomeServer certificate is not yet known. Click the "Download certificate" link. and then click "Save" and "Open".</p>	

Steps	Figure
	
	
Click "Import" in the Certificate dialog.	

# GIRA

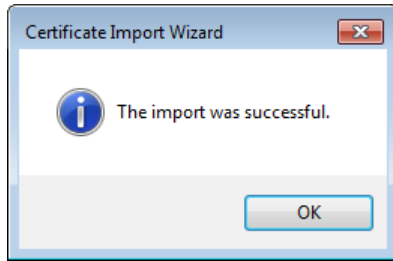
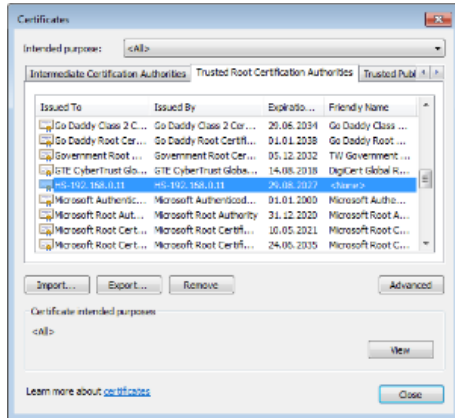
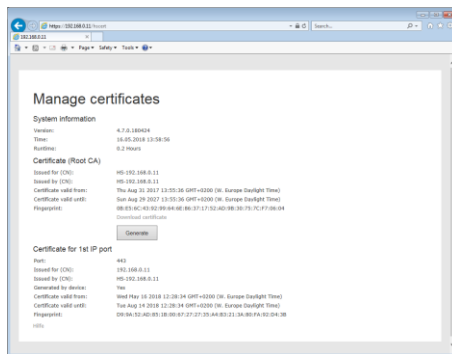
Steps	Figure
The Certificate Import Wizard opens. Follow the instructions.	
Select the "Place all certificates in the following store" option and then click "Browse".	
Select "Trusted Root Certification Authorities" in the "Select Certificate Store" dialog, and confirm by clicking "OK".	

# GIRA

Steps	Figure
Click "Next " in the wizard.	 <p>The screenshot shows the 'Certificate Import Wizard' window. The title bar says 'Certificate Import Wizard'. The main text reads: 'Certificate Store. Certificate stores are system areas where certificates are kept. Windows can automatically select a certificate store, or you can specify a location for the certificate.' There are two radio buttons: 'Automatically select the certificate store based on the type of certificate' (unselected) and 'Place all certificates in the following store:' (selected). Below the second option, there is a text box containing 'Trusted Root Certification Authorities' and a 'Browse...' button. At the bottom, there are 'Back', 'Next &gt;', and 'Cancel' buttons.</p>
Exit the wizard by clicking "Finish".	 <p>The screenshot shows the 'Certificate Import Wizard' window at the 'Completing the Certificate Import Wizard' step. The title bar says 'Certificate Import Wizard'. The main text reads: 'Completing the Certificate Import Wizard. The certificate will be imported after you click Finish. You have specified the following settings:'. Below this, there is a table with two columns: 'Certificate Store Selected by User' and 'Trusted Root Certification'. The first row shows 'Content' under the first column and 'Certificate' under the second. At the bottom, there are 'Back', 'Finish', and 'Cancel' buttons.</p>
Windows displays another "Security Warning". Confirm this by clicking "Yes".	 <p>The screenshot shows a 'Security Warning' dialog box. The title bar says 'Security Warning'. The main text reads: 'You are about to install a certificate from a certification authority (CA) claiming to represent: HS-192.168.0.11. Windows cannot validate that the certificate is actually from "HS-192.168.0.11". You should confirm its origin by contacting "HS-192.168.0.11". The following number will assist you in this process: Thumbprint (sha1): 0BE56C43 9299646E 86371752 AD983075 7CF70604. Warnings: If you install this root certificate, Windows will automatically trust any certificate issued by this CA. Installing a certificate with an unconfirmed thumbprint is a security risk. If you click "Yes" you acknowledge this risk. Do you want to install this certificate?'. At the bottom, there are 'Yes' and 'No' buttons.</p>



# GIRA

Steps	Figure
A message should be displayed confirming that the import was successful. Confirm this by clicking "OK".	
You can check whether the import was successful if you open the Windows certificate manager.	
After restarting Internet Explorer, the HomeServer certificate is classified as trusted. No security warning is displayed and there is no indication of an unsafe certificate.	

# GIRA

## Importing the HomeServer certificate into iOS

The following steps explain how to integrate the HomeServer certificate in the iOS certificate manager. By doing so, you avoid the Safari security check. This is necessary, for example, to call an Ajax visualisation in Safari.

These instructions describe the steps for an iOS 11.2 system. The steps are basically the same for other iOS systems, but may vary slightly.

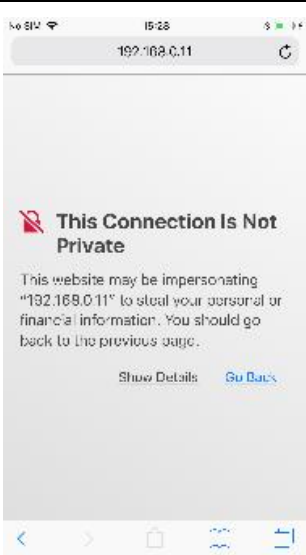
---

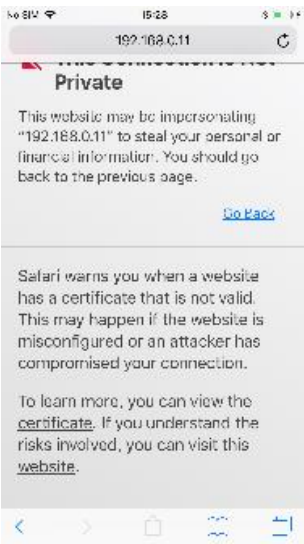
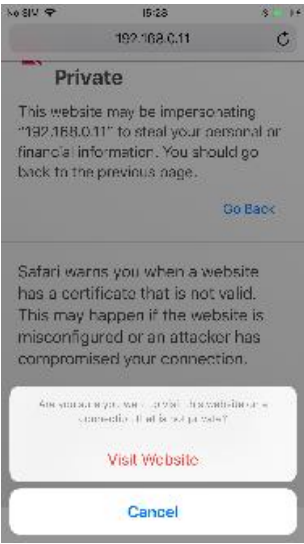
### Note: HomeServer certificates

You only need to carry out the steps described once on the devices, because the downloaded root certificate is valid for 10 years.

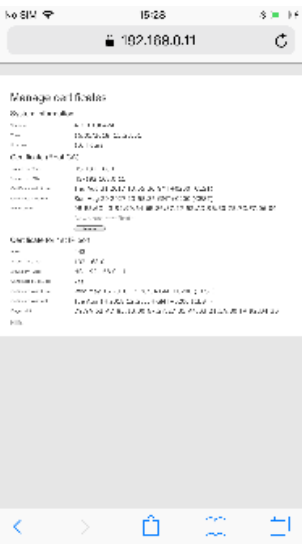
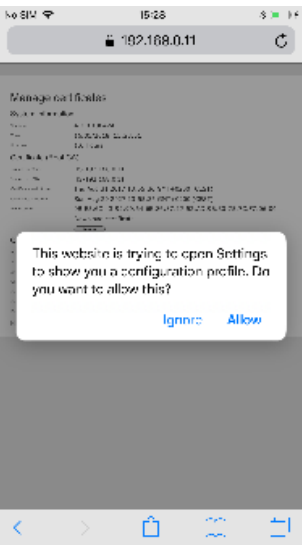
The validity period of the IP port certificates is limited to 90 days for security reasons. The certificates are automatically regenerated by the HomeServer and are thus valid again.

---

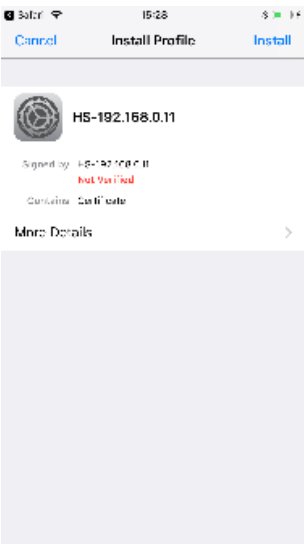
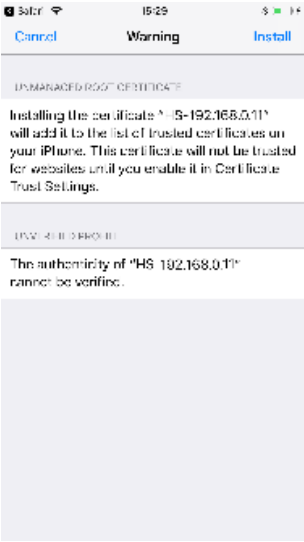
Steps	Figure
<p>Enter the following URL in Internet Explorer:</p> <p><code>https://&lt;HomeServer IP address&gt;/hscert</code></p> <p>A security warning appears, as iOS does not yet recognise the HomeServer certificate.</p>	

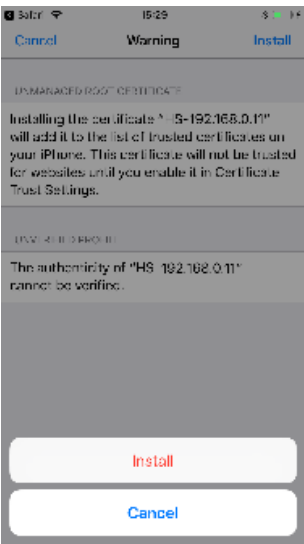
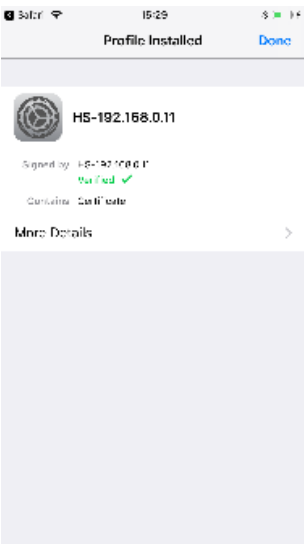
Steps	Figure
If the website is to be displayed and the certificate installed permanently to prevent the warning from appearing, the certificate needs to be installed. To do so, select "Show Details" and click the "website" link here.	
Safari displays another security warning. Confirm this by clicking "Visit Website".	

# GIRA

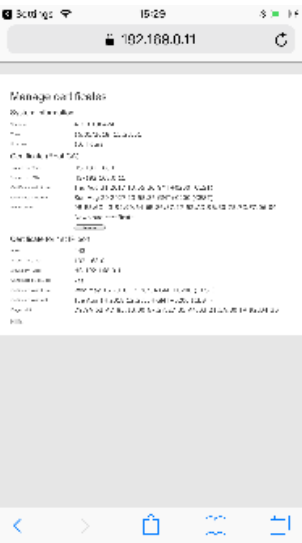
Steps	Figure
<p>Click "Download certificate" on the HomeServer certificate management page.</p>	
<p>Confirm changes to the configuration profile by clicking "Allow".</p>	

# GIRA

Steps	Figure
Then click "Install".	
Enter the PIN and click "Install" again.	

Steps	Figure
Confirm the last message once again by clicking "Install".	
iOS then displays the certificate briefly as "Not verified". Finally, confirm it as "Verified".	

# GIRA

Steps	Figure
HomeServer pages can now be opened in Safari without security warnings.	

# GIRA


## Importing the HomeServer certificate into Android

The following steps explain how to integrate the HomeServer certificate in the Android certificate manager. By doing so, you avoid the Chrome security check. This is necessary, for example, to call an Ajax visualisation in Google Chrome.

These instructions describe the steps for an Android 7 system. The steps are basically the same for other Android systems, but may vary slightly.



**Note: HomeServer certificates**  
You only need to carry out the steps described once on the devices, because the downloaded root certificate is valid for 10 years.

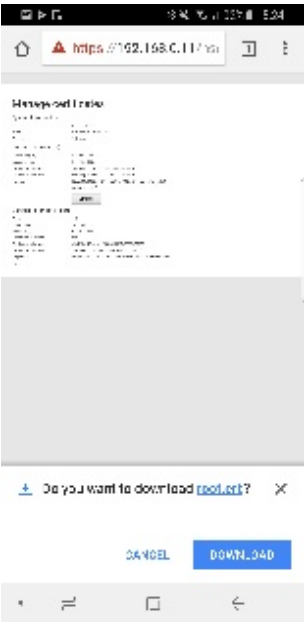

The validity period of the IP port certificates is limited to 90 days for security reasons. The certificates are automatically regenerated by the HomeServer and are thus valid again.

Steps	Figure
<p>Enter the following URL in Internet Explorer:</p> <p><code>https://&lt;HomeServer IP address&gt;/hscert</code></p> <p>A security warning appears, as Android does not yet recognise the HomeServer certificate.</p>	





# GIRA

Steps	Figure
If the website is to be displayed and the certificate installed permanently to prevent the warning from appearing, the certificate needs to be installed. To do so, click "Advanced" and then "Proceed to ...".	
Click "Download certificate" on the HomeServer certificate management page.	

Steps	Figure
Click "Download" to confirm the download root.crt message.	 A screenshot of a mobile browser interface. At the top, the address bar shows 'https://192.168.C.117'. Below it, there's a section titled 'Intercepted Traffic' with some technical details. A large grey rectangular area is in the center. At the bottom, a blue dialog box asks 'Do you want to download root.crt?'. Below the dialog are two buttons: 'CANCEL' and 'DOWNLOAD'.
Then open the "root.crt" certificate.	 A screenshot of a mobile browser interface, similar to the one above. It shows the same 'Intercepted Traffic' section and grey area. At the bottom, a dark blue bar displays 'root.crt - downloaded' with a small icon to its right.

# GIRA

Steps	Figure
In Android, you can assign a unique name to the certificate, such as "HomeServer". Confirm the dialog with "OK".	
HomeServer pages can now be opened in Google Chrome without security warnings.	

## QC - User control

### Authorisations

One of four authorisations is assigned to each QuadClient user:

- Guest user
- Group member
- Group administrator
- System administrator

The **guest user** is the lowest authorisation. In other words, this user is only permitted to operate functions in the QuadClient and may not configure any settings. A guest user cannot see which other users have access to the QuadClient either. If a guest user clicks on Change of user in the system settings, he must enter both the user name and the associated password.

A **group member** has more authorisations than the guest user. A group member is not permitted to configure settings, but may change his own password and display the list of users to see which other users have access to the QuadClient.

In addition to the group member's configuration options, a **group administrator** is permitted to configure favourites, function keys and quadrants of the user group to which the group administrator is assigned.

The **system administrator** has the most rights. In addition to the group administrator's configuration options, a system administrator is permitted to change the system settings and the passwords assigned by users in the QuadClient for all users. Thus, a system administrator can exclude users from using the QuadClient.

---

#### **Note: Configuration of user groups**

A system administrator can only configure settings within the assigned user groups. In other words, if settings are configured in other user groups to which the system administrator is not assigned, at least one group administrator must be created within a user group (see also Example of users/user groups).

---

# GIRA

Authorisations are assigned in the user properties in the QuadConfig (see figure *User properties*). The colours grey, green, yellow and red also display the authorisations (see figure *Users with colour-coded authorisations*). (grey=guest user, green=group user, yellow=group administrator, red=system administrator)

	Guest user	Group member	Group administrator	System administrator
Change of user	✓ *)	-	-	-
User list	-	✓ **)	✓ **)	✓ **)
Configure favourites settings	-	-	✓	✓
Configure navigation buttons settings	-	-	✓	✓
Configure direct functions settings	-	-	✓	✓
Configure quadrants settings	-	-	✓	✓
User settings	-	✓	✓	✓
System settings ... Return after time	-	-	-	✓
System settings ... User change rapid selection	-	-	-	✓
System settings ... Guest user management	-	-	-	✓
System settings ... Device list	-	-	-	✓
Settings Exit program	-	-	✓	✓

# GIRA

	Guest user	Group member	Group administrator	System administrator
Start cleaning	✓	✓	✓	✓
Version information	✓	✓	✓	✓

\*) In the case of a change of user, it is essential to enter the user name and password in order to change the user. The users configured in the QuadConfig are not displayed. In other words, a guest user may only change to a user with additional rights if he knows both the user name and password.

\*\*) In the case of the user list, all possible users are displayed. A user can be selected directly using this list. If the selected user has allowed his password to be saved, the user is changed directly. Otherwise, the user must enter his password (see also Save password).

# GIRA

The figure displays four screenshots of the 'Eigenschaften' (Properties) dialog boxes for different user roles in the GIRA software. Each window has a title bar with the role name and standard window controls. Below the title bar is a toolbar with icons for undo, redo, save, and help. The main content area is divided into a tree view on the left with the 'Allgemein' (General) tab selected, and a table on the right showing the properties.

**Eigenschaften [Gast-Benutzer]**

Allgemein	
Text	Gast-Benutzer
Benutzername	Gast
Passwort	Sicher_1
Passwort speicherbar	<input checked="" type="checkbox"/>
Benutzergruppen	Gruppe 1
Berechtigung	Gast-Benutzer
ID	1

**Eigenschaften [Gruppen-Mitglied1]**

Allgemein	
Text	Gruppen-Mitglied1
Benutzername	Gruppen-Mitglied1
Passwort	Sicher_2
Passwort speicherbar	<input checked="" type="checkbox"/>
Benutzergruppen	Gruppe 2
Berechtigung	Gruppen-Mitglied
ID	2

**Eigenschaften [Gruppen-Verwalter1]**

Allgemein	
Text	Gruppen-Verwalter1
Benutzername	Gruppen-Verwalter1
Passwort	Sicher_3
Passwort speicherbar	<input type="checkbox"/>
Benutzergruppen	Gruppe 3
Berechtigung	Gruppen-Verwalter
ID	3

**Eigenschaften [System-Verwalter]**

Allgemein	
Text	System-Verwalter
Benutzername	System-Verwalter
Passwort	Sicher_4
Passwort speicherbar	<input type="checkbox"/>
Benutzergruppen	Gruppe 4
Berechtigung	System-Verwalter
ID	4

Figure: User properties (guest user, group member, group administrator, system administrator)

# GIRA



*Figure - Users with colour-coded authorisations*

---

## **Note: Sort order**

The users are sorted in the QuadConfig as follows:

1. Group (ID)
  2. User role (admin—>guest)
  3. Name of the user
- 

## **Save password**

If the "Password can be saved" checkbox is activated, the user can save his password in the QuadClient. In other words, it is possible to change users without entering the password. The user can also deactivate the checkbox under User settings in the QuadClient system settings, thus making the entry of the password a requirement again for a change of user.

The "Password can be saved" setting is always active for guest users and cannot be changed in the QuadClient.

If the checkbox is deactivated in the QuadClient system settings and the project is reloaded (with the checkbox activated), the settings made in the QuadClient stay the same.

## **User group**

Users are assigned to a group under User group (see also User group and Example of users/user groups).



# GIRA

## ID

The ID is required for the change of user via a communication object. A fixed ID is assigned to each new user and increased by 1 each time. If a user is deleted, free IDs are reused.

During configuration, make sure that the respective ID assigned in the QuadConfig is addressed for a change of user from "Father" to "Guest", for example.

## QC - User groups

### General

Each user is assigned to a user group. It is possible to assign the same access rights to several users via the user group, since a user group may contain several users.

A total of 60 user groups are predefined in the QuadConfig. You can only change the names of the user groups. You cannot delete user groups or add other user groups.

### Text

Under "Text", you can assign a name of your own to the user group (e.g. "Admin", "Parents", "Children", "Guests", etc.). To simplify parametrisation, the "Text" is also displayed after each assigned user in the QuadConfig.

### Function buttons

There are six function buttons in the lower area of the QuadClient. The first and last function buttons are always set by default. The first shows "Menu" or "Plug-in". The buttons switch according to the QuadClient view that is currently displayed. The sixth function button always shows "System". If you click this button, the QuadClient switches to the system menu and the System settings can be configured.

Function buttons two to four can be configured individually for each user group. In other words, if you change to a user which is assigned to another user group, other functions can be assigned to the function buttons.

# GIRA

The following functions can be parametrised:

- no function - Nothing happens if the function button is selected, it is displayed without a label
- Favourites - Calls the configured favourites
- MyTouch - Opens the MyTouch page
- Function button - Calls the function defined under "Function button"
- Notes - Opens the Notes page
- Change of user - Opens the change of user page
- Browser - Opens one or more links configured under "Navigation button URL"

The following default settings exist for each user group (groups 1 to 60):

- Function button 1: Menu - not configurable
- Function button 2: Favourites - configurable
- Function button 3: MyTouch - configurable
- Function button 4: Notes - configurable
- Function button 5: Browser - configurable
- Function button 6: System - not configurable

## Functions

Each user group can be assigned to higher-level functions. (MyTouch and/or navigation button (URL))

## MyTouch

You can assign a MyTouch function configured in "MyTouch" here.

# GIRA

## Navigation button (URL)

You can assign a browser call configured in "Navigation button - URL" here.

---

### Note: Authorisations

Note that no functions can be parametrised that cannot be resolved by the QuadClient. In other words, the authorisations of user groups must always be parametrised meaningfully.

Example: In the menu, user group 1 is assigned to a menu tile that is to call a plug-in as well as a room. However, user group 1 is not assigned to the plug-in that is to be called. In this case, a plug-in could be called that is displayed without any content.

---

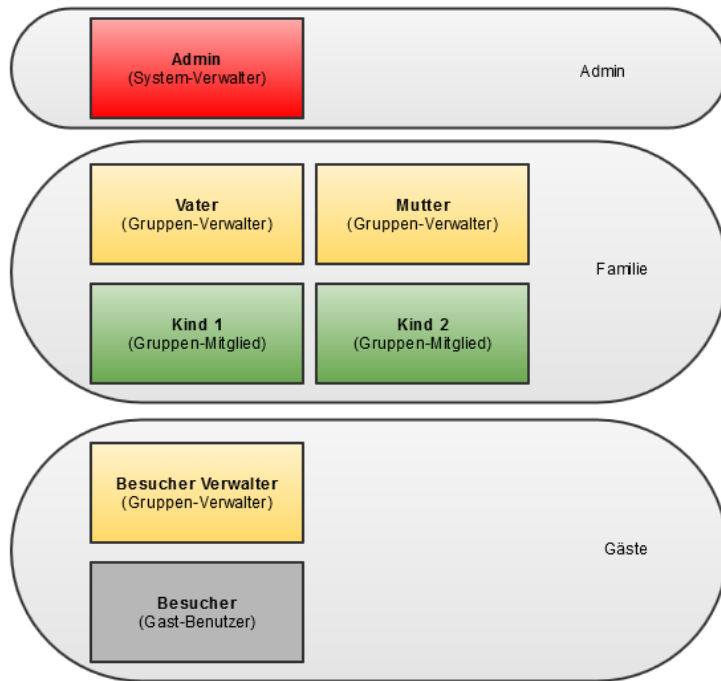
## Example of users/user groups

### Example 1 - Single-family home

The table below shows the users in a single-family home together with their authorisations and group memberships.

User	Authorisation	User group
Admin	System administrator	Admin
Father	Group administrator	Family
Mother	Group administrator	Family
Child1	Group member	Family
Child2	Group member	Family
Visitor_administrator	Group administrator	Guests
Visitor	Guest user	Guests

# GIRA



This results in the following behaviour:

- Only Admin may perform the following:
  - Make system settings
  - Change other users' passwords
  - Configure end devices
- Admin may configure the following for the **Admin** user group:
  - Favourites
  - Function button
  - Quadrants

# GIRA

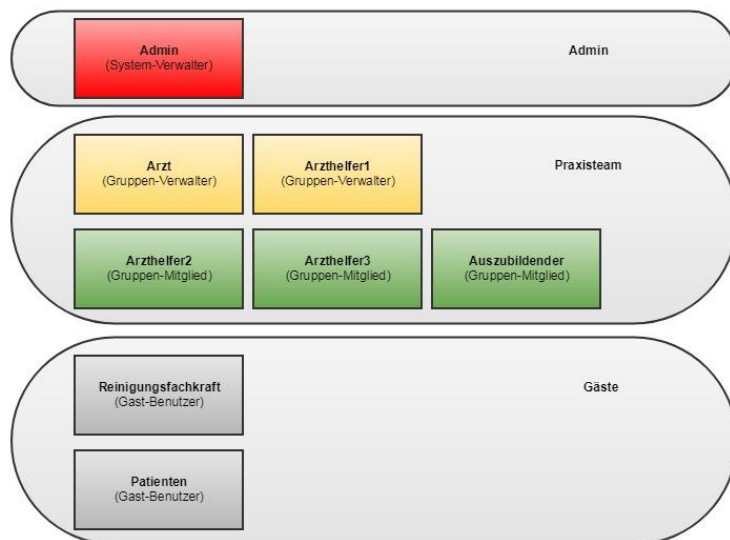
- Father and Mother may configure the following for the **Family** user group:
  - Favourites
  - Function button
  - Quadrants
- Visitor\_administrator may configure the following for the **Guests** user group:
  - Favourites
  - Function button
  - Quadrants

# GIRA

## Example 2 - Medical practice

The table below shows the users in a medical practice together with their authorisations and group memberships.

User	Authorisation	User group
Admin	System administrator	Admin
Doctor	Group administrator	Practice team
Medical assistant <sub>1</sub>	Group administrator	Practice team
Medical assistant <sub>2</sub>	Group member	Practice team
Medical assistant <sub>3</sub>	Group member	Practice team
Trainee	Group member	Practice team
Cleaning staff	Guest user	Guests
Patient	Guest user	Guests



# GIRA

This results in the following behaviour:

- Only Admin may perform the following:
  - Make system settings
  - Change other users' passwords
  - Configure end devices
- Admin may configure the following for the **Admin** user group:
  - Favourites
  - Function button
  - Quadrants
- Doctor and Medical assistant<sup>1</sup> may configure the following for the **Practice team** user group:
  - Favourites
  - Function button
  - Quadrants
- No configurations can be made for the **Guests** user group. The settings predefined in the QuadConfig apply.

## QC – Miscellaneous

### General

The QuadClient, which is delivered from Expert version 4.7 and higher, is always loaded onto the HomeServer during the project upload. The QuadClient is loaded onto the respective end device using the *QuadClient Starter*. There are two variants:

- A Windows XP operating system is installed on the end device (e.g. on the Control Client 19 or Control Client 9). In this case, a QuadClient is loaded by the HomeServer which is based on the .NET Framework 3.5.
- A higher operating system is installed on the end device (e.g. Windows 7 on the Gira Control 19 Client 2 or Gira Control 9 Client 2). In this case, a QuadClient is loaded by the HomeServer which is based on the .NET Framework 4.5.

The QuadClient Starter automatically detects which version is required. If using the QuadClient Starter on a Windows XP device, make sure that the "Permit communication via TLS v1.0" option is activated in the Expert software under "Security" in the project settings.

### Users and passwords

Several users with different rights can be created in the QuadClient (see User control).

If the QuadClient is started, there are three possible variations:

- The user name and password are already entered in the QuadClient Config Editor. When the QuadClient is started, a login mask does not appear as the user and password are already known.
- The user name is entered in the QuadClient Config Editor, but not the password. When the QuadClient is started, a login mask appears in which the user is already entered and a password must be entered. If the user presses the "ESC" button, the user is not logged onto the QuadClient and the QuadClient closes. After entering the correct password, the user is logged on with his corresponding rights.



# GIRA

- Neither the user name nor the password is entered in the QuadClient Config Editor. When the QuadClient is started, a login mask appears in which the user name and password must be entered. If the user presses the "ESC" button, the user is not logged onto the QuadClient and the QuadClient closes. After a known user and correct password has been entered for this user, the user is logged on with his corresponding rights.

---

**Note: Initial user start**

If the QuadClient is started for the first time under this user, the "Edit password" mask is displayed. The user must enter the "original" password entered in the QuadConfig once here and enter a new password twice. The new password can and should differ from the password that was entered in the QuadConfig.

---

---

**Note: Change of user**

If a change of user is carried out in the QuadClient (via the user list or change of user for guest users) and the called user is started for the first time, a pop-up is displayed stating that a new password must be entered for this user. If the pop-up is confirmed with "OK", the "User settings" mask is displayed and the password can be changed. The new password can and should differ from the password that was entered in the original QuadConfig.

---

---

**Note: Original password**

The password that was assigned in the QuadConfig is not discarded. It can be entered, for example, when a user password is lost in order to assign a new password again.

---

# GIRA

## System settings

The table below shows the navigation in the System menu.

System			
User list (only for system administrator, group administrator, group member)	<p>User list</p> <p>Log out user</p> <p>User 1 (active user is displayed in green)</p> <p>User 2</p> <p>...</p> <p>User n</p>	Password input mask opens for change of user	
Change of user (only for guest user)	<p>Change of user</p> <p>User 1</p> <p>User 2</p> <p>...</p> <p>User n</p>	Password input mask opens for change of user	
Settings ...	<p>System   Settings</p> <p>Configure favourites</p> <p>Configure function buttons</p> <p>Configure quadrants</p> <p>User settings</p>	<p>When you open "Configure favourites", "Configure function buttons" or "Configure quadrants", "Exit favourites configuration", "Exit function button configuration" or "Exit quadrant configuration" is displayed. The respective configuration is active. The configuration type is also displayed in the status bar.</p> <p>You can change your personal password in the user settings. If configured accordingly, you can also save the password permanently.</p>	

	System settings ...	<a href="#">System   Settings   System settings</a> Return after time User change rapid selection Guest user management Device list	See Return after time  See User change rapid selection  See Guest user management  See Device list
	Exit program ( <i>not for guest user</i> )		
Start cleaning			
Version information			

---

## Note: Permanent storage

If a user makes changes to the configurations in the QuadClient, these are stored permanently in the HomeServer. In other words, in the event of a mains voltage failure and subsequent restart of the HomeServer or QuadClient restart, the QuadClient always displays the last changes made (the 15-minute waiting time may need to be taken into account until the retentive data is saved again).

Even if changes are made in the QuadConfig, e.g. when arranging the function buttons, these are not applied to the QuadClient after the upload to the HomeServer. The changes last made by the user in the QuadClient always apply.

---

# GIRA

## Return after time

In "Return after time", you can specify a time after which the system jumps back to a defined function or user after a period of inactivity in the QuadClient. The default setting is no jump back (setting: Off). You can set the following times: 1 minute, 5 minutes, 10 minutes, 15 minutes, 30 minutes, 45 minutes or 1 hour.

If a time is selected, you can then specify the behaviour for jump back after time. The following behaviours are available:

- MyTouch
- Configured function (function button)
- Log out
- Change of user
- Call up browser

For MyTouch, configured function (function button) and browser, settings are accessed which are defined for the user group in the respective function buttons. For example, if call "Living room" is defined for the function button, the "Living room" would be displayed for return after 10 minutes and the function configured for the behaviour, if there is no activity for 10 minutes in the QuadClient.

If "Change of user" is selected as the behaviour, a configured user can also be specified or even "no user". If "no user" is selected, the user list is displayed for return after time.

---

### **Note: Return after time**

If "user x" is active and the same "user x" is configured for return after time, no return after time takes place as the user is already logged on.

---

# GIRA

## **User change rapid selection**

For the user change rapid selection, up to four users are displayed across the entire area, instead of the menu and plug-ins. If more than four users are created, the complete user list can be opened using the sixth function button "...more". Press the "...more" function button again to return to the user change rapid selection.

## **Guest user management**

The passwords of the guest users can be changed by the system administrator in the guest user management.

## **Device list**

Control devices preconfigured in the QuadConfig can be assigned in the device list. This is necessary for displaying the indoor temperature, for example.