ZIPABOX 2

Z-Wave™ User Manual

All in One Home Controller

Contents

Overview

Zipabox2 is a Security Enabled Plus central static controller. It is used for managing a Z-Wave™ devices within its network. This includes device inclusion/exclusion, controlling devices, firmware updates and more. The Zipabox can also handle other protocols if the corresponding modules for them are installed. For the sake of simplicity this guide will only go through Z-Wave™ as it requires no additional modules to function and works out of the box.

This product can be operated in any Z-Wave™ network with other Z-Wave™ certified devices from other manufacturers. All mains operated nodes within the network will act as repeaters regardless of the vendor to increase reliability of the network.

This document will describe how to use the Zipato Web user interface (Web UI) with Zipabox. The Web UI allows users to send commands to devices connected to their Zipabox and manage their network.

The web UI is located on the following address: https://my3.zipato.com/zipato-web/app2dashboard

Image 1 Login screen

If an account already exists it is possible to login using its email address and password. It is also possible to register a new account. To create a new account the “SIGN UP!” option must be used. After logging the following screen will be shown:

Image 2 Start screen

Setting up the Zipabox

To be able to connect to the Zipabox it first needs to be set up. To set up a Zipabox follow these steps:

- Attach the antenna to the top of the controller. The antenna will be provided in the packaging
- Attach additional modules to the box (OPTIONAL, Zipabox comes with a Z-Wave™ module installed, other modules need to be purchased separately)
- Connect the Zipabox to your home network via Ethernet
- Connect the Zipabox to its power supply (an adapter will be provided in the packaging)
- The light on the Zipabox should turn on now, if the light is not glowing something is wrong with the power supply

The light on the Zipabox tells the user of its current status:

- Stable red – online but the controller software is not running, if this persists restart the controller by holding “Button 2” for 5 seconds.
- Blue – Zipabox is booting, wait until it is booted.
- Blinking green – Zipabox is booted and controller software is running but there is no connection to the cloud. If this persists check the Ethernet connection.
- Stable green – Zipabox is booted and ready to use.

At any time the Zipabox can be reset by holding “Button 2” for 5 seconds.

If the light is stable green the Zipabox is ready for use. Now it is possible to add it to your system in the Web UI or control it if it is already added.

The Web UI can be found on the following link: https://my3.zipato.com/zipato-web/app2dashboard

Selecting a system

To be able to send commands to a Zipabox the user will need to select a system or create a new one. To enter the system selection screen the “zipato” button in the top left corner should be pressed. This will open the list of existing systems and give the option to create a new one. To select a system simply click on its name:

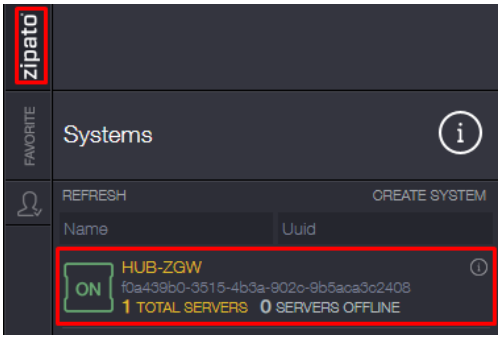

Image 3 Selecting a system

Each system consists of one or more servers. Server are controllers like the Zipabox. Each server supports the simultaneous use of multiple protocols. But for the sake of simplicity this guide will only cover the Z-Wave™ network.

Every system is marked as either “ON” or “OFF”. If a system is “ON” that means its main controller is online, if the system is marked as “OFF” that means its main controller is not online. A system can have only one main controller. By default the first controller added to the network will be marked as its main controller.

To create a new system the “CREATE SYSTEM” option should be selected:

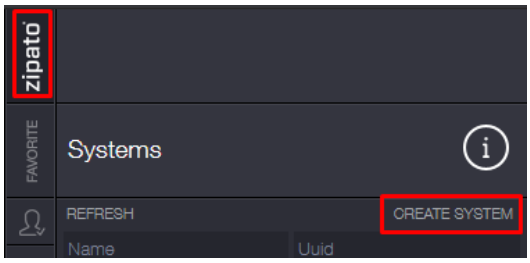

Image 4 System creation

Afterwards the system name and time zone will need to be entered. When the name and time zone have been entered the system can be created by pressing the “Save” button:

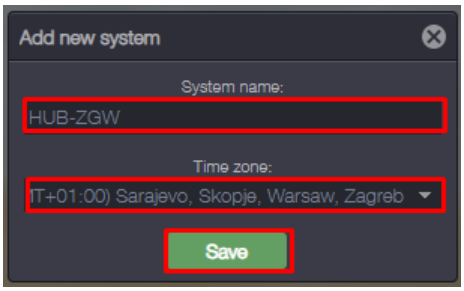

Image 5 System creation

The created system should now be selectable in the system list.

System main menu

When a system is selected the following screen will be shown:

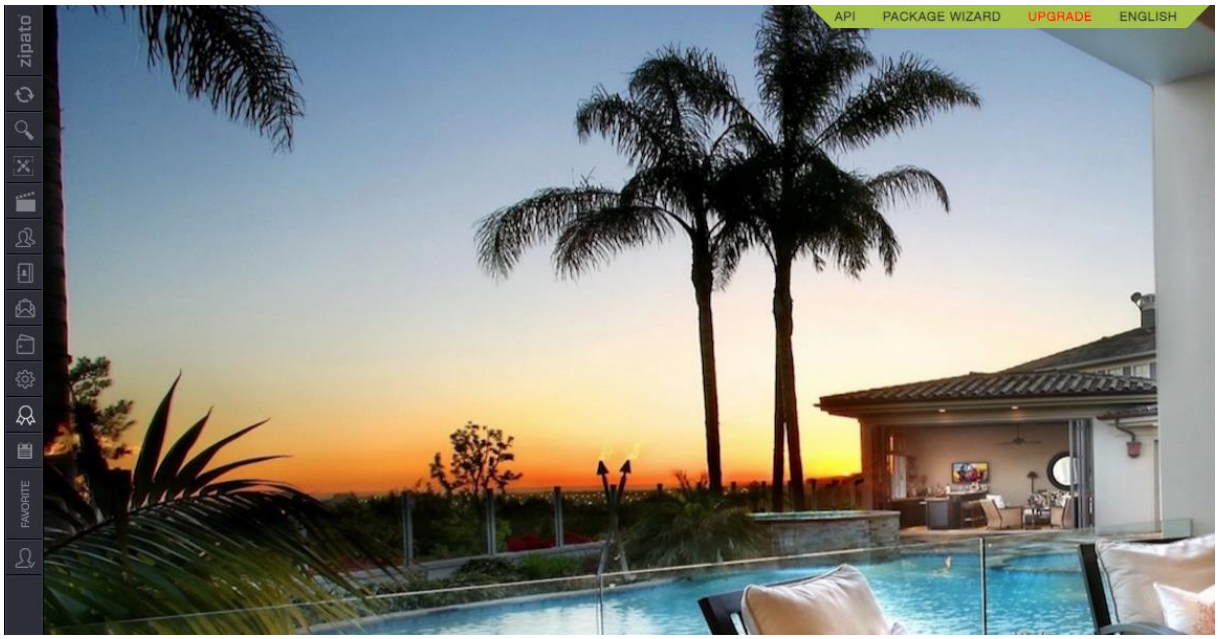

Image 6 Main menu

The left side of the screen contains all buttons used for controlling the system. Everything from controlling devices to controlling networks used by its controllers. The buttons related to network management will be explained in the following chapters. The “zipato” button will bring up the system selection tab if switching systems is necessary.

The “Synchronize” button synchronizes the systems controller with the cloud. Some actions require a synchronize action to be communicated with the controller. But for the sake of this guide it will not be necessary to use it. However, it is still a recommended to press it after booting a Zipabox. If the sync action returns a success that means that the Zipabox is up and ready to use.

Image 7 Synchronize button

Device manager – network management

Introduction

The device manager contains the list of all controllers in that system. It also shows the list of networks of each controller and device connected to those networks. Through this screen it is possible to add/remove devices, manage networks and see some basic information about the current system.

Image 8 Network manager

The image above shows the HUB-ZGW system device manager. One controller "ZB071F3F09F1CBB33C" is currently the master server of the system, and it is the only controller in the system. The controllers name by default will be its serial number. If this list does not contain any controllers it is possible to add a new one by picking the "ADD SERVER" option:

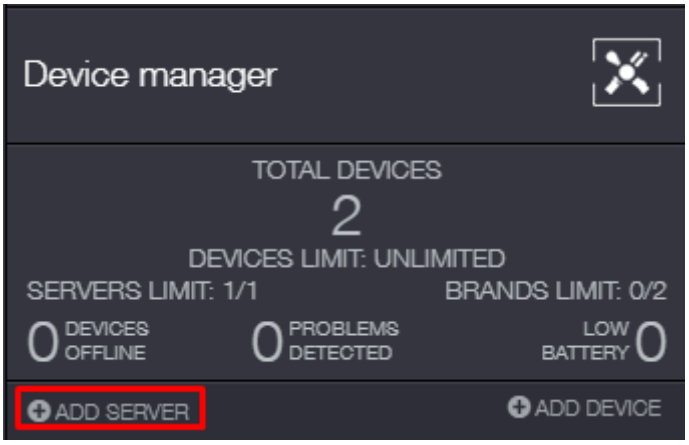

Image 9 Add server option

Afterwards a new window will pop up asking for a controller serial number. After entering the serial number the controller should be added to the system. If the controller was not added after the serial number was inputted it could be due to following reasons:

- Wrong serial number was inputted
- That controller is already added in another system

The device manager contains information about how many devices were added to the system, how many of them are currently offline or not responding. There is also information about how many

battery devices in the network are low on battery. It also contains the list off all controllers added to this system. In the image above (Image 8) the system has only one controller. Below each controller there is a list of its networks. Clicking on the network expands a list that shows all the devices added to that network. Some networks, such as Z-Wave™, have extra network management options that can be accessed through the cogwheel icon right of their name. These extra options will be explained later in the network management section.

There are also extra options for controllers such as settings and firmware updates that can be accessed through the cogwheel icon to the right of its name:

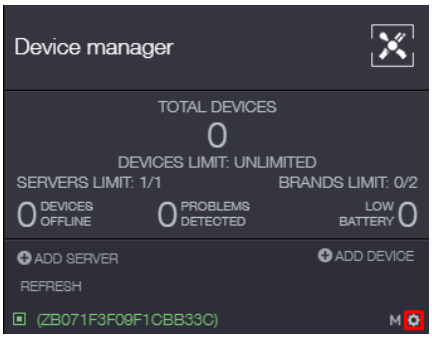

Image 10 Opening controller settings

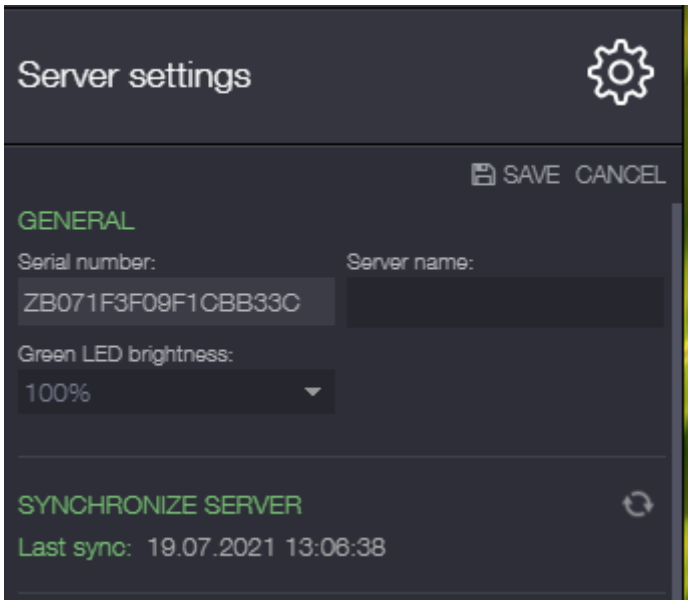

Image 11 Controller settings

The image above shows some of the controller settings, these settings can be used to get the serial number of your controller, change the server name and check when the last synchronize action was performed. Other options that you can find below are static IP options, backup options, firmware options and a reboot option. Reboot can also be performed by clicking and holding “Button 2” for 5 seconds.

Device add operation (Inclusion)

To add another device to the network you will need to select the “ADD DEVICE” option:

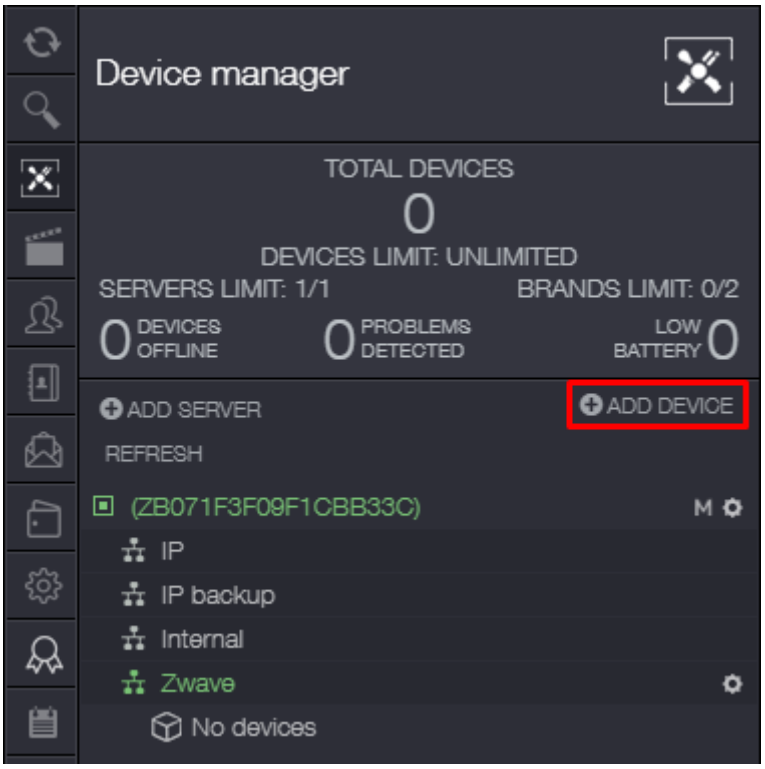

Image 12 Add device option

Afterwards a new window will pop up asking the user to choose which network the device will connect to. The network chosen network MUST be of the same type as the network the device is using. In this case a Z-Wave™ device will be added so the appropriate network (Z-Wave™) will be selected:

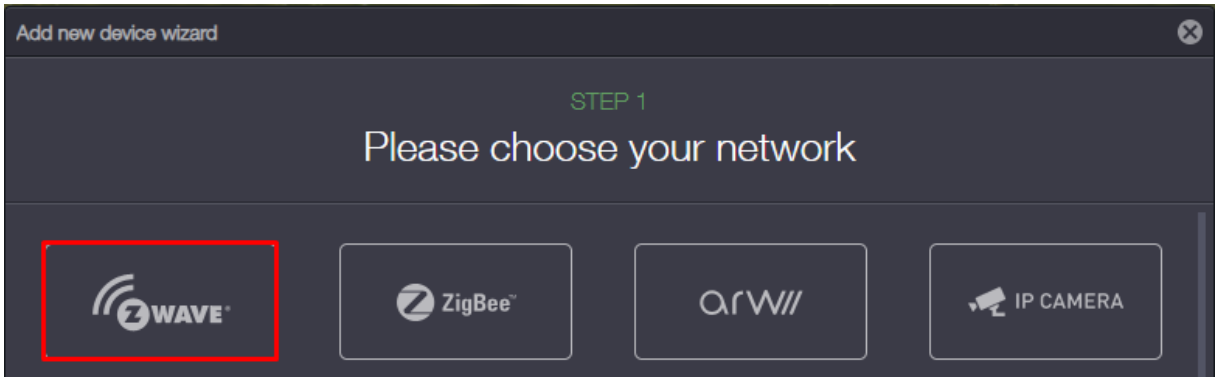

Image 13 Z-Wave™ network selection

After choosing the network a countdown will start letting the user know that the controller has entered exclusion mode:

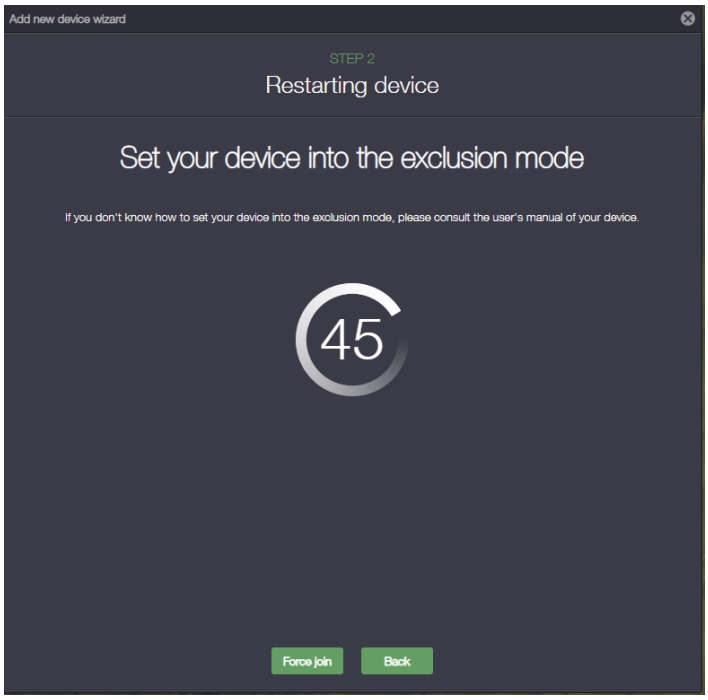

Image 14 Exclusion

It is recommended to follow the instructions on screen, but it is possible to skip the exclusion step using the “Force join” option. If “Force join” option is selected the controller will NOT exclude the device and will go into inclusion mode. If the window is closed or the “Back” button is pressed the node add process will stop and no device will be added to the network. When the device is excluded or the “Force join” option is selected the controller will start inclusion.

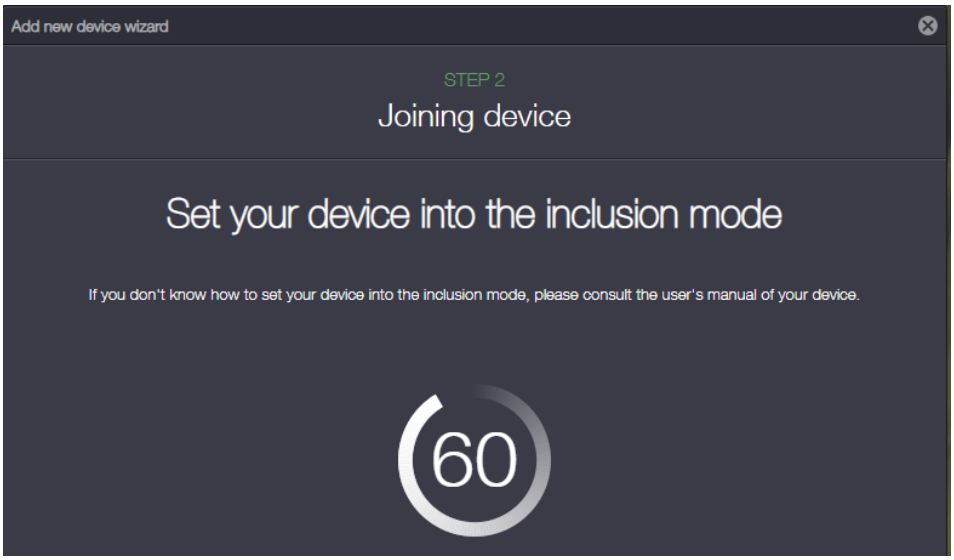

Image 15 Inclusion mode

During the inclusion step the device being included needs to be set into inclusion mode. To stop the inclusion process the window needs to be closed or the “Back” option needs to be picked.

In case the Z-Wave™ device supports security you will be prompted to select which security levels you want to grant the device. Every key that the device requests will be preselected, any granted key can be deselected if necessary. In most cases there is no need to deselect any keys and you can just confirm the selection. The key selection window is shown in the image below:

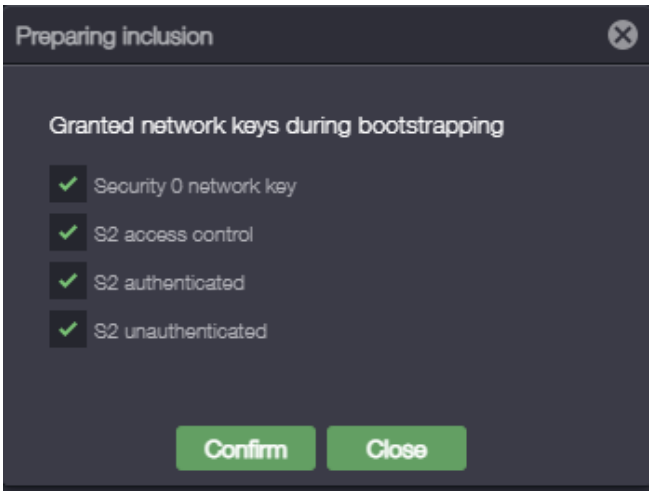

Image 16 Security key grant window

If you have selected security levels “Authenticated” and/or “Access” you will be prompted to enter the first five digits of the Device Specific Key (DSK). The DSK input window also shows the rest of the DSK so the user can confirm that the device being included is the correct one. The node add process can also be stopped here by closing the DSK input window.

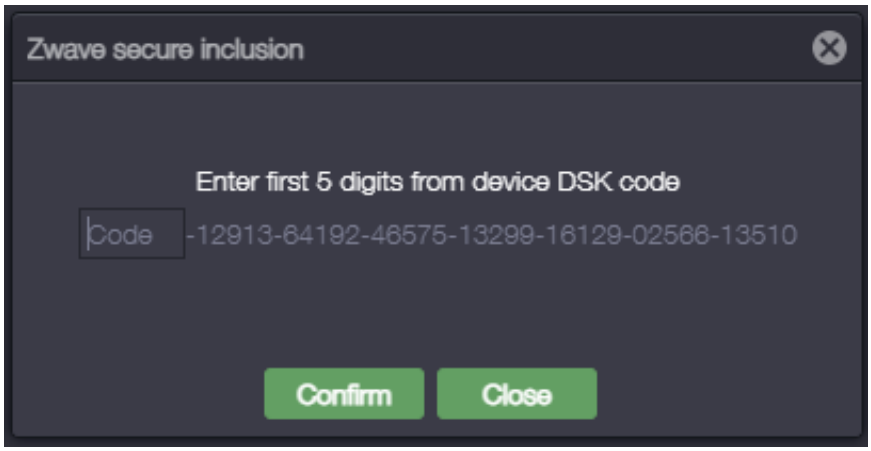

Image 17 DSK window

If the inclusion process finishes successfully the device will be added to the network and configured. Now it is possible to select its name and save the device:

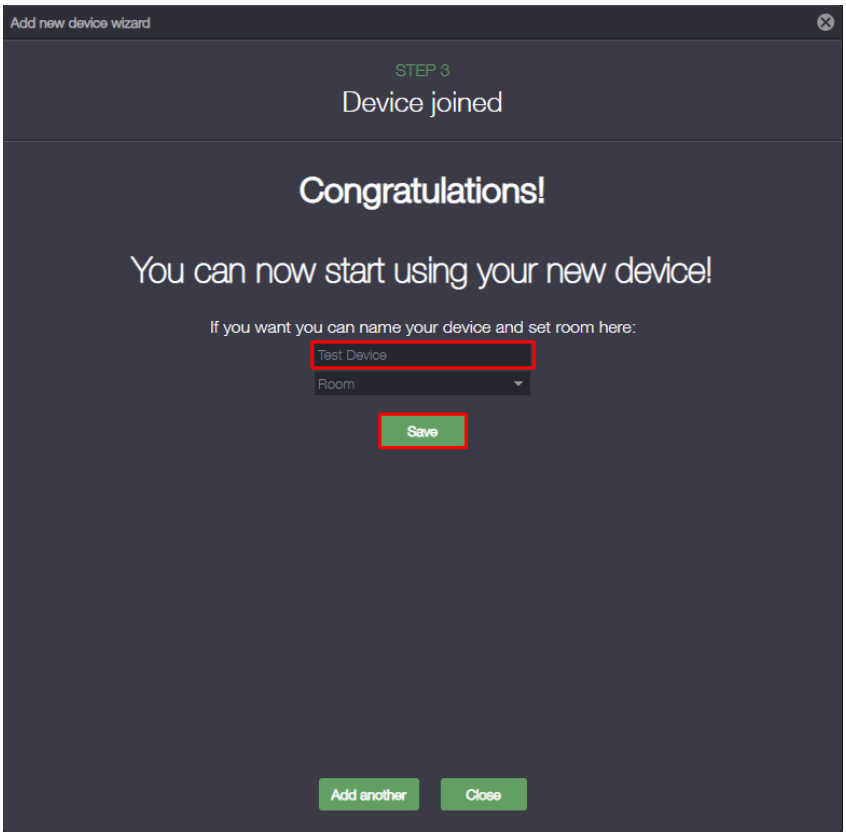

Image 18 Device added

The end-device is now displayed in the device manager, it is also possible to expand the information about this device and see all of its endpoints and clusters:

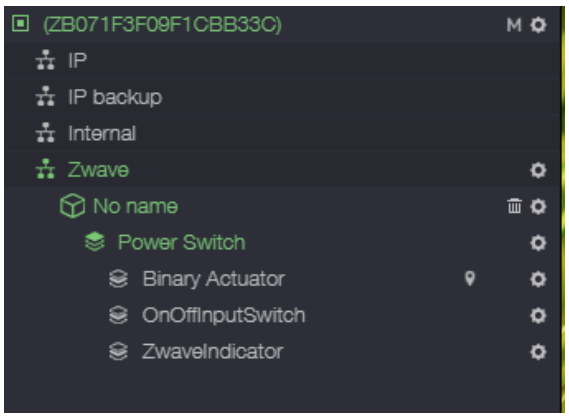

Image 19 Example of device information

In case the device is not on the list the “REFRESH” button can be used to refresh the list. If that does not help refreshing the Web page should.

Device remove operation (Exclusion)

There are two ways of removing a device:

- Exclusion (used when a working device needs to get removed from the network)
- Removing a failed device (used when an offline device needs to get removed from the network)

Device exclusion

The device exclusion option is located in the network settings. To open the network settings window the cogwheel icon right of the network name needs to be pressed:

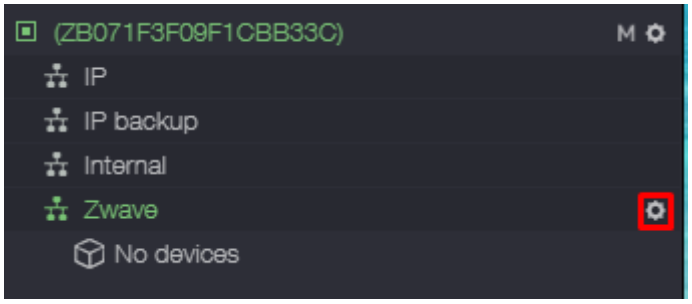

Image 20 Z-Wave™ settings

The network settings menu contains basic information about the network (this will be described in more detail later) and some network management functions. One of the network management functions is the node removal button:

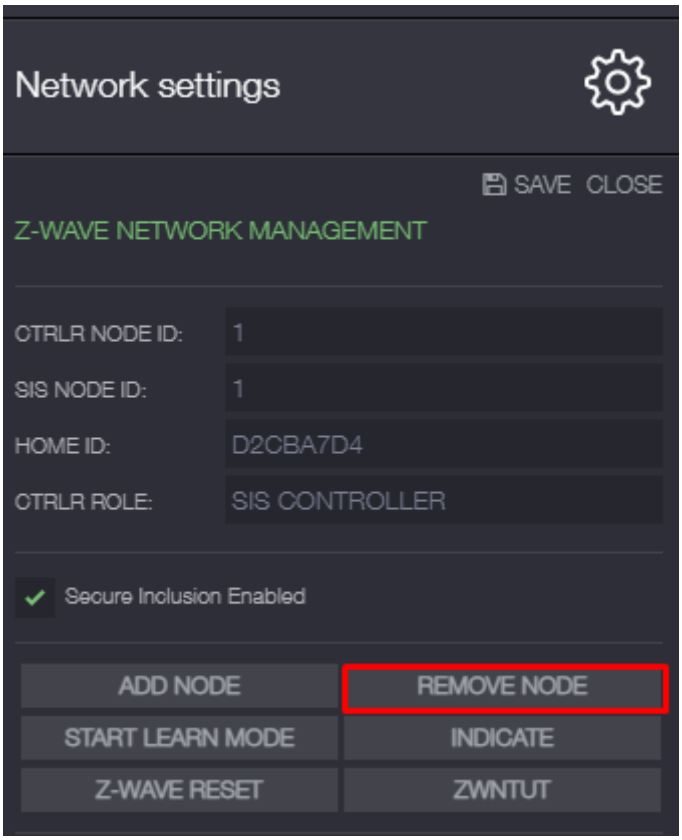

Image 21 Z-Wave™ settings

Pressing the “REMOVE NODE” button will start exclusion on the controller. This will allow a node to be removed from the network. If a node is removed in this way it will know it is no longer a part of the network. Devices removed this way will not try to communicate with the network unless they get included again.

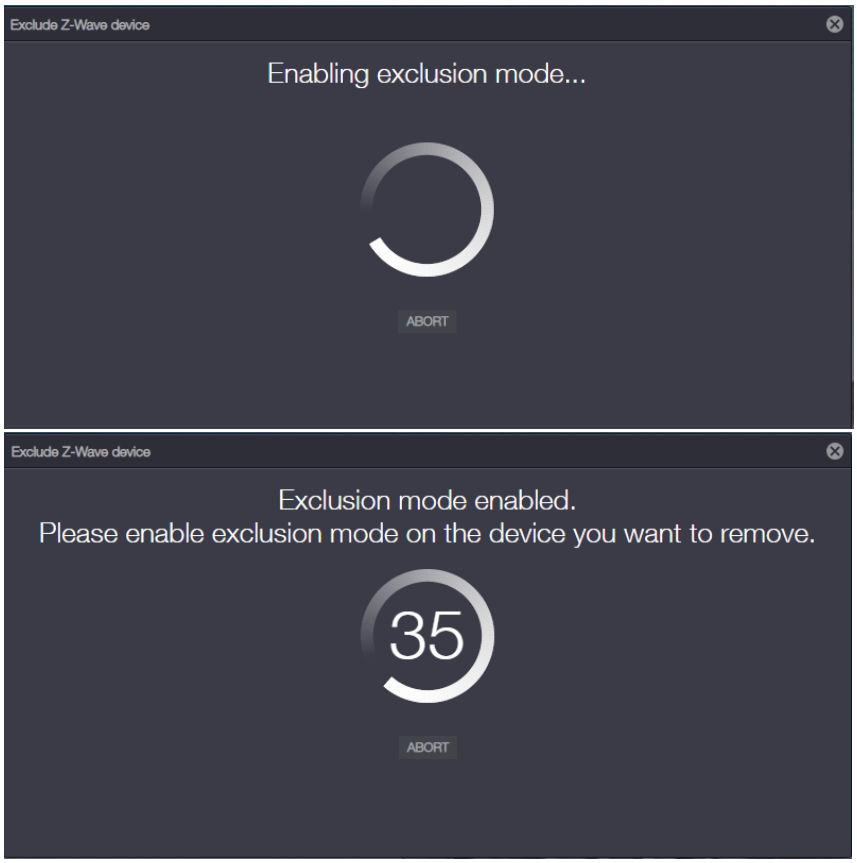

Image 22 Exclusion mode

Afterwards you will need to set your device into exclusion mode. If the process was successful you should get the following message:

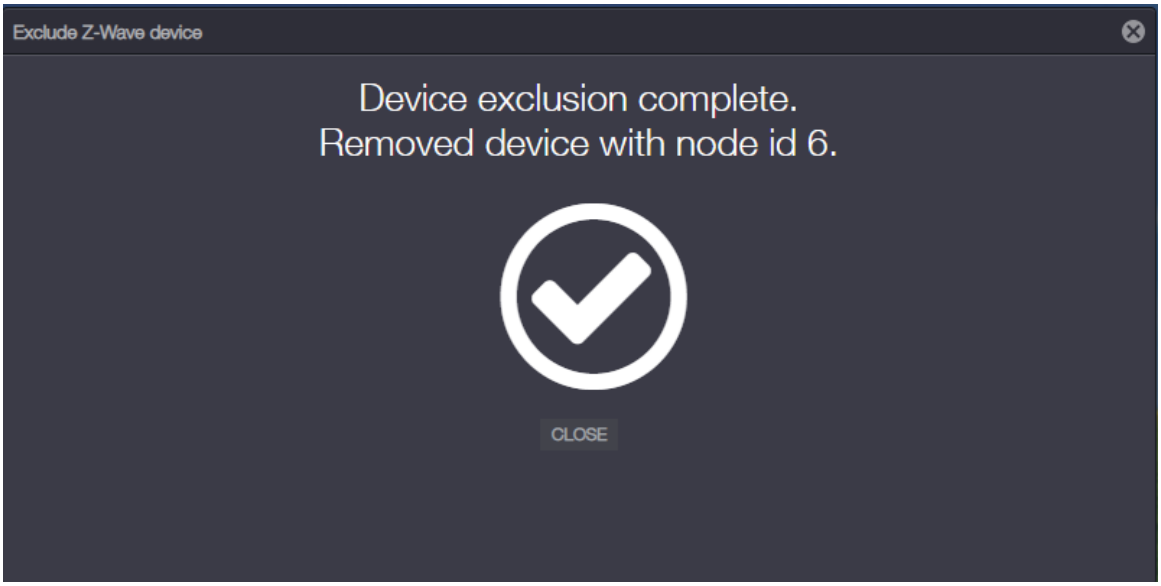

Image 23 Successful device removal

Failed device removal

In case a device is not responding to commands for a while it will be marked as “Offline” by the controller. Offline devices are marked by a red dot to the right of their name. A device will become online again if it starts communicating with the controller again. This method of device removal exists because offline devices may not be able to enter exclusion mode but still need to be removed from the network. To remove a failed device the trash can icon to the right of the devices name needs to be pressed:

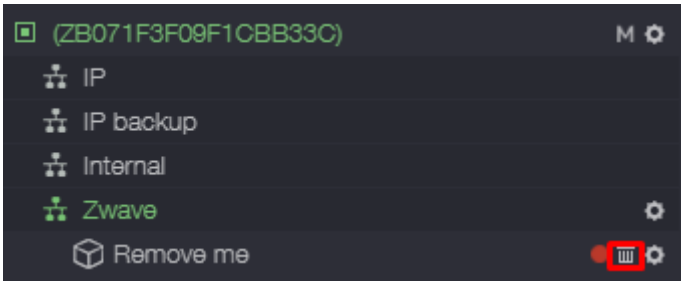

Image 24 Failed device removal

This option will check if the device is currently online, if the check fails the device will be removed from the network. If the device is online the process will fail and an appropriate message will be displayed in the UI.

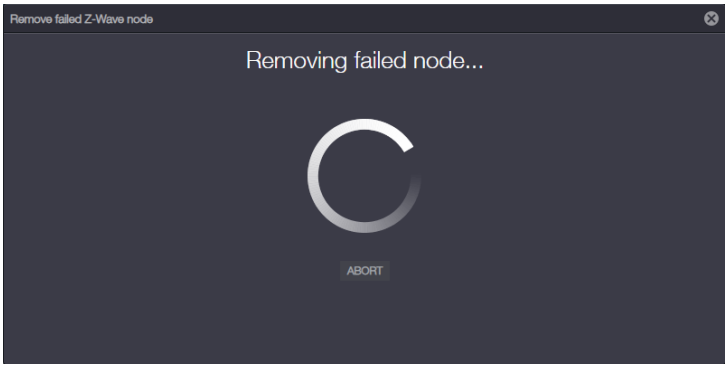

Image 25 Failed device removal process

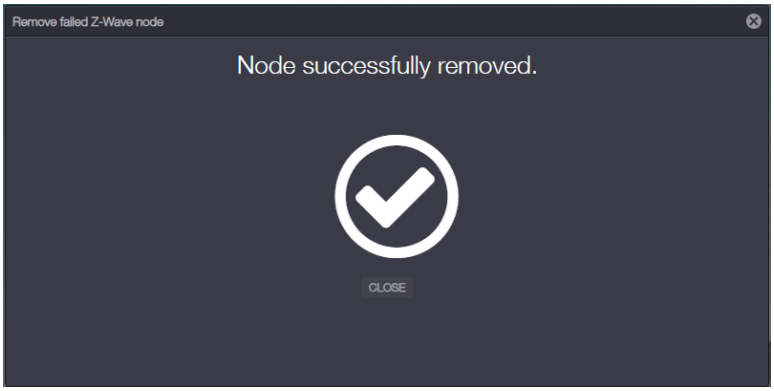

Image 26 Failed node remove success

After the process is complete device should be removed from the network. Keep in mind this option does not reset the node settings and it will still think it is connected to the network. These devices might try to communicate with the network, these messages however will be ignored by the controller. In most cases these nodes will need to be either factory reset or excluded before they can be included

again. If that devices needs to be included to a Zipabox again the standard inclusion method can be used.

Z-Wave™ - Network settings

The “Network settings” window can be accessed by pressing the cogwheel right of the Z-Wave™ network. This windows shows information about controller node ID, SIS node ID, network home ID and the controller role.

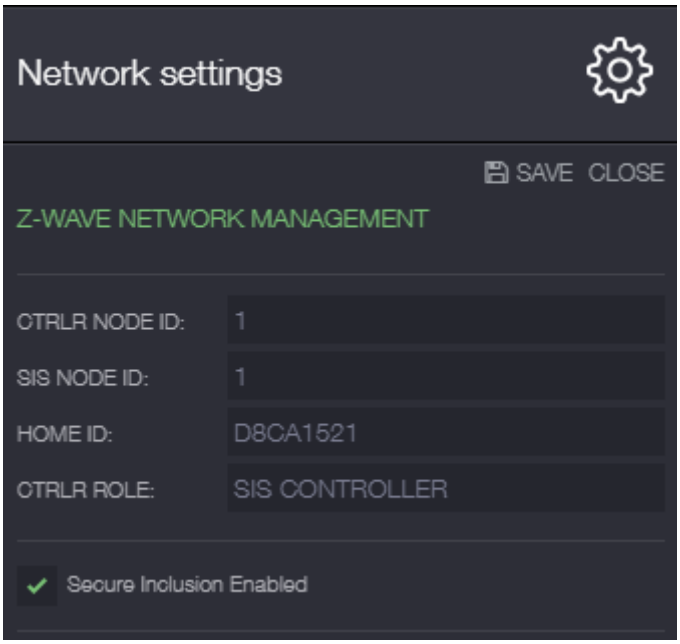

Image 27 Network management

It also has a checkbox “Secure Inclusion Enabled”, it allows the user to disable secure inclusion if they so wish. Keep in mind that changing this option will only take effect if “SAVE” button at the top right is clicked. Changing this setting has no effect on devices already added to the network. Any device that was added with or without security will keep its security level if the option is changed.

This window also contains several network management options. There are options for starting inclusion or exclusion (ADD NODE and REMOVE NODE buttons), these were already explained above and will not be explained again. The other options present in this window will be described in more detail below.

Z-Wave™ reset

Sometimes it is necessary to reset the Z-Wave™ network. Resetting the network this way will give it a new HOME ID and clear its list of added devices. This means that any devices that were included into the network will no longer be present after the restart. These device will need to be added again.

Z-Wave™ reset also clears the provisioning list. This means that any devices added for SmartStart will not be added.

Keep in mind that this only resets the Z-Wave™ network and will not reset the controller itself. To restart the controller hold the “Button 2” for 5 seconds. Pressing the “Z-WAVE RESET” button will start the reset process.

Image 28 Z-Wave™ reset button

The reset process usually takes a couple of seconds but might need up to a minute to complete:

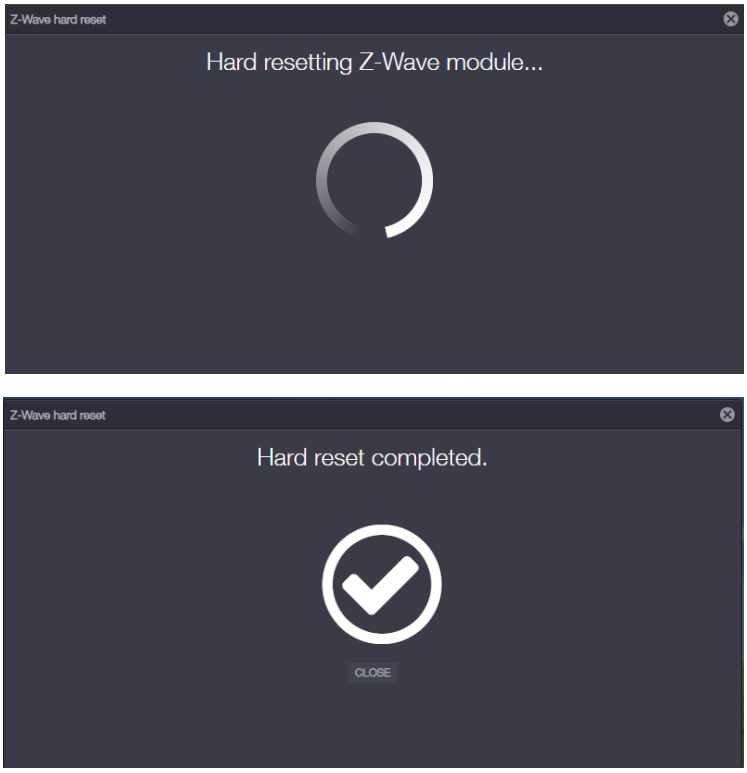

Image 29 Hard reset complete

When “Hard reset” is started the controller will attempt to send “Device Reset Locally Notification” to the device associated on its Lifeline Group (Group 1). After reset is complete the controller will be given a new home id and its network will be cleared of any included nodes.

SmartStart

SmartStart allows the devices to be automatically included into the network when they power on. For SmartStart to be able to add devices in such a way the devices need to be on the provisioning list of the controller. To add a device to the provisioning list the “ADD CODE” option must be used:

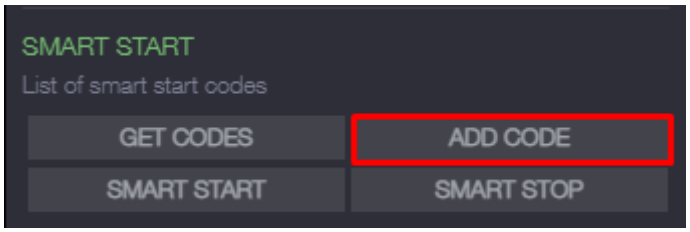

Image 30 Add SmartStart code

A new window should open, it allows the user to enter the name for the device and a choice of either the numeric representation of the QR code or the DSK:

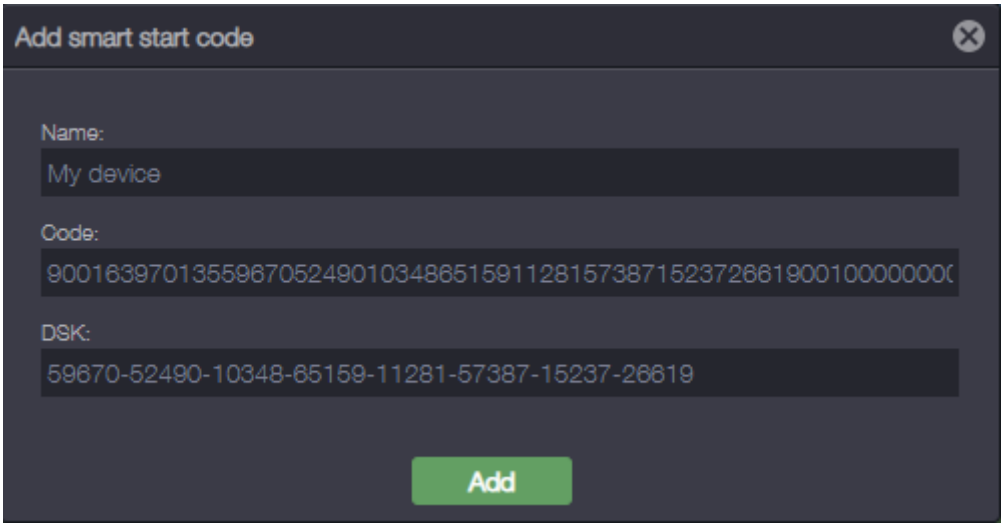

Image 31 SmartStart code window

Keep in mind that either code **OR** DSK need to be entered, entering them both is not necessary. After filling the required fields the “Add” button will add the code into the provisioning list. Now the device should get automatically included into the network when it powers on.

The “GET CODES” button gets the list of all of the devices added to the provisioning list. Here they can be viewed or removed from the provisioning list:

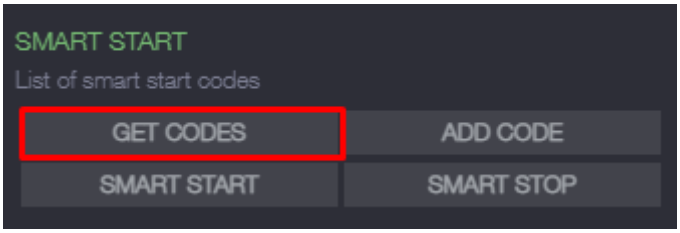

Image 32 Get codes button

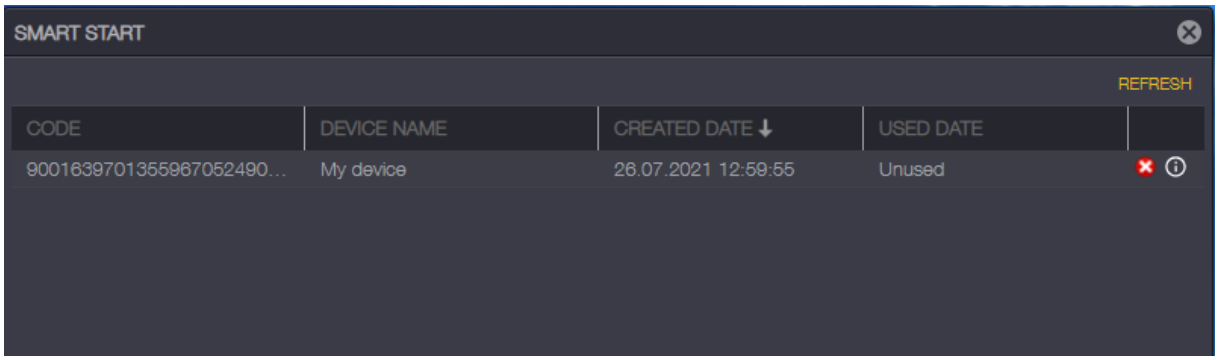

Image 33 SmartStart provisioning list

The provisioning list contains the code used to add the device, its name and when was it added to the list. The red "X" button on the right side of the window removes the current row from the controllers provisioning list:

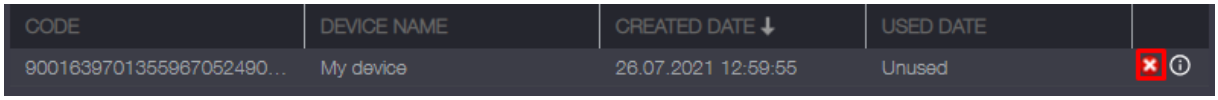

Image 34 Remove from provisioning list

Removing a device from the provisioning list will stop it from being automatically included when it powers on.

Identify

It is possible to make the controller identify itself by pressing the "INDICATE" button:

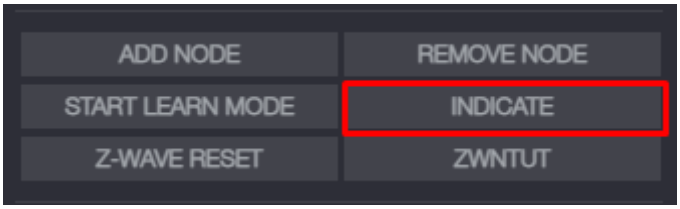

Image 35 Indicate button

This option is used to identify the controller if multiple of them are present within the network. It will make the controller light blink 3 times.

To identify the controller without using the UI send the "Indicator Command Class" command "Indicator Set" with "Indicator ID" set to 0x50 (Node Identify).

Checking the battery

If a battery device is included into the network it is possible to check the status of its battery in the Device manager. This can be done by hovering the mouse over the battery icon next to the device:

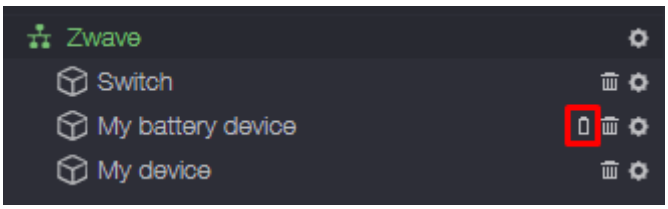

Image 36 Battery icon

Image 37 Battery percentage

If a device has widgets in the Device browser the battery percentage can also be checked there:

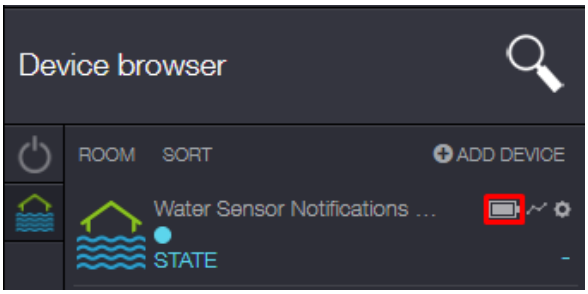

Image 38 Battery in Device browser

If a device sends the low-battery warning the icon will be shown in red:

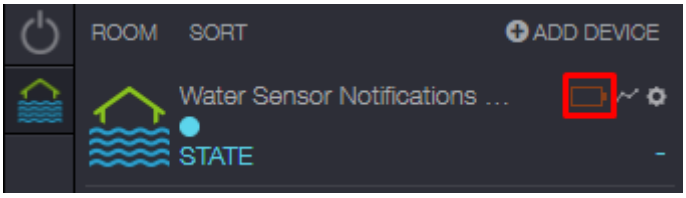

Image 39 Low battery icon

And Device manager will be updated to reflect this:

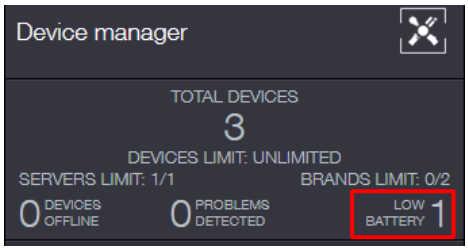

Image 40 Low battery devices

Device properties

Each device has extra options that can be configured. These options include devices name, description, extra configuration options provided by the protocol and more. Device information and configuration options can be accessed by clicking on the cogwheel to the right of the device name:

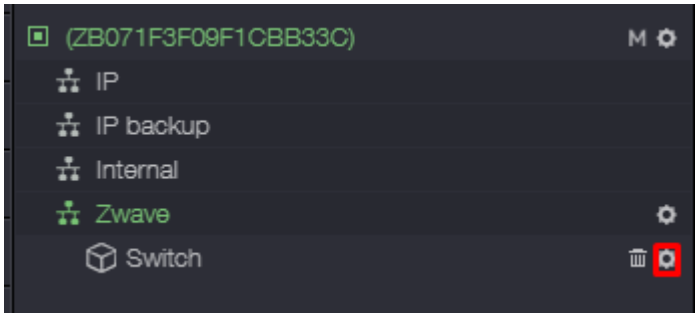

Image 41 Device properties

General tab

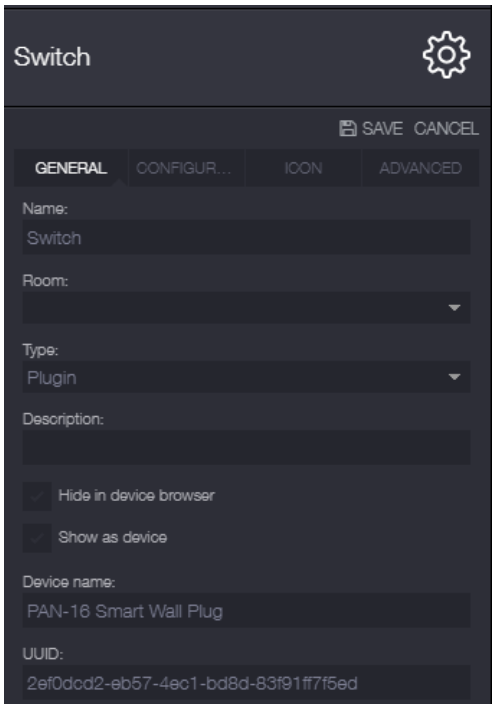

Image 42 Device properties

The device properties window has 4 tabs:

- General – device name, description and its unique identifier can be found here
- Configuration – allows changing of configuration parameters
- Advanced – node information, firmware updates, associations and node reconfiguration

The general tab contains some basic information about the device. Here the device name, room and description can be changed. All changes on this tab are only visual and do not impact the functionality of the device.

This tab also shows the UUID, this is a unique id for this device within the system. Every device, endpoint and cluster have their own unique id. These IDs can be used to run API calls towards these devices/endpoints/clusters.

Configuration tab

Configuration allows users to change the device configuration using the configuration command class. All the configuration options are device specific, as such two similar devices (ex. two different power plugs) may have completely different configuration parameters. This tab is linked to Z-Wave™ Configuration command class and is only present for Z-Wave™ devices.

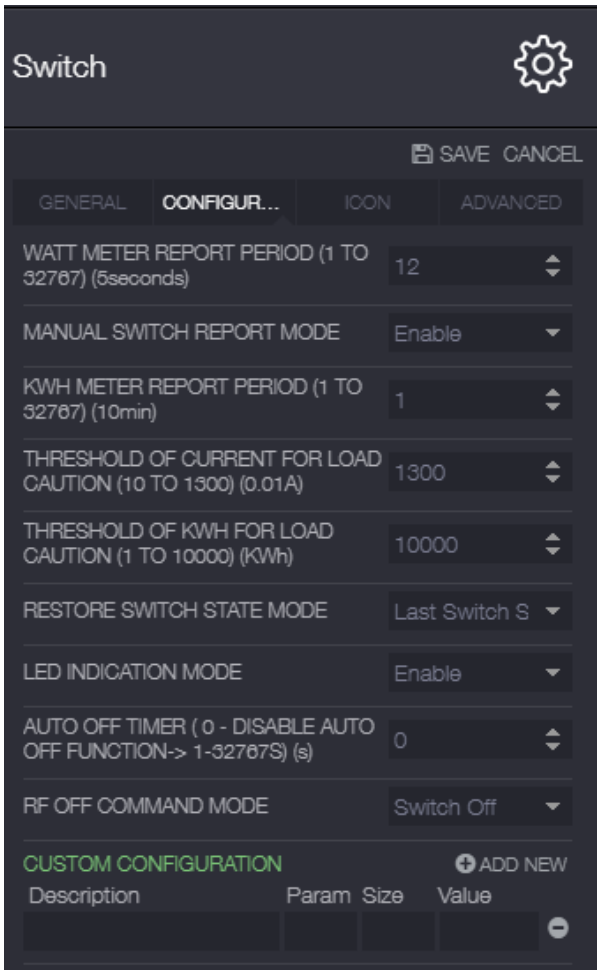

Image 43 Device configuration

This tab allows users to change the devices configuration parameters. If configuration parameters already exist they will be listed above the custom configuration option. Each option can be expanded to send/receive its value.

As an example the “LED INDICATOR MODE” option will be set to disabled. This can be done by expanding it, changing its status to “Disable” and pressing “Send”:

Image 44 Configuration setting

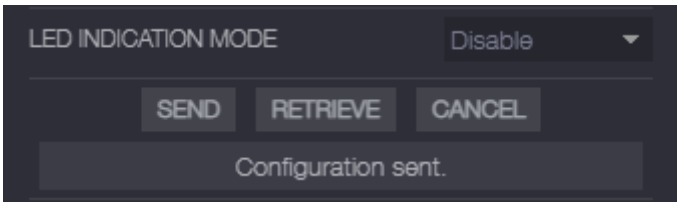

Image 45 Device configuration sent

If a configuration was set successfully the message “Configuration sent” will be shown below.

To check what is the current configuration the “RETREIVE” button can be pressed. This will make the controller ask the device what is its current value for that property.

There is also a custom configuration, if some or all of the device configuration parameters are missing the user can add them on their own. Each configuration parameter consist of:

- Description – configuration name describing what it does (Optional)
- Param – parameter number (DEC)
- Size – parameter size in bytes
- Value – value to be sent

It is suggested to look for valid parameter number, size and value in the official documentation of the device. It is not recommended to add parameters that do not exist as it might cause unexpected behavior. The process of sending the custom configuration parameter is similar to sending an existing configuration. The process starts by filling out the fields. After that pressing “SEND” should update the configuration:

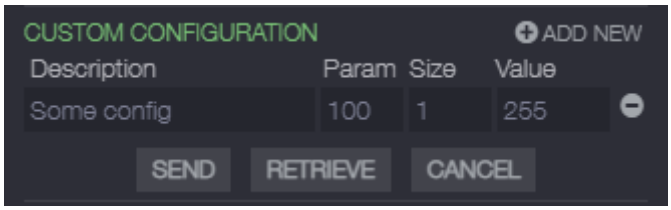

Image 46 Example of custom configuration

Advanced tab

The advanced tab contains node information such as its class, node ID and more. It also contains node management options like node reconfiguration and association management. This is also where firmware updates can be installed onto the device. These options will be described in more detail below.

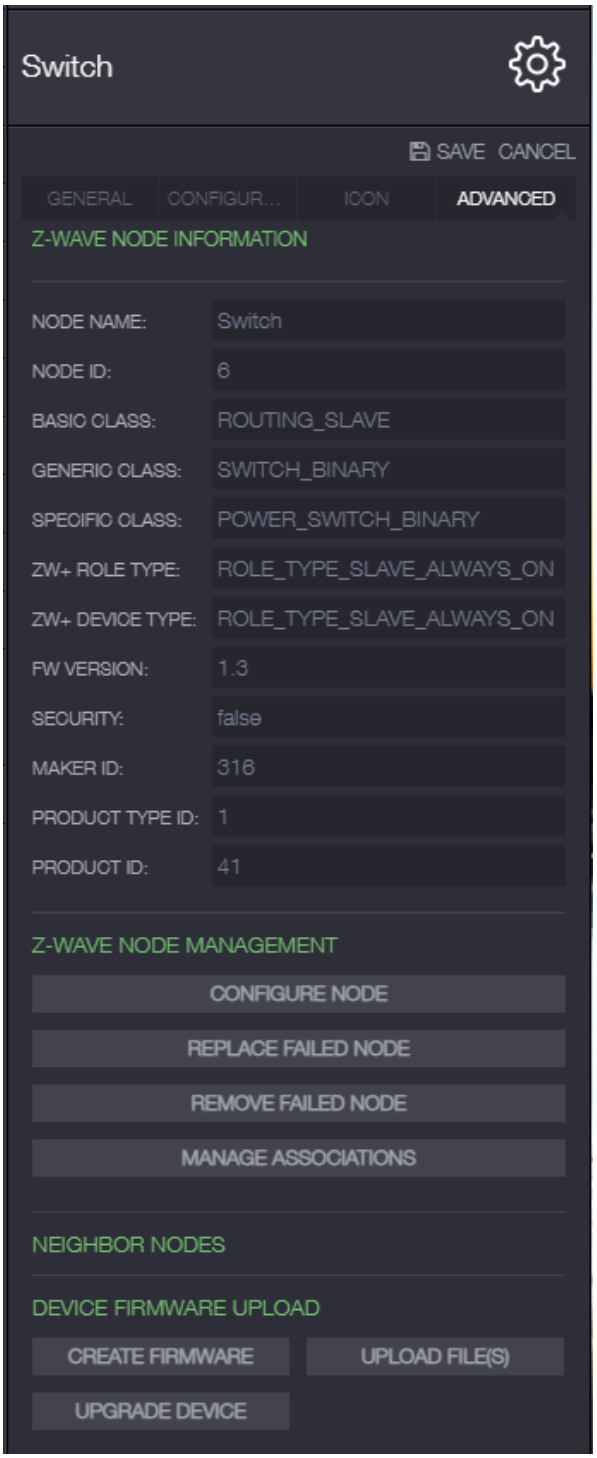

Image 47 Device advanced options

Device rediscovery

Device rediscovery can be used for when the device configuration saved on the controller end is not up-to-date. It will start a new interview with the device to get its capabilities and set up everything accordingly. To start the device rediscovery process the “CONFIGURE NODE” button needs to be pressed:

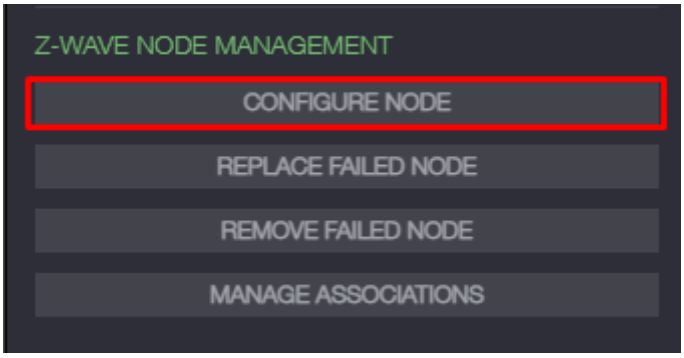

Image 48 Configure node button

After that a prompt will be asking for confirmation, pressing “Yes” will reconfigure the device. If the reconfiguration finishes successfully the following message will be displayed:

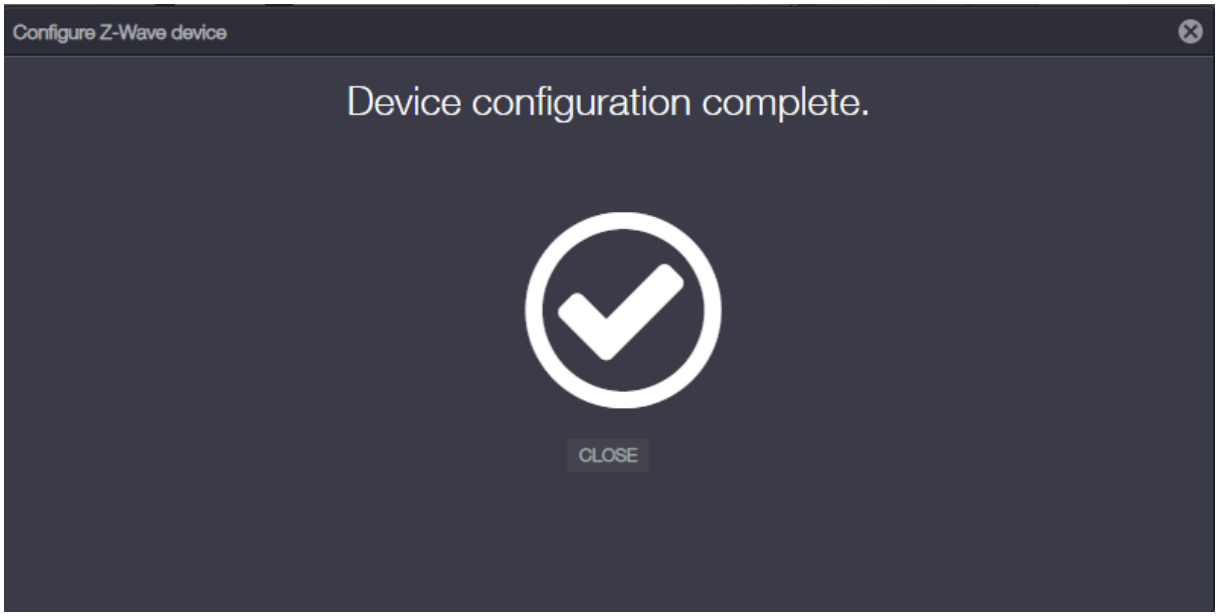

Image 49 Device reconfiguration

Device association

Device association allows devices to send commands to other devices without the help of the controller. By default all included nodes have their Lifeline Group association set to the controller, this means that when they generate a notification it will be sent to the controller. For an example, a switch and a light bulb could be associated in such a way that flicking the switch also turns the light on/off. To associate one device with another the “MANAGE ASSOCIATION” button needs to be pressed:

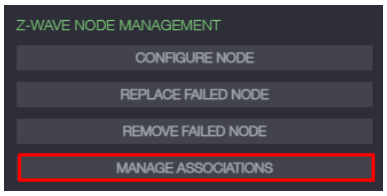

Image 50 Manage associations

This will open a new window with 3 columns. First column contains the list of devices (excluding the device that is currently selected for association management) and all of their endpoints. The second column shows the list of devices currently added to the selected group. While the third column contains all the association groups the device supports.

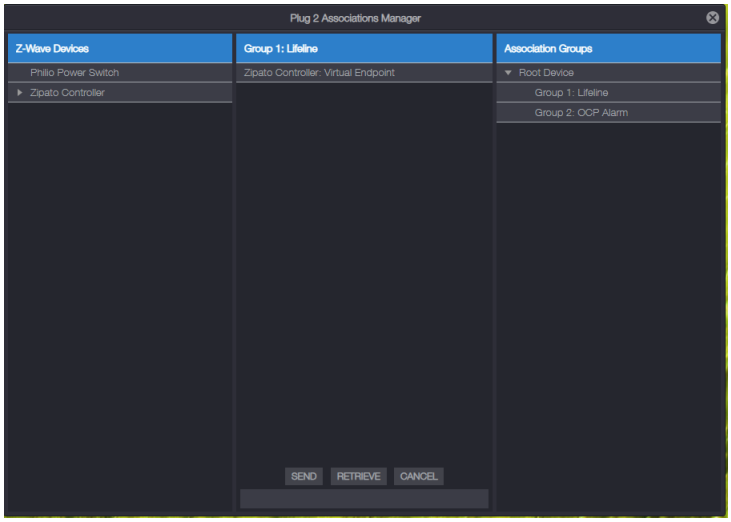

Image 51 Association manager for device "Plug 2"

NOTE: If a device or endpoint are missing from the list try refreshing the page

The image above shows the Lifeline Group association group for the device “Plug 2”. To add a new association follow these steps:

1. Select the group from association groups column
2. Optional: Click “RETREIVE” to get devices currently associated to this group
3. Drag devices from the left column to the middle column to add them
4. Right click the devices middle column and pick “Remove from group” to remove them
5. Click “SEND” to send the configuration to the device

Controller association groups

Group id	Profile (2 bytes)	Command Class	Group Name	Maximum devices
1	General : Lifeline Group	Device Reset Locally	Lifeline Group	1

NOTE: Device will send the “Device Reset Locally Notification” to its Lifeline Group when “Z-Wave™ Reset” operation is started.

Device firmware upload

Device firmware upload allows devices to receive OTA updates. To start updating a file with the firmware update will be needed. Firstly a firmware will need to be created using the “CREATE FIRMWARE” button:

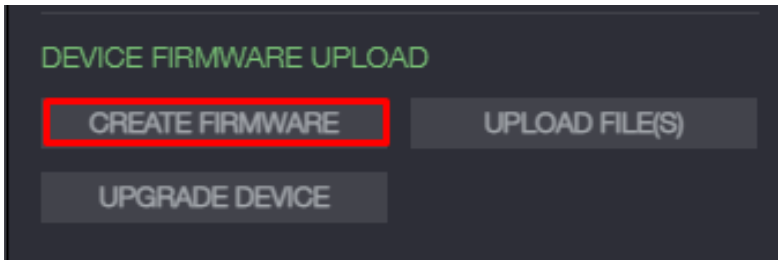

Image 52 Create firmware

This will open a window for firmware creation. The user will be prompted to enter name and description for the firmware update. These fields will be displayed when picking the firmware, it is good practice to label them based on what firmware version they are for.

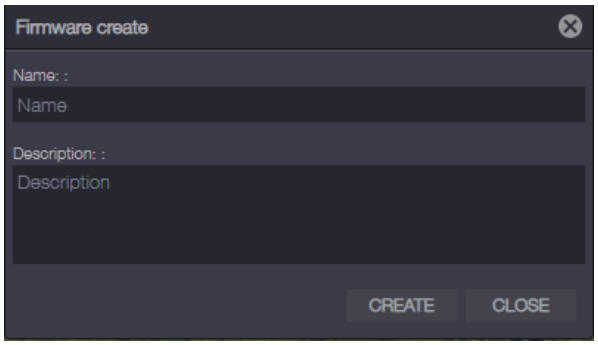

Image 53 Firmware create

After that a firmware file can be uploaded through the “UPLOAD FILE(S)” button.

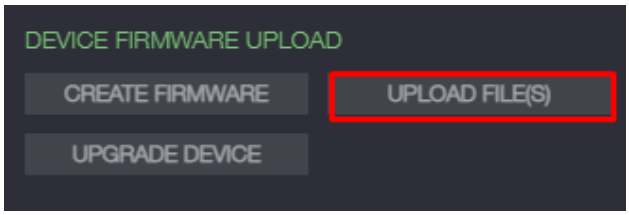

Image 54 Firmware file upload

To be able to upload a new firmware file follow these steps:

1. Select firmware
2. Select the firmware file
3. Press upload

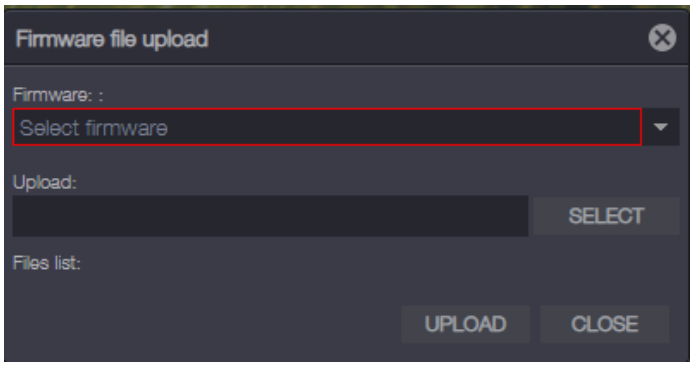

Image 55 Firmware upload window

And lastly the firmware upgrade can be transferred to the device using “UPGRADE DEVICE”.

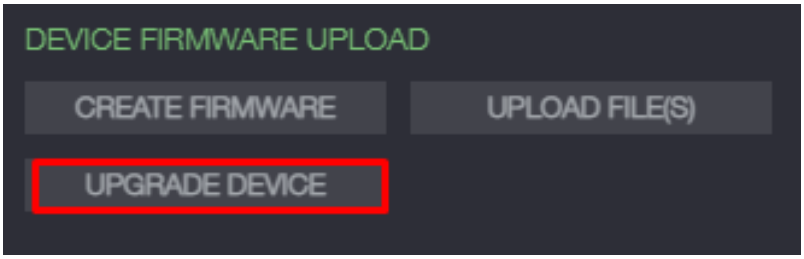

Image 56 Upgrade device

Afterwards the firmware, firmware file and firmware target will need to be selected. There is also an option to allow the firmware update to update all similar devices. For an example if the user has two or more devices from the same manufacturer, product type and product id they will all be updated.

Image 57 Upgrade device

Depending on the device the update might take a while. Devices might also indicate that an update is ongoing through its indicator. When the firmware update finishes a message will pop up informing the user that the update was successful/unsuccessful.

Anti-theft Unlock

Some devices added to the network might have been locked while they were included into another network. Such device will not function properly and will need to be unlocked. Anti-theft Unlock Command Class can be used to find out if a device has been locked and unlock the device.

Any device that supports this feature will have it displayed in its advanced tab:

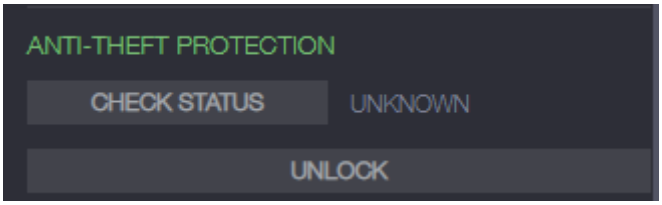

Image 58 Anti-theft Unlock feature

The “CHECK STATUS” button allows the user to find out what is the current status of the device. There are three possible statuses:

Status	Description
UNKNOWN	Default status, press “CHECK STATUS” to update it
DISABLED	Anti-theft protection is disabled, device should work normally
ENABLED / RESTRICTED MODE	Anti-theft protection is enabled, device will need to be unlocked before it can be used normally

To send the unlock command to the device the “UNLOCK” button should be used. This will open up a device unlock window:

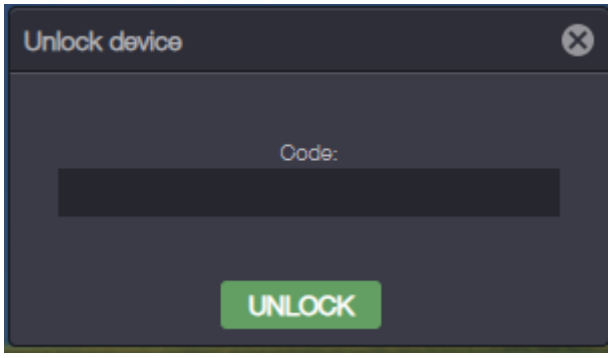

Image 59 Unlock device window

“Code” field should be the same as the code used for locking. This field only supports HEX symbols (0-9, A-F). For an example, the code: “0x01, 0x02, 0x03, 0x04” input can be inputted like

- 0x01020304 (with 0x prefix)
- 01020304 (without 0x prefix)

After the code has been input the “UNLOCK” button can be used to send the unlock command with the inputted code to the device.

If the device has been unlocked, the “CHECK STATUS” button should return the status “DISABLED”.

Device browser

The device browser allows users to control their devices and read sensor data. It can be opened with the following button in the UI:

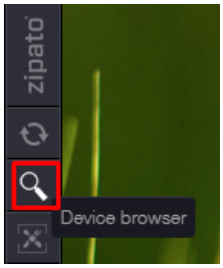

Image 60 Device browser

The device browser has all devices put into categories such as switches, plugs, sensors etc.

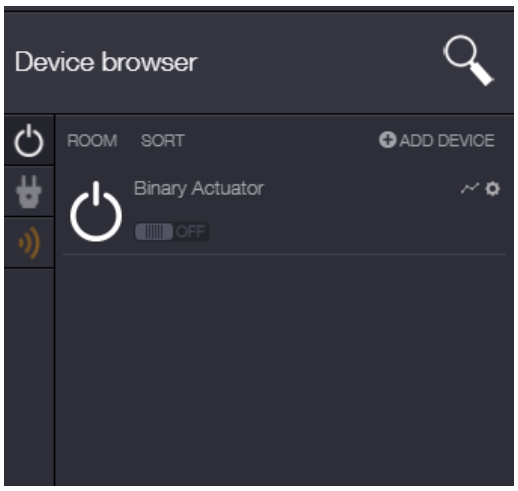

Image 61 Device browser

The image above shows a generic on/off device that can be controlled through the UI. By clicking on the switch in the UI it is possible to turn the real switch it is representing on and off:

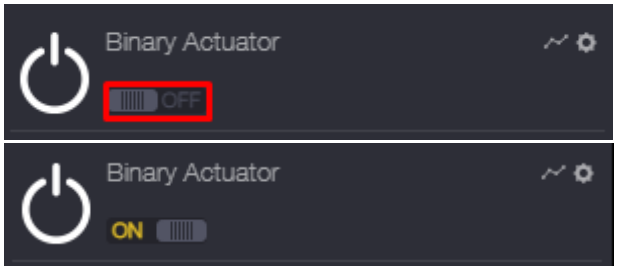

Image 62 Switch being turned on

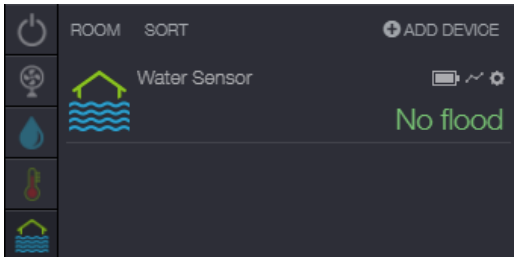

Image 63 Example of a sensor

Getting notifications from pull devices

Some notification devices might require get requests from controllers to send their notification data. Or users might want to get the notification data manually. This option allows that. To access it first find the notifications tab () in the device browser and find the one you are looking for. Afterwards click the cogwheel on the right of its name:

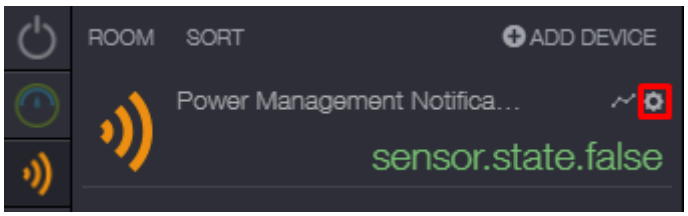

Image 64 Endpoint options

Afterwards select the “ADVANCED” tab:

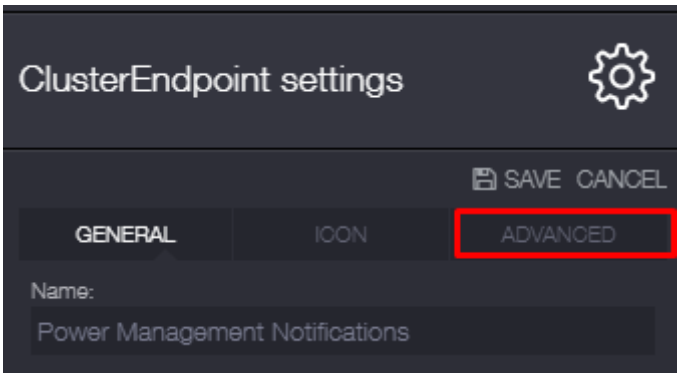

Image 65 Advanced tab

Now you can pull notifications from the device. To pull a notification three fields need to be filled:

- Alarm type
- Notification type
- Event code

These are generic Z-Wave™ codes and can be found in the official Z-Wave™ documentation. The device documentation may also contain these. Entering a non-existing combination it should not cause any issues with the device or the controller. However it is still recommended to consult the device documentation (or Z-Wave™ documentation) before attempting to get notifications from the device.

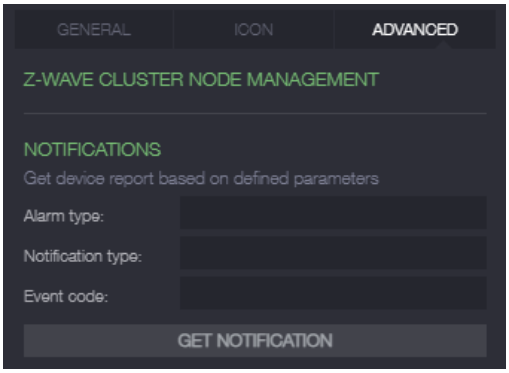

Image 66 Notification get input

Meter reset

Z-Wave™ offers the ability to reset cumulative meter measurements. If for any reason the user wishes to reset the meter cumulative measurements to their default value that can be done through the Web UI. To do it first find the meter tab ( ) in the device browser. Afterwards find the meter you are looking for and click the cogwheel icon to the right of its name:

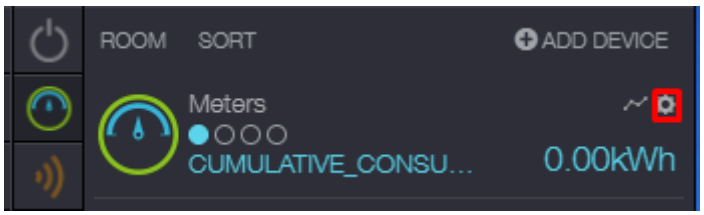

Image 67 Meter tab

And select the “ADVACNED” tab:

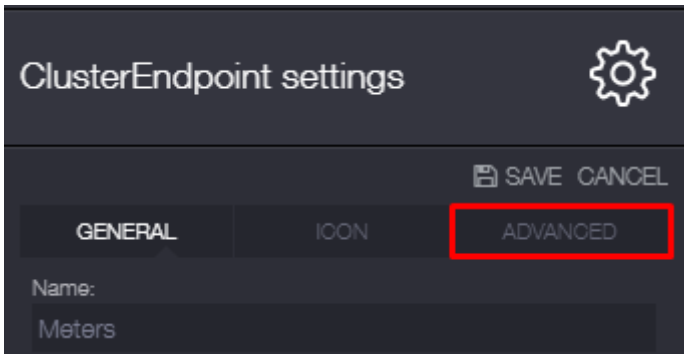

Image 68 Meter options

Pressing the “RESET” button will reset the measurements of the Z-Wave™ device to zero (if the device supports it):

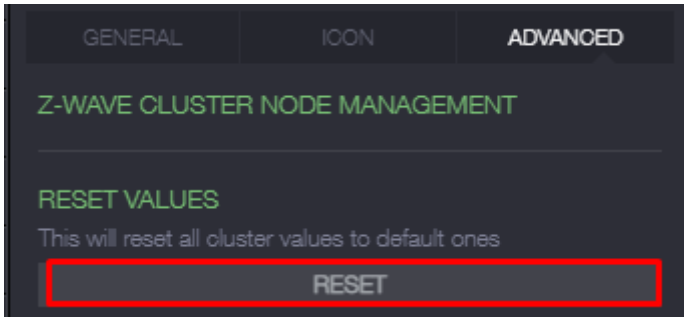

Image 69 Z-Wave™ meter reset

Keep in mind after the meter is reset it is NOT POSSIBLE to get the old measurements back and any cumulative measurement will start to count up from its default value (most likely a zero). This however will not directly affect the Web UI and it will wait for the device to report a new measurement before it updates.

Events

The events tab ( ) shows various events that happened within the system. It shows all notifications received from devices within the system even if they do not have an appropriate widget.

There are two options for displaying events:

- LATEST - shows last event received for each attribute
- LIVE - shows all events that were received since the option was selected

Image 70 Event options

There is also an attribute filter. This filter allows the user to filter the events based on what attribute/device they are related to:

Image 71 Filter

Example of an event that shows a switch being turned off and “LATEST” option selected:

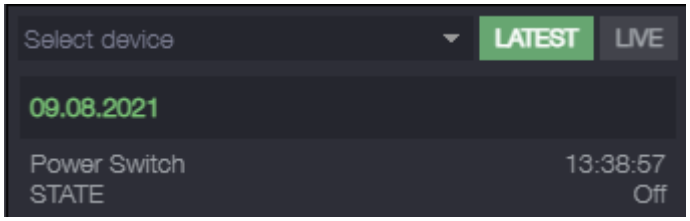

Image 72 Event example 1

Example of a switch being turned on and off while “LIVE” option was active:

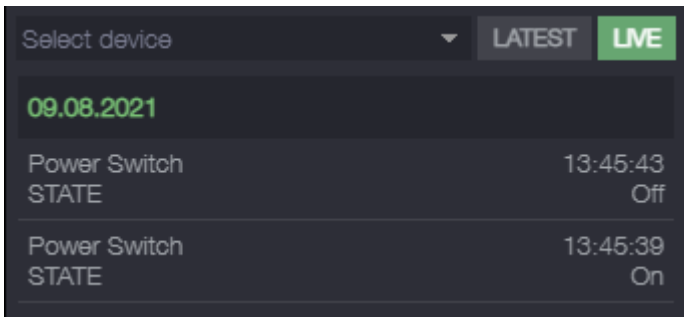

Image 73 Event example 2

Supported Command Classes

- Application Status
- Association Group Information V3
- Association V3
- CRC16 Encapsulation
- Device Reset Locally
- Firmware Update Meta-Data V5
- Inclusion Controller
- Indicator V3
- Manufacturer Specific V2
- Multi-Channel Association V4
- Multi-Command
- Network Management Basic V2
- Network Management Inclusion V3
- Network Management Installation and Maintenance V2
- Network Management Proxy V2
- Node Provisioning
- Powerlevel
- Security S0
- Security S2
- Supervision
- Time
- Transport Service V2
- Version V3
- Z-Wave Plus™ Info V2

*any classes missing the version tag are version 1

Controlled Command Classes

- Association Group Information V3
- Anti-Theft Unlock
- Association V2
- Basic V2
- Battery
- Central Scene V3
- CRC16 Encapsulation
- Device Reset Locally
- Firmware Update Meta-Data V5
- Indicator V3
- Manufacturer Specific V2
- Meter V5
- Multi-Channel Association V3
- Multi-Channel V4
- Notification V8
- Security S0
- Security S2
- Sensor Multilevel V11
- Version V2
- Wake Up V2
- Z-Wave Plus™ Info V2

*any classes missing the version tag are version 1