Downloads
  Quick Start Guide
  Declarations
Description and features
First installation
Interfaces
Devices
Migrating data
Configuration
Automation
Maintenance
Integrations
Security

Home Center 3

FGHC3-001

Downloads

Quick Start Guide

Quick Start Guide – English
Quick Start Guide – Multilanguage (PL, DE, FR, ES, IT, PT, RU)

^ Back To Top

Declarations

Declarations of conformity:

FGHC3-001.pdf

› Archive

^ Back To Top

Description and features

Description

FIBARO Home Center 3 is the core element of the FIBARO System.

It enables the integration of smart home devices into a single system to provide convenient control and a powerful automation platform. The gateway is now even more secure, reliable, and versatile.

^ Back To Top

Features

- Provides a reliable foundation for FIBARO System.
- Capable of controlling all FIBARO and other compatible devices using the following radio standards:
  - Z-Wave (500 series)
  - Wi-Fi – 2.4 GHz and 5 GHz (802.11 b/g/n/a/ac)
  - Nice FLOR, OPERA and PLN2+
  - Elero PLN2
- No Internet cable required, works also on Wi-Fi
- Modern interface designed for ease of use
- Enhanced and convenient scene editor
- Support for more advanced apps and drivers
- May be used with all devices certified with the Z-Wave Plus certificate and should be compatible with such devices produced by other manufacturers

^ Back To Top

Specifications

General information

Model	FGHC3-001
CPU	Quad-core Arm Cortex A53 (1.2GHz)
RAM	RAM 2GB LPDDR3
Flash memory	8GB eMMC
Power supply	12V DC (adapter included)
Operating temperature	0-40°C
Operating humidity	max. 75% relative humidity (non-condensing)
Network interface	10/100 (Base-T) Ethernet via RJ45 connector
USB	1 (2.0)
Power connector	barrel connector 5.5mm x 2.5mm (female)
Dimensions	220×140×35 mm

Radio Communication

Protocol	Radio frequency band		Max. transmitting power
Z-Wave (500 series)	EU	868.0-868.6 MHz 869.7-870.0MHz	+14dBm
	AU, NZ, CL	920-925Mhz	+5dBm
	BR	920-925Mhz	-2dBm
	THA	920-925Mhz	+7dBm
Wi-Fi (802.11 b/g/n/a/ac)	2.4GHz	2400-2483MHz	+20dBm
	5GHz	5150-5250MHz	+14dBm
433Mhz	EU, THA	433.05-434.04Mhz	+10dBm
	AU, NZ, CL, BR	433.05-434.04Mhz	+14dBm
868Mhz	EU	868.0-869.65MHz	+10dBm

^ Back To Top

Status indicators

Power

Copper – powered

Internet

Copper – connected to Internet
Red – disconnected from Internet

LAN

Copper – connected to LAN
Fast pulsing copper – connecting to LAN

Wi-Fi

Copper – connected to Wi-Fi
Fast pulsing copper – connecting to Wi-Fi
Red – incorrect Wi-Fi password / other error
Green – Wi-Fi in Access Point mode

Installer

Copper – installer assigned
Green – remote support enabled
Red – installer not assigned

Recovery

Red – in Recovery Mode
Fast pulsing green – creating backup
Slow pulsing copper – update available

Smart Home

Slow pulsing copper – adding mode
Fast pulsing copper – removing mode
3 green blinks – adding successful
3 red blinks – adding not successful

Security

Red – alarm armed
Green – alarm disarmed

^ Back To Top

Buttons

Power
Click – Wake up
Hold for 5s – Sleep mode
Hold for 15s – Restart

Recovery
Hold during startup – Put in Recovery mode
Hold for 10s, click when 🖧 and 🛜 are blinking green – Switch between Dynamic and Static IP:

- 🖧 and 🛜 blink yellow: IP set to Dynamic
- 🖧 and 🛜 blink green: IP set to Static

Hold for 20s, click when 🖧 and 🛜 are blinking red – Reset network settings:

- 🖧 and 🛜 blink red – settings reset

^ Back To Top

First installation

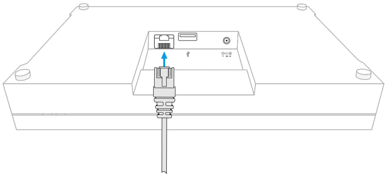
Network interfaces exposed in factory default state

Interface	Port	Description
Fibaro find server	44444, 9999	Used for finding and connecting to the hub in the local network by a web interface and mobile application
Avahi	5353	Used for resolving IP addresses in the local network, which enables access to the hub with a serial number
DNS	67	Used for resolving the network addresses, for network connections
Kamailio server for SIP	5060, 5061	Used for SIP calls
HTTPS server	443	Enables managing home and user's settings – used by a web interface and mobile application
HTTP server	80	Enables managing home and user's settings – used by a web interface and mobile application
SSH	22	Enables secure management of the hub files, configuration and applications
Systemd	5353, 5355	Enables managing the hub services

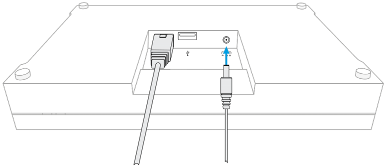
^ Back To Top

Installation using Ethernet cable

1. Connect the gateway to your home's Internet router using the provided Ethernet cable.



2. Plug the provided power adapter into an outlet and connect it to the gateway.

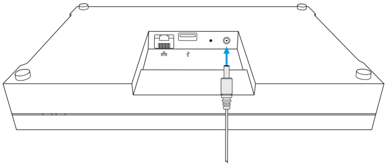


3. The gateway will turn on and ⏻ indicator will turn copper.

^ Back To Top

Installation using Wi-Fi only

1. Plug the provided power adapter into an outlet and connect it to the gateway.



2. The gateway will turn on and ⏻ indicator will turn copper.
3. Connect your computer to Wi-Fi network created by the gateway.
   You will find Wi-Fi SSID (name) and password on the bottom of the device.

^ Back To Top

First start of the device

First configuration

1. Scan the QR code and download the Yubii Home Center app.
2. Launch the application and follow the displayed instructions.

Alternative configuration

1. Go to find.fibaro.com (use 10.42.0.1 if you connect to Wi-Fi network created by the gateway and go to step 4).
2. List of all gateways in your home network will be displayed.
3. Click Open next to gateway you want to configure.
4. Choose your language.
5. Login with default credentials:
   - Login: admin
   - Password: admin
6. Configure the gateway step-by-step by following the consecutive windows in Configuration or skip it.

Adding controller to Remote Access

1. Log in to your FIBARO ID account.
2. Click *More* in the Remote Access section.
3. Click *Add New Home Center.*
4. Enter data of your Home Center (serial number, MAC address).
5. Click *Add Home Center*.
6. Your Home Center will be now visible on the list.

IMPORTANT!

Make sure to change the default credentials for your login account to improve security.

IMPORTANT!

It is recommended to disable HTTP access during configuration as it is considered unsafe protocol, unless you have specific reason no to.

^ Back To Top

Interfaces

Configuration Interface

Redesigned Configuration Interface is the new way to manage your FIBARO System. This new interface gives access to your all devices, history, and settings.

Opening Configuration Interface

Using FIND FIBARO web app

1. In your Internet browser go to find.fibaro.com.
2. List of all gateways in your home network will be displayed.
3. Click *Open* next to the gateway you want to configure.
4. Login with your local credentials (default login: *admin*, default password: *admin*).

Using Remote Access

1. In your Internet browser go to home.fibaro.com.
2. Login using FIBARO ID account.

3. List of all gateways in your Remote Access will be displayed.
4. Click *Open* next to the gateway you want to configure.
5. Login with your local credentials (default login: *admin*, default password: *admin*).

Using IP address of the gateway

1. In your Internet browser enter the gateway IP address.
2. Login with your local credentials (default login: *admin*, default password: *admin*).

Using serial number of the gateway (mDNS)

1. In your Internet browser enter gateway address in form: *serial_number.local* (e.g. http://hc3-00000001.local).
2. Login with your local credentials (default login: *admin*, default password: *admin*).

Configuration Interface elements

The top navigation bar is always visible and accessible on all pages. Navigation bar consists of:

- **User activity** – shows the user who is currently logged in and Recent logged in users,
- **Update** – in this place you can find new updates for your gateway and devices,
- **Weather** – shows current Temperature, Humidity and Wind speed,
- **Time** – shows the current date and hour,
- **Profile** – in this place you can see which profile is active and change that,
- **Account** – in this place you can go to the Account Settings, do the Recovery, Reboot the gateway or Logout.

There are four main views accessible from the sidebar:

- **Dashboard** – a place where you can manage your all devices across all the rooms and sections. You can change their location, turn them on or off, and view their statuses,
- **History** – a register/record of events that occur in your whole FIBARO system,
- **Scenes** – a list of all scenes in your system that allows to start scenes and view their status,
- **Climate** – a list of all heating and cooling schedules in your system. It allows to view their status or quickly set them to manual/vacation mode,

Additionally, in the lower left-hand corner, there are four more views that you may find important if you want to configure your system, something does not work properly or you want better insight in the gateway operations.

- **Settings** – a list of settings grouped into over a dozen categories, in which you can adjust the operation of the FIBARO System to your needs.
- **Console** – a real-time log of operations happening at the gateway, e.g. adding Z-Wave devices, removing Z-Wave devices, changing parameters, setting associations,
- **API documentation** – access to interactive REST API documentation interface (Swagger) for the gateway,
- **Support** – direct access to the FIBARO Support page.

^ Back To Top

Interface color theme

The Configuration Interface allows to choose between two color themes: light or dark. The theme can be changed manually or automatically based on the sunrise/sunset hours for the location.

To change color theme manually:

1. Open the Configuration Interface.
2. In top right corner click 👤.
3. Choose ◑ *Light/Dark Theme* to change the theme.

To change color theme automatically (besed on sunrise/sunset hours):

1. Open the Configuration Interface.
2. In top right corner click 👤.
3. Choose ⚙ *Account Settings* from the menu.
4. Change *Theme switching mode* setting to *Auto*.

^ Back To Top

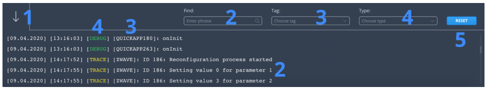
Console

The gateway has an all-new console that can provide detailed information about ongoing processes concerning the Z-Wave network, Quick Apps, and scenes. This means that the new console aggregates all messages pushed by "print", "debug", "trace", "warning", "error" methods, whether they originate from a scene, a Quick App, or Z-Wave, e.g. general notifications, adding, removing.

Console overview

The **Console** is accessible from the sidebar. Click >_ to unfold the console.

The console consists of 5 main elements:



```
[09.04.2020] [13:16:03] [DEBUG] [QUICKAPP180]: onInit
[09.04.2020] [13:16:03] [DEBUG] [QUICKAPP263]: onInit
[09.04.2020] [14:17:52] [TRACE] [ZWAVE]: ID 186: Reconfiguration process started
[09.04.2020] [14:17:55] [TRACE] [ZWAVE]: ID 186: Setting value 0 for parameter 1
[09.04.2020] [14:17:55] [TRACE] [ZWAVE]: ID 186: Setting value 3 for parameter 2
```

1 – down arrow to hide the console,
2 – "Find" field to search for the phrase in the content of messages,
3 – "Tag" field to filter messages to show only those connected to the chosen, tag,
4 – "Type" field to filter messages according to their types: debug, trace, warning, error,
5 – reset button to clear the search and filter parameters.

Using tags for better console management

Console logs may be filled with different messages which may not interest us at the moment. To narrow down the messages to the interesting ones we may introduce tags in our scenes and Quick Apps to quickly find the right messages in the log.

Tags and Quick Apps

Quick Apps create tags automatically, e.g. QUICKAPP263, where 263 is the Quick App ID. However, it doesn't mean you cannot create any new tags as you see fit.

Tags and Scenes

Scenes fallback to the default tag which is created on the basis of the scene ID, e.g. SCENE54.

That is why any output from that scene to the console will be tagged as SCENE + scene ID.

You can change the tag by specifying the first parameter in the fibaro.debug function, e.g. fibaro.debug('Your Tag', 'Content').

Tags and Z-Wave

Filtering console logs may be useful while adding, removing, or reconfiguring Z-Wave devices. Setting tag to Z-Wave ensures that only Z-Wave related messages will be displayed in the console.

Beware!

Filtering with a tag is possible only after the first use of a given tag. That is why, if you want to catch some operations done by action with a given tag, you need to send a test message first so you will be able to choose the given tag.

^ Back To Top

Mobile apps

To control the hub with a mobile device, install the **Yubii Home** app.

You can download the Yubii Home mobile app here:

- Yubii Home for iOS (iPhone)
- Yubii Home for Android

You can also scan the codes on your mobile device directly:

GET IT ON Google Play

Download on the App Store

Click **HERE** to keep up to date with the features of the mobile app.

^ Back To Top

Devices

Zigbee devices

Click **HERE** to learn more about operating Zigbee devices

^ Back To Top

Elero devices

The gateway enables control of Elero devices with support for the PLN2 bidirectional communication protocol.

Adding Elero devices

1. Open the Configuration interface.
2. Go to ⚙ > Devices .
3. Click on ⊕ Add device
4. Select the Elero device.
5. To complete the device pairing process, play the device state change at least 3 times using the keyboard buttons ⬆ and ⬇ or buttons in the interface.
6. Click the *Bind* button to start.
7. Follow the instructions shown on the screen.
8. When the pairing process is complete, the devices will be visible in *Devices > Elero.*

Note: Synchronised pairing is possible. This allows multiple devices to be paired with the controller or remote at the same time. The number of paired devices will be displayed during pairing. Synchronised pairing of Elero devices is available in the Nice/Elero settings.

^ Back To Top

Z-Wave devices

Adding Z-Wave devices

1. Open the Configuration Interface.
2. Go to ⚙ > Devices.

3. Click ⊕ Add device.
4. Select Z-Wave Device.
5. Set learning mode duration and click *Start adding.*
6. Follow instructions of the device.

There are a few adding options you can choose in the *Add Device* window:

Options you can choose:

- Device is located far from the gateway (disable it for more security),
- NWI – Network-Wide inclusion (useful for devices that are not near the gateway, but withing networks range),
- Add in security mode if device supports it.

You can also set Learning mode duration – how much time you will have to perform the adding procedure on the device.

Removing Z-Wave devices (If not added)

1. Open the Configuration Interface.
2. Go to ⚙ > Devices.
3. Click on the Z-Wave tab.
4. Click ⊖ Remove device.
5. Follow instructions of the device.

Removing Z-Wave devices (If added)

1. Open the Configuration Interface.
2. Go to ⚙ > Devices.
3. Click 🗑 next to the device you want to remove from the system.
4. Set learning mode duration and click *Continue.*
5. Follow instructions of the device.

Force removing Z-Wave devices

1. Open the Configuration Interface.
2. Go to ⚙ > Devices.
3. Click 🗑 next to the device you want to remove from the system.
4. Set learning mode duration and click *Continue.*
5. Click ⊗ which appeared in place of 🗑 .
6. Confirm the action.
7. The gateway will try to communicate with the device. If the device responds, the process will by canceled, otherwise it will be removed from the system.

Associations

Associations allow devices to control other devices directly within the Z-Wave network without the participation of the main gateway. Devices such as Dimmer, Switch, Roller Shutter, RGBW Controller can continue to work and operate selected devices even when the main gateway is damaged or turned off (in case of a fire, flood, or system malfunction). You can read more about associations here.

Setting associations

1. Open the Configuration Interface.
2. Go to ⚙ > Devices.
3. Click the device you want to associate.
4. Open Associations tab.
5. Select the source EndPoint and Group of the association appropriate for your needs.
6. Select the device you want to associate with.
7. Click ⊕ to set the association.
8. If the device is battery powered, wake it up manually or wait for next automatic wake up.

Parameters

FIBARO devices allows to customize their operation to user's needs using configurable parameters. The settings can be adjusted via Z-Wave controller to which the device is added. In the FIBARO interface parameters are presented as simple options in Advanced Settings of the device.

Setting parameters for the device

1. Open the Configuration Interface.
2. Go to ⚙ > Devices.
3. Click the device you want to change its behavior.
4. Open the Parameters tab.
5. Find the parameters you're interested in.
6. Adjust the setting.
7. Click *Save* when you finish.
8. If the device is battery powered, wake it up manually or wait for next automatic wake up.
   If the device changes configuration, you will be asked to refresh the screen.

Copying parameters from other device

Configuration of the device can be copied from another device with the same parameters list.

1. Open the Configuration Interface.
2. Go to ⚙ > Devices.
3. Click the device you want to copy the parameters to.
4. Open the Parameters tab.
5. In the *Copy configuration from* field choose device you want to copy the parameters from.
6. Click *COPY.*
7. Save parameters.

8. If the device is battery powered, wake it up manually or wait for next automatic wake up.
   If the device changes configuration, you will be asked to refresh the screen.

^ Back To Top

Nice devices

The gateway allows to control Nice doors, gates and screens control units using monodirectional (FLOR and OPERA) and bidirectional (PLN2+) communication protocols. You will find a list of verified devices here.

Adding Nice devices with already programmed transmitter:

If a transmitter is already memorized in the control unit, you can use it to bind the device actions to the gateway.

1. Open the Configuration Interface.
2. Go to ⚙ > Devices.
3. Click Add device
4. Select Nice Device.
5. Select *Device by using remote*.
6. Click *AUTODETECTION*, then on the transmitter press any key **twice**.
7. If the autodetection did not succeed, you can select the protocol manually.
8. Select Device type (selecting proper device types is important for correct operation).
9. Click *Next*.
10. You will see a list of all actions eligible for your device.
    - For gates, doors and barriers: click *Bind Mode* for an action, then on the transmitter press key responsible for this action **twice**, repeat for each action.
    - For screens: click *Bind Mode* for any action, then on the transmitter press key responsible for this action **twice.**
11. For each bound action: click *Test* to check if the action was properly bound and the device responds properly to it.

Adding Nice devices without a programmed transmitter:

If there are no transmitters memorized in the control unit, you must perform action binding directly with the control unit.

1. Open the Configuration Interface.
2. Go to ⚙ > Devices.
3. Click Add device.
4. Select Nice Device.
5. Select *Device using no remote*.
6. Select the protocol.
7. Select Device type (selecting proper device types is important for correct operation).
8. Click *Next*.
9. You will see a list of all actions eligible for your device.
    - For gates, doors and barriers: click *Bind Mode* for an action, then put the Nice device into the transmitter memorization mode according to its manual, then confirm on the Home Center, repeat for each action
      (if using Mode II, activate memorization for the specific action).
    - For screens: click *Bind Mode* for any action, put the Nice device into the transmitter memorization mode according to its manual, then confirm on the Home Center.
10. For each bound action: click *Test* to check if the action was properly bound and the device responds properly to it.

Adding Nice transmitters as scene controllers:

You can add a Nice transmitter to the system and you will be able to start scenes by clicking any remote key.

1. Open the Configuration Interface.
2. Go to ⚙ > Devices.
3. Click Add device.
4. Select Nice Device.
5. Select *Remote controller only*.
6. Select the number of keys on the transmitter.
7. Click *Bind Mode*.
8. Click any key on the transmitter twice slowly.
9. When the status changes to *Finished*, click *Finish*.
10. After finishing, a new remote will be added to the list of devices. You can use it in scenes as a trigger or create a new scene directly from its *Advanced* tab.

^ Back To Top

Linked devices

Linked Devices combine several devices into one device. Using this function results in controlling the group of related devices as if they were one single device. The group will be presented in the interfaces as a single device. The gateway offers different Linked Devices types: Thermostats, Humidifiers, Video Gates, Switches, Blinds and Sprinklers.

Thermostats

Heating systems present at our homes are quite complex and they often do not offer any smart home capabilities natively. That's why you can create a Linked Device, which can act as the given Thermostat.

How does the linked device work?

When you choose the main device for the thermostat it means that the actions of the switches selected in the Linked Device will depend on the readings from the main device.

Depending on the selected devices, different operating modes will be available. If you select a device (Switch/Wall Plug) as a heating device only, the linked device will support modes only for heating. If you select devices for cooling as well, then the Linked Device supports more modes, i.e.: ***Heat, Cool, Auto, Off.***

> Creating Thermostats

How to set schedules for this thermostat?

Heating schedule for this Linked Device is accessible in **Climate** panel.

You can read more about it in the **Climate Schedules section.**

Humidifiers/Dehumidifiers

There are many devices on the market which helps in humidifying or dehumidifying. However, these devices may not be smart, nor equipped with Z-Wave radio. Using Linked Devices enables us to create the Humidity Device which can still regulate the humidity at your home.

How does it work?

When you choose the main device for the Humidifier, it means that the actions of the switches selected in this Linked Device will depend on the readings from the main device:

If the **humidity (%)** drops **below** your desired **humidity range** , the devices selected as **humidifiers** will **turn on.**

If the **humidity (%)** rises **above** your desired **humidity range**, the devices selected as **dehumidifiers** will **turn on**.

If you have set both humidifier and dehumidifier, the Humidity Device will monitor and control the humidity within the given range. If you set only one device, only humidifier or dehumidifier, you won't be able to set the full range, just the minimum or maximum threshold.

Creating Humidifiers

1. Open the Configuration Interface.
2. Go to ⚙ > Devices.
3. Click Add device.
4. Choose Other Device.
5. Click *Humidifier.*
6. Enter the name of the humidifier.
7. Choose a Room.
8. Choose the Humidity Sensor.
9. Set desired humidity range.
10. Select humidifiers and dehumidifiers.
11. Save.

Video gates

Video gate is a combination of three devices which together can act as a video gate.

We set:

- device which provide us the preview (***camera***),
- sensor which invokes the bell (***input for bell push***),
- actor which can activate the door lock or gate (***output to open the gate***).

Creating Video Gates

1. Open the Configuration Interface.
2. Go to ⚙ > Devices.
3. Click Add device.
4. Choose Other Device.
5. Click *Video Gate.*
6. Enter the name of the video gate.
7. Choose a Room.
8. Choose the Camera.
9. Select Input for bell push and Output to open the gate.
10. Save.

Switches (a group of switches)

Advanced and complex smart homes often consist of many switches placed within close areas which we want to control at once. Instead of making a scene which will coordinate the operation of all switches, we can group switches into one Linked Device, so all selected device will follow the actions of the "Master Device".

The Linked Device may act as a device of a few types:

RGBW Controller – linked devices follow parameters such as brightness, color, and power state.

Binary switch – linked devices follow the power state of the master device (appropriate for simple switches, smart plugs).

Color controller – linked devices follow color parameters of the master device.

Multilevel switch – linked devices follow the voltage output of the master device (appropriate for Dimmers).

Creating Switches (grouping)

1. Open the Configuration Interface.
2. Go to ⚙ > Devices.
3. Click Add device.
4. Choose Other Device.
5. Choose Switches.
6. Enter the name.
7. Choose a room.
8. Choose Devices, Master Devices and Device Type (RGBW Controller, Binary switch, Color controller, Multilevel switch).
9. Save.

Blinds (a group of blinds)

If we have more blinds or awnings in the same area we usually control at once, it is a good idea to grup them in one device. All blinds in that group will follow the master device of our choice.

Usually, devices such as Roller Shutters support few devices of such type, so we need to select appropriate role for the main device:

- blind without positioning,
- blind with positioning,
- venetian blind,
- garage door without positioning,
- garage door with positioning.

Creating Blinds (grouping)

1. Open the Configuration Interface.
2. Go to ⚙ > Devices.
3. Click ⊕ Add device.
4. Choose Other Device.
5. Choose Blinds.
6. Enter the name.
7. Choose a room.
8. Choose Devices (all that you want to group).
9. Choose Master Device (the one that other devices will follow).
10. Set the Device Role according to your devices:
    - Blind without positioning,
    - Blind with positioning,
    - Venetian blind,
    - Garage door without positioning,
    - Garage door with positioning.
11. Save.

Sprinklers

If you don't have dedicated watering devices that support Z-Wave or other wireless technology, you can create Sprinklers using Linked Devices.

To create a Sprinkle you need a watering device, for example, a switch connected to a solenoid valve. Optionally, you can add a soil moisture sensor, which will stop watering whenever the set humidity level is reached.

Once you set your Linked Device, you have to configure the watering schedule in the Garden panel. You can read more about it in the **Garden Care section**.

Creating Sprinklers

1. Open the Configuration Interface.
2. Go to ⚙ > Devices.
3. Click ⊕ Add device.
4. Choose Other Device.
5. Choose Sprinklers.
6. Enter the name.
7. Choose a room.
8. Choose watering devices.
9. Select soil moisture sensor (optional).
10. Set default watering time.
11. Set humidity level to turn off watering.
12. Save.

Binary sensors

You can combine multiple binary sensors of the same type to create one main sensor. It will calculate its value from the values of the linked devices using the logical operator you choose.
Available operators:

- AND
- OR

Creating Binary sensors

1. Open the Configuration Interface.
2. Go to ⚙ > Devices.
3. Click ⊕ Add device.
4. Choose Other Device.
5. Choose Binary Sensor.
6. Enter the name.
7. Choose a room.
8. Choose Sensor Type.
9. Choose sensors that should be linked.
10. Choose which operator should be used to calculate the value.
11. Save.

Multilevel sensors

You can combine multiple multilevel sensors of the same type to create one main sensor. It will calculate its value from the values of the linked devices using the mathematical function you choose.
Available functions:

- Average
- Median
- Maximum
- Minimum

Creating Multilevel sensors

1. Open the Configuration Interface.
2. Go to ⚙ > Devices.
3. Click ⊕ Add device.

4. Choose Other Device.
5. Choose Multilevel Sensor.
6. Enter the name.
7. Choose a room.
8. Choose Sensor Type.
9. Choose sensors that should be linked.
10. Choose which function should be used to calculate the value.
11. Save.

^ Back To Top

Cameras

Adding Nice Cameras

Supported cameras: Your camera must use MJPEG video compression format. H.264, H.265, RTSP, and other streaming formats are not supported in the Configuration Interface.

1. Open the Configuration Interface.
2. Go to ⚙ > Devices.
3. Click ⊕ Add device.
4. Click *IP Camera.*
5. Choose Manufacturer and Model of your device (select Other if your camera isn't on the list).
6. Click *Next.*
7. Go to the Advanced tab.
8. Enter data for your camera.
9. Click *Save.*

^ Back To Top

Quick Apps

The concept of Quick Apps is an evolution of plugins and virtual devices found in previous FIBARO gateways.

It is possible to use Quick Apps to prepare integrations with the devices which are not Z-Wave, but offer some API which can be implemented in our Quick App.

Advantages of the new Quick Apps approach:

- easier development
- simple installation
- quick configuration
- use in scenes

Creating Quick Apps

1. Open the Configuration Interface.
2. Go to ⚙ > Devices.

3. Click Add device.
4. Choose Other Device.
5. Choose Quick App.
6. Enter the name of the Quick App.
7. Choose a Room.
8. Choose the device type .
9. Click > next to the created Quick App.
10. Go to Edit&Preview tab.
11. Click *Edit*.
12. Drag & drop items and enter the Lua code (learn more here).
13. Click *Save*.

Learn more about programming Quick Apps

Downloading file

1. Open the Configuration Interface.
2. Go to ⚙ > Devices.
3. Click > next to the Quick App.
4. Open the Advanced tab.
5. Click *Download*.

Uploading file

1. Open the Configuration Interface.
2. Go to ⚙ > Devices.
3. Click Add device.
4. Choose Other Device.
5. Choose Upload File.
6. Choose file from your computer.

Types of Quick App devices

- Binary sensor
- Binary switch
- Color controller
- Door lock
- Door sensor
- Energy meter
- Generic device
- Flood sensor
- Humidity sensor
- Multilevel sensor
- Multilevel switch
- Player
- Power sensor
- Remote controller
- Roller shutter
- Smoke detector
- Temperature sensor
- Thermostat (auto, cool, heat)
- Weather
- Wind sensor
- Window sensor

^ Back To Top

Notifications

Setting notifications for the device

1. Choose the states of the device you want to be informed about.
   Available options depend on the device type.
2. Choose the interval for the notification:
   - Once (will be done once when the event occurs),
   - Once per minute (at the full minute),
   - Once per hour (at the full hour),
   - Once per day (every day at 12.00),
   - Once per week (Monday at 12.00).
3. Choose the channel of communication:
   - E-mail,
   - Push.
4. That's all. You will now be informed every selected time interval the device will be in one of the states you chose.

^ Back To Top

Settings

Changing Name

1. Open the Configuration Interface.
2. Go to ⚙ > Devices.
3. Click on the frame next to the device you want to rename.
4. Enter new name.

Changing Room

1. Open the Configuration Interface.
2. Go to ⚙ > Devices.
3. Choose a room from the list.

Changing Category

Categories are used to filter devices in the History window and in the Home Center mobile app.

1. Open the Configuration Interface.
2. Go to ⚙ > Devices.
3. Click > next to the device.
4. Choose one of the categories:
    - Lights,
    - Blinds,
    - Ambience,
    - Climate,
    - Gates,
    - Safety,
    - Security,
    - Multimedia,
    - Remotes,
    - Other.

Changing Icon

1. Open the Configuration Interface.
2. Go to ⚙ > Devices.
3. Click > next to the device.
4. Choose one of the default icons or add new one.

Adding an icon

1. Open the Configuration Interface.
2. Go to ⚙ > Devices.
3. Click > next to the device.
4. Click *ADD ICON* (Size of the icon must be 128px/128px).

Theoretical power consumption

For switches without a built-in power metering feature, you can define the theoretical power consumption. Whenever the device is turned on, the meter will assume that it consumes power set by the user (in Watts).

1. Open the Configuration Interface.
2. Go to ⚙ > Devices.
3. Expand the device you want set the theoretical power for.
4. Open the Advanced tab.
5. Enabled the *Theoretical power consumption* and set the power.
6. Save.

^ Back To Top

Migrating data

Migrating data from Home Center 2/Lite

If you have Home Center 2 or Home Center Lite you can migrate parts of the configuration to the new gateway.

IMPORTANT:

If the transfer fails, contact the Technical Support and do not repeat the procedure!

Prerequisites

- The source and target gateways need to be added to the same FIBARO ID account.
- The source (HC2/HCL) gateway must have version 4.581 or higher.
- The target (HC3) gateway must have version 5.021 or higher.

What will be transferred

- sections, rooms, icons,
- Z-Wave devices assigned to the rooms and their icons,
- parameters of these devices,
- camera devices (but not ones created using plugins),
- associations.

Thermostats will get re-added to the gateway but they will be queued for reconfiguration. They will receive a new ID, default icon, and will be assigned to the default room.

What won't be transferred

- scenes,
- plugins,
- energy consumption,
- virtual devices,
- camera plugins,
- schedules (watering, climate).

The migration process is irreversible!

Migration from Home Center 2 to Home Center 3

1. Visit **home.fibaro.com**.
2. Click **Transfer Configuration**.
3. Choose **Source Home Center**.
4. Choose **Target Home Center**.
5. Click **Start Process**.
6. Source Home Center 2 will reset Z-Wave chip, and all backups will be moved to Home Center 3.
7. **Log in** to Home Center 3 (you can find it via **find.fibaro.com**).
8. Click **Finish Migration**.
9. Home Center 3 will now restore the latest backup.
10. Wake up all battery devices.

Configuration on the source gateway (i.e. Home Center Lite or Home Center 2) will be left in read-only state. You may find it useful for future reconstruction of your scenes and automations.

Migration from Home Center Lite to Home Center 3

1. Contact FIBARO Support and ask for setting your Home Center Lite as the **artificial donor**.
2. Visit **home.fibaro.com**.

3. Click **Transfer Configuration**.
4. Choose **Source Home Center**.
5. Choose **Target Home Center**.
6. Click **Start Process**.
7. Home Center Lite will be used to source the data and all backups will be moved to Home Center 3.
8. **Log in** to Home Center 3 (you can find it via **find.fibaro.com**).
9. Click **Finish Migration**.
10. Home Center 3 will now restore the latest backup.
11. Wake up all battery devices.

> Configuration on the source gateway (i.e. Home Center Lite or Home Center 2) will be left in read-only state. You may find it useful for future reconstruction of your scenes and automations.

^ Back To Top

Configuration

Connecting gateways

By connecting gateways, you can greatly increase the range of your Z-Wave network. You can connect multiple Slave gateways to one Master gateways. All of the configuration (like scenes, panels, etc.) is done and stored on the Master gateway.

Requirements

- All of the connected gateways must have the same firmware version.
- Slave gateways must be empty and be restored to factory defaults.
- All of the gateways must be in the same subnetwork.
- You can connect the Home Center 3 gateway with another Home Center 3, Home Center 3 Lite and Yubii Home gateway.

Note: Only the Home Center 3 gateway can be used as a master!

Connecting Slave gateway to Master gateway

1. Open the Configuration Interface of the Master gateway.
2. Go to ⚙ > Connect Gateways .
3. Under *List of gateways in your LAN* you will see a list of all gateways detected in your network.
4. Click *Connect* next to the gateway you want to connect it as Slave gateway.
   If the gateway has *Configure* button instead of *Connect* button, it means it does not meet the requirements (prepare it using the instructions below).

Preparing a gateway for connecting it as a Slave gateway

1. Open the Configuration Interface of the gateway you want to connect as a Slave gateway.
2. Go to ⚙ > Connect Gateways .
3. Click *Prepare Home Center to be Slave*.
4. Confirm.
5. Wait for the gateway to reset to factory defaults.

^ Back To Top

Rooms and sections

Rooms and sections are used to organize devices to reflect their place in your house.

Sections

Sections represent areas in your house (e.g. floors) and rooms can be assigned to them.

Adding sections

1. Open the Configuration Interface.
2. Go to ⚙ > Rooms.
3. Click *Manage sections.*
4. Type in a new name and click plus icon.

Deleting sections

1. Open the Configuration Interface.
2. Go to ⚙ > Rooms.
3. Click *Manage sections.*
4. Click 🗑 next to the section you want to delete.

Rooms

Rooms represent rooms and other places in your house (e.g. living room, corridor) and devices can be assigned to them.

Adding rooms

1. Open the Configuration Interface.
2. Go to ⚙ > Rooms.
3. Click *Add room.*
4. Set room information:
   - Category – categories are used for filtering rooms by type,
   - Name – name of the room,
   - Section – section of the house the new room will be assigned to,
   - Icon – icon that will represent the room.
5. Save.

Editing rooms

1. Open the Configuration Interface.
2. Go to ⚙ > Rooms.
3. Click ••• in the top right corner of the room icon.
4. Click *Edit.*

5. Edit room information:
    - Category – categories are used for filtering rooms by type,
    - Name – name of the room,
    - Section – section of the house the new room will be assigned to,
    - Icon – icon that will represent the room.
6. Save.

Deleting rooms

1. Open the Configuration Interface.
2. Go to ⚙ > Rooms.
3. Click ••• in the top right corner of the room icon.
4. Click *Delete*.
5. Confirm.

Default room

New devices will be automatically assigned to the default room.

To choose the default room:

1. Open the Configuration Interface.
2. Go to ⚙ > General.
3. Set Default room (under the section: Main Sensors).

^ Back To Top

Network settings

Checking network status

There are two ways to check network status of the gateway:

1) By checking the diodes on the Home Center housing:

Internet diode
Copper – connected to Internet
Red – disconnected from Internet

LAN diode
Copper – connected to LAN
Fast pulsing copper – connecting to LAN

Wi-Fi diode
Copper – connected to Wi-Fi
Fast pulsing copper – connecting to Wi-Fi
Red – incorrect Wi-Fi password / other error
Green – Wi-Fi in Access Point mode

2) By checking the network status in the Configuration Interface:

⚙ > Network > Internet Status

LAN connection

Connecting to LAN network:

1. Connect the gateway to your home's Internet router using the provided Ethernet cable.
2. Open the Configuration Interface.
3. Go to ⚙ > Network > LAN connection.
4. Set connection type :
    - DHCP – IP will be assigned dynamically by the router,
    - Static – you must enter all settings manually, remember to reserve the IP address for the gateway in the router's settings.
5. Set remaining options.

How to set static IP Address:

Setting static IP address on a gateway consists of at least three steps:
1. Determine the IP of the gateway and decide whether is it the IP you want to leave permanently.
2. Configure the home router so that it also keeps the IP for this device.
3. Set the selected IP in the Configuration Interface:

1. Open the Configuration Interface.
2. Go to ⚙ > Network > LAN connection.
3. Set *Network connection type* to Static/Manual.
4. Input the IP address you want to set for the gateway.

How to set dynamic IP Address:

1. Open the Configuration Interface.
2. Go to ⚙ > Network > LAN connection.
3. Set *Network connection type* to DHCP.

Wi-Fi connection

Connecting to a Wi-Fi network:

1. Open the Configuration Interface.
2. Go to ⚙ > Network > Wi-Fi connection.
3. Enable Wi-Fi.
4. Click *Search & Connect to Network*
    - If your network is on the list:
        - Select the network from the list and click *Next*,
        - Enter password if needed.
    - If your network is not on the list:
        - Select *Different/Hidden* and click *Next*,
        - Enter the network name (SSID) and security details.
5. Click *Connect*.

How to set static IP Address:

Setting static IP address on a gateway consists of at least three steps:
1. Determine the IP of the gateway and decide whether is it the IP you want to leave permanently.
2. Configure the home router so that it also keeps the IP for this device.
3. Set the selected IP in the Configuration Interface:

1. Open the Configuration Interface.
2. Go to ⚙ > Network > Wi-Fi connection.

3. Set *Network connection type* to Static/Manual.
4. Input the IP address you want to set for the gateway.

How to set dynamic IP Address:

1. Open the Configuration Interface.
2. Go to ⚙ > Network > Wi-Fi connection.
3. Set *Network connection type* to DHCP.

Resetting network settings

Resetting network settings will restore Wi-Fi and LAN factory settings.

Using buttons on the cover:

1. Hold the ⊕ button for 20 seconds.
2. LAN and Wi-Fi indicators will blink red.

Using Recovery Interface:

1. Open the 💊 Recovery Interface.
2. In *Network Settings* section click *Reset.*

Secure connection

The gateway can use HTTP and HTTPS protocols for communication. Use HTTPS to ensure security by encrypting communication.

To set connection type:

1. Open the Configuration Interface.
2. Go to ⚙ > Network > Secure Connection.
3. Select connection type:
    - HTTP – standard connection without additional encryption,
    - HTTPS – secure encrypted connection,
    - HTTP/HTTPS – the gateway will accept both types of connection.
4. Save.

REMEMBER: Your browser might show you a warning when connecting via HTTPS, in this case, do the following:

1) Download certificate from the Secure Connection section in Network settings and install it on your system (and browser),

2) Use the gateway's serial number to connect locally, i.e. use serial_number.local, e.g. https://hc3-00000001.local

› Installing root certificate on Windows

^ Back To Top

Users and access

Users

User roles

- **Admin** – only one user, can configure the system, operate devices, add users and give them permissions.
- **User** – one or more users, can switch devices on/off, see the state and history data of devices.

Adding users

1. Open the Configuration Interface.
2. Go to ⚙ > Access > Users.
3. Click *Add user.*
4. Enter Name and E-mail (we recommend using FIBARO ID) of added user and click *Next.*
5. Message with local password for the new account will be sent to entered e-mail address.

Sharing remote access via FIBARO ID

Only owner can share access to the gateway via FIBARO ID.

1. Log into Remote Access with your FIBARO ID.
2. Chose the gateway which you want to add the user to.
3. Click > next to the Open button.
4. Click *Add user* button.
5. Enter FIBARO ID e-mail address of the user you want to give access to your gateway.
6. Click *Add.*
7. Open the Configuration Interface.
8. Go to ⚙ > Access > Users.
9. Click *Synchronize.*
10. User with access via FIBARO ID will have ✓ icon on the list.
11. If the user didn't already have an account, message with local password for the new account will be sent to entered e-mail address.

Giving permissions to user

For a new user to be able to use the gateway, admin must give it appropriate privileges.

1. Open the Configuration Interface.
2. Go to ⚙ > Access > Users.
3. Click *Manage Access* on the user list.
4. Select sections and/or devices to give the user access to them.
5. Click *Save.*

Managing user's mobile devices

1. Open the Configuration Interface.
2. Go to ⚙ > Access > Users.
3. Click > next to the user.
4. To add a mobile device to the gateway, log in to the mobile application on the given device.
5. To remove a mobile device from the gateway, click the 🗑 next to it and then confirm action by clicking *DELETE.*
6. Select "Send notifications" checkbox if you want to receive notifications on mobile devices.

Setting PIN for the user

1. Open the Configuration Interface.
2. Go to ⚙ > Access > Users.
3. Click > next to the user
4. Enter the PIN code. Remember it, you will need this to change it and to disarm the alarm.
5. Select "Ask for PIN when arming" checkbox to increase safety and prevent unintentional arming.

Setting local password for the user

1. Open the Configuration Interface.
2. Go to ⚙ > Access > Users.
3. Click the > next to the user.
4. Enter new local password.
5. Click *Save.*

Transferring admin privileges

1. Open the Configuration Interface.
2. Go to ⚙ > Access > Users.
3. Choose the non-admin user to transfer the rights.
4. Click > next to this user.
5. Click *TRANSFER ADMIN ROLE.*
6. Click *Transfer* to confirm.
7. Message about transferring the admin role will be sent to the chosen user's e-mail address.
8. User has to log into the gateway. In the top right corner click its e-mail address and choose *Account Settings.*
9. Click *ACCEPT* to accept the transfer.

Remote access

Remote Access allows you to connect and manage your control panel and devices from a remote area outside your home. The gateway must be connected to the Internet and powered on.

Enabling remote access

Remote access is enabled by default.

To enable/disable remote access:

1. Open the Configuration Interface
2. Go to ⚙ > Access > Remote Access.

3. Enable/disable Remote Access toggle.

Support Access

You should enable Support Access when you have an issue that you cannot resolve on your own. By granting access to your gateway, the support team may be able to find problems faster.

Enabling Support Access

To enable support access:

1. Open the Configuration Interface.
2. Go to ⚙ > Access > Remote Access.
3. Enable Support Access toggle.

Installer Access

The FIBARO System can be configured on your own or by a certified FIBARO Installer. In case your system has been configured by the FIBARO Installer, the Installer Access may facilitate his later work by allowing him to monitor and access to selected information of your system.

Enabling Installer Access

Enabling Installer Access enables FIBARO Installer to check up on your system and fix smaller issues remotely.

Setting Installer permissions

You can allow installer to:

- monitor your gateway (current status, active LEDs, status of services, backups etc.),
- give access for 24h to perform remote actions on your gateway.

Enter Installers FIBARO ID and click Add Installer to give him access to your gateway. Choose mobile devices that can receive push notifications from the installer.

^ Back To Top

Time and units

The gateway gives you possibility to set the time, time zone, units and even separators!

To adjust the settings:

1. Open the Configuration Interface.
2. Go to ⚙ > General.
3. Open the Time & Units tab.

Now you can change settings, such as:

Date and time:

- Time zone,
- Date and time (you can get it from the NTP server or set manually),
- NTP server,
- Date format,
- Hour format (12-hour, 24-hour),
- Date,
- Time.

Units and separators:

- Temperature unit (Celsius, Fahrenheit),
- Wind speed unit (km/h, mph),
- Decimal mark (comma, dot).

^ Back To Top

Location

Setting location in the gateway allows you to personalize your smart home experience.

Location is used for weather retrieving and can also be useful for automation purposes.

Once you set your home and/or work location, you can trigger certain scenes via entering or leaving the zone.

To set your home location:

1. Go to ⚙ > General > Location (tab).
2. Drag the map so that you see your home address.
3. Click the location of your home to update the pin.
4. Set the radius accordingly to your house and property size, e.g. 100m.
5. Save.

To add another location:

1. Go to ⚙ > General > Location (tab).
2. Click **Add Location**.
3. Enter the name of your new location, e.g. Work.
4. Drag the map and click the place of your work.
5. Set the radius of your work, e.g. 300 m.
6. Save.

^ Back To Top

VoIP

Home Center VoIP server

Home Center can act as a VoIP server. Once configured, it can manage the VoIP connections between the clients. To use VoIP on end devices, you must use a compatible VoIP app on your mobile device. The Home Center gateway must be reachable via the given medium of transmission and configured first.

Adding clients

1. Open the Configuration Interface.
2. Go to ⚙ > VoIP.
3. Click *Add VoIP client*.
4. Enter Display name, VoIP username, and VoIP password.
5. Click *Add* to Save.
6. The new VoIP user has been created and it is at the end of the list.

> You can always temporary disable the user without removing him by changing his Active state.

VoIP in mobile apps

Each VoIP app may differ in configuration, but the most important is the IP of the Home Center gateway and user credentials.

When you configure VoIP on Home Center, you set up users and their passwords/pins.

During configuration on your mobile device you need to enter those things:

1. The IP address of the gateway.
2. User credentials for a specified earlier VoIP user.

^ Back To Top

Z-Wave

This screen is dedicated to Z-Wave configuration.

Z-Wave Settings allows to:

- Reconfigure all devices,
- Reconfigure mesh network (You can choose if you want to configure entire Z-Wave network or single devices),
- Broadcast “Node Information” frame,
- Add secondary controller,
- Transfer controller,
- Reset energy metering,
- Reset Z-Wave,
- Enable devices polling,
- Poll unavailable devices,
- Mark nodes as unavailable,
- Set devices polling time interval,
- See number of devices added to your gateway.

^ Back To Top

Automation

Scenarios

Click **HERE** to find out more about the Scenarios.

^ Back To Top

Scenes

Scenes allow automating your system to provide the real Smart Home experience. They can integrate multiple devices included in your system and may be activated by weather conditions, a series of intuitive timers or various sensor/module states.

There are two types of scenes to create in the interface:

- **Block Scenes** are easy to build. Using number of available customizable blocks complex scenes can be visually created. It is not possible to implement all functionalities of the FIBARO System with Block Scenes, but are the best way for a basic user to enhance home automation.
- **Lua Scenes** are most advanced, but allow user to fully utilize all FIBARO System capabilities. Such scenes are based on the Lua programming language and require basic programming skills.

Creating scenes

1. Open the Configuration Interface.
2. Go to ⚙ > Scenes.
3. Click *Add scene.*
4. Choose scene type.
5. Set basic settings:
   - Name – name of the scene.
   - Run scene – choose if the scene will be run automatically (when conditions are met) or manually (ignore conditions).
   - Allow to restart a running scene – if set to*Yes*, every new activation of the scene restarts it, if set to *No*, scene can’t be activated again if it is already running.
   - Category – categories are used for filtering scenes by type.
   - Icon – icon that will represent the scene.
6. Save.

Read further on creating scene using blocks here.

Editing scenes

1. Open the Configuration Interface.
2. Go to ⚙ > Scenes.
3. Click the ✎ to edit the scene.
4. Edit scene.
5. Save.

Deleting scenes

1. Open the Configuration Interface.
2. Go to ⚙ > Scenes.
3. Click the 🗑 to delete the scene.
4. Click *Delete*.

Duplicating scene

1. Open the Configuration Interface.
2. Go to ⚙ > Scenes.
3. Click 🗐 next to the scene you want to duplicate.
4. Click *Copy* to confirm.

Converting Block Scene to Lua Scene

1. Open the Configuration Interface.
2. Go to ⚙ > Scenes.
3. Click LUA→ next to the scene you want to duplicate.
4. Click *Copy & Convert* to confirm.

Managing scene settings

Changing name

1. Open the Configuration Interface.

2. Go to ⚙ > Scenes.
3. Click on the frame next to the scene you want to rename.
4. Enter new name.

Disabling/enabling

1. Open the Configuration Interface.
2. Go to ⚙ > Scenes.
3. Click *Disable/Enable* button next to the scene you want to disable/enable.

Changing triggering mode (manual/auto)

In auto mode, the scenes runs automatically, when triggers and conditions are met, in manual mode the scene can be triggered only manually by the user.

1. Open the Configuration Interface.
2. Go to ⚙ > Scenes
3. Click toggle to change triggering mode.

Changing other settings

1. Open the Configuration Interface.
2. Go to ⚙ > Scenes.
3. Click > to expand the scene.
4. Edit scene settings:
    - Allow to restart a running scene – if set to*Yes*, every new activation of the scene restarts it, if set to *No*, scene can't be activated again if it is already running.
    - Category – categories are used for filtering scenes by type.
    - Scene hidden – check to hide scene from interfaces.
    - Require PIN to run – check if you want to protect the scene by requiring PIN to run it.
    - Icon – icon that will represent the scene.
5. *Save*.

Running scenes

1. Open the Configuration Interface.
2. Go to ⚙ > Scenes.
3. Click *Play* button next to the scene which you want to run.

Variables

Variables allow you to create more advanced scenes and home automations which goes beyond just a scene setup. There are situations and things that you want to keep track outside the particular scene, or you want to share the variable across different scenes.

Standard variable – The Standard variable can store any value you wish. The value stored in the Standard variable can be set manually in ⚙ > General > Variables or from a scene. It can then be used as part of a condition in other scenes.

Enumerated variable – The Enumerated variable has set values that you configure when you create the variable. The variable can then only be set to one of these preset values. It is useful having defined values such as Night, Day, Home, Away etc.

1. Open the Configuration Interface
2. Go to ⚙ > General > Variables.
3. Click *Add Variable*.
4. Choose Standard or Enumerated variable.
5. Enter the Name and Value/Values.
6. Click *Add*.

Events

Custom events may be used to expand the functionality of scenes. Similar to variables, they can be used to connect different scenes, but they do not store any additional information, only that something happened (specified by you). You can emit your custom event in scenes and QuickApps, then use it to trigger other scenes.

Creating an event

1. Open the Configuration Interface
2. Go to ⚙ > General > Events.
3. Click *Add Event*.
4. Choose the name for the event.
   The name cannot contain:
    - digits at the beginning of the name,
    - special characters (only letters from English alphabet),
    - spaces.
5. Fill in the description.
6. Click *Add*.

^ Back To Top

Block Scenes

Check here to see documentation for Block Scenes.

^ Back To Top

Lua Scenes

Check here to see documentation for Lua Scenes.

^ Back To Top

Climate schedules

Temperature schedules allow for automatic control of heating and cooling for each area (zone) of the house.

Devices controlling temperature (e.g. thermostats) are required to a create the temperature zone. You can create your own thermostats by connecting a temperature sensor and actor that turns heating/cooling on/off.

Creating Thermostats

1. Open the Configuration Interface.
2. Go to ⚙ > Devices.
3. Click ⊕ Add device.
4. Choose Other Device.
5. Click *Thermostat*.
6. Enter the name of the thermostat.
7. Choose a Room.
8. Choose the main device.
9. Select heating and/or cooling devices.
10. *Save*.

Adding zones

1. Open the Configuration Interface.
2. Go to ⚙ > Climate.
3. Click *Add Zone*.
4. Select how zones should be created:
    - Automatically – zones will be created automatically for all rooms with temperature devices.
    - Manually – manually select devices to be included in the new zone.

Zone modes

- Schedule – zone works according to the set schedule.
- Manual – constant temperature is set for a specified time duration.
- Vacation – constant temperature is set until disabled.

Configuring zone schedule

1. Open the Configuration Interface.
2. Go to ⚙ > Climate.
3. Click > to expand the zone.
4. Select operating mode:
    - Heating: devices increase the temperature to reach the temperature setpoint,
    - Coolin: devices decrease the temperature to reach the temperature setpoint,
    - Auto: devices determine if they should cool or heat to reach the temperature setpoint,
    - Off: devices are always off.
5. Set start times for periods by moving the sliders or entering them below.
6. Enter temperatures to be set on each period.
7. *Save*.

If you want to use the same schedule on multiple days, you can set it once, then copy it to the remaining days.

Editing zone name and devices

1. Open the Configuration Interface.
2. Go to ⚙ > Climate.
3. Click the ✎ to edit the zone.
4. Change name or devices in the zone.
5. *Save*.

^ Back To Top

Garden care

Watering schedules allow for automatic control of your sprinklers.

You need to create sprinklers first in order to configure watering schedules.

Creating sprinklers

1. Open the Configuration Interface.
2. Go to ⚙ > Devices.
3. Click ⊕ Add device.
4. Choose Other Device.
5. Choose Sprinklers.
6. Fill in new sprinkler settings:
    - Enter the name.
    - Choose a room.
    - Choose watering devices.
    - Choose watering default time.
    - Select soil moisture sensor (optional).
    - Set humidity level to turn off watering.
7. *Save*.

Editing sprinklers

1. Open the Configuration Interface.
2. Go to ⚙ > Devices.
3. Find your sprinkler on the list.
4. Click > next to the sprinkler you want to edit.
5. Click *EDIT DEVICE*.
6. Edit settings and *Save*.

Adding and configuring watering schedules

Adding watering schedule

1. Open the Configuration Interface.
2. Go to ⚙ > Garden.
3. Click *Add Schedule*.
4. Insert name for watering schedule.
5. Click > to expand the schedule.
6. Choose days to apply the schedule for.
7. Click *Save*.

Adding watering sequences to a schedule

1. Click > to expand the schedule.
2. Click *ADD SEQUENCE* to add new sequence to the schedule.
3. Choose devices to use in this sequence.
4. Click > next to the sequence to configure it.
5. Set order of the sprinklers and modify duration if needed.
6. Repeat steps 2-5 to add and configure more sequences.
7. Click *Save*.

^ Back To Top

Profiles

Profiles are sets of states (of devices, zones, scenes) that can be activated quickly by the user or a scene.

At least one profile is required. There are four default profiles, but you can add more if you want to.

Creating profiles

1. Open the Configuration Interface.
2. Go to ⚙ > Profiles.
3. Click *Add Profile*.
4. Name the new profile.
5. If you want to copy settings from another profile, select it in *Based on* field.
6. Select icon for the new profile.
7. Click *Add*.

Configuring profiles

1. Open the Configuration Interface.
2. Go to ⚙ > Profiles.
3. Set how your scene, devices and zones should work in each profile.

Editing profile name and icon

1. Open the Configuration Interface.
2. Go to ⚙ > Profiles.
3. Next to profile name click •••.
4. Click *Edit*.
5. Change name or click new icon.
6. *Save*.

Deleting profiles

1. Open the Configuration Interface.
2. Go to ⚙ > Profiles.
3. Next to profile name click •••.
4. Click *Delete*.
5. Confirm.

Activating profiles manually

1. Open the Configuration Interface.
2. On the top bar click the name of current profile.
3. Click on the name of the profile you want to activate.

^ Back To Top

Alarms

Alarm feature allows to create alarm zones using sensors in your system. Breaching any sensor in an armed zone will trigger an alarm. The system will inform you about an alarm, you can also activates scenes when alarm triggers.

🚨 icon indicates the occurrence of an alarm. When alarm occurs, icon becomes red and clickable. Clicking 🚨 icon will direct you to Settings > Alarm so that you can see in which zone the alarm occurred.

Adding zones

1. Open the Configuration Interface.
2. Go to ⚙ > Alarm.
3. Click *Add Zone*.
4. Name the new zone.
5. Select rooms or devices to be included in the new zone.

Arming/disarming zones

Arming zone will arm all devices in this zone, and disarming the zone will disarm all devices in this zone.

1. Open the Configuration Interface.
2. Go to ⚙ > Alarm.
3. Under *Arming* column click the toggle to arm/disarm the zone.
4. Enter PIN if required (default PIN is 1111).

Setting PIN

The default PIN is 1111, we strongly recommed changing it.

1. Open the Configuration Interface.
2. In top right corner click your user name.
3. Choose *Account Settings* from the menu.
4. In *Alarm Settings* section:
    - Set 4-digit PIN.
    - Choose if you want the gateway to ask for PIN also while arming (not only disarming).
5. *Save*.

Setting delay for arming/disarming

1. Open the Configuration Interface.
2. Go to ⚙ > Alarm.
3. Enter delay time (in seconds) for the zone:
    - Entry delay – the alarm will delay triggering to allow you to disarm the zone when you enter it.
    - Exit delay – the alarm will delay arming to allow you to leave the zone without triggering it.

Editing zone name and devices

1. Open the Configuration Interface.
2. Go to ⚙ > Alarm.
3. Click the ✎ to edit the zone.
4. Change name or devices in the zone.
5. *Save*.

^ Back To Top

Maintenance

System report

The system allows to print a full report of the configuration for easier management and diagnostics.

The report gives you all the necessary information about the system at first glance. This can be useful for example for finding devices needing battery replacement or creating scenes.

The report includes information about:

- network configuration,
- rooms,
- devices,
- scenes,
- users,
- alarm zones,
- climate zones,

- garden schedules,
- profiles,
- general settings,
- variables and events,
- backups.

To generate system report:

1. Open the Configuration Interface.
2. Go to ⚙ > General.
3. Click *Generate* next to *Generate system report*
4. A new window with the report will open ready to print.

^ Back To Top

Recovery Mode

Recovery Mode allows retrieving the gateway operating system in case of technical problems, e.g. when the Configuration Interface is not reachable after update.
Using Recovery Mode you can repair the system or restore the default configuration (to its initial state).

The gateway maintains two copies of the system (System A and B) to ensure safety of your data during the firmware update. Updating system is always performed on the inactive system, then the gateway switches to it, thus maintaining copy of your data from before the update. In case of any problems, you can switch back to it.

Entering Recovery Mode

Using buttons on the cover:

1. Press and hold the ⏻ button for 15s, release when all indicators blink red at once.
2. Press and hold the ⊕ button, release when indicators start to blink a sequence from left to right.
3. When ⊕ indicator turns red, open the Recovery Interface in your Internet browser, as you would normally open the Configuration Interface.

Using Configuration Interface:

1. Open the Configuration Interface.
2. In top right corner click 👤.
3. Choose 🔗 Recovery Mode from the menu.
4. Confirm.
5. Wait for the system to reboot, ⊕ indicator will turn red.
6. Refresh the browser tab.

Auto-repairing system

In case of problems after updating your system, you can quickly repair it by using auto-repair. It will switch to copy of your system from before the last system update.

1. Enter the Recovery Mode.
2. Click Auto-repair.
3. Confirm.

Switching between systems

You can switch between system A and B at any moment using the Recovery Mode, e.g. when current system encounters a problem.

1. Enter the Recovery Mode.
2. Click Switch to System A/B.
3. Choose if you want to restore Latest version or use Local file.
4. Confirm.

Repairing system

This feature allows you to restore the operating system to the latest version or version from a file without deleting any user data. Only the system will be refreshed.
Depending on how you have entered the Recovery Mode, different system will be available for repairing: inactive when entered via configuration interface or active when entered using ⊕ button. Switch system to repair the other one.

1. Enter the Recovery Mode.
2. Click Repair System A/B.
3. Choose if you want to restore Latest version or use Local file.
4. Confirm.

Resetting network settings

In some cases, problems with the gateway may be caused by changes in the network configuration of the environment in which the gateway is located. If you do not want to restore the entire system to factory settings, try resetting the network settings first, as this may solve your problems with the gateway.

1. Enter the Recovery Mode.
2. Click Reset in the Reset Network Settings section.
3. Confirm.

Recovering system

CAUTION: The configuration will be removed and lost if not backed up.
This feature allows you to restore the operating system to the latest version or version from a file and delete all data from this system (users, devices, scenes etc.).
Depending on how you have entered the Recovery Mode, different system will be available for recovering: inactive when entered via configuration interface or active when entered using ⊕ button. Switch system to recover the other one.

1. Enter the Recovery Mode.
2. Click Recover System A/B.
3. Choose if you want to restore Latest version or use Local file.
4. Confirm.

Restoring factory defaults

CAUTION: The whole configuration will be removed and lost if not backed up.

This feature allows you to restore the gateway to factory settings. It means factory software version will be restored and all data from system A and B will be deleted (users, devices, scenes etc.).

1. Enter the Recovery Mode.

2. Click Factory Reset button under Network Status section.
3. Check “Yes, I’m sure and I know what I’m doing” checkbox.
4. Confirm action.

^ Back To Top

Updates

Updating the gateway

The gateway will inform you if there is a new update to be installed with ⊕ indicator pulsing copper. Updates may include new features, improvements, and bug fixes.
We recommend installing those updates as soon as they are available to ensure best operation and security.

> Updating the gateway in not possible via the Remote Access.

To update the gateway:

1. Go to ⚙ > Update > Home Center.
2. Click *Download Update* for the respective update.
3. Wait for the update to be downloaded.
4. Determine whether you want to do the cloud backup, local backup or no backups before the update.
5. Accept Terms & Privacy Policy.
6. Click *Install Update.*
7. Click *Update* to confirm the update.

Updating connected devices

> Updating the devices is not possible via the Remote Access.

To update devices:

1. Go to ⚙ > Update > Devices (tab).
2. Click *Update* next to available update or select multiple and click *Install Updates.*
3. Read the changelog and check the tickbox that you want to continue.
4. Click *Update.*

^ Back To Top

Backups

Backups of your entire system are the best way to prevent losing configuration data in case of any issues or unintentional changes. We recommend creating backups regularly.

There is limited storage for backups! You can store up to 2 local and up to 10 MB of backups in our cloud service. If you need more you can download and save them on your computer.

Creating backups

Creating cloud backups ☁

> Cloud backups require configured and enabled Remote Access (see link enable remote access).

1. Open the Configuration Interface.
2. Go to ⚙ > Backup > Cloud Backup.
3. Click *Create backup.*
4. Enter a description for the new backup.
5. Confirm.
6. Wait for the process to end (interface will be unavailable while creating the backup).
7. The backup will be added to your cloud backups.

Creating local backups

1. Open the Configuration Interface.
2. Go to ⚙ > Backup > Local Backup.
3. Click *Create backup.*
4. Enter a description for the new backup.
5. Confirm.
6. Wait for the process to end (interface will be unavailable while creating backup).
7. The backup will be added to your local backups.

Downloading local backup file

1. Open the Configuration Interface.
2. Go to ⚙ > Backup.
3. Click *Download* next to the local backup you want to download.
4. File with last local backup will be downloaded on your computer.

Restoring backups

> Cloud backups require configured and enabled Remote Access (see link enable remote access).

Restoring backup from the list

1. Open the Configuration Interface.
2. Go to ⚙ > Backup.
3. Next to backup you want to restore click *Restore.*

4. If provided with options:
    - Click *Restore & Convert* – backup created on earlier software version will be restored on the current version.
    - Click *Restore with version* – backup created on earlier software version will be restored with that version.
5. Confirm.
6. Wait for the process to end (interface will be unavailable while restoring backup).

Restoring local backup from file

1. Open the Configuration Interface.
2. Go to ⚙ > Backup > Local Backup.
3. Click *Upload backup.*
4. Select backup file on your computer.
5. Backup will be added to your list.
6. If you want to restore the backup, click *Restore* next to it.

^ Back To Top

Diagnostics

Diagnostics screen presents technical data about actual use of particular components, i.e. CPU, RAM, Storage, Z-Wave. This can help in troubleshooting or understanding how certain actions influence our system.

There are 4 tabs:

- **CPU** – shows the actual use of each core,
- **RAM** – shows the actual use of RAM memory and indicated how much percent is used for what purpose,
- **Storage** – shows the status of internal memory,
- **Z-Wave** – lists all Z-Wave devices that are not configured or without templates.

^ Back To Top

Integrations

Assistants

Are you tired of constantly searching for functions on your smartphone? Do you want your smart home to work on demand? This is possible thanks to the assistants. Check out the assistants that work with FIBARO!

Assistants that works with FIBARO:

- Google Assistant,
- Amazon Alexa,
- FIBARO Smart Home Bot.

Read articles about assistants:

- Google Assistant – FIBARO integration
- Amazon Alexa – FIBARO integration
- Amazon Alexa – Frequently Asked Questions
- List of FIBARO Smart Home Bot commands
- Connecting FIBARO Smart Home Bot
- FIBARO Smart Home Bot – Frequently Asked Questions

^ Back To Top

Security

Reporting a security issue

There are two ways to report a security issue:

1. **Report directly on FIBARO Security** (preferred)
    - Click on the “Report a security vulnerability” link. This file will expand the list of items to be filled.
    - Please provide all required elements and confirm.
    - Complete the form, which will be immediately incorporated into the Security Team workflow.
2. **Send an e-mail**
    - Send an e-mail to support@fibaro-security.atlassian.net

IMPORTANT! Do not post any information about the vulnerability to the public issue trackers or discuss it in public. FIBARO security team will investigate your report and then work with you and the project maintainer to create a fix. Once the fix is ready and released, FIBARO will announce the information to a wider audience.

Security report is acknowledged by e-mail within 3 working days by Fibaro security team. You will be updated using e-mail communication on the status of the issue once the team has started working on the issue and additionally every 2 weeks after that.

^ Back To Top

CUSTOMER
FIBARO ID
Marketplace
Compatibility
Smart Home App
FIBARO Android app
FIBARO iOS app
FIBARO Intercom app
HomeKit

SUPPORT
FIBARO forum
FAQ
Warranty
Privacy Policy

B2B
Distributor
Installer
Architect
Real estate development
FIBARO Installer iOS App
FIBARO Installer Android App

ABOUT
Newsroom
About us
Why FIBARO
Works with FIBARO
Where to Buy
Contact

© 2024. Nice - Polska Sp. z o.o. All rights reserved.