UFO manual
II genration

Version 3.8

2024

VITRUM DESIGN

Subject:	System Integrator Manual UFO II Generation
Autor:	Vitrum Design S.r.l.
Revision:	3.8

The present document is to be considered STRICTLY CONFIDENTIAL. The contents described therein are to be deemed the intellectual property of Vitrum Design S.r.l. and have been produced by authorized personnel on behalf of the company.

Disclaimer

Legal disclaimers

Privacy

- *Pursuant to Legislative Decree 196/2003 (Privacy), it is specified that the use of the data and information contained in this document is prohibited, as well as their disclosure or communication to individuals and/or subjects unrelated to the proposed operation. It is therefore explicitly understood that the recipient of this document, upon receiving it, commits to confidentiality regarding the data and information contained in it, explicitly approving such restriction on use.*
- *If the recipient should ever disagree with this constraint, please promptly return this document, including any attachments, to Vitrum Design.*

Information

- *This document does not represent the entirety of either the Company or the project that the Company intends to carry out (the "UFO Project"), and thus, some information related to it may have been omitted. Vitrum Design does not undertake to provide the recipient with any updates or additions to this document even if errors, omissions, or incompleteness are identified.*
- *The information contained in this document has been prepared by the management of Vitrum Design or obtained through access to databases containing information and data in the public domain.*
- *Vitrum Design, therefore, does not guarantee anything about the completeness of the information contained therein, nor does it promise that the expected events will occur, although care and diligence have been exercised in preparing this document.*
- *Neither Vitrum Design nor its employees and collaborators assume any responsibility for the content of this document, even in cases where the recipient may suffer, even implicitly, damages or losses resulting from the omission of information, data, and analysis.*

Index

First steps

UFO is a smart home gateway developed by Vitrum Design S.r.l. is simple to use by the final user but with evolved functions.

It works with different devices (and device families, protocols) and provides a secure, reliable, and cost-effective ecosystem to integrate UFO with other protocols like Amazon Alexa™ and Google Home™.

UFO can be used with other dashboard or apps (for Google Android or Apple iOS), to meet various needs.

The backlite **brain button** provides visual feedback on the system's status and allows for quick operations with a simple touch.

The **backup batteries** allow for temporary power outages while preserving the integrity of the data and basic analysis functions of the smart home.

The integrated **USB** port allows interfacing the net with other systems or extending its functionalities.

Turning on

Once the UFO device is connected to the power, you should hear a confirmation beep, after this the system will be operational within the next 5 minutes.

If the device is already enabled for connection to the local network, it will be possible to access it through the discovery procedure. Alternatively, it will be possible to configure the network using one of the provided procedures.

Connection to your home network

"At the first power-up, or in case of modification to the WiFi router configuration (and if no **Ethernet dongle** is present), the system will automatically enter 'Access Point Mode'. To continue working, it will be necessary to provide UFO with access to the network through one of the following procedures:

- Connecting to the WiFi network (via connection to the device's access point or via Bluetooth, if supported)
- Connection via Ethernet dongle
- Enabling offline connection (the device must already be activated on the cloud, and there must be a user with the 'owner' role)."

USB/Ethernet interface

Through the USB port located next to the power connector, you can connect a USB Ethernet dongle (ensure that the device is supported), which will be automatically recognized by the system and enabled. The presence of the Ethernet dongle does NOT automatically disable the WiFi system; it will be the responsibility of the installer/user to manually proceed with the disablement from the settings section of the dashboard.

NOTE: In this scenario, any loss of connectivity due to the unplugging of the Ethernet dongle or signal loss on Ethernet will result in the automatic re-enablement of WiFi (connecting to the last configured SSID or enabling Access Point mode).

WiFi Configuration

If the system is in Access Point mode, you can connect to the exposed SSID to proceed with the network configuration through the following procedure:

1. Connect to the Access Point exposed by UFO. The suggested SSID will be equivalent to the product code (SKU) present on the device label (e.g., VTUF.1910.000.001).

NOTE: In the case of non-updated devices, the SSID consists of the string "UFO" followed by a series of **13** characters or numbers (e.g., UFO xxxxyxxxxyxxx). The password for the exposed Access Point will always be **12345678**.

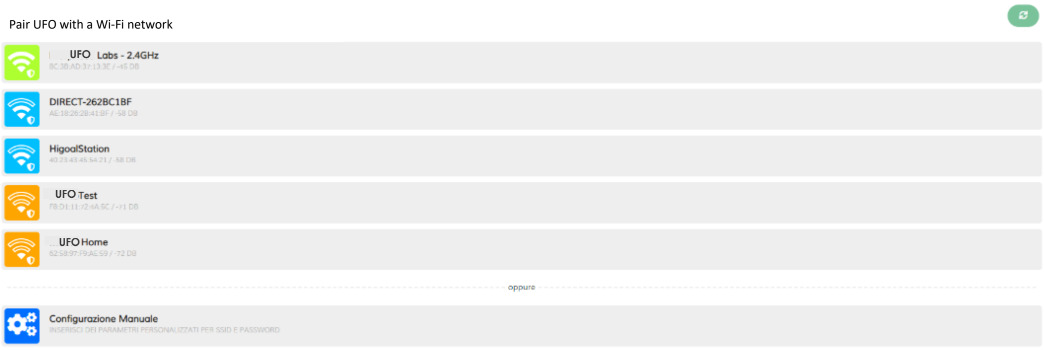
2. Enter the URL 192.168.12.1:8080 in a web browser (Google Chrome recommended).

3. A web interface will be presented, allowing you to select a network from a list of available networks or manually enter SSID and password.

NOTE: UFO only supports 2.4 GHz WiFi networks with WPA (or WPA2) encryption. WiFi networks with WEP encryption or without protection are NOT supported.

Wi-Fi Configuration

Pair UFO with a Wi-Fi network



UFO Labs - 2.4GHz
8C:3B:AD:37:13:3E / -45 DB

DIRECT-262BC1BF
AE:18:26:2B:41:BF / -58 DB

HigoalStation
40:23:43:45:54:21 / -58 DB

UFO Test
F8:D1:11:72:4A:5C / -71 DB

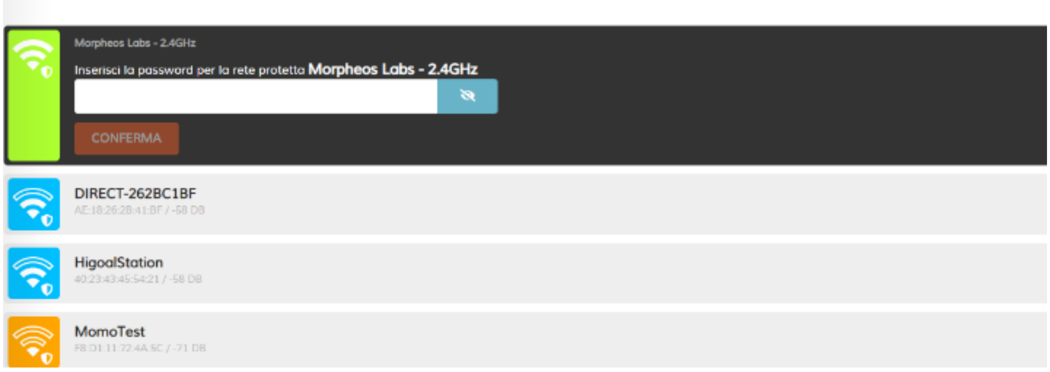
UFO Home
62:58:97:F9:AE:59 / -72 DB

oppure

Configurazione Manuale
INSERISCI DEI PARAMETRI PERSONALIZZATI PER SSID E PASSWORD

Wi-Fi Configuration

Pair UFO with a Wi-Fi network



Morpheos Labs - 2.4GHz

Inserisci la password per la rete protetta **Morpheos Labs - 2.4GHz**

DIRECT-262BC1BF
AE:18:26:2B:41:BF / -58 DB

HigoalStation
40:23:43:45:54:21 / -58 DB

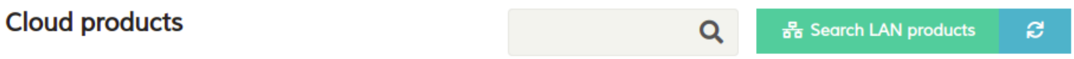
MomoTest
F8:D1:11:72:4A:5C / -71 DB

WiFi configuration with BLE

In case the system supports it (sys component >= 19.0.4 is required), it will be possible to configure UFO also through Bluetooth access, using the web dashboard or the mobile app (Refer to the mobile app manual for the specific configuration procedure).

Configuration from web dashboard

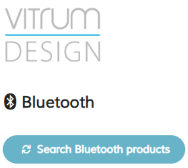
1. Access with a browser compatible with *WebBluetooth* technology (tested with MS Edge, Google Chrome, Mozilla Firefox) at https://dashboard.vitrum.com and select "Search LAN products" (or "Search the network")



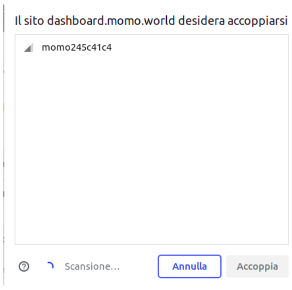
NOTE: It is ESSENTIAL to access using the HTTPS protocol; otherwise, Web-Bluetooth functionalities will not be available.

NOTE: If the dashboard is already displayed on a product, the relevant menu will be accessible by clicking on the box related to your user.

2. Click on the "Search Bluetooth products" button; a box will open, prompting the user to select the device to pair. Choose the device and click the "Pair" button.



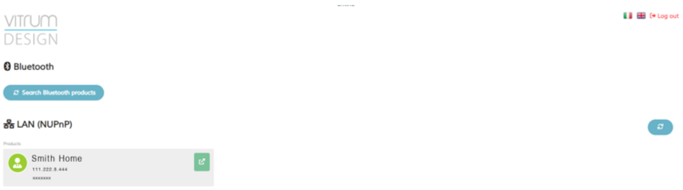
Bluetooth



Il sito dashboard.momo.world desidera accoppiarsi

momo245c41c4

3. A box related to the chosen device will appear. By pressing the orange button, you can proceed with the network configuration.



Bluetooth

LAN (NUPnP)

Products

Smith Home
111.222.3.444
xxxxxxx

4. Once the procedure has been successfully completed, it will be possible to connect to UFO via the local network.

Configuration from the Vitrum Design mobile app.

The Vitrum Design app, starting from version 1.7.1, allows configuring UFO's WiFi through Bluetooth.

1. Install the app on your device

    Google Android: https://play.google.com/store/apps/details?id=com.vitrum.ufo

    Apple iOS: https://apps.apple.com/it/app/vitrum-design/id1548058257

2. Log in to the app using valid credentials.
3. After logging in, go to the app's main menu using the burger menu at the top left and select the "Discovery UFO" menu.

    NOTE: If not confirmed previously, the app will ask the user for permission to enable Bluetooth scanning. If not confirmed, the scan cannot be completed.

    NOTE: In some cases, on Android systems, make sure that location permissions are also enabled.

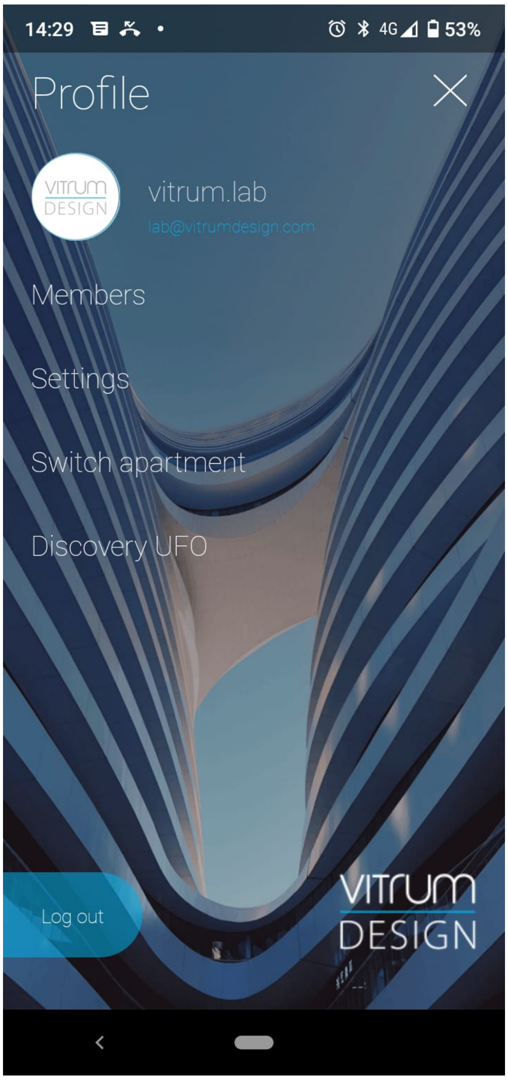
4. On the next page, the list of products available on the local network (LAN) and the results of Bluetooth scanning will be displayed. Select the device for which you want to configure WiFi from this second list.
5. Follow the activation procedure by providing valid SSID and Password.

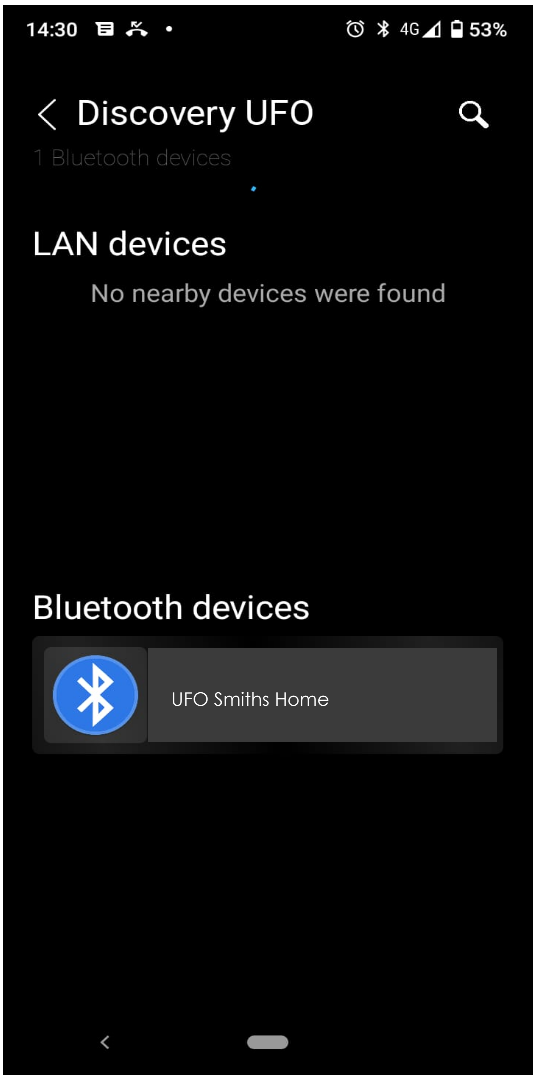
    NOTE: During configuration, ensure that UFO and the device (smartphone or tablet) from which the configuration is being done are close, and UFO is near the router to which you want to connect.

    NOTE: UFO supports only WiFi networks with WPA (or WPA2) encryption. WEP-encrypted or unprotected WiFi networks are not supported.

6. At the end of the procedure, the app should display a confirmation message, and the newly configured UFO should appear in the list of devices connected via LAN.

NOTE: At the current version it is not possible to carry out the first activation from the app mobile.

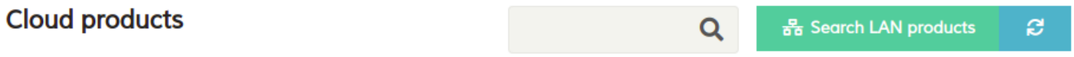




No nearby devices were found

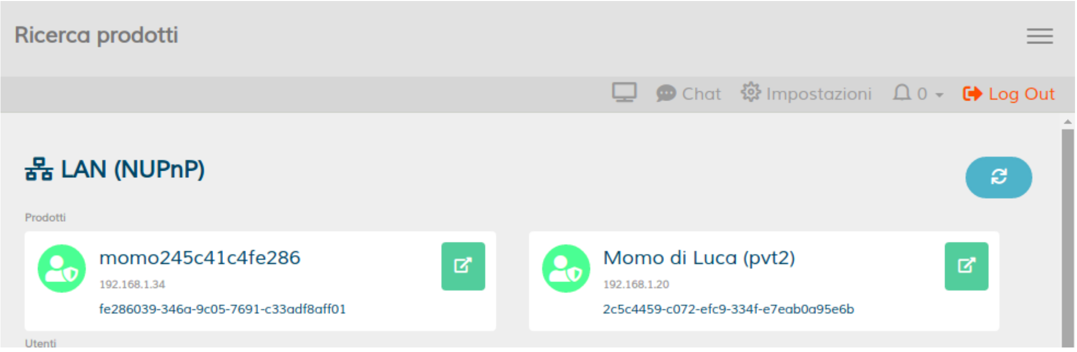
Searching for a product on the network (Discovery)

1. Go to https://dashboard.UFO .world and select “Search LAN pro-ducts” (or “Search the net-work”)



NOTE: if the dashboard is already present on a product, the menu in question will be available by clicking on the box relating to your user.

2. A list of all the devices present in the network will open, by clicking on the green icon it will be possible to access the product.
It is possible to update the list using the refresh button at the top right (light blue).



momo245c41c4fe286
192.168.1.34
fe286039-346a-9c05-7691-c33adf8aff01

Momo di Luca (pvt2)
192.168.1.20
2c5c4459-c072-efc9-334f-e7eab0a95e6b

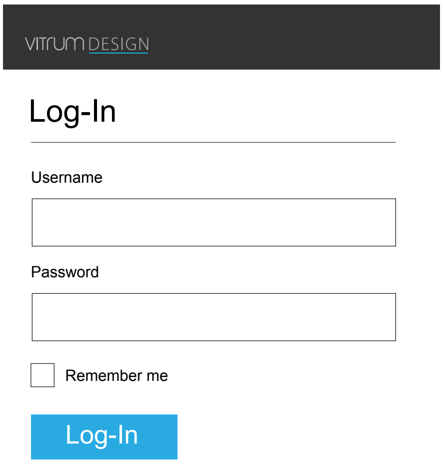
NOTE: the list on this page uses a service displayed by Vitrum Design. This list updates **every 5 minutes.**

Login and account registration

Once the address of the UFO dashboard has been entered, the user will be redirected to the login page or creation of a new account.

If you already have a valid account you can enter your credentials and click on the "Login" button.

In case you don't have a valid account, you can click on the link "Don't have an account? **Sign in".**



NOTE: Once logged in, the system stores a token within the browser that is valid for 180 days, upon expiry of which you will be asked to re-enter your credentials**.**

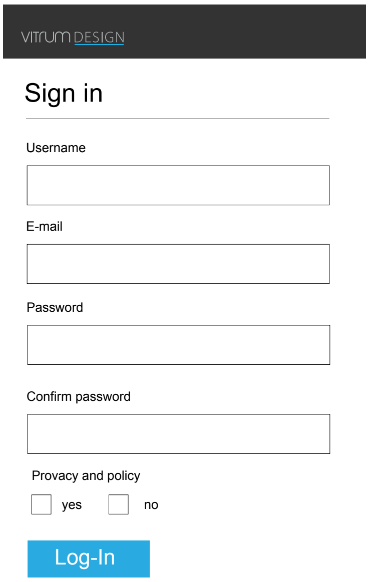
NOTE: browser cleaning procedures could delete your login data with the consequent obligation to re-enter them the next time you log in.

If you have forgotten your credentials, you can access the password recovery procedure via the "Have you forgotten your password?" link. which involves confirmation by clicking on a link to an email never sent to the email address associated with the user**.**

NOTE: before contacting support, check that the email has not been categorized as SPAM or is not in any custom folder (e.g. in the case of GMAIL it has often happened that emails are categorized as SPONSOR).

NOTE: There is no procedure for recovering your email address and you will therefore need to contact technical support**.**

New account creation



VITRUM DESIGN

Sign in

Username

E-mail

Password

Confirm password

Provacy and policy

□ yes □ no

Log-In

Fill out the registration form by entering your data and click on the "Register" button.

An email will be sent to the address provided inviting you to complete the registration by clicking on the link provided.

NOTE: before contacting support, check that the email has not been categorized as SPAM or is not in any custom folder (e.g. in the case of GMAIL it has often happened that emails are categorized as SPONSOR).

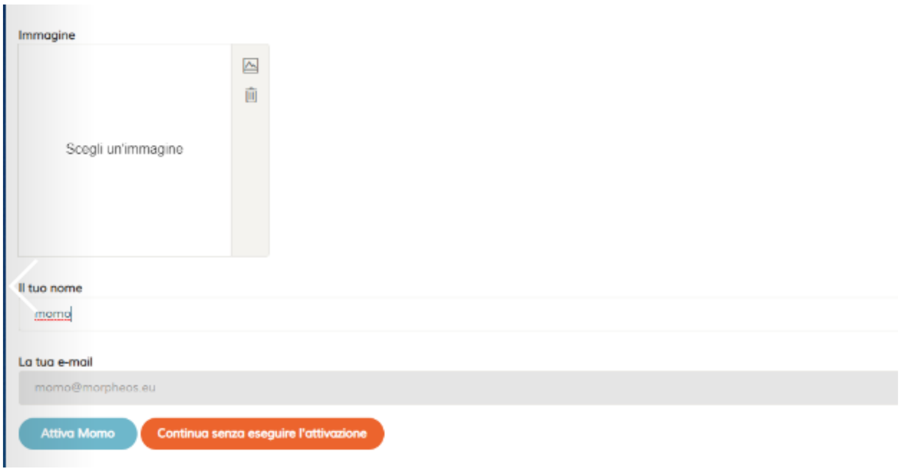
First activation

To use UFO, you need to first proceed with the **first activation**, which involves associating an owner user ("OWNER") and a home ("PROPERTY").

After logging in, if the product you are trying to access has not been activated yet, a window like the one shown in the figure will be presented, inviting the user to choose their name and image. This user will be the OWNER of UFO, the only user capable of having total system management and impossible to remove by any other user associated with UFO.

In the case of a user with the Vitrum Design Admin cloud role, the "Continue without activating" button will also be presented, useful for debugging or forcing updates.

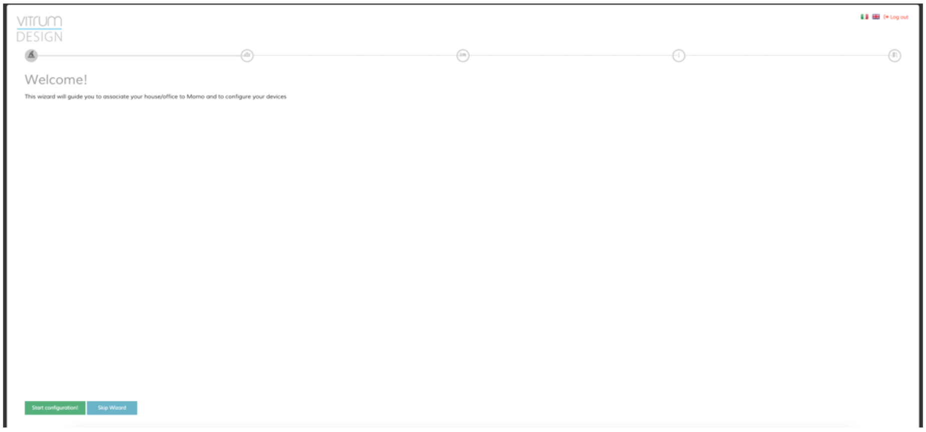
Once you click on the "Activate UFO" button, the system will proceed to register the product in the cloud, and the page will reload to allow for the initial configuration.



Il tuo nome: momo

La tua e-mail: momo@morpheos.eu

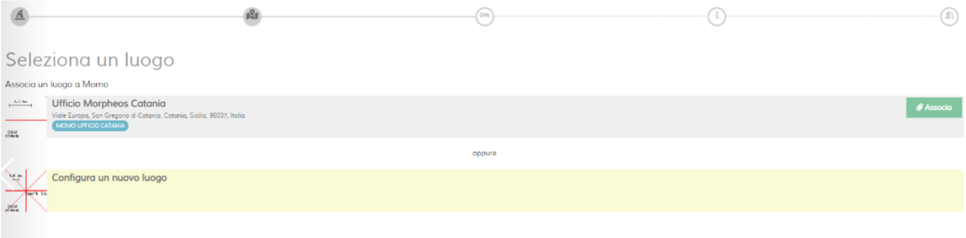
Start the configuration procedure by clicking on “let's get started”



Welcome!

This wizard will guide you to associate your house/office to Momo and to configure your devices

Choose a previously created home or set up a new one.



Seleziona un luogo

Associa un luogo a Momo

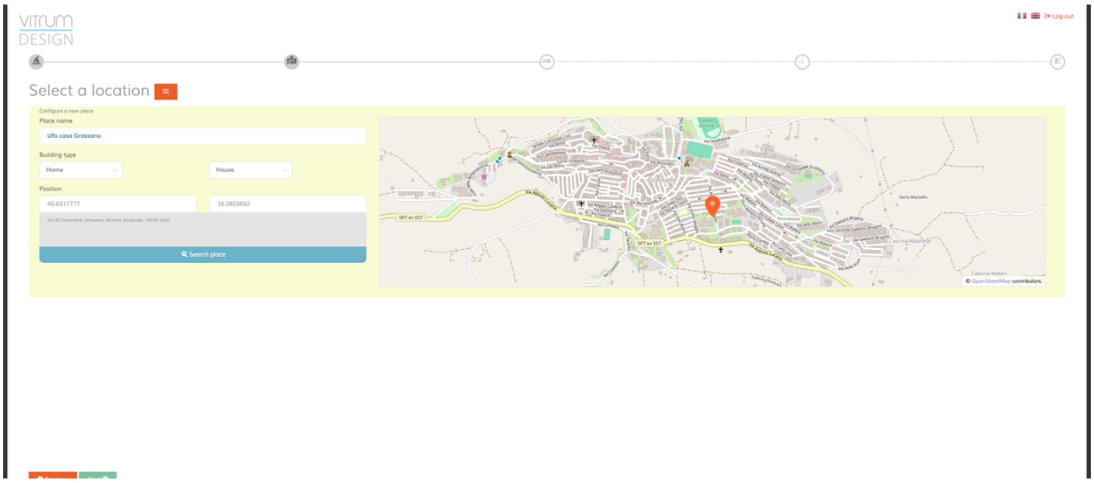
Ufficio Morpheos Catania

Viale Europa, San Gregorio di Catania, Catania, Sicilia, 95037, Italia

MOMO UFFICIO CATANIA

Configura un nuovo luogo

If you do not have any already configured home (or if you want to force the creation of a new residence), click on the "Configure a new place" button, enter the address, and select "Search place". From the list, select the entry corresponding to your search and refine the location by moving the center of the map.
Once the configuration is complete, enter the name you want to give to the house (e.g., UFO House Rossi) and click on the "Next" button.



Select a location

Configure a new place

Place name: Ufo casa Grassano

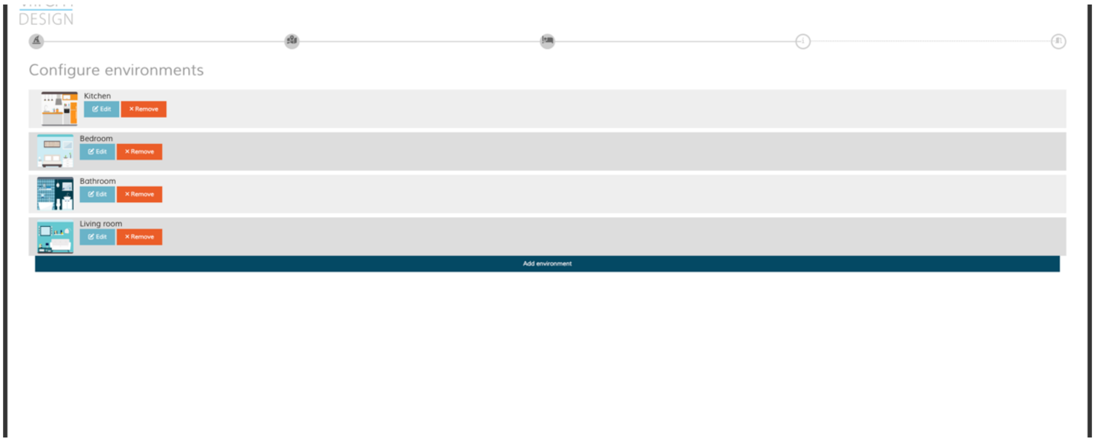
Building type: Home | House

Position: 40.6317777 | 16.2853652

Via 20 Settembre, Grassano, Matera, Basilicata, 75014, Italia

NOTE: In the case of changing homes or reactivating a product, this procedure might involve a restart of UFO, taking more time and causing a temporary disconnection from the dashboard. It is an expected and entirely normal behavior, which generally should not take more than 3 minutes but could involve downloading all the house information from the cloud (thus depends on the Internet connection speed).

Configure the rooms in the house and click on the "Next" button (rooms can also be created or modified later).



Configure environments

Kitchen

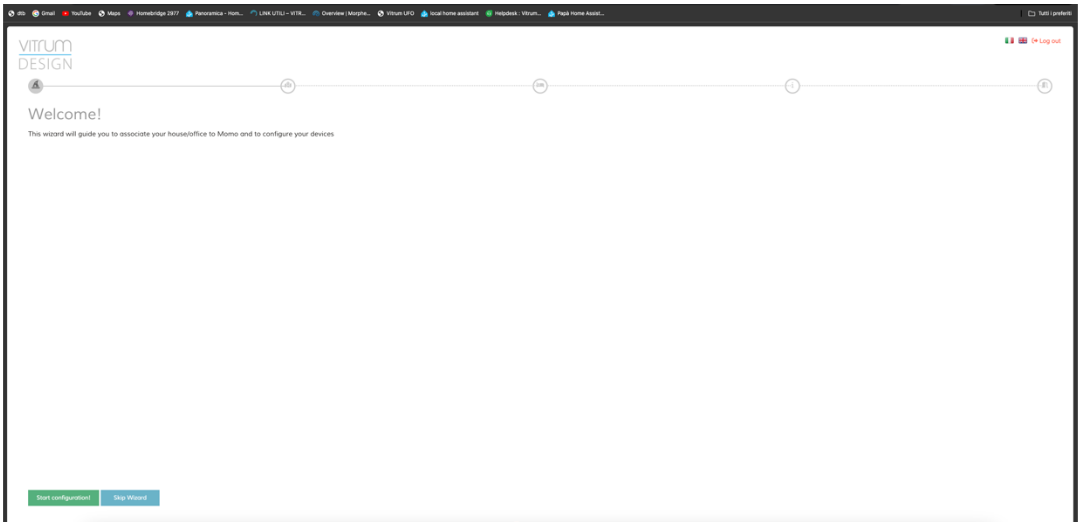
Bedroom

Bathroom

Living room

E

Finally choose a name for the UFO (Smith’s UFO) and click on the “Next” button.



Welcome!

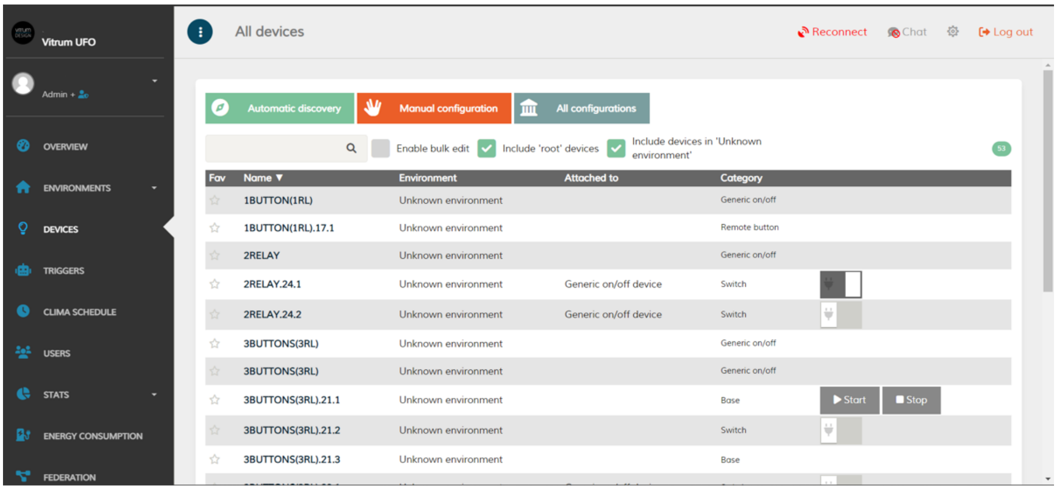
This wizard will guide you to associate your house/office to Momo and to configure your devices

From this moment on, the product will be fully activated, and it will be possible to start configuring your devices and create users and automations.

NOTE: If two UFOs are connected to the same home, they will create a federation of devices (see chapter).

Devices management

In the context of the Smart Home, the fundamental role is played by devices.



☐ Enable bulk edit ☑ Include 'root' devices ☑ Include devices in 'Unknown environment'

Fav	Name ▼	Environment	Attached to	Category
☆	1BUTTON(1RL)	Unknown environment		Generic on/off
☆	1BUTTON(1RL).17.1	Unknown environment		Remote button
☆	2RELAY	Unknown environment		Generic on/off
☆	2RELAY.24.1	Unknown environment	Generic on/off device	Switch
☆	2RELAY.24.2	Unknown environment	Generic on/off device	Switch
☆	3BUTTONS(3RL)	Unknown environment		Generic on/off
☆	3BUTTONS(3RL)	Unknown environment		Generic on/off
☆	3BUTTONS(3RL).21.1	Unknown environment		Base
☆	3BUTTONS(3RL).21.2	Unknown environment		Switch
☆	3BUTTONS(3RL).21.3	Unknown environment		Base

Protocols

There are various manufacturers, various network protocols, and devices of different types: on the UFO side, this translates into the concepts of

- Network protocol: Ethernet, ZigBee, Z-Wave, etc.
- Discovery protocol: which answers the question "How do I automatically find (and possibly configure) a device?"
- Factory: which represents the database that allows instantiating the specific device driver and mapping it to a generic UFO device
- Driver: code that allows the real interface between UFO and the device

There are standardizations, such as Z-Wave, or ONVIF for cameras, or even REST or similar for some calls to external services, but often these standards are disregarded. This is why, for the user to be able to enjoy the features/functionality of the device uniformly concerning their implementation, it is necessary for UFO to determine as accurately as possible the physical device it is interacting with.

Environment

Every device is connected to an "environment": if a specific environment has not been defined, the device is in the "Unknown Environment," which also represents the default in the case of automatic discovery. To view and use a device from the Vitrum Design app, the device must be in a specific environment. Another system environment is "Internet," where all "virtual" devices that belong to an external service are automatically placed (for example, connecting to a remote account or a virtual weather station).

Multiple devices can be part of the same environment; in this case, UFO allows the user to send actions to the entire environment, which will be received by all (and only) devices capable of handling them.

Categories

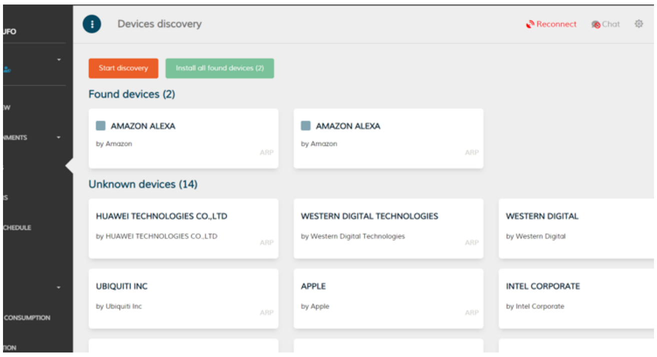
Devices are categorized to break down the functionalities that each one exposes. Each category defines a set of actions and properties that the device MUST or CAN support. For example, a switch MUST allow on/off functionality, but it may not allow setting a timer for turning off. A thermostat CAN allow setting the mode to HEAT/COOL/OFF, but it may not expose both HEAT/COOL modes or the ability to set a setpoint (or the speed of a fan coil system).

Another very useful category is "Light," which, in automation, allows using the generic action "Lighting -> Turn Off (or On)" to, for example, perform a master switch-off of all lights.

To configure the category, such as Light, if it has not been configured through the template, it is necessary to do so from the "Device Information" page, reachable from the devices page (https://ufo.vitrum.com/#/devices/all), configuring "Connected to -> Generic Light."

Devices Discovery

Device discovery only works for Ethernet/Wi-Fi networks and causes UFO to invoke various automatic detection strategies (SSDP, mDNS, Onvif probe, etc).



NOTE: Some of these protocols might be blocked by home firewalls (for example, mDNS) and may not work in specific contexts.

To initiate device discovery from the dashboard, click on the "Devices" menu and select "Auto Search" (or Discovery).

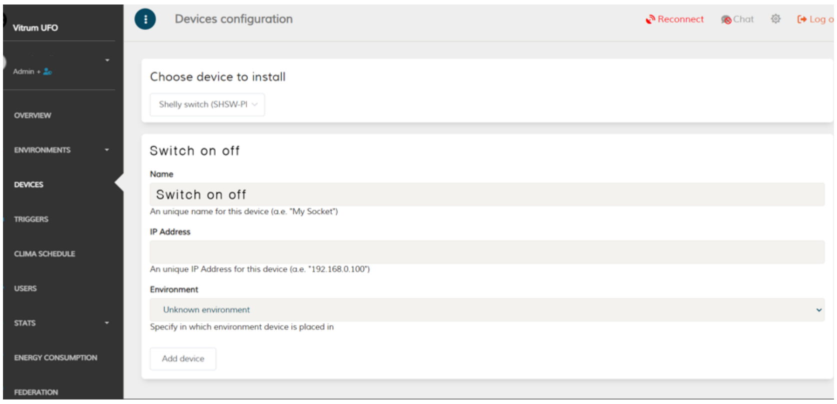
For about 30 seconds, the system will send and analyze various network packets and start displaying the found devices (including those already installed), allowing a precise selection of only some.

Once the devices are selected, you can click on the "Install Selected Devices" button (or "Install All Devices" if no checkbox is selected) or repeat the search by clicking on "Start Search."

NOTE: Some protocols and devices may not respond to every discovery attempt due to internal debounce mechanisms or because they are engaged in activities that temporarily disable the ability to "discover" them.

Manually configuring a device

In case a certain device is not "discoverable" (due to firewall presence or because it is a device interfaced only through the cloud), you can proceed with a manual installation by defining some information manually. To access this interface, go to the "Devices" menu on the dashboard and select the "Manual Configuration" option.



Devices configuration

Choose device to install

Shelly switch (SHSW-PI

Switch on off

Name

Switch on off

An unique name for this device (a.e. "My Socket")

IP Address

An unique IP Address for this device (a.e. "192.168.0.100")

Environment

Unknown environment

Specify in which environment device is placed in

It will open a page with a dropdown menu presenting the list of devices supported by UFO. Once you select the device, a form will appear allowing you to manually specify properties (generally Name, IP Address, and Environment).

In the case of a cloud device (such as Netatmo), you will be redirected to a page hosted by the manufacturer that will enable communication with Vitrum Design servers.

Finally, for a "Generic Camera," the user will have the option to manually define endpoints for capturing the video stream and snapshot (PTZ functionalities are not supported on the generic camera).

Z-Wave

Z-Wave was initially developed in 2001 by the Danish startup Zen-Sys, later acquired in 2008 by the American company Sigma Designs (Silicon Labs), and over time, it has also become an international standard for building interoperable and low-power mesh networks.

The protocol supports bidirectional communication between enabled devices, allowing products from different manufacturers to work together seamlessly.

Z-Wave uses a reduced data flow by design, enabling low-latency communication with a data transmission speed of up to 100 kbps. Interoperability of products from different manufacturers is one of Z-Wave's strengths, pursued through a device certification process.

Z-Wave operates around the 900 MHz frequency, avoiding interference with Wi-Fi, Bluetooth, and other systems operating in the 2.4 GHz band. This frequency choice also allows.

Z-Wave signals to penetrate building walls more easily than Wi-Fi signals, ensuring more efficient and reliable message transmission.

The transmission speed between two devices on the Z-Wave network can vary between 9.6 kb/s, 40 kb/s, and 100 kb/s depending on the signal quality. However, certain specific operations (such as inclusion) are always handled at lower speeds.

Node Types, Controller, SUC, SIS

Nodes in a Z-Wave network can be divided into two main categories: controller nodes and slave nodes (**routing slave**).

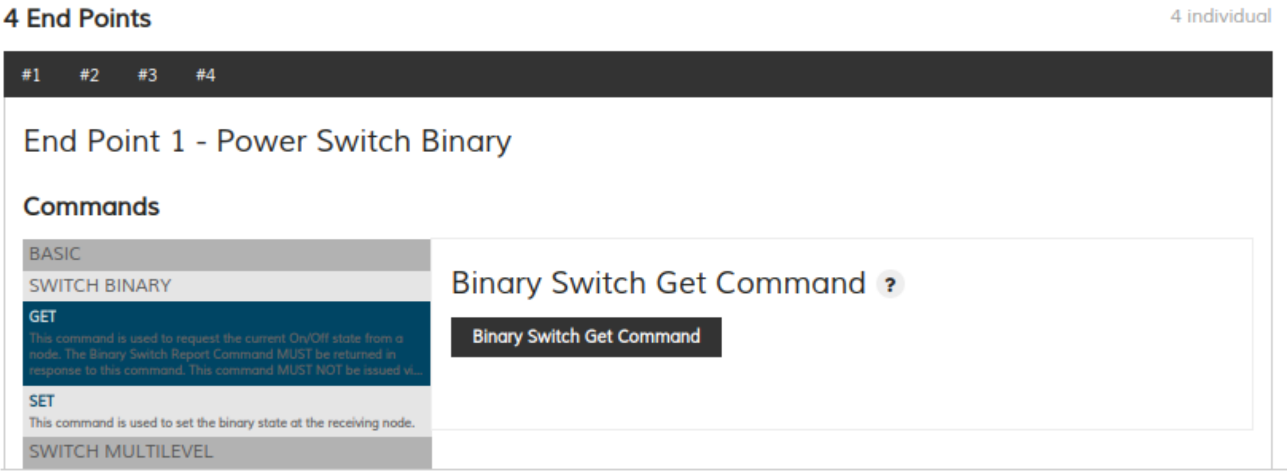
- Controller nodes can host a table of the entire network's addresses and calculate paths based on it. These nodes can transmit paths to slave devices to enable them for routed signal transmission.

- Slave nodes, on the other hand, cannot establish paths and generally function as input and output units in Z-Wave applications.

To create a Z-Wave network, at least one of its nodes must be a controller. A single Z-Wave network can extend up to 232 nodes. Each Z-Wave network is identified by a Network ID (also called Home ID) with a length of 32 bits, which identifies all nodes belonging to the same network. Nodes with different Network IDs cannot communicate with each other. Each device within each network is identified by a Node ID with a length of 8 bits, representing the node's address within the network. The controller assigns this ID to each device during the inclusion process.

A node can offer logical child devices called EndPoints, where each EndPoint can have its own command classes and support a specific set of commands. EndPoints can be dynamic and aggregate into various configurations. An EndPoint is defined by <NodeId>.<EndPointId>; for example, 5.2 identifies endpoint 2 of node 5.

NOTE: The concept of exposed aggregated EndPoints is not related to the behavior of Vitrum products. For the Z-Wave standard, it should not be possible for an EndPoint to change its type at runtime, as is the case with these products.



4 End Points

4 individual

#1 #2 #3 #4

End Point 1 - Power Switch Binary

Commands

BASIC

SWITCH BINARY

GET

This command is used to request the current On/Off state from a node. The Binary Switch Report Command MUST be returned in response to this command. This command MUST NOT be issued vi...

SET

This command is used to set the binary state at the receiving node.

SWITCH MULTILEVEL

Binary Switch Get Command ?

Binary Switch Get Command

The controller used to include the first node is automatically designated as the Primary Controller and is responsible for including and excluding all subsequent nodes in the network. The primary controller imposes its own Home ID on all nodes in the network and assigns a unique Node ID to each of them. Being a Primary Controller is just a role; any controller can be the Primary, but, of course, only one controller can be at a time.

Additional controllers can be added to the network as it grows, and these will be Secondary Controllers. A controller can be either static (**Static Controller**) or dynamic (**Dynamic Controller**). In the latter case, it is assumed that the controller may not always be present in the network.

A controller can also be configured as an **SUC** (**Static Update Controller**): when a static controller is configured as an SUC, the primary controller automatically sends network updates to the SUC, e.g., when a new node is included in the network. The node will then automatically appear in the SUC's network topology map. Other controllers in the network can individually request a network topology update from the SUC. If there is no SUC, the primary controller is responsible for updating all controllers in the network, which will generally be a manual process for the end user. The SUC can create a new primary controller in case of loss or malfunction of the original primary controller. There can be only one SUC in each network.

A controller can also be configured as an **SIS** (**SUC ID Server**): in this case, it allows all other controllers to include/exclude nodes. The SIS automatically becomes the primary controller in the network when enabled. There can be only one SIS in each network. To avoid inconsistencies, all node ID allocations are managed by the SIS.

In a typical home, a single controller is usually sufficient, while the use of secondary controllers can be useful for more complex and articulated installations. In general, controllers allow for network configurations: inclusions and exclusions, configuring associations, and defining the node routing table.

As mentioned earlier, every Z-Wave device must be certified. The certification process involves assigning a triple of hexadecimal codes to each node, uniquely identifying it: **Manufactured** (unique to the manufacturer), **Product TypeId**, **ProductId.**

It is understood that identical products rebranded by different manufacturers must go through the certification process again. Additionally, if a manufacturer releases a new product version that is not compatible with the previous version (breaking change), they are required to go through the certification process again.

Topology and routing

Z-Wave uses a source-routed mesh network topology, where the data path is defined by the source node. As mentioned earlier, controllers can host a routing table calculated based on the network. Slave nodes are devices that do not contain a routing table. An exception is made for the so-called **Routing Slave** nodes and **Enhanced Routing Slave** nodes, which can contain a certain number of preconfigured paths assigned to them by the controller. Therefore, controller nodes and (Enhanced) Routing Slave nodes can initiate communication.

The reliability of a Z-Wave network comes from the fact that message transmission from one node to another can occur through direct radio communication or indirectly by leveraging the nodes' ability to function as repeaters. Nodes can retransmit messages to ensure connectivity, creating a mesh network with multiple possible paths. This way, a Z-Wave network can have a much greater range than the radio range of a single unit. Devices can communicate with each other using intermediate nodes to bypass obstacles or reach Z-Wave network nodes that are out of direct range.

In a typical home, the presence of large metallic objects such as refrigerators, reinforced drywalls, or sliding door frames can act as barriers to device communication. With a Z-Wave network, these problems are automatically circumvented, thanks to the network's ability to propagate the signal through triangulation in cases where direct communication is impossible.

Therefore, when a direct path is not available, the source device will attempt other paths using other network nodes until it successfully transmits the command to the destination device. Routing slave devices can store "learned new paths" and automatically using them as the first choice for subsequent communications.

Z-Wave makes it possible to cover any distance within a typical residential environment. If the path from the source node to the destination node involves many hops, there might be a slight delay between the command and the expected result.

Battery-powered devices, which spend most of their time in sleep mode to ensure longer battery life, cannot function as repeaters. An exception is made for so-called FLiRS (Frequently Listening Routing Slave) devices, which are battery-powered and, as such, are at rest most of the time but can be awakened by a special Z-Wave signal called a "wakeup beam" and remain awake for the time strictly necessary to act as a repeater.

Inclusion, Exclusion, Failed Node Remove, Failed Node Replace

To add or remove a device from a Z-Wave network, specific procedures called Inclusion and Exclusion must be performed. Both procedures are initiated with appropriate actions, defined by the respective manufacturers, to be carried out on both the node to be included (or excluded) and the controller. For slave devices, these actions can vary from a sequence of clicks on a physical button to a combination of clicks on multiple buttons on the device itself. For controllers, the action typically involves choosing an appropriate command on the web interface accessed by the controller (as in the case of UFO).

The inclusion/exclusion procedure is initiated by the controller and requires that the device to be removed or added to the network enters a state called "learning mode." During this mode, the slave device broadcasts (to the entire network) its node information (Home ID and Node ID), which, for a device not yet included, are a random number and zero, respectively.

During the inclusion procedure, the controller responds by sending the Home ID and Node ID to the slave device, which, being in learning mode, accepts these values and uses them to update its own node information. The inclusion procedure must be executed only once; afterward, the device is always recognized by the controller. This process needs to be repeated for each device to be included in the network.

During the exclusion procedure, once the controller has identified the device to be excluded through the reception of broadcast messages from the device in learning mode, it proceeds to remove all information related to the device. The device, in turn, resets all its network information, configurations, and customizations, sets its Node ID to zero, and the Network ID to a random number, ready to be included in a new network.

Z-Wave network devices can support Network Wide Inclusion, which allows the inclusion of a device in a network even if it is not in direct connection with the controller. It is also possible for an uninitialized device to automatically enter Network Wide Inclusion as soon as it is powered on without any action required from the user (as seen in some products of the Qubino family, for example).

In normal use, a node may fail; in such a case, it is possible to perform Failed Node Remove procedures to remove the node from the network or Failed Node Replace procedures to replace it with an identical device (meaning it must identify itself with the same triplet of ManufacturerId / ProductTypeId / ProductId).

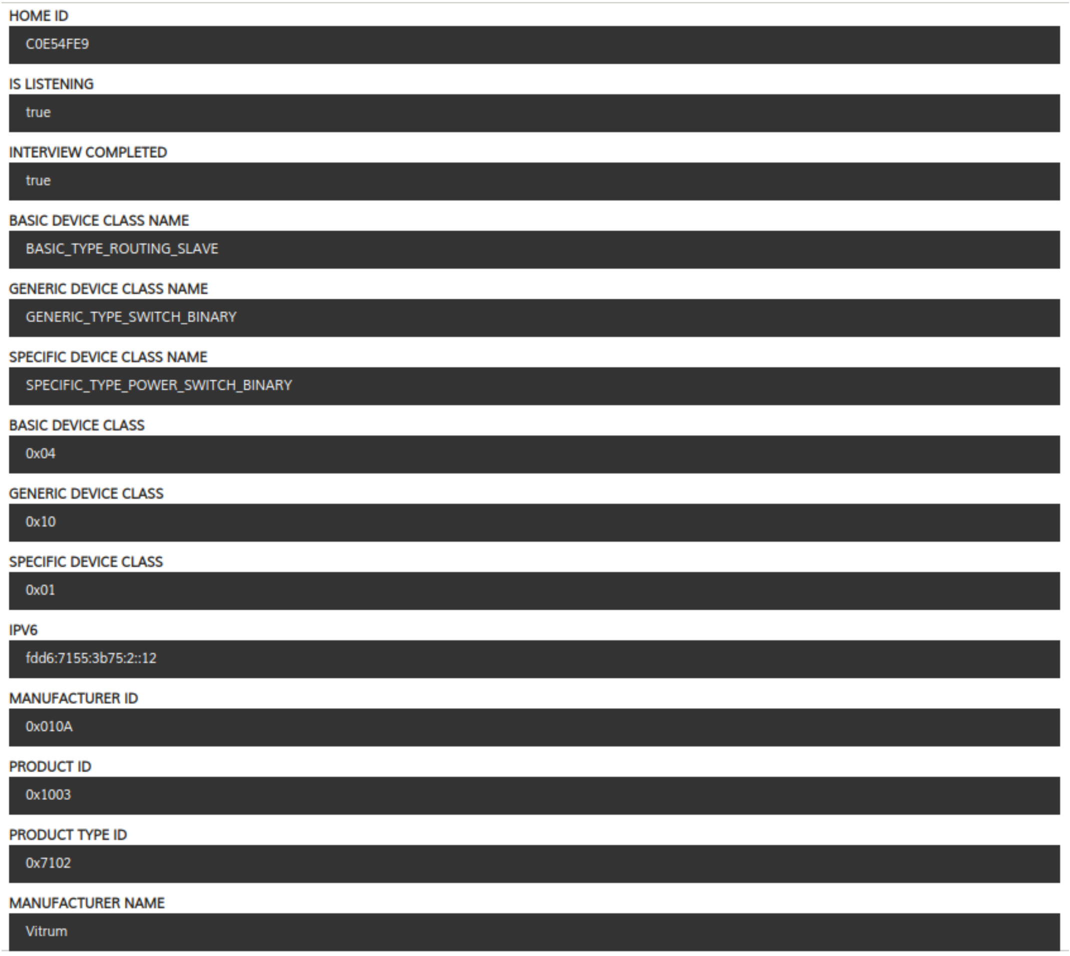
NOTE: The statement about the replacement with different nodes has been observed but might not hold true in all cases.

NOTE: To perform these procedures, it is essential for the controller to put the node in a "**Failed**" state. This can be achieved by executing a NOP (which, of course, must fail).

Characteristics of a node (Ids, Types and Command Classes)

The characteristics of each node in the Z-Wave network are communicated to the controller during the inclusion phase through the Node Information Frame (**NIF**).

NOTE: After inclusion, the Z/IP Gateway initiates subsequent requests to the node to obtain the list and type of EndPoints, as well as the possible support for command classes related to battery-powered devices (WAKE_UP). It also generates an IPv6 address for the node. For this reason, the inclusion phase of a Z-Wave node is slightly slower, and the notification of the successful inclusion is received by UFO with a visible delay compared to the confirmation provided by the device.



HOME ID
C0E54FE9

IS LISTENING
true

INTERVIEW COMPLETED
true

BASIC DEVICE CLASS NAME
BASIC_TYPE_ROUTING_SLAVE

GENERIC DEVICE CLASS NAME
GENERIC_TYPE_SWITCH_BINARY

SPECIFIC DEVICE CLASS NAME
SPECIFIC_TYPE_POWER_SWITCH_BINARY

BASIC DEVICE CLASS
0x04

GENERIC DEVICE CLASS
0x10

SPECIFIC DEVICE CLASS
0x01

IPV6
fdd6:7155:3b75:2::12

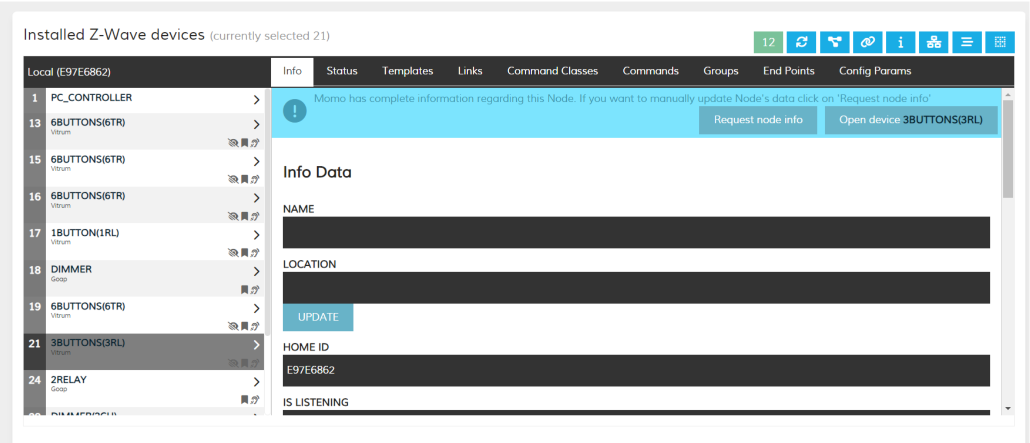
MANUFACTURER ID
0x010A

PRODUCT ID
0x1003

PRODUCT TYPE ID
0x7102

MANUFACTURER NAME
Vitrum

NOTE: Simultaneously with sending the packet containing the NIF information, UFO requests the same information (trying, where possible, to ask Z/IP to avoid stressing the node) to finally present it to the user. In this exchange of information, it may happen that when UFO requests, for example, the list of Z/IP End Points, it may not be able to provide it (because the communication might have failed and it might have rescheduled it with a certain timeout). In these cases, it may be necessary to perform some manual operations or click on the "Request node information" button in the "Info" tab of the dashboard.



Installed Z-Wave devices (currently selected 21)

Momo has complete information regarding this Node. If you want to manually update Node's data click on 'Request node info'

Info Data

NAME

LOCATION

HOME ID
E97E6862

IS LISTENING

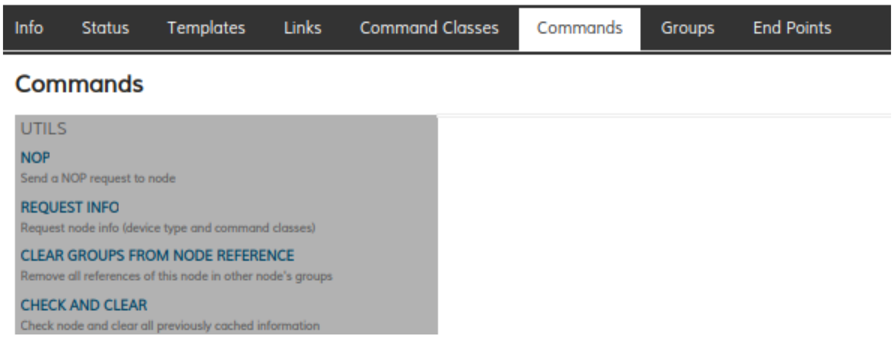
NOTE: To ensure that a node can be fully functional, it is **ESSENTIAL** to make sure that UFO knows:

- ManufacturerId, ProductTypeId, and ProductId to identify the device.

- List of Command Classes associated with the device (Command Classes tab in the dashboard).

- Complete list of the device's End Points.

If at least one of these pieces of information is missing, it is necessary to attempt the restoration (using the "Request node information" button) or, if this procedure does not yield results, try the button located in Commands > UTILS > Request Info.


Info
Status
Templates
Links
Command Classes
Commands
Groups
End Points
Commands
UTILS
NOP
Send a NOP request to node
REQUEST INFO
Request node info (device type and command classes)
CLEAR GROUPS FROM NODE REFERENCE
Remove all references of this node in other node's groups
CHECK AND CLEAR
Check node and clear all previously cached information

In the NIF packet, the node exposes:

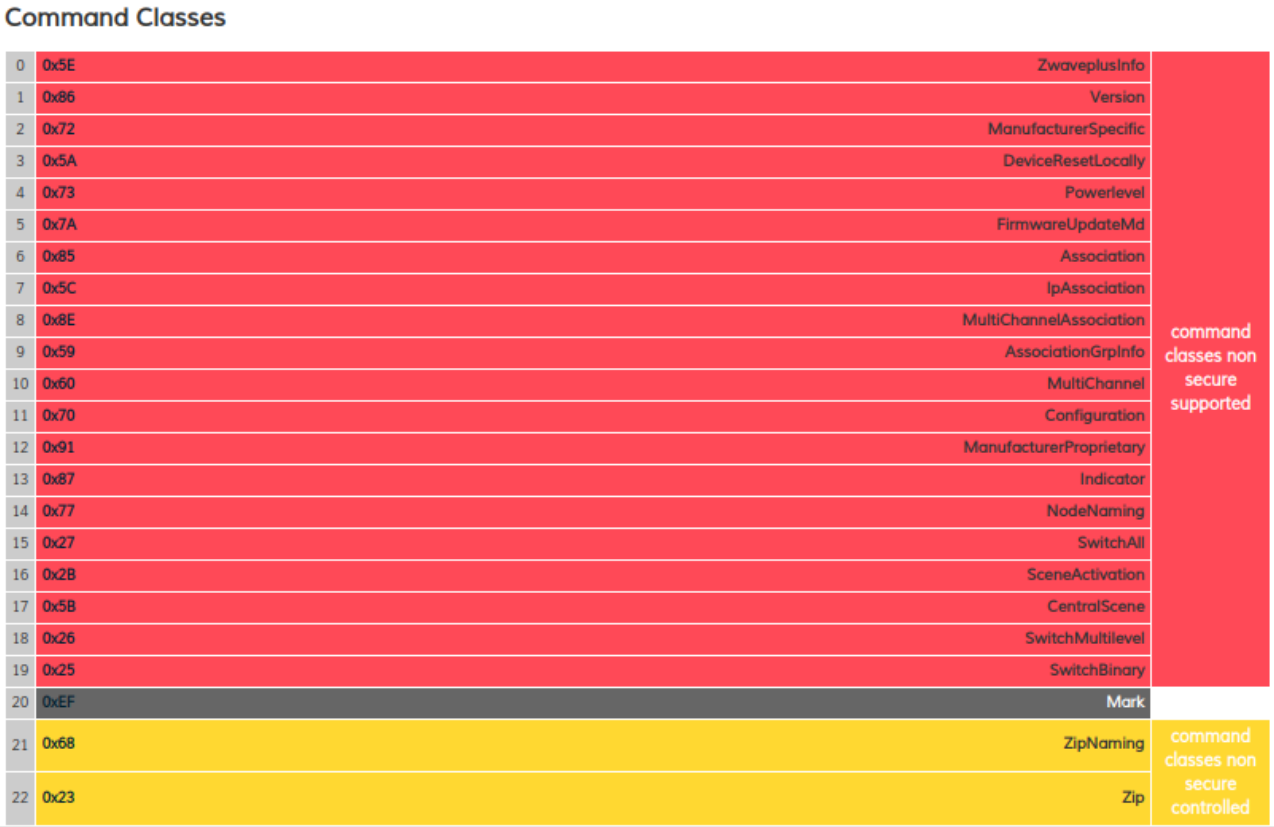
- Its type, identified by the values of **BASIC_TYPE, GENERIC_TYPE, and SPECIFIC_TYPE**.

- If is a **Listening** node, meaning it is always available for communication (unlike battery-powered nodes, which need to wake up).

- The macro categories of supported commands, known as Command Classes.

Each Command Class (identified by a hexadecimal number) supports a set of commands (which can vary depending on the version). The result of the command may also vary with the version. In some specific cases, the meaning of certain fields in the response can also vary between different versions (some thermostat management commands).

The only Command Class that is not explicitly notified, as every Z-Wave network node must implement it, is the **BASIC** command class. The meaning of GET, SET, and REPORT actions in this case is not predefined by the standard.



Command Classes

0	0x5E	ZwaveplusInfo	command classes non secure supported
1	0x86	Version	
2	0x72	ManufacturerSpecific	
3	0x5A	DeviceResetLocally	
4	0x73	Powerlevel	
5	0x7A	FirmwareUpdateMd	
6	0x85	Association	
7	0x5C	IpAssociation	
8	0x8E	MultiChannelAssociation	
9	0x59	AssociationGrpInfo	
10	0x60	MultiChannel	
11	0x70	Configuration	
12	0x91	ManufacturerProprietary	
13	0x87	Indicator	
14	0x77	NodeNaming	
15	0x27	SwitchAll	
16	0x2B	SceneActivation	
17	0x5B	CentralScene	
18	0x26	SwitchMultilevel	
19	0x25	SwitchBinary	
20	0xEF	Mark	
21	0x68	ZipNaming	command classes non secure controlled
22	0x23	Zip	

For a comprehensive list of supported Command Classes and commands, please refer to the official documentation.

Z-Wave and UFO: Z/IP Gateway

The UFO Z-Wave stack is developed on top of Silicon Labs Z/IP Gateway product: UFO is, therefore, a Z/IP Client for a Z/IP Gateway service running locally on the same machine, and it is a Gateway Controller for other nodes in the network.

Z/IP Gateway is a Linux operating system application that allows clients to contact and control nodes in a Z-Wave network (HAN, Home Area Network). Through the Z/IP gateway, each device on the Z-Wave network behaves as if it were an IP client on the network. In Z/IP, a certain number of addresses (in the current version 4) are reserved for internal management and are called Virtual Nodes, so the maximum number of devices supported by Z/IP is 225.

Features and customizations of the service

By default, Z/IP enables communication with nodes through encrypted communication with **DTLSv1.0** (UTDP) on port 41230 or unencrypted on port 4123 (UDP). However, starting from UFO version 1.2.x, communication occurs exclusively in an unencrypted manner to avoid unnecessary overhead.

UFO communicates with the Z/IP layer through a tunnel interface (tap) created automatically by the service. In normal usage, the TAP0 interface is typically visible among the network interfaces.

By default, Z/IP Gateway bridges the network interface provided during configuration with the HAN network. However, in UFO, traffic visibility externally is limited. This decision was made to prevent complications in automatically and stably managing the creation of automatic IPv6 routes to and from Z/IP Gateway. There were often instances of strong instability, especially in the case of multiple installations in the same network (ravdaemon services, parprouted).

Z/IP Gateway normally advertises nodes on the network using the mDNS protocol. This behavior has also been disabled in UFO to speed up the service startup and avoid unnecessary overhead.

The current version of Z/IP Gateway (2.81) was originally developed for x86 architectures, with x64 support provided through emulation. Vitrum Design has developed the necessary patches to enable its use on System On Chip (SoC) platforms.

The Z-Wave standard assumes that if a node supports it, it utilizes Security mechanisms (S1 and S2). This makes it impossible to associate (see Link) a node that does not support the same security level. Unlike other products that use the serial protocol directly (no longer officially supported by Silicon Labs), such as PC Controller (also by Silicon Labs), which allows choosing whether to enable these mechanisms during controller initialization, Z/IP Gateway does not provide this option. For this reason, Vitrum Design has made customizations to avoid using security mechanisms (S1 and S2) and streamline internal communication by disabling DTLS communication and external access.

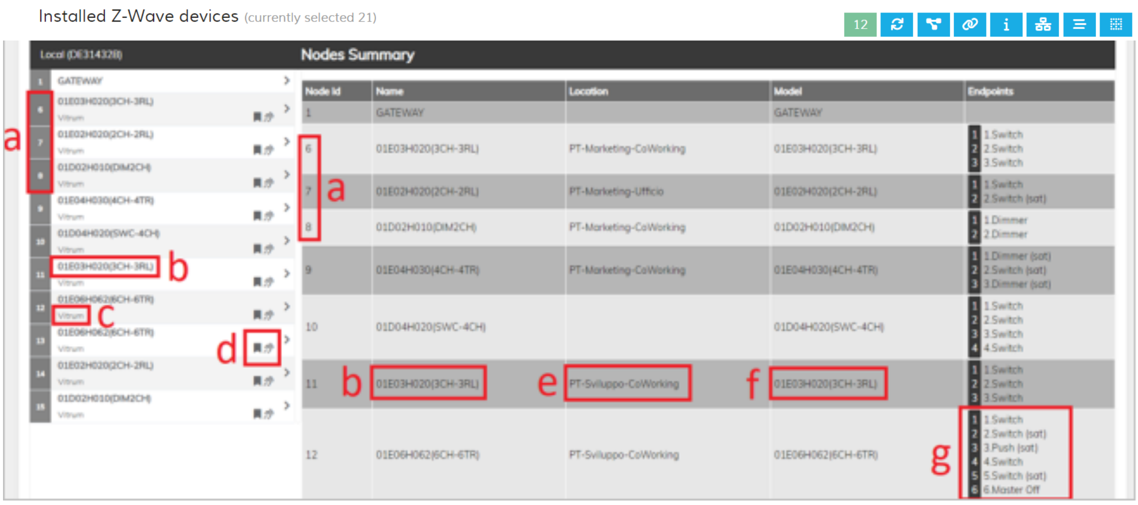
Finally, the current implementation... (text truncated; please provide the continuation)

Z-Wave node and UFO device

As mentioned, generally, each driver comes with specific customizations, but in the case of Z-Wave, that is a "closed" standard, it was possible to define basic rules that allow translating the “capabilities” of the actual device with UFO functionalities.

This system is called "Z-Wave Templates." To access the Z-Wave control panel from the dashboard, select the "Devices" menu and then "Z-Wave."

A screen like the following will appear



Installed Z-Wave devices (currently selected 21)

Local (DE314328)

Nodes Summary

1	GATEWAY	
6	01E03H020(3CH-3RL)	Vitrum
7	01E02H020(2CH-2RL)	Vitrum
8	01D02H010(DIM2CH)	Vitrum
9	01E04H030(4CH-4TR)	Vitrum
10	01D04H020(SWC-4CH)	Vitrum
11	01E03H020(3CH-3RL)	Vitrum
12	01E06H062(6CH-6TR)	Vitrum
13	01E06H062(6CH-6TR)	Vitrum
14	01E02H020(2CH-2RL)	Vitrum
15	01D02H010(DIM2CH)	Vitrum

Node Id	Name	Location	Model	Endpoints
1	GATEWAY		GATEWAY	
6	01E03H020(3CH-3RL)	PT-Marketing-CoWorking	01E03H020(3CH-3RL)	1 1.Switch 2 2.Switch 3 3.Switch
7	01E02H020(2CH-2RL)	PT-Marketing-Ufficio	01E02H020(2CH-2RL)	1 1.Switch 2 2.Switch (sat)
8	01D02H010(DIM2CH)	PT-Marketing-CoWorking	01D02H010(DIM2CH)	1 1.Dimmer 2 2.Dimmer
9	01E04H030(4CH-4TR)	PT-Marketing-CoWorking	01E04H030(4CH-4TR)	1 1.Dimmer (sat) 2 2.Switch (sat) 3 3.Dimmer (sat)
10	01D04H020(SWC-4CH)		01D04H020(SWC-4CH)	1 1.Switch 2 2.Switch 3 3.Switch 4 4.Switch
11	01E03H020(3CH-3RL)	PT-Sviluppo-CoWorking	01E03H020(3CH-3RL)	1 1.Switch 2 2.Switch 3 3.Switch
12	01E06H062(6CH-6TR)	PT-Sviluppo-CoWorking	01E06H062(6CH-6TR)	1 1.Switch 2 2.Switch (sat) 3 3.Push (sat) 4 4.Switch 5 5.Switch (sat) 6 6.Master Off

a) **Node ID**. The node with ID=1 is the Z-Wave Controller. The numbering of other nodes starts from ID=6;
b) **Node Name**. If not manually changed, it corresponds to the device model.
c) **Manufacturer** of the device.
d) The first icon (flag) indicates that a template has been applied to the node. The second icon (ear) indicates that the device is always listening (i.e., not a battery-powered device);

NOTE: If the device supports it, this icon group also shows the "indicator" button to quickly identify it.

NOTE: Starting from version 1.6.3 of UFO, an additional flag is available only for Vitrum Design admins, allowing the activation of logs for a specific node (see later).

e) **Environment** in which the node is installed.
f) Device model.
g) Functionality of individual endpoints.

Upon accessing an unconfigured UFO, this screen will only show node 1, corresponding to the onboard Z-Wave controller.

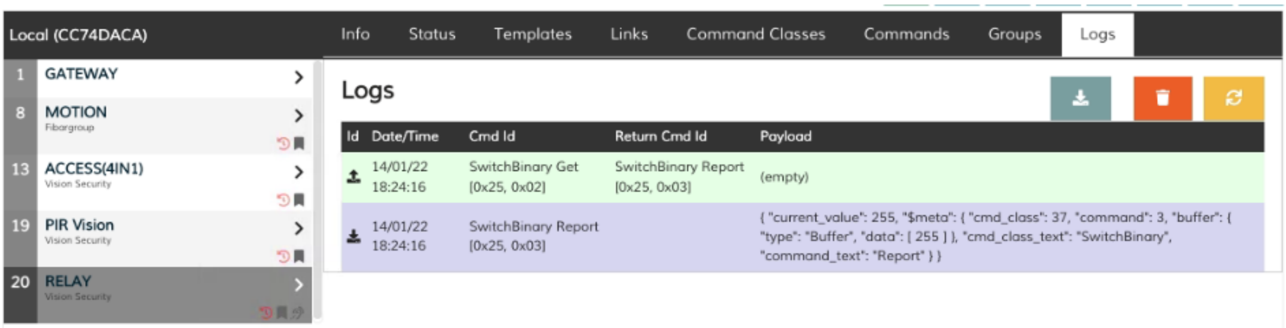
Indicator Button

If the device supports it, you can activate the "Indicator" command class to start the functionality on the device (for example, in the case of Vitrum keypads, all buttons will start flashing). The functionality is linked to the icon.

If the functionality is active, the icon will be flashing red.

Activation of Logs for a Specific Node

Starting from UFO version 1.6.3, Vitrum Design admins have the option to conditionally activate an additional specific log for each node.



Logs

Id	Date/Time	Cmd Id	Return Cmd Id	Payload
	14/01/22 18:24:16	SwitchBinary Get [0x25, 0x02]	SwitchBinary Report [0x25, 0x03]	(empty)
	14/01/22 18:24:16	SwitchBinary Report [0x25, 0x03]		{ "current_value": 255, "$meta": { "cmd_class": 37, "command": 3, "buffer": { "type": "Buffer", "data": [255] }, "cmd_class_text": "SwitchBinary", "command_text": "Report" } }

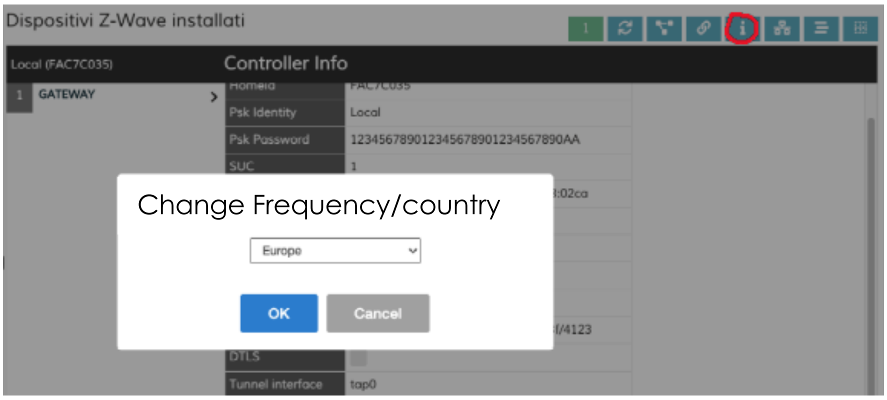
Clicking on the clock-shaped icon will allow you to enable or disable the log functionality. If the functionality is active, the icon will be flashing red. The logs can be viewed at any time through the "Logs" tab available for each device.

NOTE: It is possible to force the logs to turn off by setting the Discover.zwave.enable_logs entry to false in the configuration file. Starting from version 1.6.3, the default value for this setting will be true.

Z-wave region selection (UFO 2.0 only)

Z-Wave supports different "Regions," each with different operating frequencies. UFO 2.0 uses a controller from the 700 series that allows frequency selection via software.

Before starting to include Z-Wave devices, you need to set the working Region. To do this, select the GATEWAY device, click on the "i" icon, and then choose "change" in the frequency menu item, selecting the region:



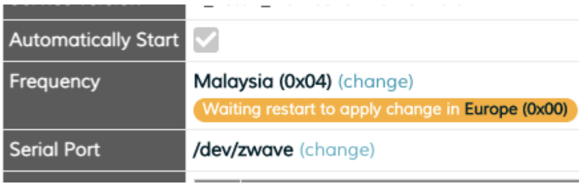
Controller Info

Homeid	FAC7C035
Psk Identity	Local
Psk Password	12345678901234567890123456789OAA
SUC	1
	:02ca
	/4123
DTLS	
Tunnel interface	tap0

Change Frequency/country

Europe

Once ok you will need to restart UFO:

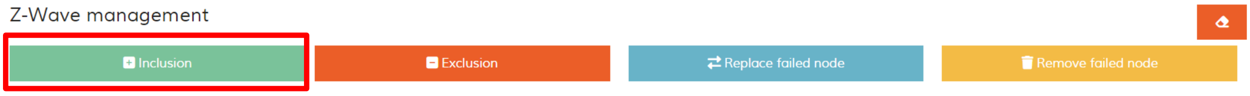


Automatically Start	☑
Frequency	Malaysia (0x04) (change) Waiting restart to apply change in Europe (0x00)
Serial Port	/dev/zwave (change)

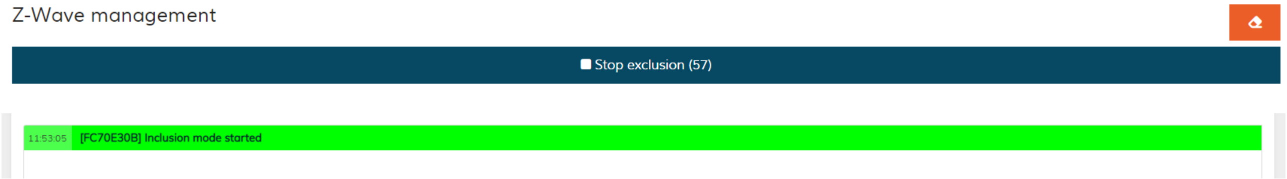
Including a node/Replacing a “failed” node

Z-Wave networks do not support automatic discovery and pairing/installation. To install a device, it is necessary to go through an "inclusion" phase, where the controller enters a "waiting" state, and the device you want to connect communicates a certain type of message to it.

To perform an inclusion from the Z-Wave management panel, select the "Inclusion" option. You then have 60 seconds to include a node.



NOTE: Each Z-Wave device has its own inclusion procedure, typically involving a prolonged press of a button (external or internal). Refer to the manual of the specific device for the inclusion procedure.



```
11:53:05 [FC70E30B] Inclusion mode started
```

If error messages appear on the screen after the inclusion of a node, perform the exclusion as indicated in the following paragraph and then retry the inclusion procedure.

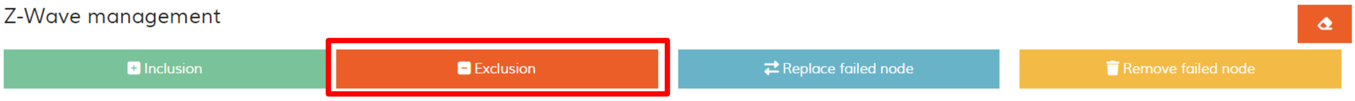
Once the inclusion process is complete, UFO (or the controller) will assign a unique ID to the device and proceed with an "Interview" phase. During this phase, it determines the product type (manufacturer, type, and product ID) to identify its capabilities (in terms of supported command classes) and allows the selection of the template.

If an already included device stops working, you can replace it with an IDENTICAL device by assigning the same node ID as the previous one using the "Replace failed node" procedure.

NOTE: At the end of the replacement procedure, it will be necessary to reapply the template and manually check the links to and from the node in question.

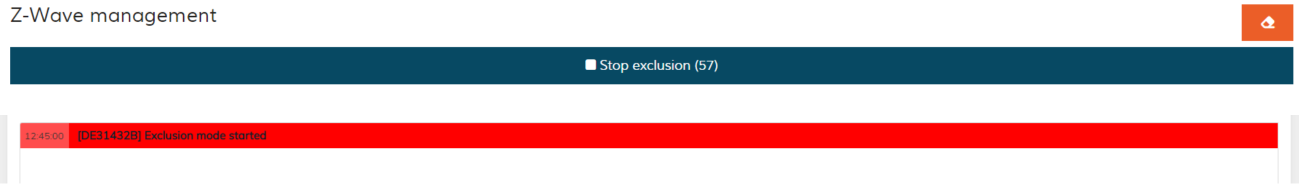
Excluding a Node/Removing a “Failed”

To be able to include from the Z-Wave management panel, select the "Exclusion" item



From this moment you have 60 seconds to exclude a node.

NOTE: Each Z-Wave device has its own inclusion procedure, usually involving a short or prolonged press of a button (either external or internal). For the specific steps to include the node, refer to the manual of the respective device.



12:45:00 [DE31432B] Exclusion mode started

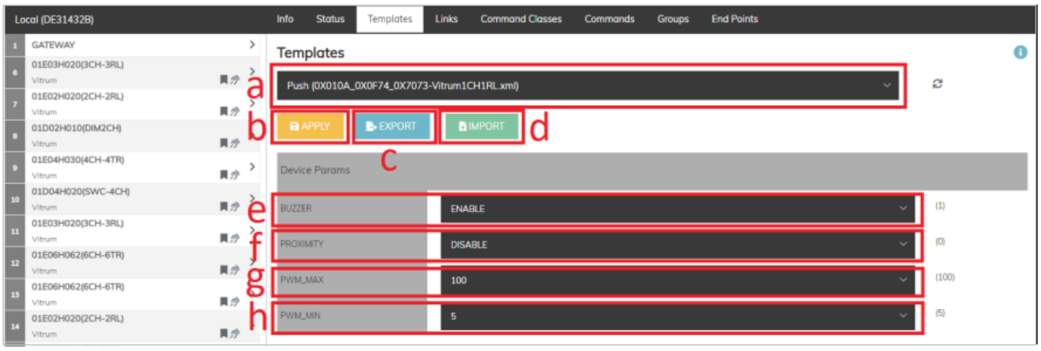
NOTE: Excluding a node does not automatically free up the slot of the previously occupied ID. Subsequent inclusions will always resume from the last unused node ID.

NOTE: The exclusion phase can also be performed by a controller different from the one the node was registered on. This can be useful to avoid strange factory reset procedures before including a previously used device. However, in this case, the controller on which the node was registered will not be aware that the device has been excluded, and it will be necessary to perform the "Remove failed node" procedure to remove it from the list.

Modello di domanda

Per ogni nodo, è necessario applicare un modello in modo che UFO abbia conoscenza delle funzionalità del dispositivo. Per eseguire questa operazione, selezionare il nodo e aprire la scheda Modelli.

Di seguito è riportato un esempio di modello per un dispositivo Vitrum 01E01H020 (1CH-1RL) e una breve descrizione di ciascun parametro modificabile.

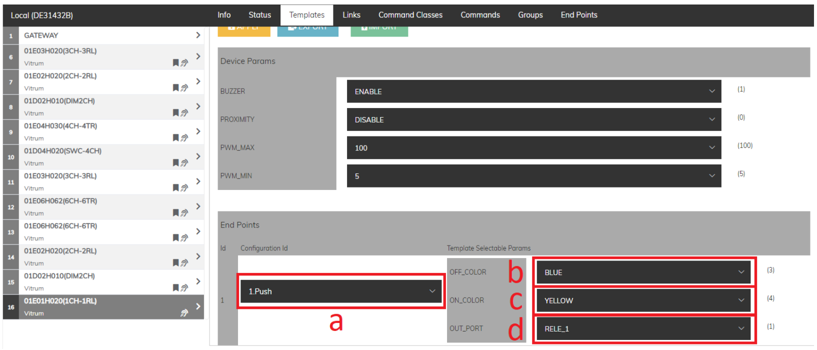


1 GATEWAY
6 01E03H020(3CH-3RL) Vitrum
7 01E02H020(2CH-2RL) Vitrum
8 01D02H010(DIM2CH) Vitrum
9 01E04H030(4CH-4TR) Vitrum
10 01D04H020(SWC-4CH) Vitrum
11 01E03H020(3CH-3RL) Vitrum
12 01E06H062(6CH-6TR) Vitrum
13 01E06H062(6CH-6TR) Vitrum
14 01E02H020(2CH-2RL) Vitrum

Push (0X010A_0X0F74_0X7073-Vitrum1CH1RL.xml)

BUZZER ENABLE (1)
PROXIMITY DISABLE (0)
PWM_MAX 100 (100)
PWM_MIN 5 (5)

a) Node template;
b) Template application;
c) Template export;
d) Template import;
e) Enable/disable device sounds;
f) Enable/disable proximity;
g) Maximum brightness of the device;
h) Minimum brightness of the device;
In some cases, a device may offer endpoints, which are logical child devices.



1	GATEWAY
6	01E03H020(3CH-3RL) Vitrum
7	01E02H020(2CH-2RL) Vitrum
8	01D02H010(DIM2CH) Vitrum
9	01E04H030(4CH-4TR) Vitrum
10	01D04H020(SWC-4CH) Vitrum
11	01E03H020(3CH-3RL) Vitrum
12	01E06H062(6CH-6TR) Vitrum
13	01E06H062(6CH-6TR) Vitrum
14	01E02H020(2CH-2RL) Vitrum
15	01D02H010(DIM2CH) Vitrum
16	01E01H020(1CH-1RL) Vitrum

Device Params

BUZZER	ENABLE	(1)
PROXIMITY	DISABLE	(0)
PWM_MAX	100	(100)
PWM_MIN	5	(5)

End Points

Id	Configuration Id	Template Selectable Params		
1	1.Push	OFF_COLOR	BLUE	(3)
		ON_COLOR	YELLOW	(4)
		OUT_PORT	RELE_1	(1)

a) Endpoint functionalities;
b) Endpoint color when OFF;
c) Endpoint color when ON;
d) Output driven by the endpoint;
Each device can be considered as consisting of a root device and, if present, endpoints. For example, in a 6-button Vitrum panel, the entire panel can be identified as the root device, and each button as an endpoint. In this case, you can configure each of the 6 endpoints differently (e.g., switch, push, dimmer, etc.).

Another important distinction to make during the configuration of a device is between a satellite device (e.g., switch sat, dimmer sat, motor sat, etc.) and a non-satellite device (e.g., switch, dimmer, motor, etc.). The satellite device does not perform any physical actuation and is not electrically connected to the load but communicates only via Z-Wave with other devices (e.g., to perform required actions or communicate its status). Therefore, for example, if you press a button configured as a switch sat, and this button is linked to a switch device (electrically connected to a load), then a power on/off command will be sent to the switch device upon pressing, which will turn on/off the connected load.

From the above considerations, it follows that for satellite devices, it is not necessary to configure a specific environment; they should be left in an unknown environment. The environment should be configured only for devices with a connected load that perform the actual physical actuation.

Also, the category for satellite devices should not be manually configured because automatically, through the template, they will be seen as the "REMOTE BUTTON" category.

Link creation

When two nodes are included in the same network, it's also possible to associate them with each other.

The expression "A is associated with B" means that A is under the control of B. For example, A could be an outlet, and B could be a remote control, or A could be a device that controls a lamp, and B could be a brightness sensor that automatically turns it on.

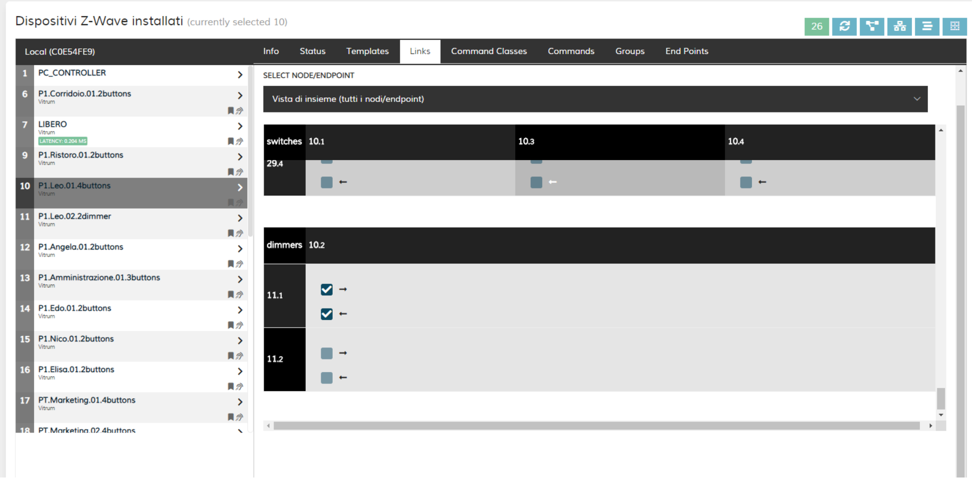
Associations are introduced to allow nodes that can initiate communication to control another node in the network without the need for controller intervention (as is the case with Triggers). In this sense, they simplify the interaction between two nodes and reduce the time between sending the command and the controlled device's response.

Each device can have one or more logically distinct association groups. The same node can be associated with different groups of the same device, and it's also possible to associate the same device with multiple nodes.

Associations make the network faster and more robust because once configured through the controller, they no longer require the controller itself to operate: the controller could be turned off, and everything would still work.

UFO extends the concept of association to that of a "link," taking care, through the template mechanism, to present to the user only "compatible" associations and dividing them into some general types. For example, a "switch" device will only be linkable to "switch_sat," and vice versa, but never with a "motor_sat."

To create links between Vitrum Z-Wave devices, choose the device, click the Link tab, select the endpoint of the node to configure, and the device to link with. At this point, you need to click to decide whether to create a bidirectional or unidirectional link.



Dispositivi Z-Wave installati (currently selected 10)

Local (C0E54FE9)

1 PC_CONTROLLER
6 P1.Corridoio.01.2buttons Vitrum
7 LIBERO Vitrum LATENCY: 0.204 MS
9 P1.Ristoro.01.2buttons Vitrum
10 P1.Leo.01.4buttons Vitrum
11 P1.Leo.02.2dimmer Vitrum
12 P1.Angela.01.2buttons Vitrum
13 P1.Amministrazione.01.3buttons Vitrum
14 P1.Edo.01.2buttons Vitrum
15 P1.Nico.01.2buttons Vitrum
16 P1.Elisa.01.2buttons Vitrum
17 PT.Marketing.01.4buttons Vitrum
18 PT.Marketing.02.4buttons

SELECT NODE/ENDPOINT: Vista di insieme (tutti i nodi/endpoint)

switches	10.1	10.3	10.4
29.4	□ ←	□ ←	□ ←

dimmers	10.2
11.1	☑ → ☑ ←
11.2	□ → □ ←

Difference between links and automations

Triggers and Z-Wave Links serve a similar purpose but have very different scopes.

For a trigger to be executed, it's necessary for UFO to be active and connected to the devices; this is not the case for Z-Wave Associations and Links.

A trigger can evaluate conditions and, for example, allow two different actions to be performed on the ON and OFF states of a specific button. A trigger can be manually executed by a user.

In triggers, the concept of bidirectionality does not exist because no state is associated with it. A trigger can be temporarily disabled.

Triggers are protocol-independent, allowing devices from different ecosystems to interact with each other. **Triggers can operate across two federated UFOs**, while Z-Wave associations can only occur within the same mesh network (Home ID).

Tools for debugging and error analysis

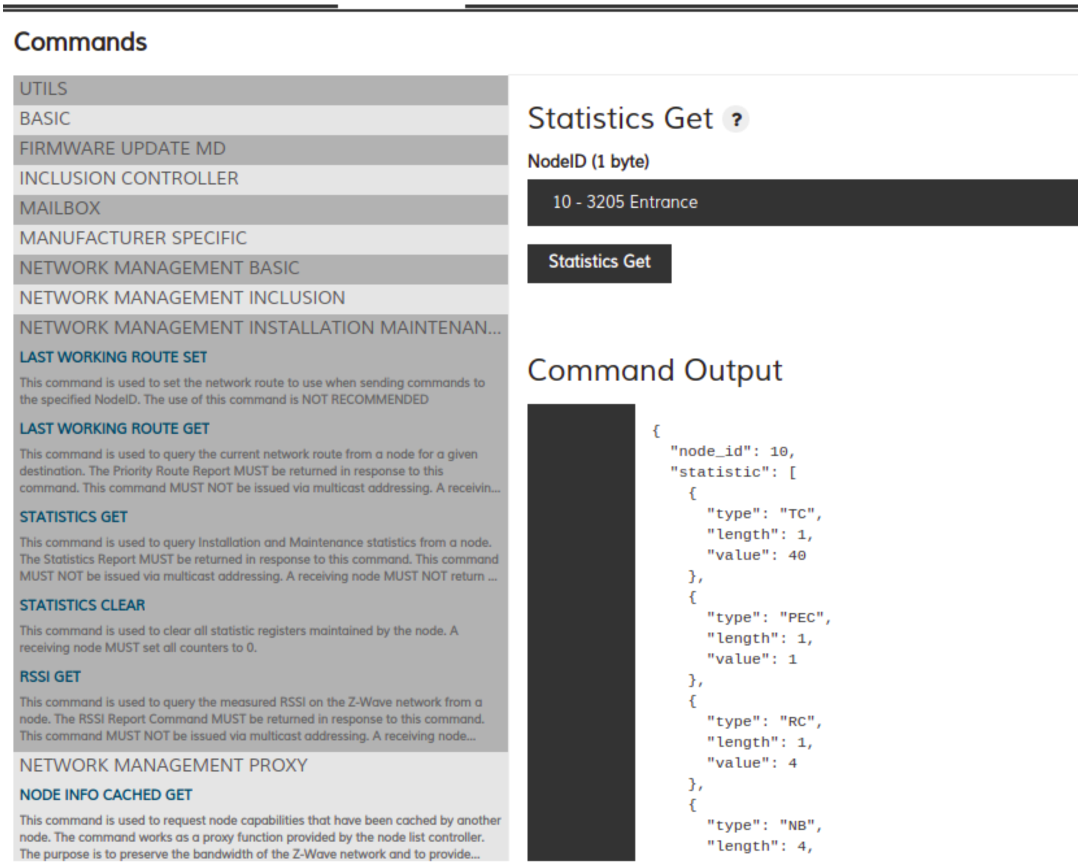
Zniffer

[TODO]

Command Class Network Management Installation Maintenance

The "**Network Management Installation Maintenance**" command class allows performing maintenance operations (read/write) on the Z-Wave network.

NOTE: This document refers to the official documentation (SDS13784-Z-Wave-Network-Protocol-Command-Class-Specification.pdf, starting from page 102) and version 2 of the Command Class.



Commands

UTILS

BASIC

FIRMWARE UPDATE MD

INCLUSION CONTROLLER

MAILBOX

MANUFACTURER SPECIFIC

NETWORK MANAGEMENT BASIC

NETWORK MANAGEMENT INCLUSION

NETWORK MANAGEMENT INSTALLATION MAINTENAN...

LAST WORKING ROUTE SET

This command is used to set the network route to use when sending commands to the specified NodeID. The use of this command is NOT RECOMMENDED

LAST WORKING ROUTE GET

This command is used to query the current network route from a node for a given destination. The Priority Route Report MUST be returned in response to this command. This command MUST NOT be issued via multicast addressing. A receivin...

STATISTICS GET

This command is used to query Installation and Maintenance statistics from a node. The Statistics Report MUST be returned in response to this command. This command MUST NOT be issued via multicast addressing. A receiving node MUST NOT return ...

STATISTICS CLEAR

This command is used to clear all statistic registers maintained by the node. A receiving node MUST set all counters to 0.

RSSI GET

This command is used to query the measured RSSI on the Z-Wave network from a node. The RSSI Report Command MUST be returned in response to this command. This command MUST NOT be issued via multicast addressing. A receiving node...

NETWORK MANAGEMENT PROXY

NODE INFO CACHED GET

This command is used to request node capabilities that have been cached by another node. The command works as a proxy function provided by the node list controller. The purpose is to preserve the bandwidth of the Z-Wave network and to provide...

Statistics Get ?

NodeID (1 byte)

10 - 3205 Entrance

Statistics Get

Command Output

```
{
  "node_id": 10,
  "statistic": [
    {
      "type": "TC",
      "length": 1,
      "value": 40
    },
    {
      "type": "PEC",
      "length": 1,
      "value": 1
    },
    {
      "type": "RC",
      "length": 1,
      "value": 4
    },
    {
      "type": "NB",
      "length": 4,
```

The commands exposed by this command class (excluding the related reports) are:

a) Statistics Clear/Get

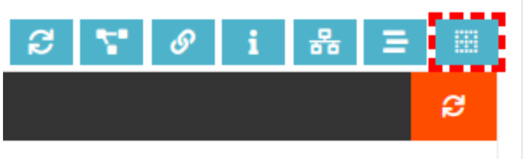
b) Last Working Route Get/Set

c) RSSI Get

NOTE: UFO does not use any automations based on the results of these commands but allows access to them through the "Commands" panel of node 1.

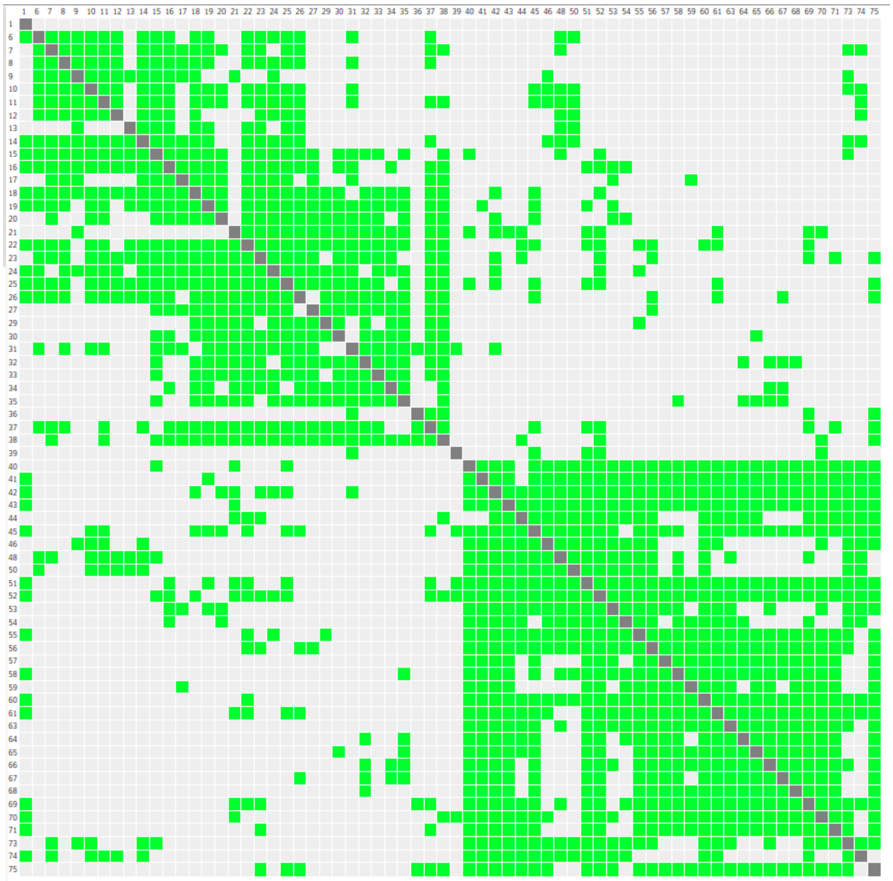
Statistics Get/Clear

UFO offers a utility for quickly viewing the Statistics Get commands on a node or the entire network through the Show Topology button (top right on the ZWave management page):



It is possible to manually refresh the entire topology (or a single node) using the orange button.

The command is asynchronous and may take variable time depending on the number of nodes and the Z-wave network. However, you can view the progress of the scan immediately by exiting and re-entering the page (the grid does not update in real-time).



The figure shows the result of a scan. It can be observed that the network has settled into a configuration with two clusters, which corresponds to the presence of a day zone and a night zone connected by a couple of "boundary" nodes.

NOTE: In this type of installation, communication problems may arise between the two zones since the "bridge" nodes between the two clusters suffer from having to support the entire network traffic between the two zones.

NOTE: It should be noted that the fact that two nodes tell the controller they "know" each other does not necessarily mean that one will use the other in mesh network communications. This list only indicates to the controller that two nodes A and B "see/talk to" each other at a certain speed (which can be 100, 40, or 9.6 kb/s). The routing phase is slightly different and has different logics that cannot be forced in node-to-node communication. See the next chapter "Last Working Route Get/Set."

The invoked command in a "raw" manner allows reading various statistics beyond just the "NB" (Nearby Nodes) related to neighboring nodes.

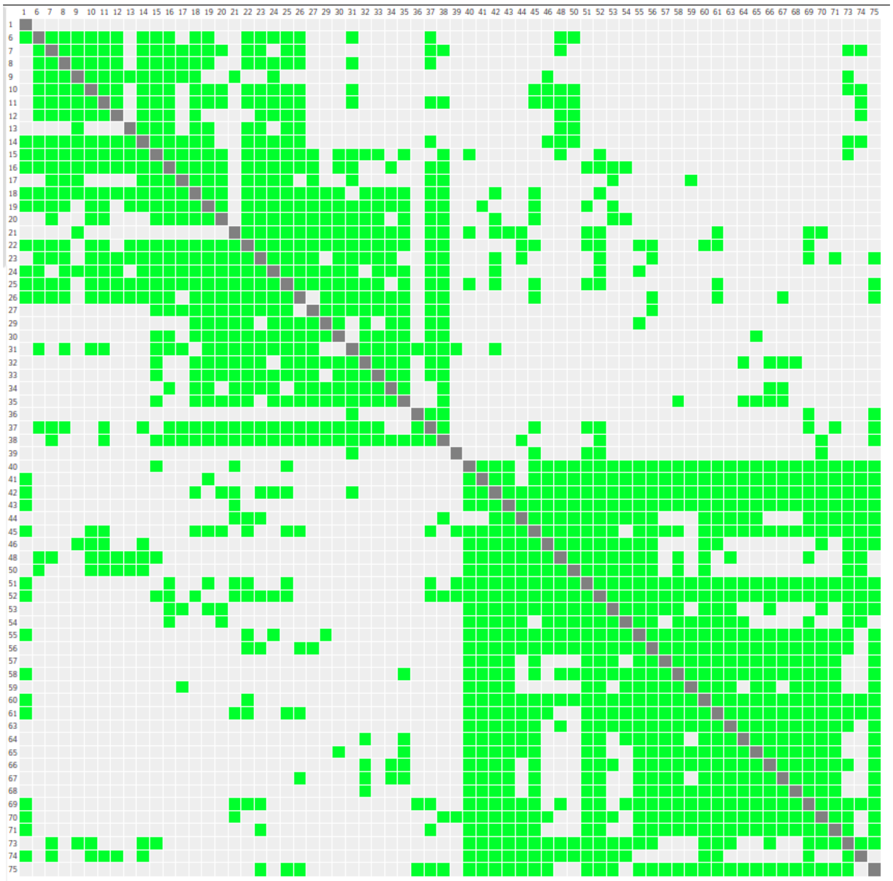
Route Changes (RC)

From the official documentation: The RC field is used to advertise the number of routing attempts needed to reach a destination. The number is a combination of Last Working Route (LWR) changes and Jitter measurements during transmission attempts between the Z/IP Gateway and the Z-Wave device. RC is incremented automatically by the Z/IP Gateway when either of the below conditions is true:

a) Last Working Route changed from the transmission of one command to the next
b) Tn – Tn-1 > 150ms where Tn and Tn-1 = the time needed to complete a transmission of a command
   I. IF 2 channels and FLIRS node, RC: Tn = Tn mod 1100
   II. . IF 3 channels and FLIRS node, RC cannot increment based on time calculation.

Transmission Count (TC)

From the official documentation: Total number of transmissions sent by all Z/IP Clients through the Z/IP GW to the specified Z-Wave destination node.



List of "nearby" nodes, connection speed and a flag to identify if the node is a repeater

Packet Error Count (PEC)

From the official documentation: Also sometimes referred to as PER. PEC is measured by the Gateway. The PEC value MUST be incremented each time the Gateway detects a failing transmission for each specific Z-Wave destination node.

Sum of Transmission Times (TS)

From the official documentation: The sum of all transmission times. This may be used to calculate the average transmission time. The time is given as a 32-bit unsigned integer MSB in millisec-onds.

$$(T) = \frac{1}{N} \sum_{i}^{N} T_i$$

Where N is the number of transmissions

Sum of Transmission Times Squared (TS2)

From the official documentation: The sum of the squares of all transmission times. This may be used to calculate the variance of the transmission time. The time is given as a 32 bit unsigned integer MSB in milliseconds2. The Variance may be calculated as follows:

$$(T^2) = \frac{1}{N} \sum_{i}^{N} T^2_i$$

(König-Huygens theorem)

Where N is the number of transmissions. A high variance is a sign of a bad link.

Last Working Route Get/Set

Previously called "Primary Route Get/Set."

The official documentation states:

> This command is used to set the network route to use when sending commands to the specified NodeID. The use of this command is NOT RECOMMENDED.

In theory, the command seems to allow manually managing the routes of a node (with a maximum of 4 hops set by the protocol). However, in practice, this command does not seem to have any effect on the network. In any case, the official documentation explicitly advises AGAINST using this command, making it highly likely that this command has already been deprecated by the protocol.

RSSI Get

The command is used to obtain the measurement of RSSI (Received Signal Strength Indication) for a specific node. The following values are allowed:

a) 0x7F**: RSSI_NOT_AVAILABLE** - No RSSI measurements are available for the node.

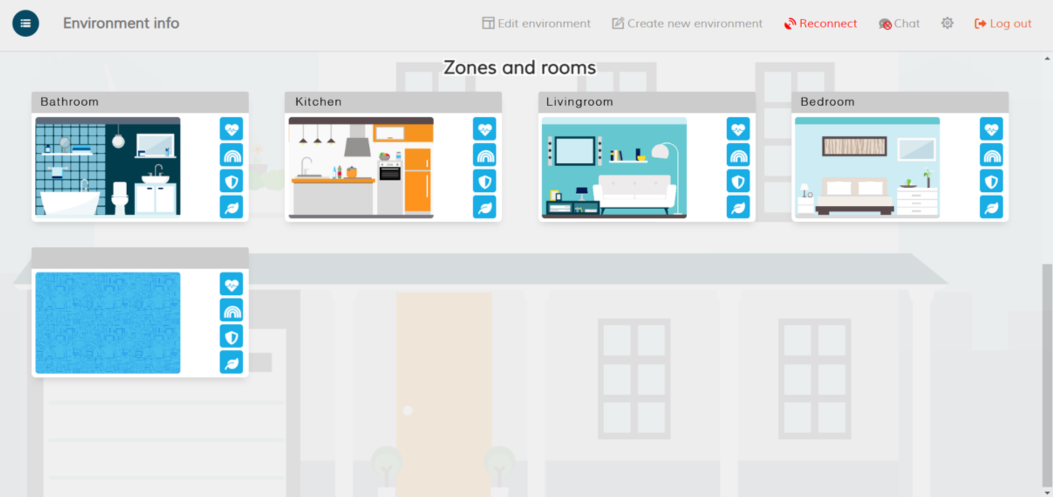
b) 0x7E: **RSSI_MAX_POWER_SATURATED** - The RSSI value exceeds the maximum allowed.

c) 0x7D: **RSSI_BELOW_SENSITIVITY** - The RSSI value is below the minimum level.

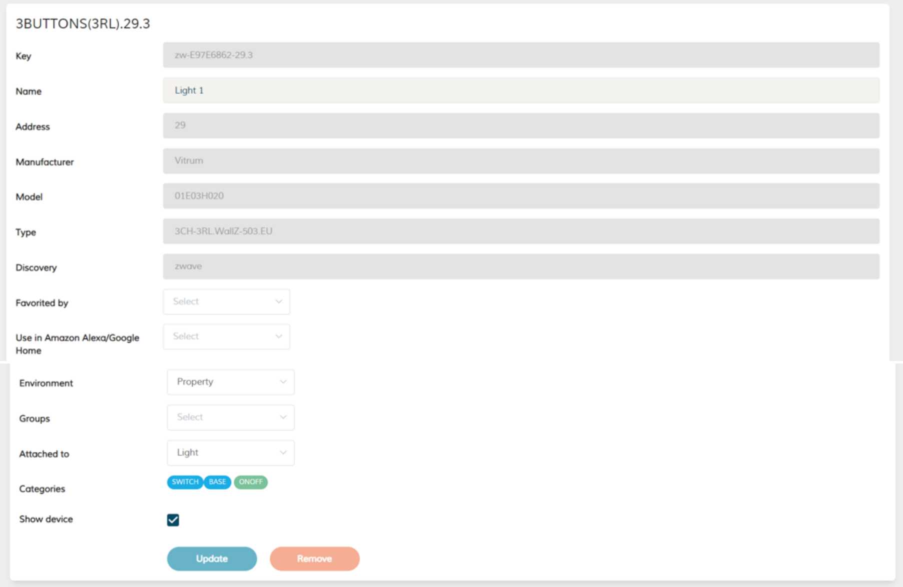
d) 0xE0..0xA2 - The value represents the RSSI *measurement in hexadecimal format, ranging from 0xE0 = -32 dBm to 0xA2 = -94 dBm.*

Environment Management

Once the Z-Wave configuration has been completed we move on to configuring the environments. If not all the environments in the building have been created during the activation phase, it will be possible to create new environments by clicking on "Create new environment"



Simply enter the "Name", a "Description" (optional), the "Type" of the environment if it is an "Internal or external environment" and if it has a "Parent environment" (for example if it is part of a specific floor of the building or if it is within another environment) and then click “Add”.



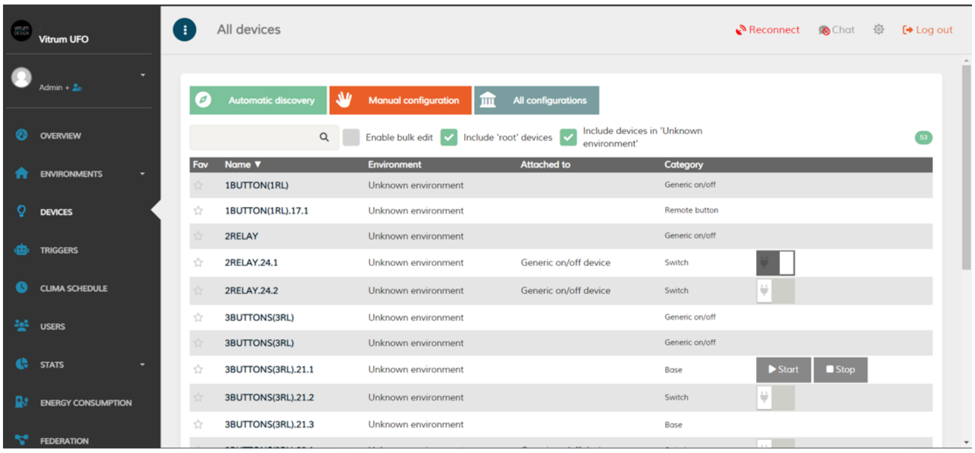
3BUTTONS(3RL).29.3

Key	zw-E97E6862-29.3
Name	Light 1
Address	29
Manufacturer	Vitrum
Model	01E03H020
Type	3CH-3RL.WallZ-503.EU
Discovery	zwave
Favorited by	Select
Use in Amazon Alexa/Google Home	Select
Environment	Property
Groups	Select
Attached to	Light
Categories	SWITCH BASE ONOFF
Show device	☑

It will also be possible to modify the fields of the environments created by clicking on the environment icon and then "Edit Environment."

Devices configuration

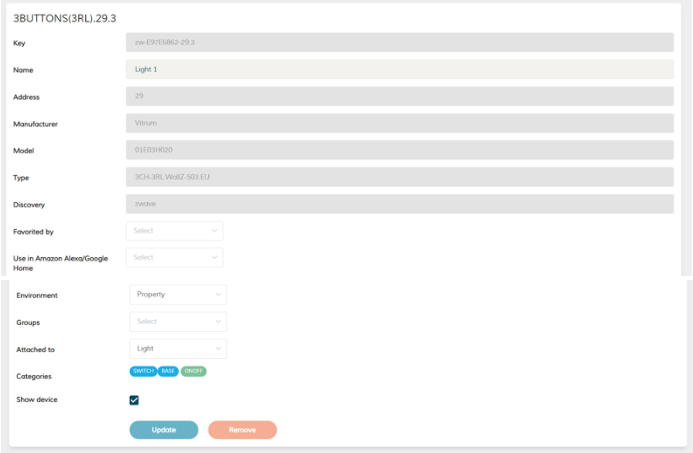
Let's move on to configuring the Devices previously included and configured and inserting them into the reference environments.



☐ Enable bulk edit ☑ Include 'root' devices ☑ Include devices in 'Unknown environment'

Fav	Name ▼	Environment	Attached to	Category	
☆	1BUTTON(1RL)	Unknown environment		Generic on/off	
☆	1BUTTON(1RL).17.1	Unknown environment		Remote button	
☆	2RELAY	Unknown environment		Generic on/off	
☆	2RELAY.24.1	Unknown environment	Generic on/off device	Switch	
☆	2RELAY.24.2	Unknown environment	Generic on/off device	Switch	
☆	3BUTTONS(3RL)	Unknown environment		Generic on/off	
☆	3BUTTONS(3RL)	Unknown environment		Generic on/off	
☆	3BUTTONS(3RL).21.1	Unknown environment		Base	▶ Start ■ Stop
☆	3BUTTONS(3RL).21.2	Unknown environment		Switch	
☆	3BUTTONS(3RL).21.3	Unknown environment		Base	

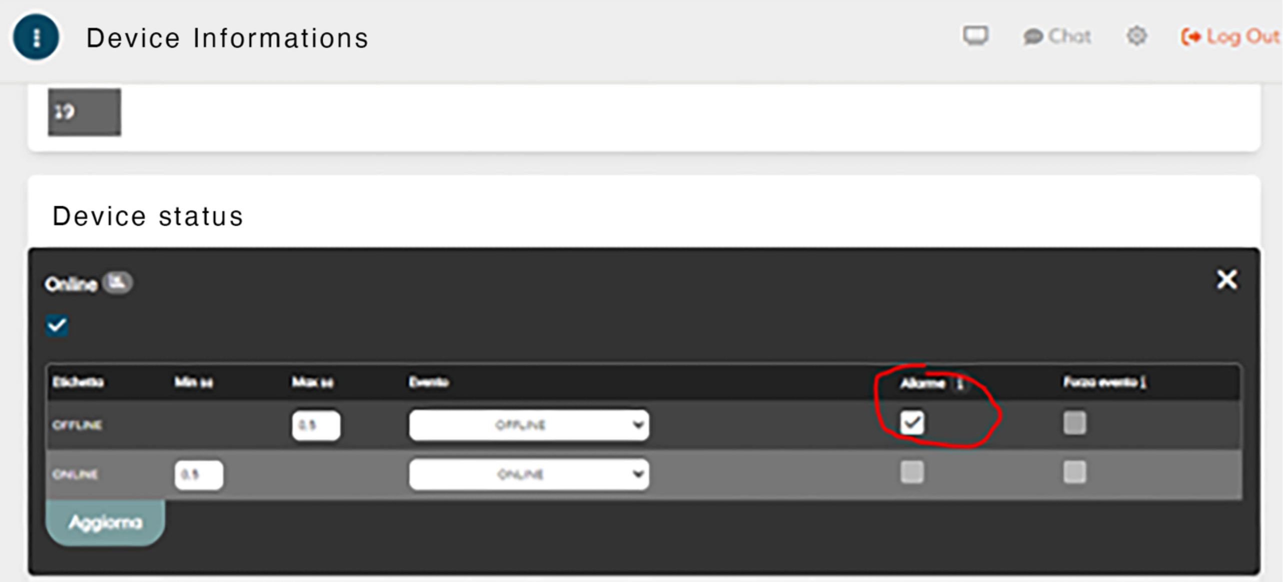
By clicking on a device, we will enter the edit page, where we can change the name, associate it with an environment and define what it is connected to (for example to logically "transform" a switch into a light)



3BUTTONS(3RL).29.3

Key	zw-E97E6862-29.3
Name	Light 1
Address	29
Manufacturer	Vitrum
Model	01E03H020
Type	3CH-3RL.WallZ-503.EU
Discovery	zwave
Favorited by	Select
Use in Amazon Alexa/Google Home	Select
Environment	Property
Groups	Select
Attached to	Light
Categories	SWITCH BASE ONOFF
Show device	☑

From the same Device Information page, you can also disable disconnect notifications.



Device Informations

Device status

Online

☑

Etichetta	Min se	Max se	Evento	Allarme	Forza evento
OFFLINE		0.5	OFFLINE	☑	□
ONLINE	0.5		ONLINE	□	□

Automations

With UFO, it is possible to create automations that could be triggered by events (such as pressing a button on a satellite, changing a switch, detecting motion, or simply a date/time rule).

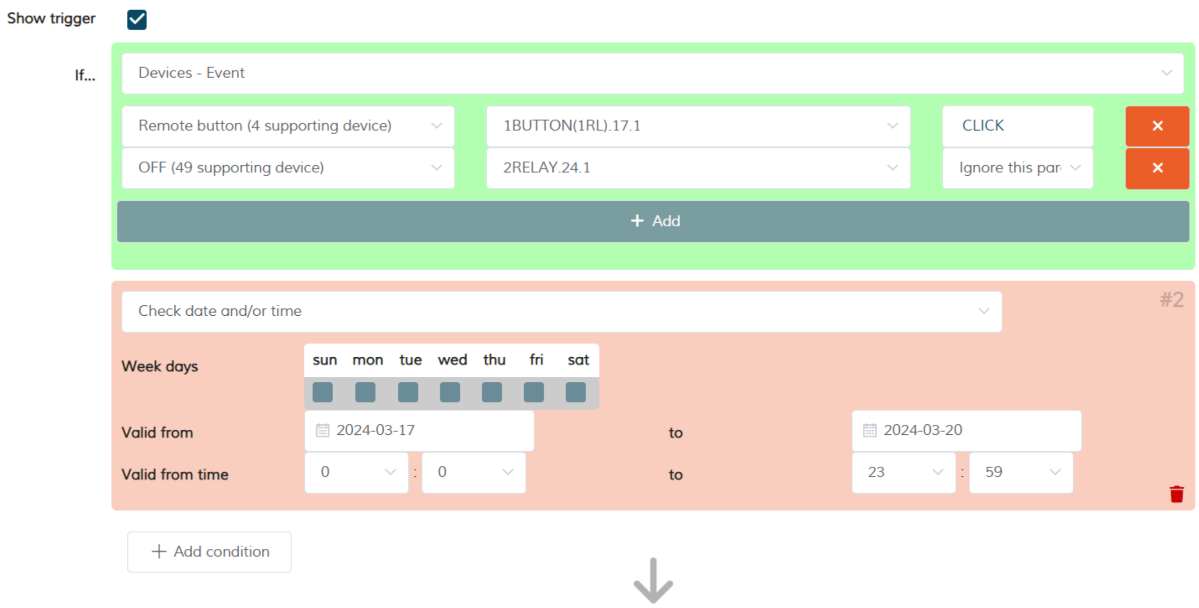
In the case of Vitrum II keypads, the button that "triggers" the associated automation can be configured in one of the following ways:

- Master off → To trigger the associated automation (within the automation, the condition to use is Remote button -> CLICK), a long press of the button is required, and the event will be indicated by a flashing light and a series of beeps.
- Switch sat → To trigger the associated automation (within the automation, the condition to use is Remote button -> ON or OFF), a simple press of the button is required. (e.g., If you want to create an automation to turn off all the lights in the house, you can include turning off the same button within the same automation after all the actions).
- Trigger → To trigger the associated automation (within the automation, the condition to use is Remote button -> ON or OFF), a simple press of the button is required. (e.g., If you want to create an automation to turn off all the lights in the house, you can include turning off the same button within the same automation after all the actions). Compared to the Switch Sat configuration, this configuration is faster.

In a Vitrum keypad, only one button configured as a master off type can be used.

Multiple conditions and actions

In the creation of automations, it is possible to choose multiple conditions to trigger the automation. Events on devices can be logically ORed together. Moreover, it is possible to configure the first condition with a logical AND by evaluating an additional state condition:



Show trigger ☑

If... Devices - Event

Remote button (4 supporting device) | 1BUTTON(1RL).17.1 | CLICK

OFF (49 supporting device) | 2RELAY.24.1 | Ignore this par

Check date and/or time

Week days: sun mon tue wed thu fri sat

Valid from 2024-03-17 to 2024-03-20

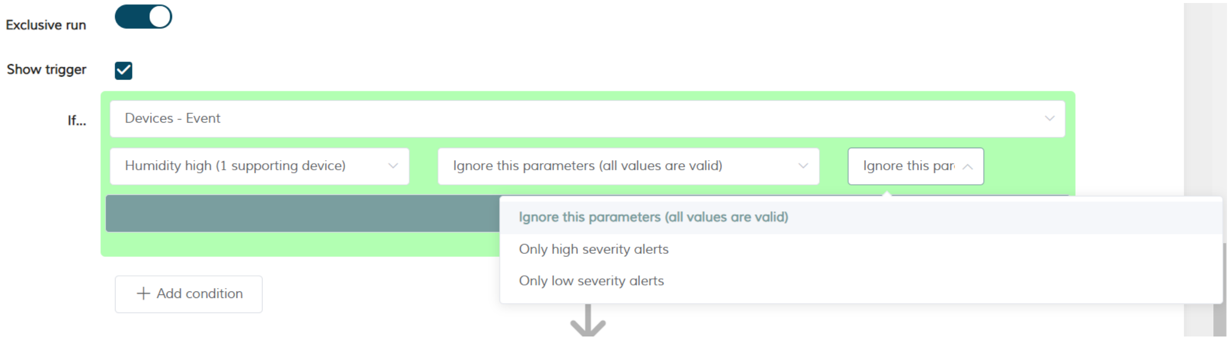
Valid from time 0 : 0 to 23 : 59

Conditions on weather service events

It is also possible to use events from the "weather service" device, such as those related to wind intensity, rain level, humidity, or temperature.

In the right box of the image below, you can choose what type of alarm will trigger the automation, whether a severe alarm or even non-severe alarms.

If you choose only severe alarms, then to trigger the automation, it is necessary to create a severe alarm by checking the "alarm" box in the relevant measurement type (e.g., VERY HIGH wind speed as shown in the figure below) inside the weather service page.



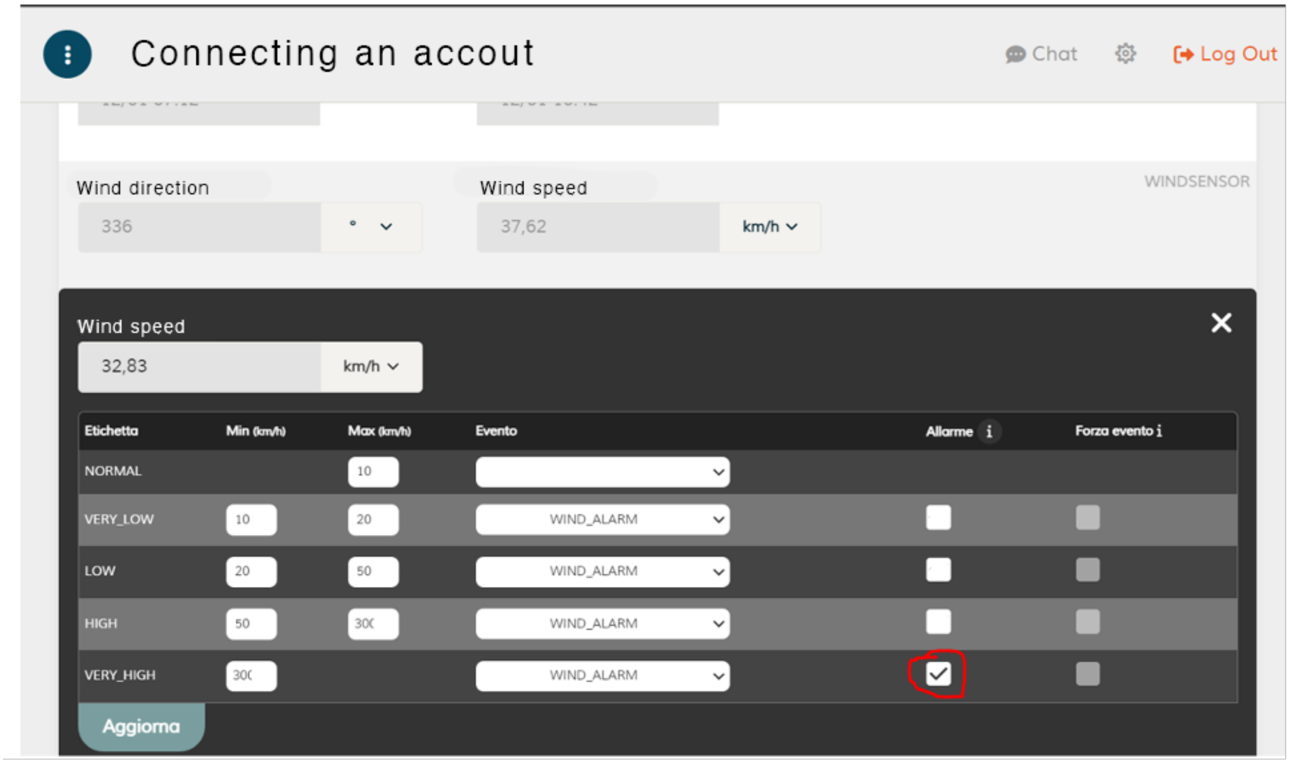
Exclusive run

Show trigger ☑

If... Devices - Event

Humidity high (1 supporting device) | Ignore this parameters (all values are valid) | Ignore this par

Ignore this parameters (all values are valid)
Only high severity alerts
Only low severity alerts
+ Add condition



Connecting an accout

Wind direction: 336 °

Wind speed: 37,62 km/h

WINDSENSOR

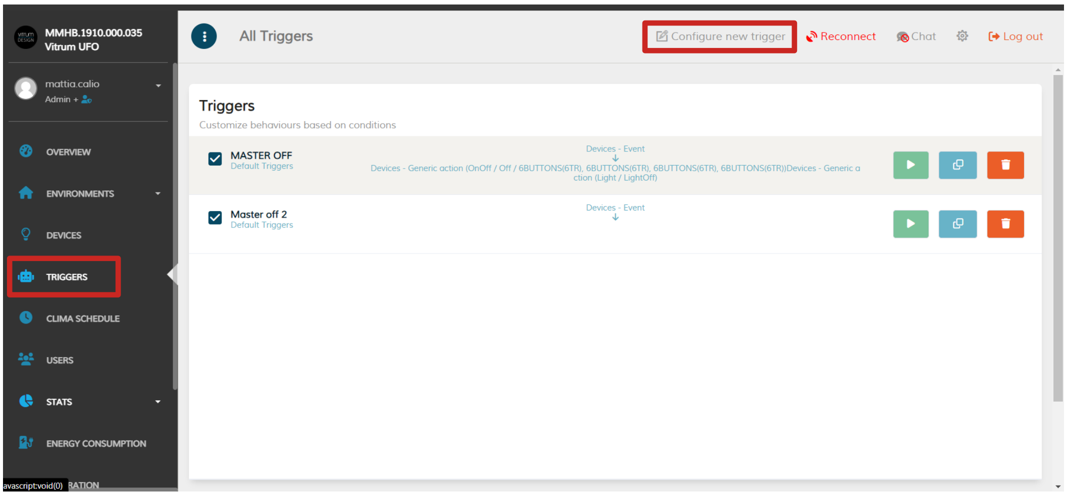
Wind speed: 32,83 km/h

Etichetta	Min (km/h)	Max (km/h)	Evento	Allarme i	Forza evento i
NORMAL		10			
VERY_LOW	10	20	WIND_ALARM	☐	☐
LOW	20	50	WIND_ALARM	☐	☐
HIGH	50	300	WIND_ALARM	☐	☐
VERY_HIGH	300		WIND_ALARM	☑	☐

Below, by way of example, we show the creation of various types of automation.

Master Off

Click on the “automation” menu item and on “configure a new automation” (Figure 33)



Triggers

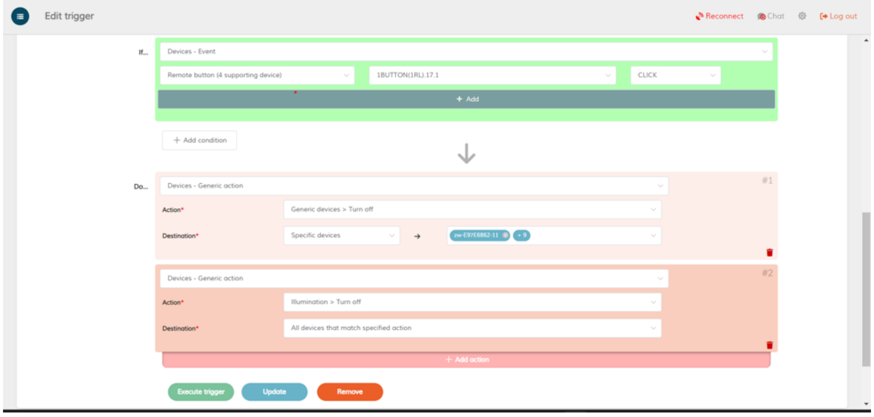
Customize behaviours based on conditions

☑ MASTER OFF
Default Triggers
Devices - Event
↓
Devices - Generic action (OnOff / Off / 6BUTTONS(6TR), 6BUTTONS(6TR), 6BUTTONS(6TR), 6BUTTONS(6TR))Devices - Generic action (Light / LightOff)

☑ Master off 2
Default Triggers
Devices - Event
↓

At this point, we will enter the Automation Name, click on Enabled if we want it to be active immediately, choose the condition "Device Event," then select the device type, in our case, "Remote Button," and choose the device and endpoint that will trigger the event. Finally, choose the "Off" action in our case.

Now, we will select what we act on; in our case, we will choose "generic action," select the action, choose lighting -> Turn Off, and then decide whether the action applies to all lighting devices (see the Categories chapter), a specific room, or specific devices. In our case, we choose specific devices and select them from the available ones, finally, click on Add.



If... Devices - Event
Remote button (4 supporting device) | 1BUTTON(1RL).17.1 | CLICK

Do... Devices - Generic action
Action* Generic devices > Turn off
Destination* Specific devices → zw-E97E6862-11 +9

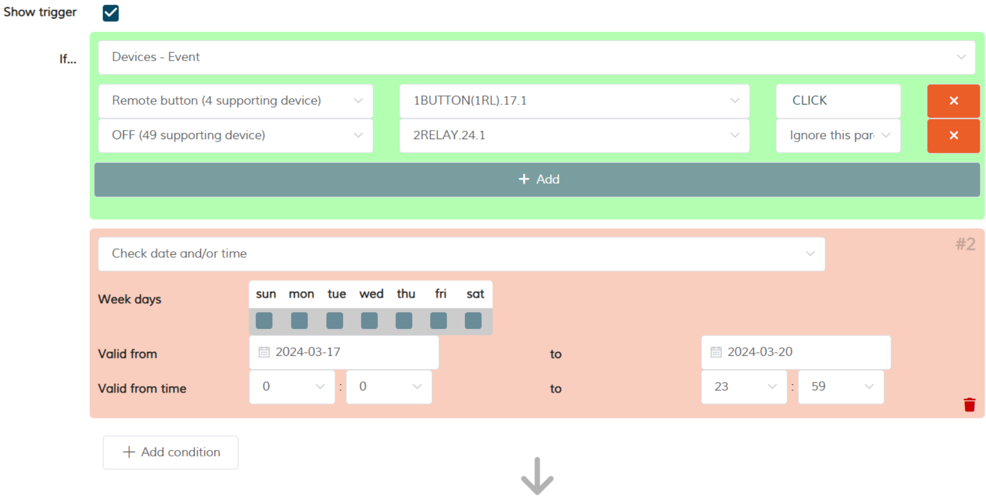
Devices - Generic action
Action* Illumination > Turn off
Destination* All devices that match specified action

Returning to the just-created automation, we can click on "Execute Trigger" to test the automation. In addition to the triggering condition (If/Se), it is possible to have secondary conditions to be evaluated sequentially to decide whether to execute the automation.

Timed lights switch on

Click on the "Automation" menu item and then on "Set up a new automation" (Figure 33).

Once the name is entered and the automation is enabled, choose the "Date/Time" condition. You will see a weekly calendar with an activation time; in our case, the rule will be valid every day at 4:00 PM. For the action, choose a generic action, this time "Lighting->Turn On," and as the destination, choose a specific room. This way, at 4:00 PM every day, all the lights configured within that specific room will be turned on.

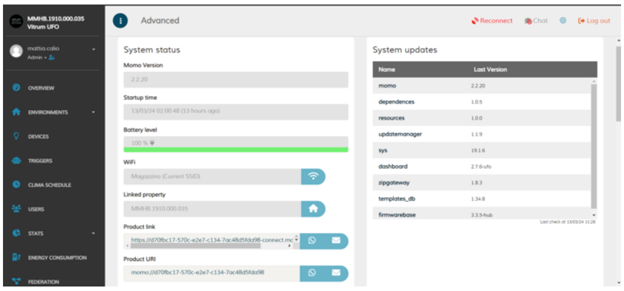


Show trigger ☑

If... Devices - Event
Remote button (4 supporting device) | 1BUTTON(1RL).17.1 | CLICK | ×
OFF (49 supporting device) | 2RELAY.24.1 | Ignore this par | ×

Check date and/or time
Week days: sun mon tue wed thu fri sat
Valid from 2024-03-17 to 2024-03-20
Valid from time 0 : 0 to 23 : 59

Settings



System status

Momo Version: 2.2.20

Startup time: 13/03/24 02:00:48 (13 hours ago)

Battery level: 100 %

WiFi: Magazzino (Current SSID)

Linked property: MMHB.1910.000.035

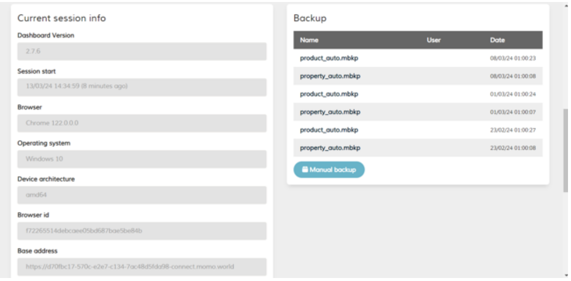
Product link: https://d70fbc17-570c-e2e7-c134-7ac48d5fda98-connect.mc

Product URI: momo://d70fbc17-570c-e2e7-c134-7ac48d5fda98

System updates

Name	Last Version
momo	2.2.20
dependences	1.0.5
resources	1.0.0
updatemanager	1.1.9
sys	19.1.6
dashboard	2.7.6-ufo
zipgateway	1.8.3
templates_db	1.34.8
firmwarebase	3.3.5-hub

Last check at 13/03/24 11:28



Current session info

Dashboard Version: 2.7.6

Session start: 13/03/24 14:34:59 (8 minutes ago)

Browser: Chrome 122.0.0.0

Operating system: Windows 10

Device architecture: amd64

Browser id: f72265514debcaee05bd687bae5be84b

Base address: https://d70fbc17-570c-e2e7-c134-7ac48d5fda98-connect.momo.world

Backup

Name	User	Date
product_auto.mbkp		08/03/24 01:00:23
property_auto.mbkp		08/03/24 01:00:08
product_auto.mbkp		01/03/24 01:00:24
property_auto.mbkp		01/03/24 01:00:07
product_auto.mbkp		23/02/24 01:00:27
property_auto.mbkp		23/02/24 01:00:08

The settings menu it will be possible to carry out maintenance on the product:

Sistem status

- □ UFO Version: displays the current version of the UFO process.
- □ Start Date: shows the date/time of the last UFO restart.
- □ Battery Charge: indicates the charge status visually and as a percentage.
- □ Wi-Fi: shows Wi-Fi connection information and provides a button for Wi-Fi change. If an Ethernet dongle is present, it also allows enabling/disabling Wi-Fi.
- □ Connected Building: displays the name of the house associated with the product and offers a button to change the house.
- □ Product Link: provides a link to share access to the specific product.
- □ Reboot: allows for a full system reboot.
- □ Restart: allows for restarting only the UFO process.
- □ Close Installation: to be pressed at the end of the system startup to generate the configuration backup for the entire system.

System updates

- □ The button in the top right allows you to check for the presence of updates.
- □ The yellow button allows you to set a different update server than the official one.
- □ The "Battery conditions for updating" flag, only present for Vitrum Design Admin users, allows enabling updates even if the battery level is low (or not available if the batteries have been removed from the device).
- □ If available, the "Update" button will allow you to download and install the available updates.

Session information

It contains various information about the client (browser) connected to UFO. The browser identifier allows uniquely identifying a specific user connected from a specific device to a specific product.

Backup

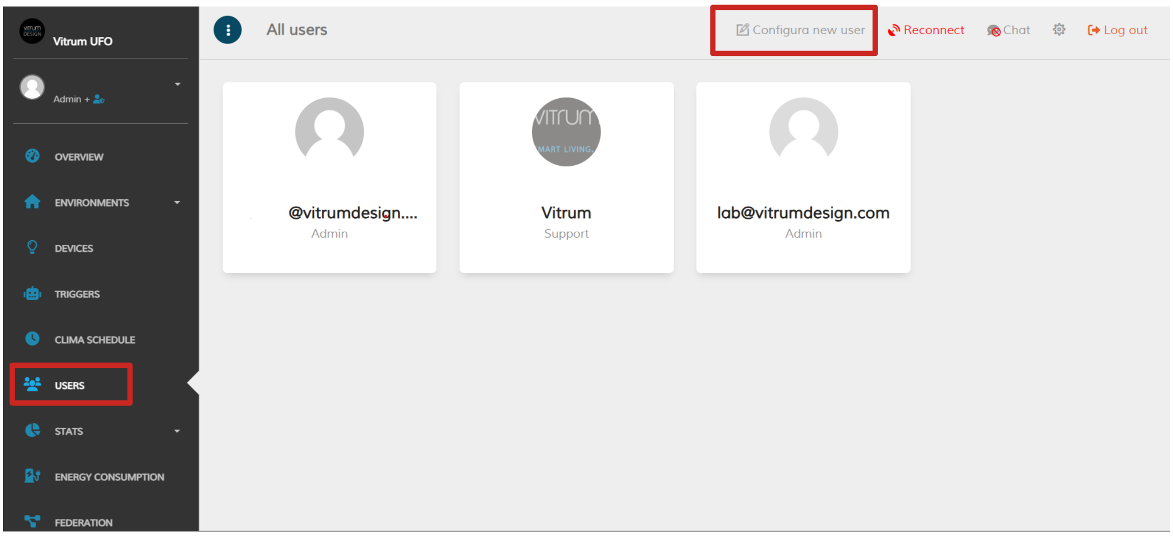
- □ The yellow icon allows you to modify the default time for automatic backups (by default, at one o'clock at night).
- □ Clicking on "Manual Backup" will perform a backup of the entire system (both product-related, i.e., Z-Wave and logs, and "home"-related, i.e., databases of devices, environments, automations, and users).

Users management

The system integrator, once the device configuration is complete, can create users who will then manage the home through the app. A user can have different roles:

- **Owner**: This user is associated with the home and the product. They have the same permissions as an admin but cannot be deleted from the databases. This user is automatically used in case offline mode is enabled.
- **Admin**: This user is an administrator and, as such, can perform any operation on the system (except deleting the owner).
- **User**: This is a limited user who can only use the installed devices. **NOTE**: This is the recommended role for standard installations.
- Guest: This is a "guest" user (who can also be defined in terms of start/end access date and time).
- **Not Authorized**: This is a user who has been explicitly denied access (e.g., following a change of role).
- **Not Defined**: This is a user who has attempted direct access to the product, which has been tracked by the system.

To add a user, click on the "Users" menu and then "Configure New User."



Fill in the mandatory fields (in particular Name, Role and Email) and click "Add".

Permissions

Regardless of the role, it is possible to configure specific permissions for the user using the "Permissions" tab.

In general, you can choose to Allow (Yes), Deny (No), or continue inheriting the permission from the role (Inherit parameter from role). However, for some permissions, it is also possible to make a more specific customization. For example, in the case of permissions for devices, you can choose the start/end date and time of authorization, as well as a list of authorized environments/devices. This feature allows assigning customized privileges even to service personnel such as housekeepers, caregivers, babysitters, etc.

Device Hardware Management

Reset (only UFO 1.0)

NOTE: In UFO releases after the first one, the reset procedure is no longer provided because it has been replaced by the new "Shipping" functionality.

To perform a system reset, press the button on the back of UFO for a duration between 3 and 5 seconds. If the operation is successful:

- The buzzer emits a short sound (200ms).

- The Brain button lights up at maximum brightness for 2 seconds, then decreases to minimum brightness.

It is not possible to perform two consecutive resets within a time interval of less than one minute.

Factory reset

To perform a factory reset of the system:

1. Press the button on the back of UFO for at least 10 seconds.
    a. If the operation cannot be executed:
    b. The buzzer emits two beeps.
2. If the system enters factory reset mode:
    a. The Brain button blinks slowly (HeartBeat Normal).
    b. The buzzer emits a short sound (500 ms).
3. Confirm the execution of the procedure by touching the Brain button for at least 2.5 seconds (Long Touch):
    a. The Brain button starts blinking rapidly (HeartBeat Fast).
4. If the operation is successful:
    a. The buzzer emits a short sound (200 ms).
    b. The Brain button lights up at maximum brightness for 2 seconds and then sets the brightness to 20%.
5. If the operation fails:
    a. The buzzer emits a beep followed by a short sound (800 ms).
    b. The Brain button stops blinking and sets the brightness to 20%.

Firmware update

When the UFO system enters firmware update mode, the following events occur:

- The Brain button blinks rapidly (HeartBeat Fast).
- The touch sensor is not active.

If the firmware update is successfully completed, the following events occur:

- The buzzer emits a short sound (200 ms).
- The Brain button lights up at maximum brightness for 2 seconds, then reaches minimum brightness.

The same events occur if the firmware update is not completed within 30 minutes.

Power supply OFF/ON

□ When the power supply is disconnected, the buzzer emits a sound (1s).

□ When the power supply is connected, the buzzer emits a short sound (100ms).

System standby (solo UFO 1.0)

Standby Input

To set the system in standby mode, press the Brain button for at least 2 seconds (Long Click).

- The Brain button starts flashing slowly (HeartBeat Normal).

From this point, you can choose to either perform a Shutdown (Double click) or a Power Off (Long Click) of the SoC.

If neither option is selected within 10 seconds, the operation is canceled:

- The Brain button stops flashing and turns on at minimum brightness.

If any of the two modes is selected, for the next 10 seconds:

- The Brain button flashes rapidly (HeartBeat Fast).
- The touch sensor is not active.

When the Brain button turns off, the system is in standby. You have:

- Touch sensor active only for Long Click events (to exit standby).
- SoC and sensors in Low Power mode.

Standby Output

To exit standby mode, press the Brain button for at least 2 seconds (Long Click).

When this operation is performed:

- *The buzzer emits a Play (200ms).*
- *SoC and sensors exit Low Power mode.*
- *The Brain button flashes rapidly (HeartBeat Fast).*
- *The touch sensor is not active.*

  When the Brain button no longer flashes, the system has restarted. You have:

  - *Brain button on at minimum brightness.*
  - *Touch sensor active for Click and Long Click events.*

System Shipping (UFO 2.0 or next)

To set the system to shipping mode:

1. Press the button on the back of UFO for at least 3 seconds and release within 6 seconds.

   ✓ If the press does not follow the specified times (3-6 seconds), the buzzer emits a Beep.

   ✓If the operation cannot be performed, the buzzer emits three Beeps.

2. The Brain button starts flashing slowly (HeartBeat Normal).

3. Confirm the operation by quickly and decisively tapping the Brain button twice (Double Touch).

4. If no confirmation is given within 10 seconds, the operation is canceled:

   ✓ The Brain button stops flashing (repeat from step 1).

5. The system enters Shipping Mode:

   ✓ Until the SoC is turned off, the Brain button flashes rapidly (HeartBeat Fast).

   ✓ The touch sensor is not active.

6. When the SoC shutdown is complete:

   ✓ The Brain button flashes slowly (HeartBeat Normal).

   ✓ The buzzer emits a Play (500 ms) every 500 ms.

6. Remove the power supply:

   ✓ The Brain button turns off.

   ✓ The system is completely turned off.

Shipping OutputNote

To exit shipping mode when you are at step 6 of the previous steps:

1. Press the button on the back of UFO for at least 3 seconds and release within 6 seconds.

   ✓ The buzzer no longer emits any effects.

   ✓ The Brain button turns on and off (HeartBeat onOFF).

   ✓ The SoC is turned on.

2. When the SoC startup is complete:

   ✓ The Brain button stops flashing and sets the brightness to 20%.

Refused shipping.

If shipping is temporarily not possible:

- The buzzer emits three plays (200 ms)

This happens, for example, during the first 2 minutes after system startup.

System reboot during shipping

In case the system undergoes a restart while in the shipping state:

- The buzzer emits a Play (200 ms).

If the system has restarted due to a lack of power, the shipping state is unloaded:

- The Brain button lights up to maximum brightness for 2 seconds, then sets the brightness to 20%.

If the system has restarted for some other reason, the shipping state is confirmed:

- The Brain button flashes quickly (HeartBeat Fast) until the SoC is turned off.

Low Battery Before User Confirmation

If a low battery condition occurs during the waiting period for confirmation, the shipping request is discarded, and the system enters Low Power mode. It is possible to activate Shipping mode even when in Low Power mode. Refer to the "Low Battery" chapter.

Low Battery During SoC Shutdown

If a low battery condition occurs during the shutdown of the SoC, the system transitions into Low Power mode while maintaining the Standby request. In this case, once the shutdown of the SoC is complete, the system shuts down entirely:

- The Brain button turns off.
- The touch sensor is inactive.

Low Battery

When the batteries are low:

- The Brain button flashes rapidly (HeartBeat Fast) until the SoC turns off.

Once the shutdown of the SoC is complete:

- The Brain button stops flashing and sets the brightness to 10%.
- The touch sensor is active for Single Touch events.

When you touch the Brain button (Single Touch):

- The Brain button varies its brightness between 10% and 30%.

To enter standby mode, refer to the "System Shipping" chapter.

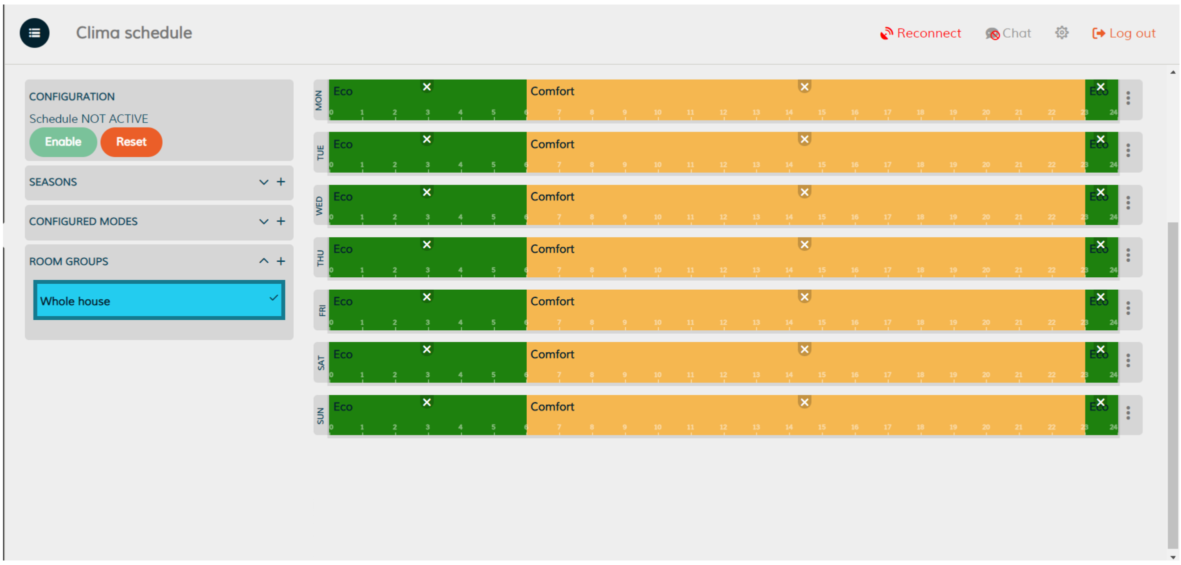
If the power supply is connected, when the battery charge reaches a sufficient level:

- The SoC is turned on.
- The Brain button turns on and off (HeartBeat onOFF).

Once the SoC startup is complete:

- The Brain button stops flashing and sets the brightness to 20%.
- The touch sensor is active for Single Touch events.

- Clima Scheduling

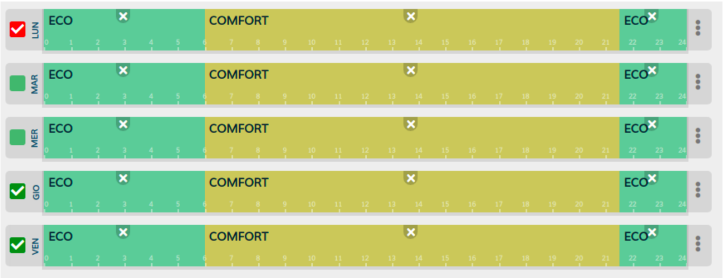


Schedule NOT ACTIVE

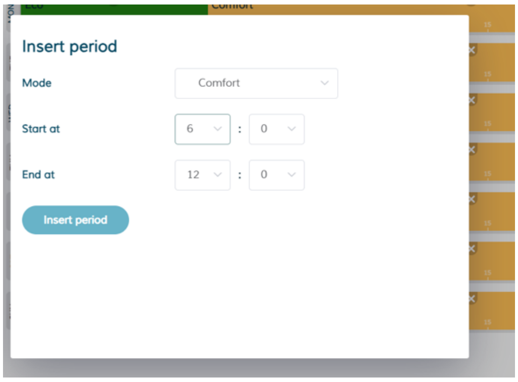
Whole house

Through the Climate scheduling, it is possible to plan the mode/setpoint of one or more thermostats on an hourly, daily, and weekly basis, also allowing to divide the mode based on different zones (**room groups**).

The interface allows you to create an hourly schedule for each day of the week by adding and removing intervals (or dragging them with a simple drag and drop). It is also possible to copy a configured schedule for a specific day or manually modify each period.



Still edit the setpoint associated with a certain **mode**.

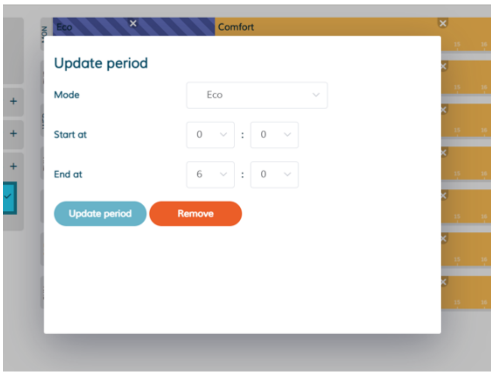


Insert period

Mode: Comfort

Start at: 6 : 0

End at: 12 : 0



Update period

Mode: Eco

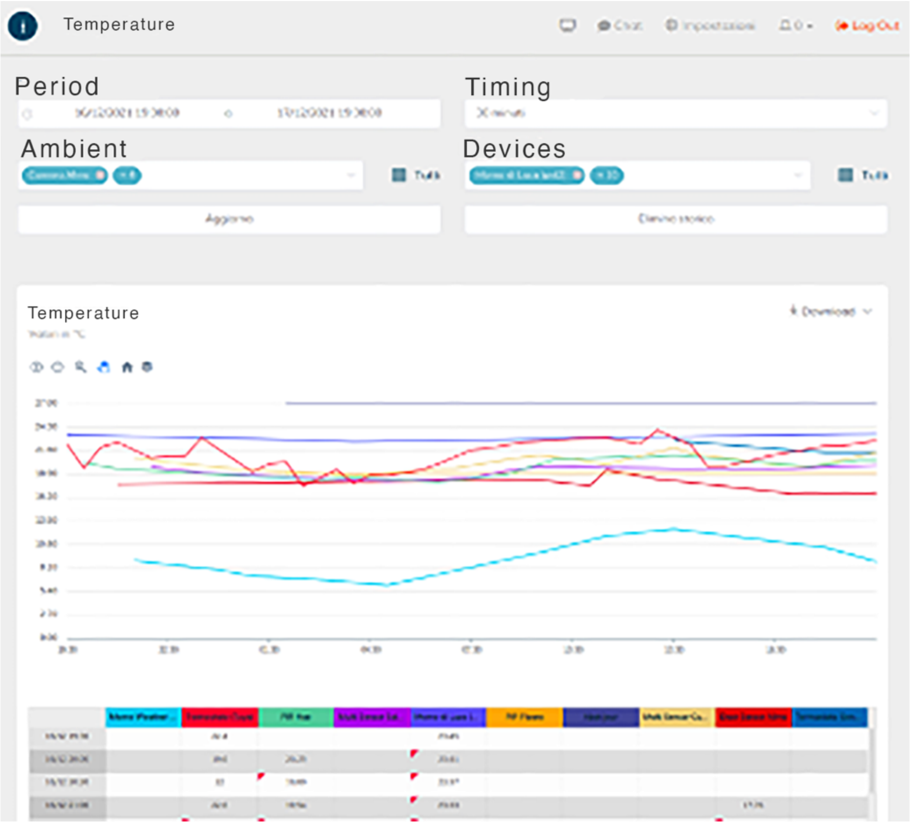
Start at: 0 : 0

End at: 6 : 0

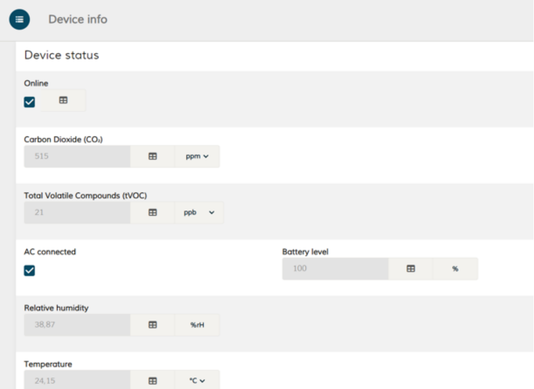
The modes are finally grouped into different seasons, and for each of them, you can choose the devices to use (in case a room has both an air conditioner for the summer season and a valve connected to a radiator for the winter season).

Statistics and Consumption

The "Statistics" interface, provided by the dashboard, allows access to measurements collected for each of the various dimensions that UFO internally archives. This enables defining a query for extraction, providing a graphical and tabular output of the data collected by the system.



NOTE: For each of the different measurements, both filters and graphical output may vary. Moreover, from the details of each device, in the "**Status**" section, you can click on the icon next to the name of the status property to access a graph depicting the detail of the samplings for the specific measurement over the last two days.


Device info

Device status

Online
☑

Carbon Dioxide (CO_2)
515 ppm

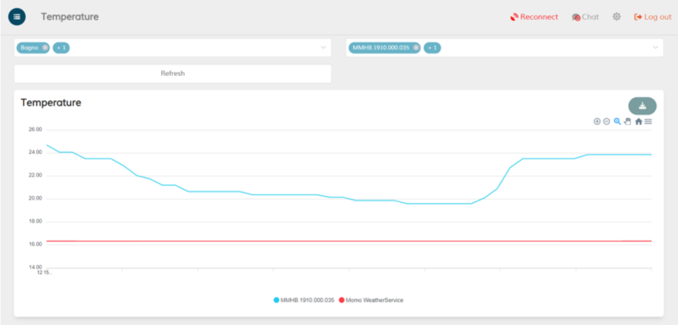
Total Volatile Compounds (tVOC)
21 ppb

AC connected
☑

Battery level
100 %

Relative humidity
38,87 %rH

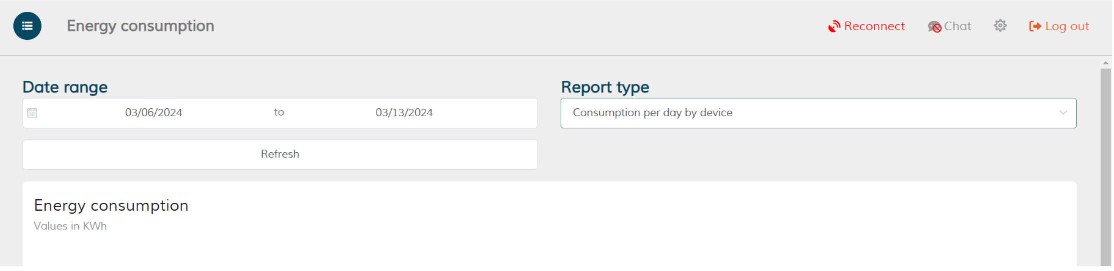
Temperature
24,15 °C



The "Consumption (Consumptive)" menu is primarily aimed at viewing electrical consumption (grouped by user type or reference environment).

NOTE: Internally, the collection of this data is carried out in three different ways depending on the functionalities exposed by the device:

- If the device provides a consumed energy value (e.g., in KWh) at midnight each day, the system compares this value with the one collected the previous evening, and the difference represents the total consumption for the day.
- If the device provides a power value, then this value is considered during the device's usage time (on time) to calculate the energy consumed by the device. Naturally, this value is subject to calculation errors due to system rounding.
- If the parameters "Consumption when on/off" are associated, then the calculation from the previous point is applied to these parameters. In this case as well, the final value is subject to calculation errors.


Energy consumption

Date range

03/06/2024 to 03/13/2024

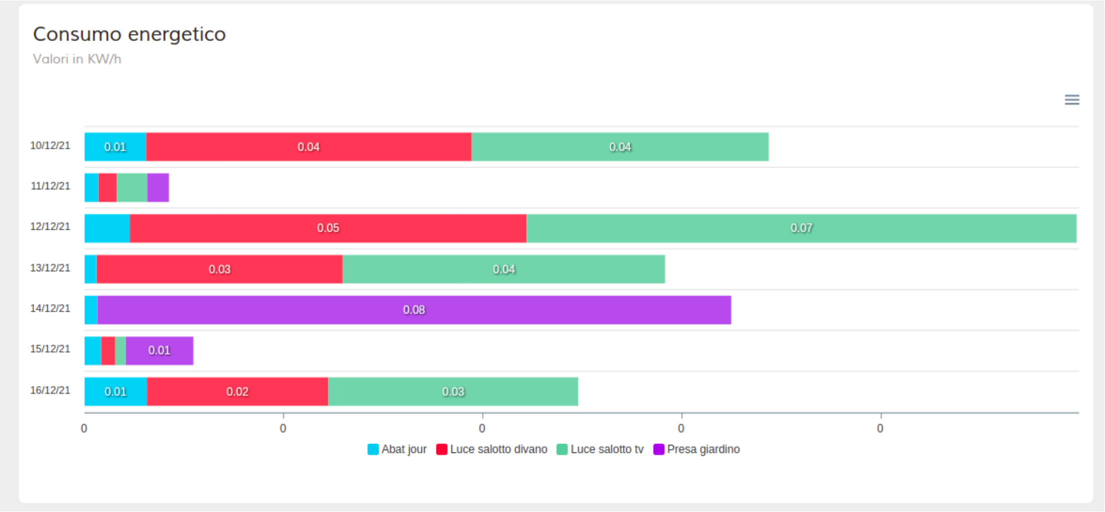
Refresh

Report type

Consumption per day by device

Energy consumption

Values in KWh


Consumo energetico

Valori in KW/h

Federation

The federation allows for transparent management of devices, enabling their control independently of the UFO to which these devices are connected for the end-user.

Each UFO will have the ability to directly control the devices connected to it and indirectly control the devices connected to other UFOs within the federation.

To enable the federation, no special configuration steps are required. It is only necessary that the two (or more) UFOs are associated with the same property (home).

The federation is based on the concept of roles:

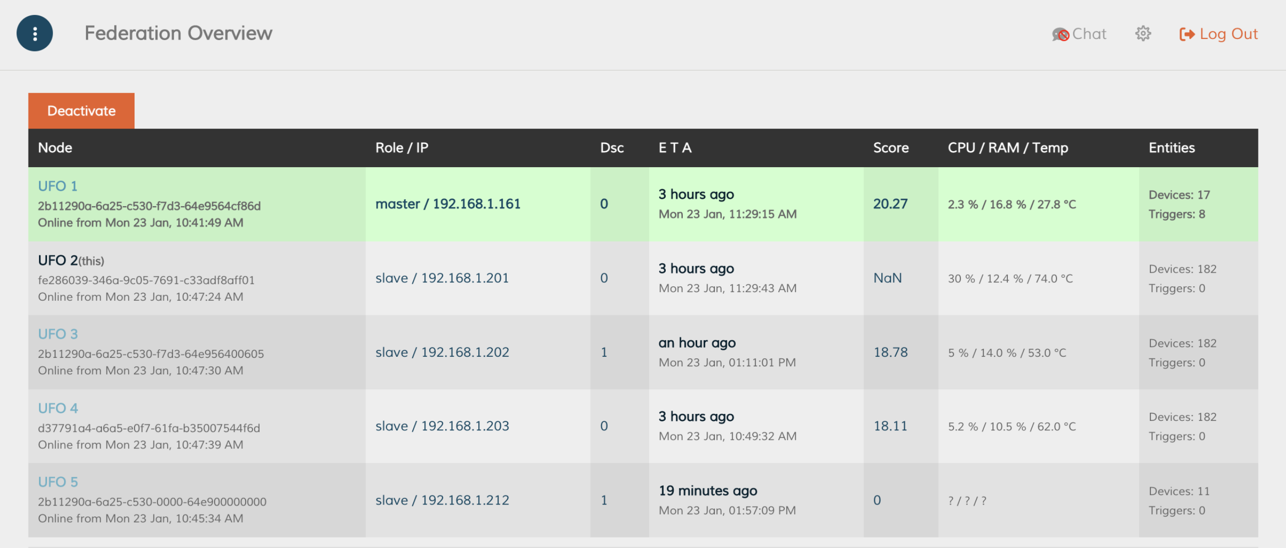
- **Master**: It is the collecting node of the federation, responsible for keeping all information distributed across various UFOs synchronized and routing messages between two slaves.
- **Slave**: It is a peripheral node, responsible for keeping its list of devices up to date and receiving federation information from the master node.

Regardless of the role, each node in the federation can send information to any other node. The main difference lies in the number of "hops" a message will have to make. A message sent from Slave A to Slave B, for example, must necessarily pass through the master (so it has to make a "jump" through the master), while a message sent from Master to Slave B will be "direct."

The election of the master is based on the concept of "age" and the concept of available resources: all else being equal, the older node will be elected as the master.

NOTE: This is why connections from the Vitrum App assume that the user is automatically connected to the master product of the federation.

Communication between different nodes is based on WebSocket connections (TCP on port 8080), while the discovery protocol is based on UDP packets on port 7123.



Node	Role / IP	Dsc	E T A	Score	CPU / RAM / Temp	Entities
UFO 1 2b11290a-6a25-c530-f7d3-64e9564cf86d Online from Mon 23 Jan, 10:41:49 AM	master / 192.168.1.161	0	3 hours ago Mon 23 Jan, 11:29:15 AM	20.27	2.3 % / 16.8 % / 27.8 °C	Devices: 17 Triggers: 8
UFO 2(this) fe286039-346a-9c05-7691-c33adf8aff01 Online from Mon 23 Jan, 10:47:24 AM	slave / 192.168.1.201	0	3 hours ago Mon 23 Jan, 11:29:43 AM	NaN	30 % / 12.4 % / 74.0 °C	Devices: 182 Triggers: 0
UFO 3 2b11290a-6a25-c530-f7d3-64e956400605 Online from Mon 23 Jan, 10:47:30 AM	slave / 192.168.1.202	1	an hour ago Mon 23 Jan, 01:11:01 PM	18.78	5 % / 14.0 % / 53.0 °C	Devices: 182 Triggers: 0
UFO 4 d37791a4-a6a5-e0f7-61fa-b35007544f6d Online from Mon 23 Jan, 10:47:39 AM	slave / 192.168.1.203	0	3 hours ago Mon 23 Jan, 10:49:32 AM	18.11	5.2 % / 10.5 % / 62.0 °C	Devices: 182 Triggers: 0
UFO 5 2b11290a-6a25-c530-0000-64e900000000 Online from Mon 23 Jan, 10:45:34 AM	slave / 192.168.1.212	1	19 minutes ago Mon 23 Jan, 01:57:09 PM	0	? / ? / ?	Devices: 11 Triggers: 0

Observations and advanced management

In the case of proceeding with federation, some basic principles need to be observed.

It is important to note that each UFO "owns" a device, meaning that within the federation, a certain UFO has the unique delegation for its management. This concept of "ownership" can be either locked and not modifiable, as in the case of Z-Wave networks (see later), or it can vary based on the need.

It becomes evident that if a UFO is offline, turned off, or otherwise unreachable, everything related to the devices connected to it (device control, sensor readings, automation) will not function.

Z-Wave Limits

In Z-Wave networks, each node is uniquely associated with the Z-Wave hardware controller of each UFO (or, more precisely, with its HomeId). Each Z-Wave network node can communicate only with devices that belong to its Home Area Network (HAN).

This limitation also has repercussions on federation configurations, meaning:

- **It is NOT** allowed to access Z-Wave networks of UFOs other than the one to which you are connected. Therefore, to perform inclusions and maintenance operations on a specific UFO, you will need to connect from the dashboard to that specific product.
- **It is NOT** possible to create Z-Wave LINKs and ASSOCIATIONS between different UFOs. In this scenario, you can only use automations (TRIGGERs).
- **It is NOT** possible to connect UFOs placed in different LAN networks (or even just different subnets).

Given what has just been said, the basic principle for configuring Z-Wave devices on different UFOs is to consider the following factors:

- Each Z-Wave device should be configured on the nearest or most stable UFO to minimize the chance of communication errors.
- Devices that need to participate and cooperate in the same environment should be configured on the same Z-Wave network to enable the management of links and associations, the functioning of which is independent of the federation's state and the UFO.

App limitation

Currently, some additional apps may experience certain bugs if they are not explicitly designed to be used in this scenario as well. The reason for this limitation is that some apps, for latency and performance reasons, do not use the internal service bus (which abstracts UFOs in federation as if they were the same product) but automatically hook into local system events.

Latency and bandwidth occupancy

Especially during the initial bootstrap phase, each UFO is responsible for sending its configurations to the master as they are instantiated. This causes a significant bandwidth and resource occupation (bandwidth because the data is continually sent across the network to other UFOs, and performance because each UFO must merge its configuration into the network).

Latencies and bandwidth usage are closely related to the number and type of devices configured on each UFO (Z-wave devices tend to occupy more space than devices on other protocols).

In general, it is also preferable to equip each **UFO with a USB Ethernet dongle and disable the Wi-Fi** connection to prevent temporary disconnections from affecting the functioning and health of the federation. Each disconnection, in fact, requires a series of resynchronization messages like those that occur during the bootstrap phase.

Useful tips

To mitigate the impact of some undesirable effects in case of federation, consider the following annotations:

- In the case of a configuration with more than two nodes, ensure that the federation always prefers the same UFO by adjusting the reboot time to be slightly earlier than the others.
- Equip each UFO (or at least the UFO with the Master role) with a USB Ethernet dongle and disable Wi-Fi to mitigate disconnections.
- Configure devices (nodes, rooms, etc.) gradually and avoid performing configuration operations only at the end. Continuous modification forces the federation to continually update, and some of the configured data may be lost in synchronization operations, requiring the user to reapply the changes.
- Configure each Z-Wave device on the nearest or most stable UFO to minimize the possibility of communication errors.
- Devices that need to operate together in the same environment should be configured in the same Z-Wave network to enable the management of links and associations, the operation of which is independent of the federation's status and UFOs.
- If it is necessary to install an app (e.g., Clima Control), plan to install all involved devices on the same UFO before installing the app.

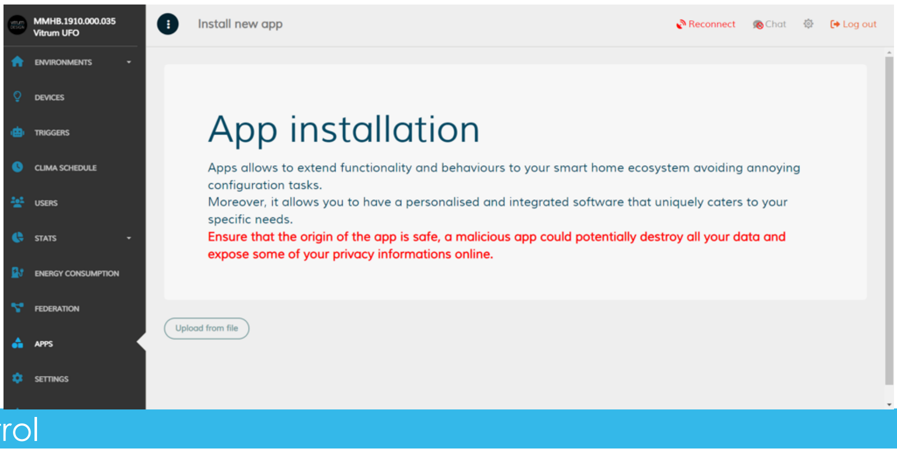
Other Apps

The apps allow extending UFO's native functionalities and behaviors, providing a quick and portable way to integrate it with third-party systems.

Starting from version **1.6.2**, UFO allows users to directly load apps (in the proprietary UFO format) or define their own (in JavaScript format, .js).

NOTE: To enable the integration mode and allow the product to use custom apps, a request to Vitrum Design is required.

By way of example, we provide an overview of some of the apps currently in use.



App installation

Apps allows to extend functionality and behaviours to your smart home ecosystem avoiding annoying configuration tasks.
Moreover, it allows you to have a personalised and integrated software that uniquely caters to your specific needs.
Ensure that the origin of the app is safe, a malicious app could potentially destroy all your data and expose some of your privacy informations online.

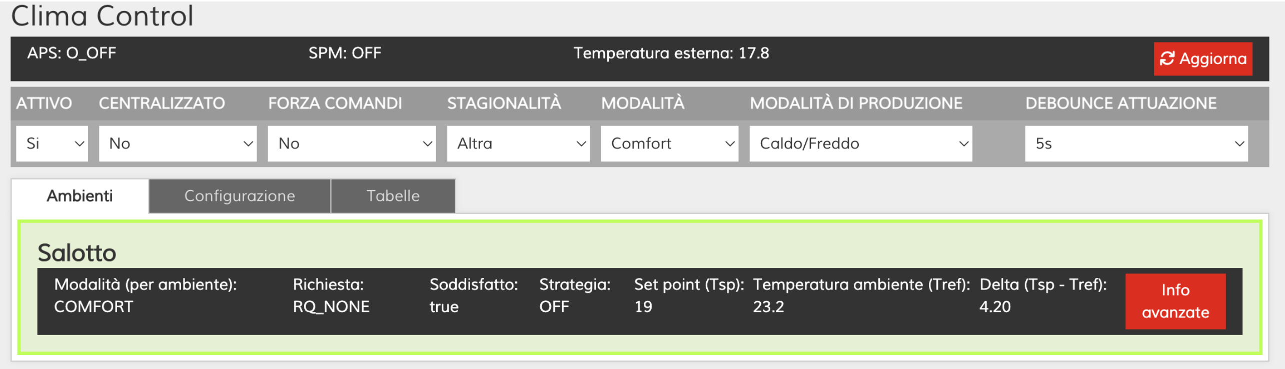
Clima Control

UFO Clima Control is a plugin (app) for UFO that enables advanced climate management.

Some of the most important features include:

Separate multi-zone management from the environment configuration: This allows you to separate what is shown to the user from what is managed by the air conditioning.

- **Extreme customization:** For example, it is possible (but not mandatory) to define specific hysteresis or setpoints for the individual zone or for a specific mode (COMFORT, ECONOMY).
- (Added in version 1.0.21 dated 19/11/22) **Trigger interaction** triggers support: added events on APS/SPM change and added hooks to activate/deactivate/change the production mode.
- Based on device **roles**.



Clima Control

APS: O_OFF SPM: OFF Temperatura esterna: 17.8

ATTIVO	CENTRALIZZATO	FORZA COMANDI	STAGIONALITÀ	MODALITÀ	MODALITÀ DI PRODUZIONE	DEBOUNCE ATTUAZIONE
Si	No	No	Altra	Comfort	Caldo/Freddo	5s

Salotto

Modalità (per ambiente):	Richiesta:	Soddisfatto:	Strategia:	Set point (Tsp):	Temperatura ambiente (Tref):	Delta (Tsp - Tref):
COMFORT	RQ_NONE	true	OFF	19	23.2	4.20

Roles

The concept of Device Roles is used to define the roles of various devices. The following roles are currently defined:

Virtual Thermostat: A virtual thermostat created at runtime by UFO to interface with Clima Control. Functions as a configuration entry point for the zone (see the "Virtual Devices" section).

Thermostat: Physical device serving as the main user interface for control. Can be configured to allow synchronization of SetPoint, Action/Mode, and FanSpeed with the Virtual Thermostat.

NOTE: In the case covered by this document, it must be configured to synchronize SetPoint and Action/Mode.

Temperature Sensor: Physical device for temperature detection.

- If possible, it is preferable to use the same device assigned to the Thermostat role.

HVAC (Heating, Ventilation, and Air Conditioning): Device for controlling the fan coil fan speed.

- If configured, it receives a command to change the fan speed based on the temperature difference between the detected ambient temperature and SetPoint.

NOTE: The fan coil speed is autonomously determined by the system if the Virtual Thermostat is set to Fan Speed = AUTO; otherwise, it is limited to the maximum speed set. If the Virtual Thermostat is set to MEDIUM speed, for example, the HVAC will be controlled at OFF, LOW, and MEDIUM speeds, but the system will avoid setting it to HIGH. Similarly, if the Virtual Thermostat is set to OFF, the system will never turn on the fans.

Valve Fan Coil: Device for controlling the opening of the fan coil valve.

- If configured, it receives an ON command whenever the environment requests enhanced climate control based on the set deltas and the central production status.

Valve Radiant Floor: Device for controlling the opening of the radiant floor valve.

- If configured, it receives an OFF command whenever the environment requests heating (RQ_HEAT), OFF when the system requests cooling (RQ_COOL), or when there are no requests (RQ_NONE).

Valve Cooling: Device for controlling the opening of the cold-water valve.

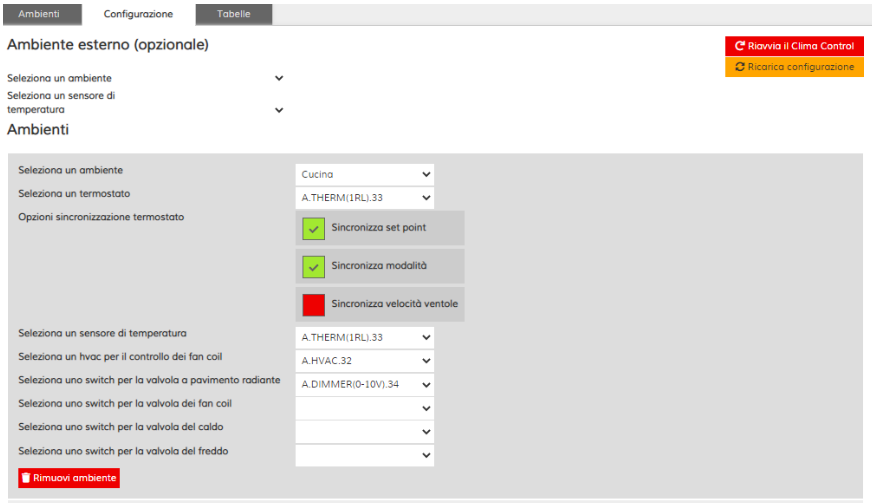
- If configured, it receives an ON command whenever the environment requests cooling (RQ_COOL), OFF when the system requests heating (RQ_HEAT), or when there are no requests (RQ_NONE).

Valve Heating: Device for controlling the opening of the hot water valve.

- If configured, it receives an OFF command whenever the environment requests heating (RQ_HEAT), OFF when the system requests cooling (RQ_COOL), or when there are no requests (RQ_NONE).

Clima Control creates a **virtual thermostat** for each configured environment, allowing the management of a group of Z-Wave devices. The virtual thermostat synchronizes with the physical thermostat, only for the properties defined during configuration.

For example, if the configuration in the image below is chosen: [image not provided]



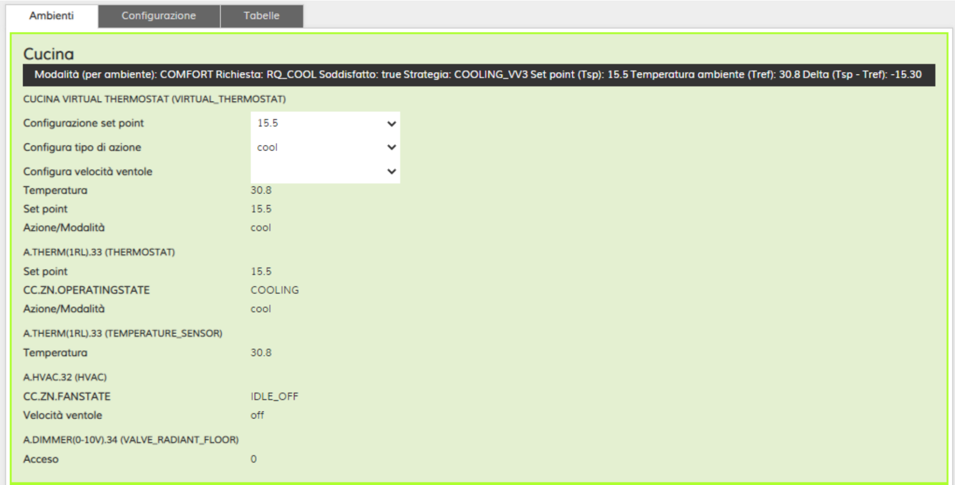
Ambiente esterno (opzionale)

Seleziona un ambiente
Seleziona un sensore di temperatura

Ambienti

Seleziona un ambiente	Cucina
Seleziona un termostato	A.THERM(1RL).33
Opzioni sincronizzazione termostato	☑ Sincronizza set point ☑ Sincronizza modalità 🟥 Sincronizza velocità ventole
Seleziona un sensore di temperatura	A.THERM(1RL).33
Seleziona un hvac per il controllo dei fan coil	A.HVAC.32
Seleziona uno switch per la valvola a pavimento radiante	A.DIMMER(0-10V).34
Seleziona uno switch per la valvola dei fan coil	
Seleziona uno switch per la valvola del caldo	
Seleziona uno switch per la valvola del freddo	

A device named "kitchen virtual_thermostat" will be created, and the "setPoint" and "mode" will be synchronized. The result will be as follows: [image not provided]



Cucina

Modalità (per ambiente): COMFORT Richiesta: RQ_COOL Soddisfatto: true Strategia: COOLING_VV3 Set point (Tsp): 15.5 Temperatura ambiente (Tref): 30.8 Delta (Tsp - Tref): -15.30

CUCINA VIRTUAL THERMOSTAT (VIRTUAL_THERMOSTAT)

Configurazione set point	15.5
Configura tipo di azione	cool
Configura velocità ventole	
Temperatura	30.8
Set point	15.5
Azione/Modalità	cool

A.THERM(1RL).33 (THERMOSTAT)

Set point	15.5
CC.ZN.OPERATINGSTATE	COOLING
Azione/Modalità	cool

A.THERM(1RL).33 (TEMPERATURE_SENSOR)

Temperatura	30.8

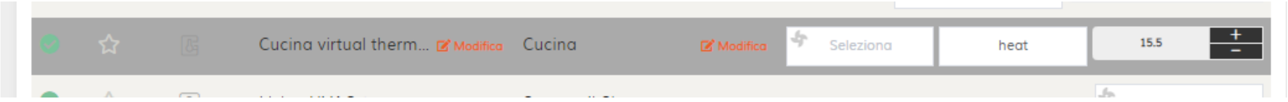
A.HVAC.32 (HVAC)

CC.ZN.FANSTATE	IDLE_OFF
Velocità ventole	off

A.DIMMER(0-10V).34 (VALVE_RADIANT_FLOOR)

Acceso	0

The device will be present in the list of devices with a situation similar to the one shown in the image. [image not provided]



General operation

The Clima Control configuration is logically divided into a "general" part and various "zones."

The general configuration defines:

- The **season** (SUMMER/OTHER), associated with different needs
- The **status of the production system** (APS, Actual Production Mode Per Season).
- **"force commands"** flags to impose that the strategy implementation configuration be resent at each processing loop (about every minute). This allows saving bandwidth in the case of wireless devices (Wi-Fi/Z-wave/ZigBee).
- **Implementation debounce** to introduce a delay in sending implementation commands, to avoid too sudden changes in some devices that might be affected.

Individual zones define:

- Action (or mode) requested by the user (HEAT/COLD/OFF)
- SetPoint (ideal temperature)
- Sensors and actuators

For each zone, the Clima Control verifies the delta between the detected temperature and the Setpoint temperature. Based on this value, it proceeds to implement various devices associated with different roles to achieve the climatic comfort situation as quickly as possible.

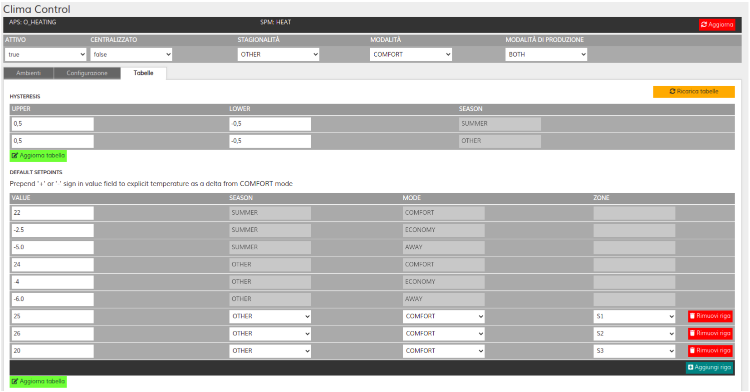
The Clima Control keeps track of requests in individual zones and allows the various zones to "communicate" with each other: with each change in request from one zone, the system informs all others and recalculates the best management **mode for the current configuration** (SPM, Suggested Production Mode).

Example: The central system is producing hot and cold water, but all zones only require heating. The SPM variable will highlight that for the current state, it is technically possible to switch to producing only hot water.

Advance Configuration

Through the "Tables" tab, it is possible to make advanced customizations regarding the hysteresis values associated with the thermostat and the default ideal temperatures.

NOTE: In any case, the system, during operation, proceeds to synchronize the ideal temperatures (for each zone, for each operating mode) based on user choices.



Clima Control

APS: O_HEATING

SPM: HEAT

ATTIVO	CENTRALIZZATO	STAGIONALITÀ	MODALITÀ	MODALITÀ DI PRODUZIONE
true	false	OTHER	COMFORT	BOTH

HYSTERESIS

UPPER	LOWER	SEASON
0,5	-0,5	SUMMER
0,5	-0,5	OTHER

DEFAULT SETPOINTS

Prepend '+' or '-' sign in value field to explicit temperature as a delta from COMFORT mode

VALUE	SEASON	MODE	ZONE
22	SUMMER	COMFORT	
-2.5	SUMMER	ECONOMY	
-5.0	SUMMER	AWAY	
24	OTHER	COMFORT	
-4	OTHER	ECONOMY	
-6.0	OTHER	AWAY	
25	OTHER	COMFORT	S1
26	OTHER	COMFORT	S2
20	OTHER	COMFORT	S3

Configuration Exemple

As stated in the initial chapter, the configuration recommended by Vitrum Design envisages that each UFO has a subset of devices DIRECTLY controlled, to which it will link one or more environments/zones (as seen in the image above).

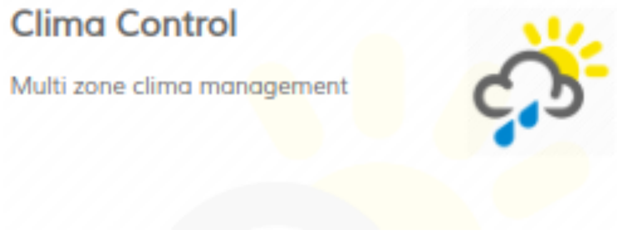
Each UFO in the federation will DIRECTLY manage only its environments/zones and related devices, and INDIRECTLY manage environments/zones/devices of other UFOs.

For this example, let's assume a building containing three environments S1, S2, and S3.

For each of these environments, let's assume that the inclusions and configurations described earlier have already been performed.

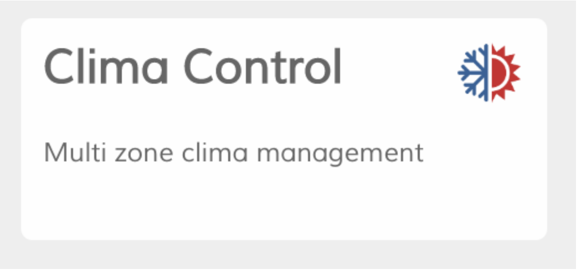
NOTE: Depending on the type of thermostat and HVAC used, the display may appear different.

Click on Apps in the side menu and select Clima Control.



Clima Control

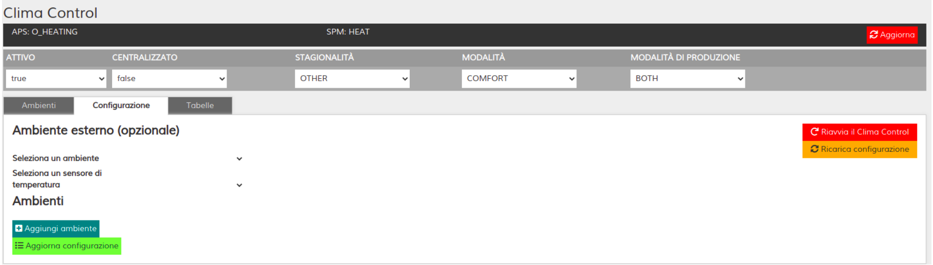
Multi zone clima management



Clima Control

Multi zone clima management

Then go to the “Configuration” tab



Clima Control

APS: O_HEATING   SPM: HEAT

ATTIVO	CENTRALIZZATO	STAGIONALITÀ	MODALITÀ	MODALITÀ DI PRODUZIONE
true	false	OTHER	COMFORT	BOTH

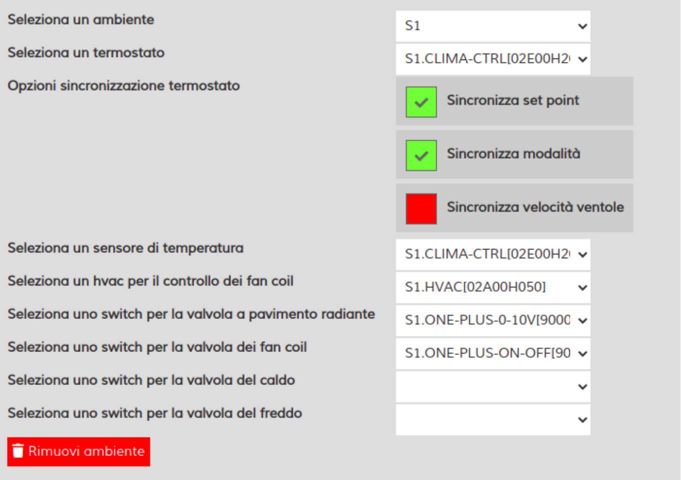
Ambiente esterno (opzionale)

Seleziona un ambiente

Seleziona un sensore di temperatura

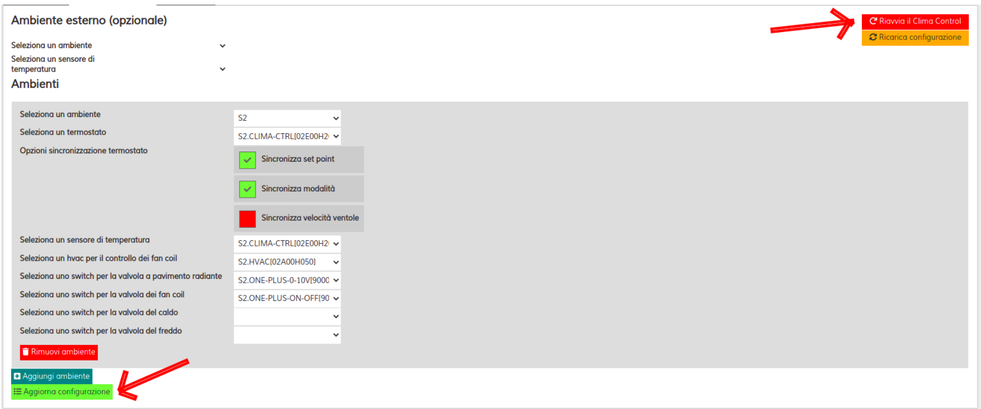
Ambienti

and carry out the configuration of the different zones.



Seleziona un ambiente	S1
Seleziona un termostato	S1.CLIMA-CTRL[02E00H2(
Opzioni sincronizzazione termostato	✓ Sincronizza set point ✓ Sincronizza modalità 🟥 Sincronizza velocità ventole
Seleziona un sensore di temperatura	S1.CLIMA-CTRL[02E00H2(
Seleziona un hvac per il controllo dei fan coil	S1.HVAC[02A00H050]
Seleziona uno switch per la valvola a pavimento radiante	S1.ONE-PLUS-0-10V[9000
Seleziona uno switch per la valvola dei fan coil	S1.ONE-PLUS-ON-OFF[90
Seleziona uno switch per la valvola del caldo	
Seleziona uno switch per la valvola del freddo	

Once finished, click on the "Update Configuration" button and then on the "Restart Clima Control" button in the same tab.



Ambiente esterno (opzionale)

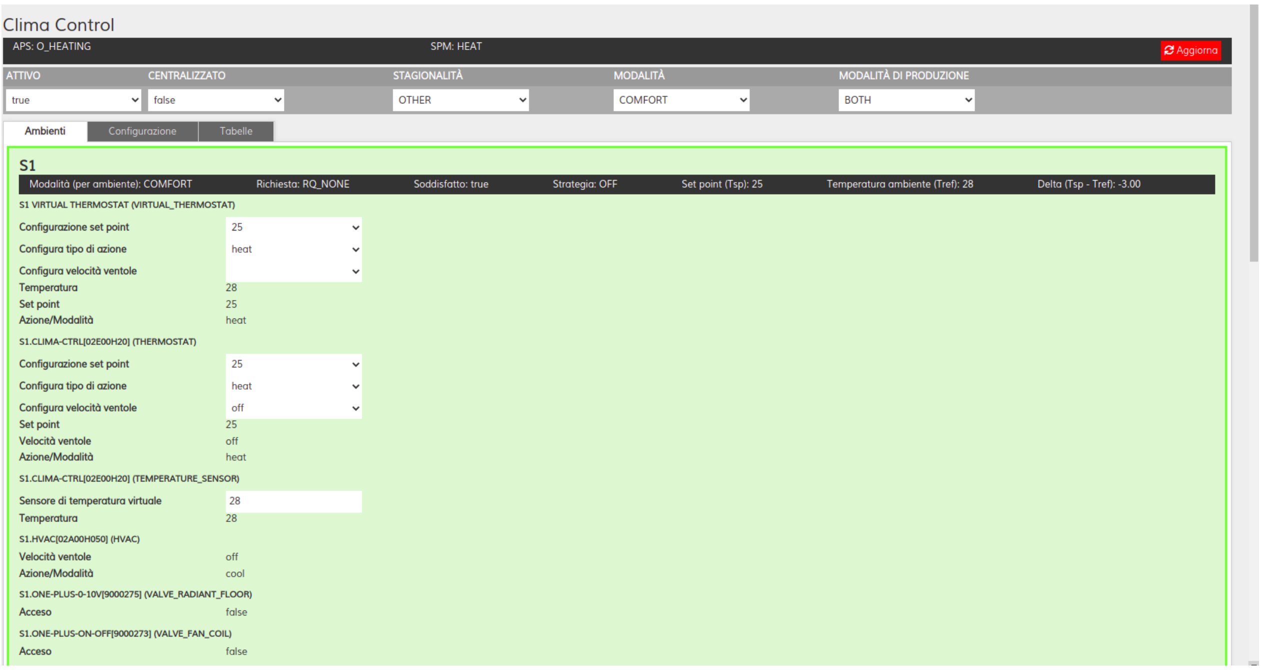
Seleziona un ambiente

Seleziona un sensore di temperatura

Ambienti

Seleziona un ambiente	S2
Seleziona un termostato	S2.CLIMA-CTRL[02E00H2
Opzioni sincronizzazione termostato	✓ Sincronizza set point ✓ Sincronizza modalità 🟥 Sincronizza velocità ventole
Seleziona un sensore di temperatura	S2.CLIMA-CTRL[02E00H2
Seleziona un hvac per il controllo dei fan coil	S2.HVAC[02A00H050]
Seleziona uno switch per la valvola a pavimento radiante	S2.ONE-PLUS-0-10V[9000
Seleziona uno switch per la valvola dei fan coil	S2.ONE-PLUS-ON-OFF[90
Seleziona uno switch per la valvola del caldo	
Seleziona uno switch per la valvola del freddo	

Once the loading is complete, the "Environments" tab of the Clima Control should therefore present a list of boxes for each environment.



Clima Control

APS: O_HEATING SPM: HEAT

ATTIVO	CENTRALIZZATO	STAGIONALITÀ	MODALITÀ	MODALITÀ DI PRODUZIONE
true	false	OTHER	COMFORT	BOTH

S1

Modalità (per ambiente): COMFORT Richiesta: RQ_NONE Soddisfatto: true Strategia: OFF Set point (Tsp): 25 Temperatura ambiente (Tref): 28 Delta (Tsp - Tref): -3.00

S1 VIRTUAL THERMOSTAT (VIRTUAL_THERMOSTAT)

Configurazione set point	25
Configura tipo di azione	heat
Configura velocità ventole	
Temperatura	28
Set point	25
Azione/Modalità	heat

S1.CLIMA-CTRL[02E00H20] (THERMOSTAT)

Configurazione set point	25
Configura tipo di azione	heat
Configura velocità ventole	off
Set point	25
Velocità ventole	off
Azione/Modalità	heat

S1.CLIMA-CTRL[02E00H20] (TEMPERATURE_SENSOR)

Sensore di temperatura virtuale	28
Temperatura	28

S1.HVAC[02A00H050] (HVAC)

Velocità ventole	off
Azione/Modalità	cool

S1.ONE-PLUS-0-10V[9000275] (VALVE_RADIANT_FLOOR)

Acceso	false

S1.ONE-PLUS-ON-OFF[9000273] (VALVE_FAN_COIL)

Acceso	false

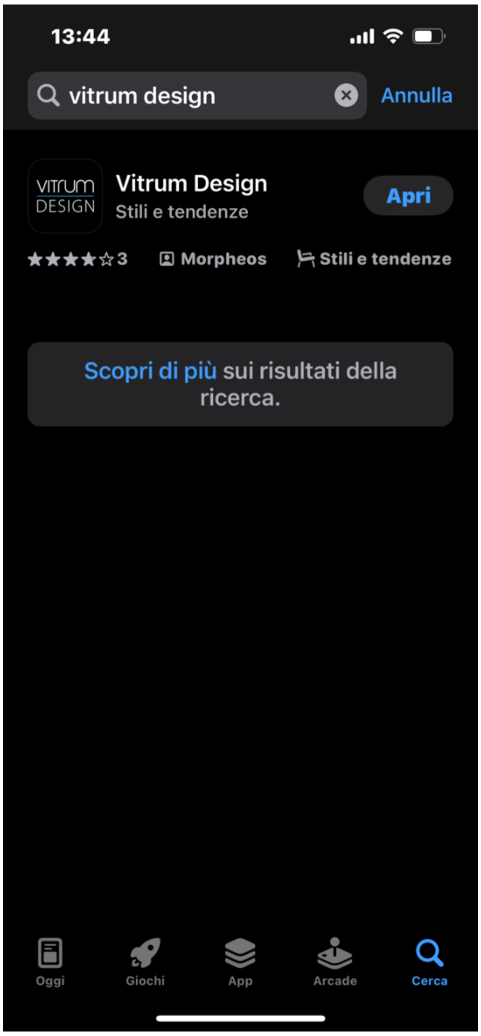
Voice assistant management (Amazon Alexa and Google Home)

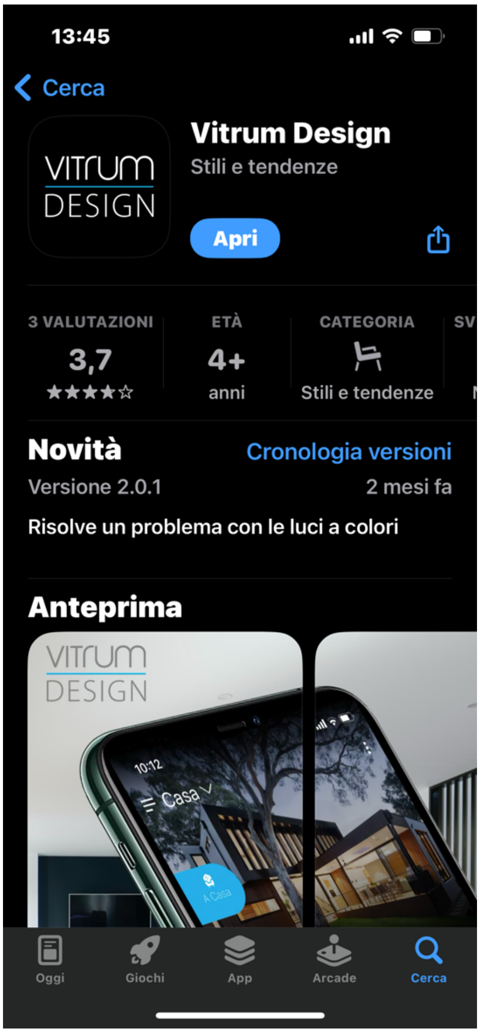
Amazon Alexa voice assistants are supported through the appropriate published **Skill**, and similarly, the **Action** is provided for integration with **Google Home**.

NOTE: Not all categories supported by UFO are available on voice assistants (for example, many sensor-type devices or some actuators like those in the push category), and conversely, some categories managed by these products (such as cars or certain specific appliances) currently do not have a correspondence with the UFO system. Refer to the specific integration document for more details.

Amazon Alexa

1. Open the Amazon Alexa app and go to the "More" page, then select "Skills & Games."
2. Select the magnifying glass search icon located in the top right corner.
3. In the search field, type the name of the skill you want to install ("UFO" or "Vitrum Design"). Select the found skill.





4. On the skill detail page, press the "ENABLE SKILL" button to enable it. If the "DISABLE SKILL" option is available, it means the skill has already been enabled, and you can choose to disable it.

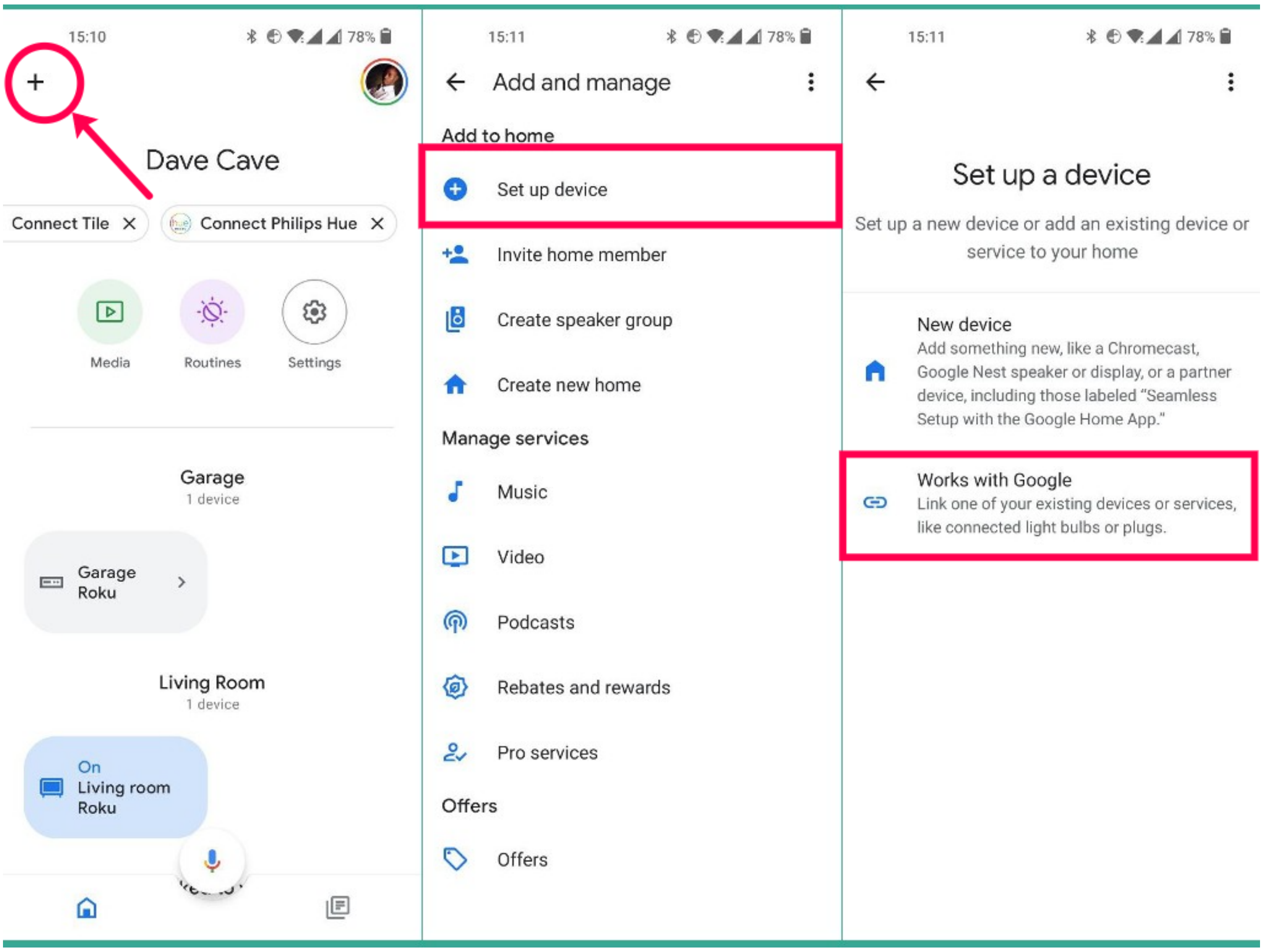
5. You will be redirected to the Vitrum Design login screen, and after a moment, the new devices will be available through Amazon Alexa.

NOTE: For details regarding the implementation of different categories of devices, refer to the specific documentation. Si verrà ridirezionati alla maschera di login Vitrum Design, e dopo qualche istante i nuovi dispositivi saranno disponibili attraverso Amazon Alexa

Google Home

1. Open the Google Home app, click on the "+" button at the top left, and select "Set up device."
2. On the "Set up a device" page, select "Works with Google."
3. In the new "Home control" page, click on the magnifying glass search button and search for the desired action "Vitrum Design" or "UFO."
4. You will be redirected to the Vitrum Design login screen, and after a moment, the new devices will be available through Google Home.

NOTE: For details regarding the implementation of different categories of devices, refer to the specific documentation.



Offine management

"Offline mode" allows the use of UFO even in contexts without connectivity by disabling the internal verification of user credentials and enabling direct use of UFO through the direct connection of a smartphone, tablet, or PC to the provided Access Point.

NOTE: This mode must be enabled by Vitrum Design personnel.

NOTE: Currently, the only client that allows offline connections is the appropriately configured Vitrum app. For further details on operation, refer to the specific user manual.

IFTTT

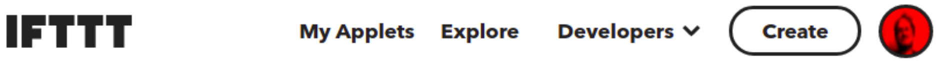
IFTTT is a web service that allows the creation of chains of conditions called applets. In the current free plan, it's possible to use up to 5 applets, and there is also a paid plan available.

An applet can be triggered by external services, including Gmail, Facebook, Instagram, and others. For instance, it can send an email when the user uses a specific hashtag in a tweet or send a copy of a Facebook photo to an archive when the user is tagged.

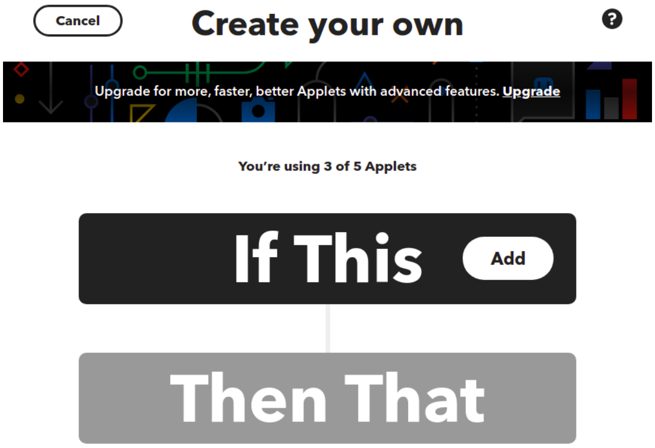
Integration with UFO utilizes the **Maker** applet, enabling the sending of events from UFO to IFTTT via webhook (calling a specific URL) or executing commands on UFO using the specific product's public address.

UFO → IFTTT integration example

After registering and logging into the IFTTT portal (https://ifttt.com/) click on the "Create" button in the top right corner



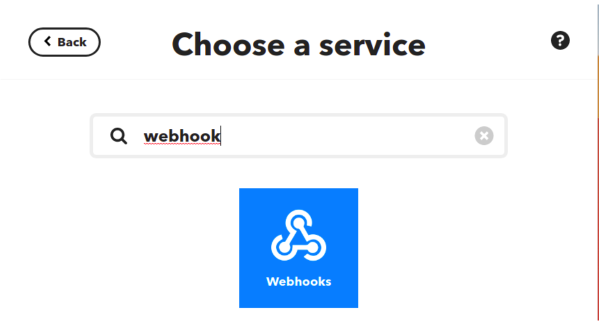
In the “If This” section, click on the “Add” button to add an applet.



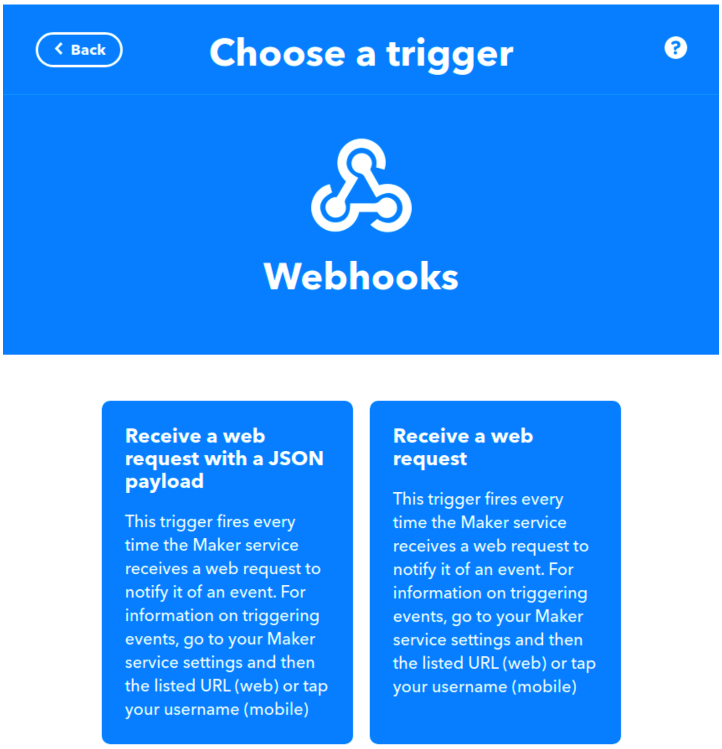
Upgrade for more, faster, better Applets with advanced features. Upgrade

You’re using 3 of 5 Applets

In the service selection box, select “Wehooks”



and on the next page select “Receive a web request”



Receive a web request with a JSON payload

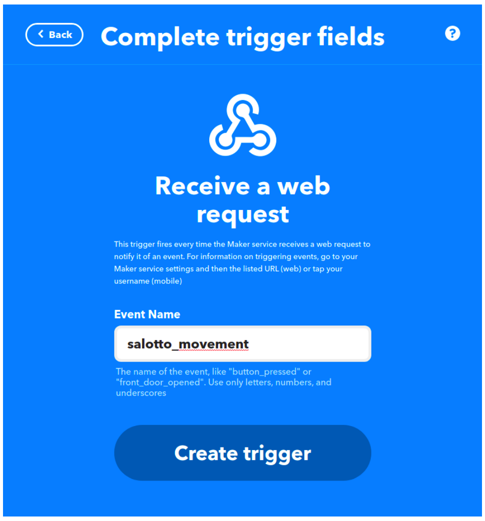
This trigger fires every time the Maker service receives a web request to notify it of an event. For information on triggering events, go to your Maker service settings and then the listed URL (web) or tap your username (mobile)

Receive a web request

This trigger fires every time the Maker service receives a web request to notify it of an event. For information on triggering events, go to your Maker service settings and then the listed URL (web) or tap your username (mobile)

NOTE: Actions with JSON payloads are not currently supported.

In the “Event Name” box, enter a valid string, for example “salotto_movement” and click on the “Create trigger” button.



Receive a web request

This trigger fires every time the Maker service receives a web request to notify it of an event. For information on triggering events, go to your Maker service settings and then the listed URL (web) or tap your username (mobile)

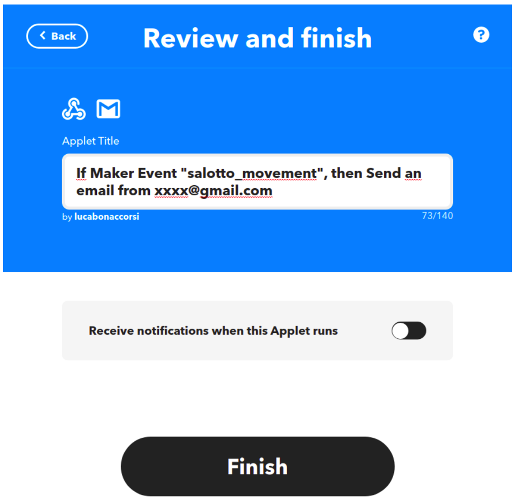
Event Name: salotto_movement

The name of the event, like "button_pressed" or "front_door_opened". Use only letters, numbers, and underscores

Back on the main page of the applet, click the "Add" button in the "Then That" box and select an "action" to perform in response to the action defined in the previous step, for example, Gmail to send an email.

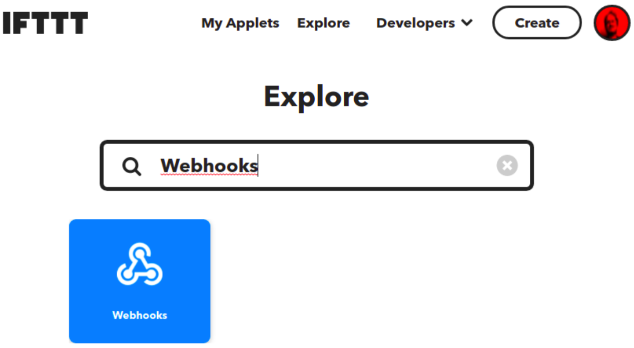
NOTE: IFTTT offers a wide range of actions with external services but also allows integration with a specific device through the integrated mobile app. For example, you can send push notifications, mute the phone, or play a music track.

Once the action is configured, click the "Continue" button, give a title to the newly created applet, and click the "Finish" button.



If Maker Event "salotto_movement", then Send an email from xxxx@gmail.com

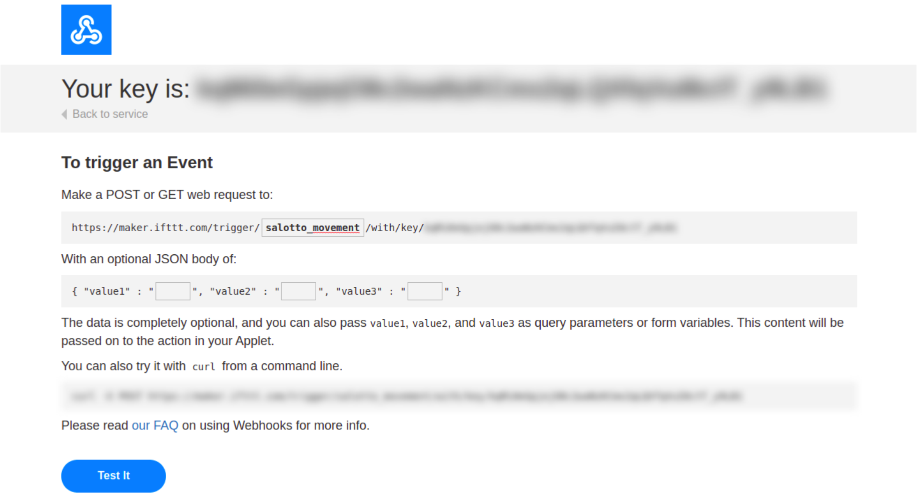
At this point, it is necessary to retrieve the URL to be entered in UFO to allow it to notify the IFTTT service of the event. Return to the main page, click the "Explore" button, and search for "Webhooks."



Select the service and click the "Documentation" button; a second browser page will open showing the data generated for the service. To generate the URL, enter the string created in the previous step, namely "salotto_movement," in the "event_name" box. The URL to be used will be generated.

You can use the "Test It" button to verify that the action is performed.

NOTE: Actions with JSON payloads are not currently supported.



Your key is: [redacted]

To trigger an Event

Make a POST or GET web request to:

```
https://maker.ifttt.com/trigger/salotto_movement/with/key/[redacted]
```

With an optional JSON body of:

```
{ "value1" : "", "value2" : "", "value3" : "" }
```

The data is completely optional, and you can also pass `value1`, `value2`, and `value3` as query parameters or form variables. This content will be passed on to the action in your Applet.

You can also try it with `curl` from a command line.

[redacted]

Please read our FAQ on using Webhooks for more info.

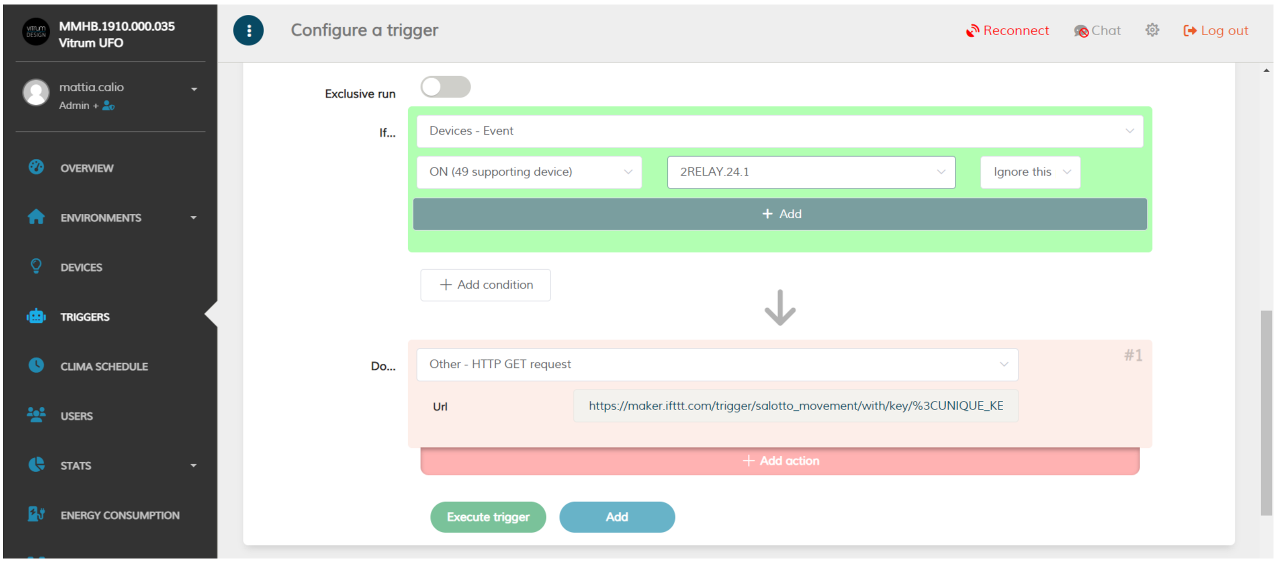
Then copy the generated URL which should look like this

```
https://maker.ifttt.com/trigger/salotto_movement/with/key/<UNIQUE_KEY>
```

and open UFO dashboard.

Create an automation and select the condition you want the IFTTT Webhook service to query for. In this example we will pair a Philips Hue motion sensor.

In the “Do…” section, enter the URL generated in the previous step and click on “Add”.



Exclusive run

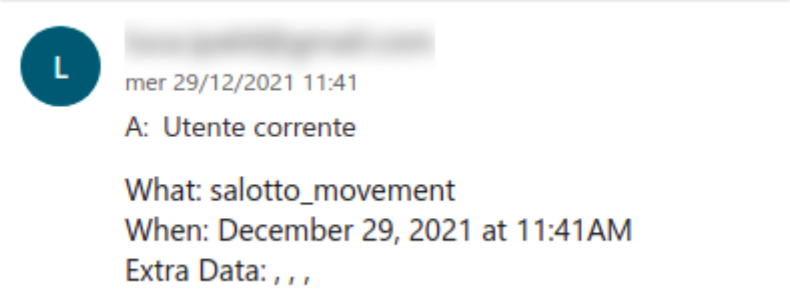
If... Devices - Event

ON (49 supporting device) | 2RELAY.24.1 | Ignore this

Do... Other - HTTP GET request

Url https://maker.ifttt.com/trigger/salotto_movement/with/key/%3CUNIQUE_KE

Test the automation using the "Run Trigger" button; if everything is configured correctly, the configured action should be executed within about ten seconds. In our example, you will receive an email at the configured address.



L [redacted]

mer 29/12/2021 11:41

A: Utente corrente

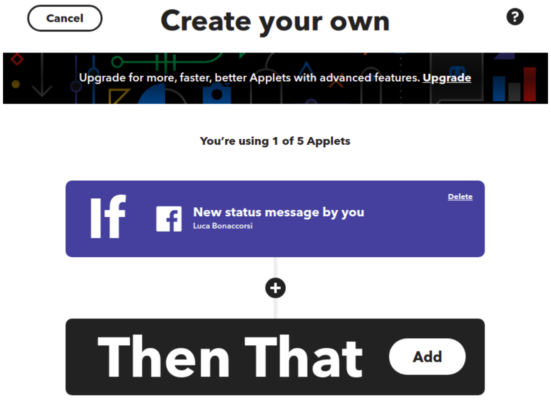
What: salotto_movement
When: December 29, 2021 at 11:41AM
Extra Data: , , ,

IFTTT → UFO integration example

After registering and logging in to the IFTTT portal (https://ifttt.com/), click on the "Create" button at the top right.

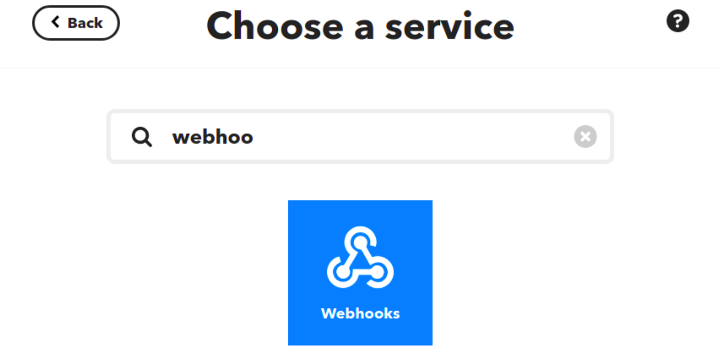
Select an applet to connect to an external service: in the example, we will create a rule to turn on a light bulb (through UFO) whenever we update our status on Facebook.

After configuring the "If" section, proceed to link the UFO action. From the applet creation page, click on the "Add" button in the "Then That" section.

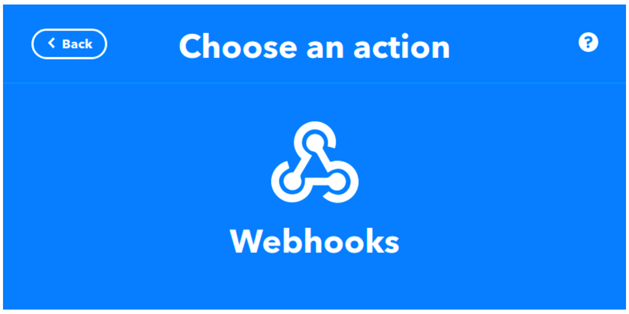


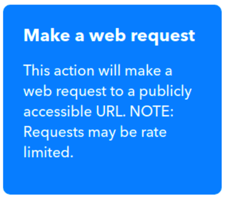
Cancel
Create your own
Upgrade for more, faster, better Applets with advanced features. Upgrade
You're using 1 of 5 Applets
If
New status message by you
Luca Bonaccorsi
Delete
Then That
Add

On the service selection page we select "Webhooks"



and than "Make a web request"

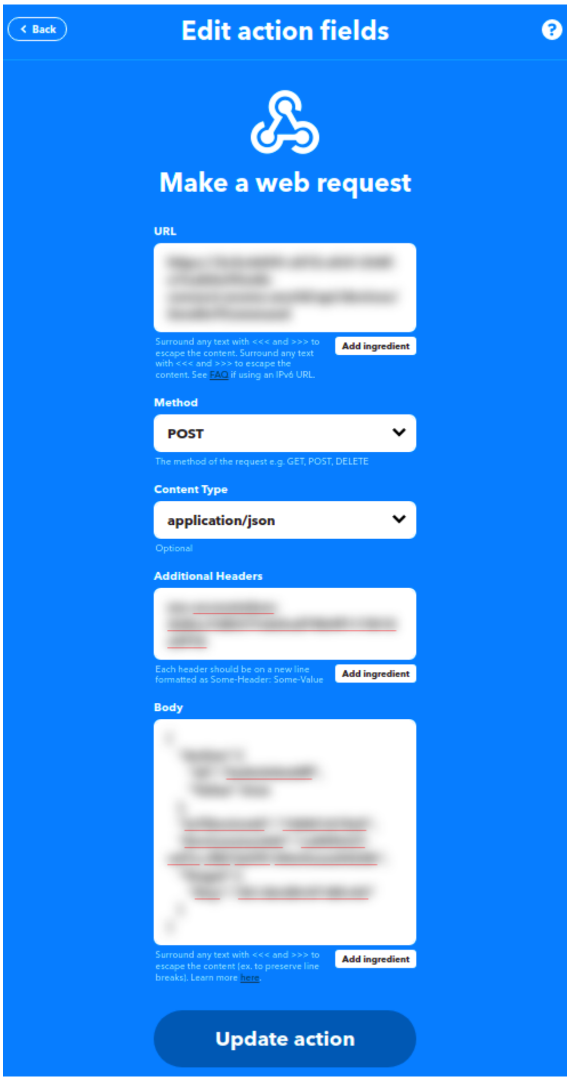




Make a web request

This action will make a web request to a publicly accessible URL. NOTE: Requests may be rate limited.

At this point, it is necessary to compose the HTTP request to be executed on UFO; refer to the integration/developer manual for details on available commands. In our example, we will execute a command to turn on a specific device; thus, we will make a request with the following characteristics:



Edit action fields

Make a web request

URL

[redacted]

Surround any text with <<< and >>> to escape the content. Surround any text with <<< and >>> to escape the content. See FAQ if using an IPv6 URL.

Method

POST

The method of the request e.g. GET, POST, DELETE

Content Type

application/json

Optional

Additional Headers

[redacted]

Each header should be on a new line formatted as Some-Header: Some-Value

Body

[redacted]

Surround any text with <<< and >>> to escape the content (ex. to preserve line breaks). Learn more here.

URL[1]	**https://*<UFO _ID>*-connect.UFO .world/api/devices/SendIoTCommand**
Method	**POST**
Content Type	**application/json**
Additional Headers[2]	**mo-accesstoken: *<YOUR_TOKEN>***

Body[3]	{
	"Action":{ "Id":<ACTION_ID>, "Value":<ACTION_VALUE> },
	"EnvironmentId":<ENVIRONMENT_ID>,
	"Target":{ "Key":<DEVICE_KEY> }
	}

- Modify <UFO_ID> with the UFO's ID to which you want to send the request.
- Replace <YOUR_TOKEN> with your user token.

NOTE: For privacy reasons, the user token has a limited duration (currently 3 months), so it will be necessary to update the rule upon expiration.

NOTE: Refer to the developer/integrator guide for retrieving your user token.

- Replace <ACTION_ID>, <ACTION_VALUE>, <ENVIRONMENT_ID>, and <DEVICE_KEY> with the correct values.

NOTE: For details on available fields, refer to the developer/integrator guide.

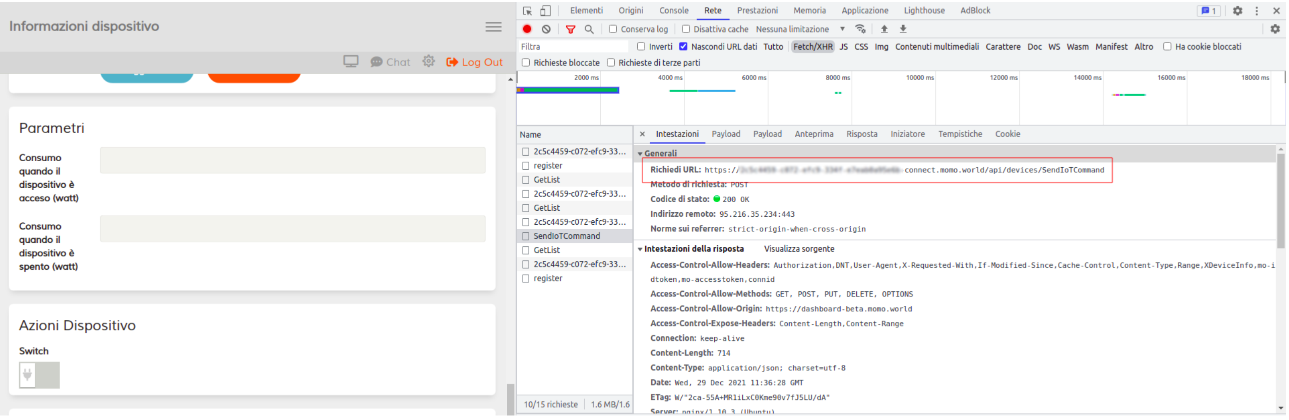
Obtain request data from Google Chrome

It is possible to obtain the data mentioned in the previous paragraph by analyzing the network flow in Google Chrome.

Open the dashboard and before executing the command, open the "Developer Tools" tab using the F12 key (or CTRL+SHIFT+J or CMD+SHIFT+F12).

Open the "Network" tab and select the filter for "Fetch/XHR" requests.

Send the action you want to analyze (for example, in the case of an action on a device, a line like "SendIoTCommand" will appear), and by clicking on it, a box with additional detail tabs will open.



2c5c4459-c072-efc9-33…
register
GetList
2c5c4459-c072-efc9-33…
GetList
2c5c4459-c072-efc9-33…
SendIoTCommand
GetList
2c5c4459-c072-efc9-33…
register

Generali

Richiedi URL: https://[redacted]connect.momo.world/api/devices/SendIoTCommand
Metodo di richiesta: POST
Codice di stato: ● 200 OK
Indirizzo remoto: 95.216.35.234:443
Norme sui referrer: strict-origin-when-cross-origin

Intestazioni della risposta   Visualizza sorgente

Access-Control-Allow-Headers: Authorization,DNT,User-Agent,X-Requested-With,If-Modified-Since,Cache-Control,Content-Type,Range,XDeviceInfo,mo-idtoken,mo-accesstoken,connid
Access-Control-Allow-Methods: GET, POST, PUT, DELETE, OPTIONS
Access-Control-Allow-Origin: https://dashboard-beta.momo.world
Access-Control-Expose-Headers: Content-Length,Content-Range
Connection: keep-alive
Content-Length: 714
Content-Type: application/json; charset=utf-8
Date: Wed, 29 Dec 2021 11:36:28 GMT
ETag: W/"2ca-55A+MR1iLxC0Kme90v7fJ5LU/dA"
Server: nginx/1.10.3 (Ubuntu)

From the "Headers" tab, you can retrieve the product URL from the "Request URL" field.

while further down on the same tab, in the "Request Headers" section, you can retrieve the header related to the "mo-accesstoken" field containing the token to use in the requests (you can ignore all other headers, including "mo-idtoken").

Finally, from the "Payload" tab, you can view the JSON-formatted request corresponding to the executed action.

NOTE: In the case of switches, lights, or generic devices with On and Off commands, if you simply want to perform a "toggle" (i.e., a switch between on and off), you can replace the *OnOff action with *Toggle (for example, SwitchOnOff with SwitchToggle, or LightOnOff with LightToggle) and set the "Value" field to "undefined."

OPTIMIZATIONS

Reduction of implementation and automation execution latency

One of the possible causes of latency in executing actions (e.g., turning on lights) or automation execution is excessive Z-Wave data traffic. To reduce this latency, you can minimize Z-Wave traffic through these strategies:

- Disable the periodic consumption report (or similar) in the device configuration through the appropriate field in the template (refer to the device manual, e.g., Qubino, Fibaro, etc.).
- In the case of keypads with all satellites and no associated automations, remove the controller (node 1 or endpoint 1.0) from Group 1 (Lifeline) using the "Multi-Channel Association -> Remove" command.
- In the case of multiple actions from multiple satellites to the same load, link each satellite to the load first and then establish links between the satellites.

VEMER TERMOSTAT

Installation of Vemer WiFi Dafne or Asso thermostat

To install a Vemer WiFi thermostat (Dafne or Asso) in the UFO home automation network, follow these steps:

1. Install the Clima WiFi Vemer mobile app and register through the app following the guide on page 16: https://www.vemer.it/static/upload/is_/0000/is_ve792200_it_1.pdf.

1) Connect the thermostat to WiFi following the guide on pages 17, 18, 19: https://www.vemer.it/static/upload/is_/0000/is_ve792200_it_1.pdf.

2. After connecting the thermostat to WiFi, from the dashboard, select Devices, click on Manual Configuration at the top, choose External Service -> Vemer, enter a name to identify the connection between UFO and Vemer thermostats, and click "Add Device." On the Vemer page that opens, enter the Username and Password used to register on the Clima Vemer app and click update.
3. After a few minutes, the Vemer thermostat will appear in the list of devices and can be placed in the desired environment.

VITRUM DEVICES 1

Configuration, links and automation

Unlike Vitrum series 2 devices, where device configuration is done by applying the template, the configuration of Vitrum series 1 devices is performed by physically interacting with the devices, pressing a particular combination of buttons that allows entering the configuration mode as described in the device manual. In any case, applying the template is necessary to let UFO understand the type of device.

As for links and automations, these are created in the same way as for Vitrum series 2 devices. The only Vitrum series 1 device that deserves specific treatment is the "Master Off" device. This device allows turning off all devices that were chronologically included later and, therefore, have a lower Node ID.