

Certification Manual

Table of Contents

1. Introduction	5
1.1 Understanding GW status	5
1.2 Accessing service for operation.....	5
2. Gateway Connection Configuration Ethernet and WIFI.....	7
3. Considerations	7
3.1 View Devices	8
3.2 View Control	9
3.3 View Comfort	9
3.4 View Security	11
4. Inclusion and exclusion of a Z-Wave Device	12
4.1 Inclusion.....	12
4.1.1 Unsecured & S0 device	12
4.1.2 S2 device	13
4.1.3 SmartStart device.....	13
4.2 Exclusion of Z-Wave Device	14
4.2.1 SmartStart device.....	14
4.3 Remove failed device	15
5. Device Configuration	16
5.1 Configuration parameters for security devices.	16
5.2 Configuration parameters for energy meter devices.	17
5.3 Configuration parameters for comfort devices	17
5.4 Configuration parameters for control devices.	17
6. Z-Wave advance actions	18
6.1 Send NIF	18
6.2 Node provisioning for smart start	19
6.3 Learn mode	20
6.3.1 Inclusion of controller into an existing network.....	20
6.4 Gateway's DSK.....	21
6.5 Reset.....	22
7. Z-Wave Network.....	23
7.1 Devices and manufacturers	23
7.2 Associations.....	23
7.3 Devices support and S2 Security.	23
7.4 Basic command class	24

7.5	Controller replication.....	24
8.	Trouble Shooting.....	25

List of figures

Figure 1: Gateway led information	5
Figure 2: Installation selection.....	6
Figure 3: user settings	6
Figure 4: GW network configuration.....	7
Figure 5: UI Dashboard	7
Figure 6: UI Device view (sensors)	8
Figure 7: UI control view.....	9
Figure 8: UI Comfort view (central control).....	10
Figure 9: UI Comfort view (areas).....	10
Figure 10: UI Security view.....	11
Figure 11: Removing failing device	15
Figure 12: Removing non failing (online) device.....	15
Figure 13: request NF	18
Figure 14: Provisioning List	19
Figure 15: Provisioning list management	19
Figure 16: Learn mode.....	20
Figure 17: Learn mode interface.....	21
Figure 18: Show GW disk.....	21
Figure 19: GW default reset.....	22
Figure 20: Notification of finalisation of reset procedure.	22
Figure 21: GW connected to service and ready for interaction.	22

1. Introduction

Before you continue, you should have read the quick start guide, which informs you about the steps you have to take to connect the gateway to mains and your local area network. Also read “Precautions and Guarantee” document for safety knowledge.

This document provides information about UI views that will be need during certification (an extended user manual is provided for wider view of the UI), so the Z-Wave™ Certification team can perform their tests easily.

Important: For best experience we strongly recommend using Chrome web browser.

1.1 Understanding GW status

It is important to understand that the DUT (gateway) needs internet connectivity to perform all tasks related to homologation.

The device provides information about its state using LEDs as following:

Mode	Function	Blue (*1)	Green	Red
Normal	Initialization/busy	continuous	continuous	off
	connected with service	continuous	off	off
	Initialization / Z/IP Middleware	continuous	heartbeat	heartbeat
	initialization / no RF (Z-Wave/rf)	continuous		continuous
	no network	continuous		slow flashing
	no internet	continuous		2 slow flash 1 off
	Inclusion (Z-Wave)		slow flashing	off
	Exclusion (Z-Wave)	continuous	2 slow flash 1 off	off
	App Update	continuous	continuous	continuous

Figure 1: Gateway led information

The device will be ready for interaction with web service when BLUE led is ON (GREEN and RED is OFF) after booting.

The booting sequence is as following:

- 1) SO starts and lunch daemons
- 2) Wait for Z/IP operation
- 3) Wait for LAN
- 4) Wait for Internet
- 5) Connect with service

The gateway uses following ports to connect with cloud service:

- 1) HTTP: 80
- 2) HTTPS: 443
- 3) TCP: 9350, 9355
- 4) SSH: 22 (for remote support)

1.2 Accessing service for operation

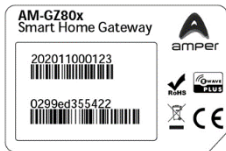
You are supplied with two DUT samples:

- 1) DUT_1
 - a. GW id = 02b9eb22e49c

- b. GW SN = 202011000001
- c. GW SDK = 00617-15924-08724-01767-47067-03287-32661-05525

2) DUT_2

- a. GW id = 023608dee17c
- b. GW SN = 202011000002
- c. GW SDK = 21511-19469-00212-18883-20894-34601-43162-45244



The information is printed in the label that can be found at the button of the GW as described in following example:

For accessing the service, use Chrome web browser and with following URL:

- <https://dev.encontrol.io>

Use the following user and password to access the platform and manage the provided gateway:

- 1) User: hm_eu@sensingcontrol.com
- 2) Password: HmEu2020!

After successful login in, URL will move to dashboard (where *GWID* is as described above).

- <https://dev.encontrol.io/installations/00000000-0000-0000-0000-GWID/Dashboard>

The default installation is DUT_1, you can change to DUT_2 at any moment through the menu's Installations option during the session. (Notice that the installation in use is shown in bright white)

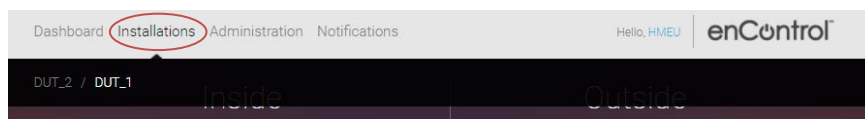


Figure 2: Installation selection

For permanently change, you can have to access settings from “Hello, HMEU” and select DUT_2 as default installation (remember to delete asterisks in account field before clicking save button).

Figure 3: user settings

2. Gateway Connection Configuration Ethernet and WIFI

In case you need to configure Wi-Fi connectivity, you have to jump to the web page of configuration of the gateway. For this you have to know the local IP of your Gateway and go to <http://iplocal/login>.

You will see the following web page, enter user = admin and password = IDGW (is in the GW box or shown in the URL as shown as example in previous section (02a1591d3b2b)). Once you enter, you will see the following website.

Once you have registered, the following configuration options will appear (see the following figure).

Network Configuration

Gateway Network Settings

Network interface eth0 with MAC 02:A1:59:1D:3B:2B

DHCP
Enabled

Network interface wlan0 with MAC 18:BB:26:B7:1A:DC

DHCP
Enabled

SSID
no network Refresh

Update

Remarks:

- It is advisable to use the "DHCP" option for Wifi and Ethernet.
- Make a note of changes made if you are going to work with static IPs.
- The gateway will always use the Ethernet connection, then Wifi.
- Network settings default reset is achieved by triple click on user button of Gateway. This button is located side to power supply connector.

Figure 4: GW network configuration

3. Considerations

Once logged in, you will have access to the main dashboard and can go either to: (i) add Z-Wave devices (from menu); (ii) manage the installation for advanced use cases (from menu) or (iii) go to the different sections of the platform as show in following subsections (from menu or central view icons; comfort, security, consumptions, and control).

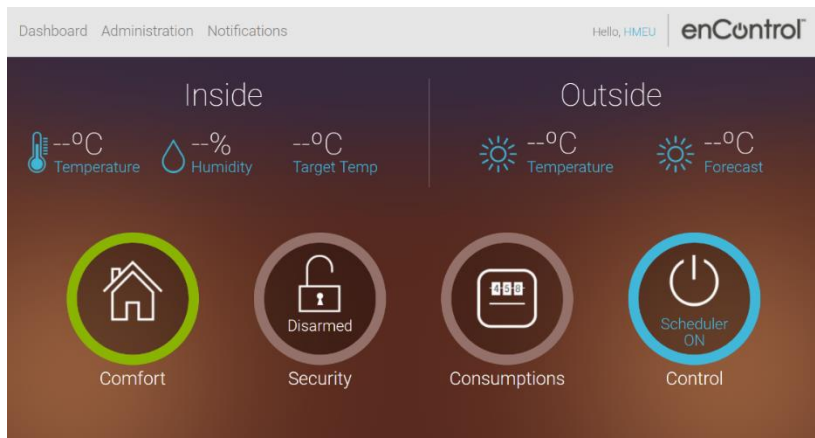


Figure 5: UI Dashboard

enControl will not always show one device as a single item, for example a Z-Wave device with 2 identical endpoints will appear as two separate items in all the relevant views (the automatic naming after inclusion makes it easy to distinguish them, however the user can change their names independently).

enControl does not allow to freely send any command to any Z-Wave device present in the network, however it provides the capability to send all the relevant commands associated to a specific device while automatically

handling some of the command classes that do not require user intervention, for example for a Switch device enControl will provide ON/OFF controls and meter readings.

There are four main interfaces to handle Z-Wave devices and their interactions, Control, Comfort, Security and Devices.

3.1 View Devices

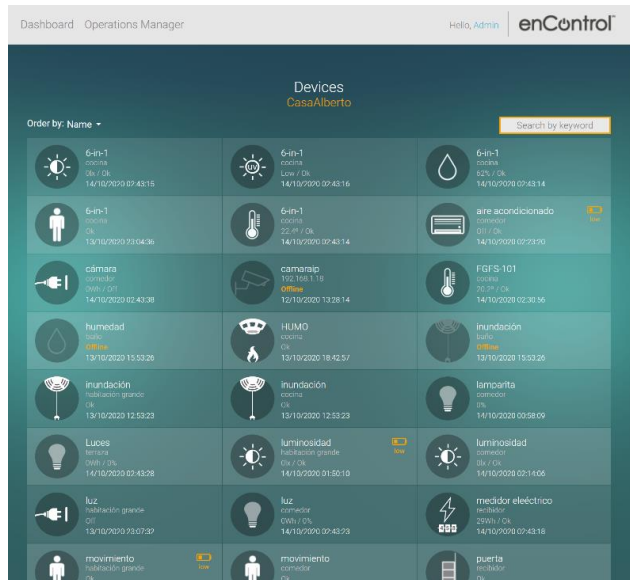


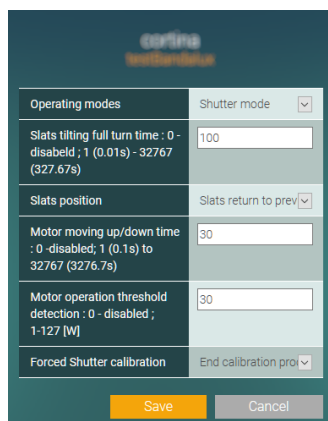
Figure 6: UI Device view (sensors)

This section is accessible from the top-level menu (when logged in as regular user) “Dashboard” -> “Devices”.

It provides an overview of all included Z-Wave devices, it will show an icon depending on the device type (for known¹ devices) and all relevant information. It does not provide means of interaction with devices.

For battery operated devices, it will show yellow battery icon when the device has issued battery low message or (for old devices) when battery is below a certain level (as indicated by the manufacturer).

Most of the information shown in this view is automatically updated, however in case of doubt just refresh the view.

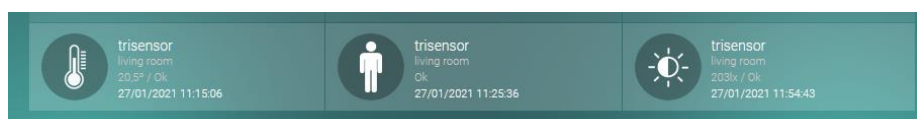


By clicking on each device, the user can access historical information and device configuration.

Left figure shows device configuration for Qubino Shutter. The UI provides access to selected configuration registers of the device for user personal configuration.

Why I see more icons than physical devices?

Some manufacturer product includes more than one sensor or actuator per device, if so, each sensor or actuator will appear in devices view separately (also in the other views). For instance, a product with Movement, Temperature and Lux sensors, will appear in this view as 3 separate devices (sensors) as can be seen in following capture.



¹ Unknown devices are those devices that have not been included in service data base. They will appear with “?” icon. They will be operable with required functionality.

3.2 View Control

This section is accessible from the top-level menu (when logged in as regular user) “Dashboard” -> “Control”. It provides an overview of most “actionable” Z-Wave devices, it will only show devices that can receive actions from the user (for example a binary switch will be shown here but not a temperature sensor).

The only “actionable” sensors excluded from this view are comfort related devices (such as thermostats and airco controllers), the only exception would be for devices detected as “unknown” that are not included in any of the supported Home Control Groups, then they will be shown in this section even if they are comfort related devices (with the minimum control widgets available).

To send a command to a specific device, just use the intuitive widgets provided by the UI (it will show all the relevant controls such as binary switches or sliders). Additionally, it provides BASIC GET/SET capabilities for Pc Controller which is useful for some of the tests.

Most of the information shown in this section is automatically updated via WebSockets, however in case of doubt just refresh the view.



Figure 7: UI control view

Devices supported that will be shown in this view are:

- 1) On/Off Switches
 - a. Plugs
 - b. Relays
- 2) Lights
 - a. On/off
 - b. Dimmable
 - c. RGB
- 3) Curtain shutters
- 4) Door locks
- 5) Sirens

3.3 View Comfort

This section is accessible from the top-level menu (when logged in as regular user) “Dashboard” -> “Comfort”. It provides an overview of comfort “actionable” Z-Wave devices, so mostly thermostats and airco controllers, it provides means of access to the device capabilities, unavailable options would be disabled in the UI (for instance the UI will disable “cool” mode for thermostats unable to manage this mode)

Since enControl does some automatic actions whenever more than one “comfort” device is included in the system, we recommend testing the network when only one is present, otherwise the interface will only show the “main” thermostat (or airco controller) and the “secondary” devices will have their UI available under “Areas” subsection, changes to the “main” thermostat might end up changing some of the “secondary” devices.

Most of the information shown in this section is automatically updated via WebSockets, however in case of doubt just refresh the view.

“Areas” section in the UI will show (grouped) virtual sensors (like temperature, humidity, etc.) per home room (= area). In such a case, by clicking each one, a plot view will show each sensing value separately, otherwise only one sensor plot will be shown. To view sensors ungrouped, devices must be assigned to different areas².

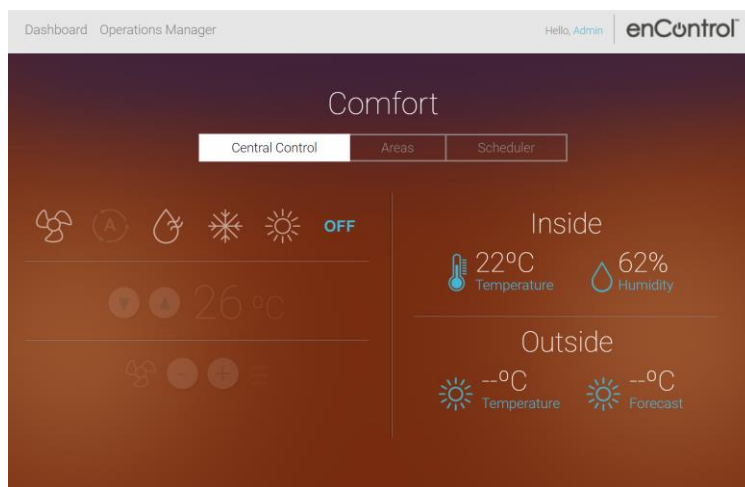


Figure 8: UI Comfort view (central control)



Figure 9: UI Comfort view (areas)

Devices supported that will be shown in this view are:

- 1) Thermostats (actionable) - (the UI will enable controls for those modes supported by the device)
 - a. Target temperature
 - b. Thermostat mode
 - c. Manage ventilation level
- 2) Various sensors
 - a. Temperature
 - b. Humidity

² A Z-Wave device included in the network is always assigned to “default area”.

- c. Lux
- d. CO2 levels
- e. Ultraviolet

3.4 View Security

This section is accessible from the top-level menu (when logged in as regular user) “Dashboard” -> “Security” and within the section, view “Devices”. It provides an overview of security/safety status of the installation and includes Z-Wave devices info, so mostly magnets, movement detectors, smoke detector, CO detectors, flood detectors, etc.

An intuitive UI is provided according to the device capabilities showing information about the devices. (for example detections)

Most of the information shown in this section is automatically updated via WebSockets, however in case of doubt just refresh the view.

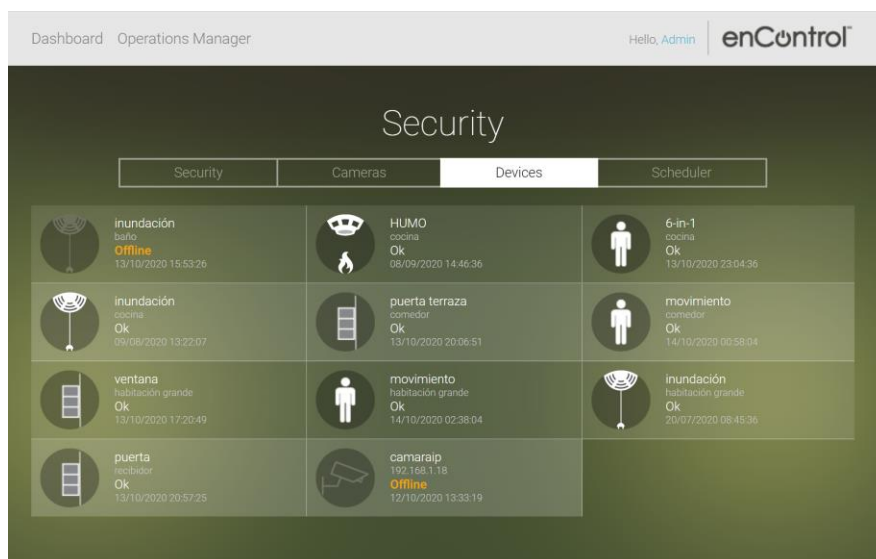


Figure 10: UI Security view

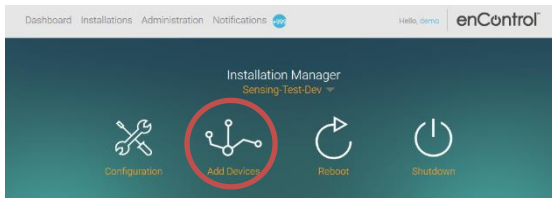
Devices supported that will be shown in this view are:

- 1) Magnetic sensor (door/window sensors)
- 2) Movement/presence
- 3) Water leakage
- 4) CO
- 5) Smoke

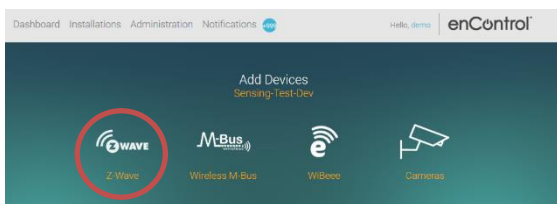
4. Inclusion and exclusion of a Z-Wave Device

4.1 Inclusion

You can access this view selecting “Administration”->”Installations” menu option.



Click in the “Add Device” Icon, a screen shown different protocols will appear (see below).



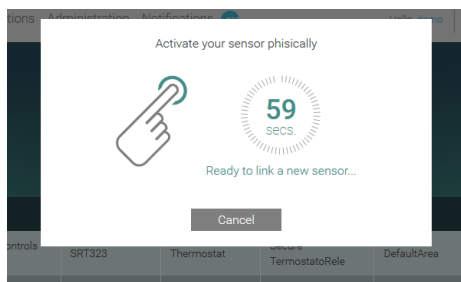
Click Z-Wave icon



To start inclusion, click the “+” icon.

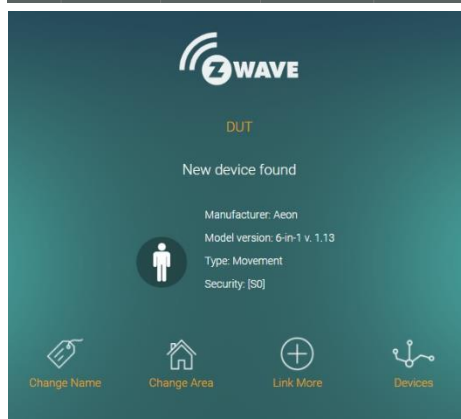
The System will guide you through the process, please follow the instructions online.

4.1.1 Unsecured & S0 device



The System will wait for you to activate the device that you want to include in the installation.

Follow the instructions of the manufacturer to know how to initiate the inclusion and how to wake up.



Once the system successfully includes the device, you will get the information of the device as shown on the left capture.

On this screen, you can:

- 1) Assign device name
- 2) Assign area
- 3) Add another device
- 4) Go into view of all the devices

4.1.2 S2 device

In case you are linking a S2 devices, the link process will pop up a window for you introduce the DSK of the device. The window will be visible for certain period as shown in the next capture.

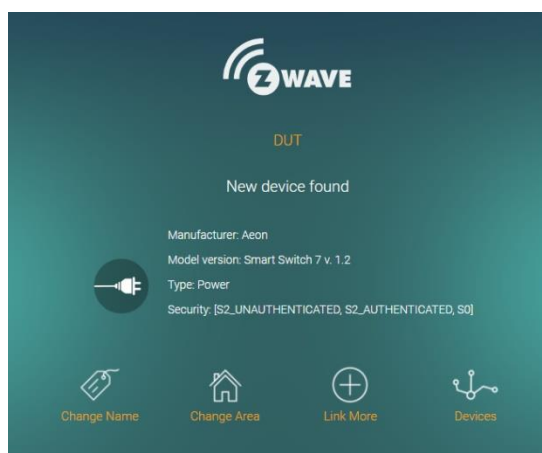
Before proceeding, read device manual about the link process.

Locate DSK in the device itself or in the device's box.

Be sure if the DSK provided is written in decimal (default) or hexadecimal format. In the second case, select "hex input".

Enter the 5-digit code and press confirm.

In case a device that does not need PIN confirmation (for type S2 Unauthenticated), the windows will show device DSK information so the DSK can be compared against device being linked.



Follow the instructions on the web page and wait for the device to be displayed as shown in the next capture.

Once the system successfully links the device, you will get the information of the device as shown on the left capture.

On this screen, you can:

- 1) Assign device name
- 2) Assign area
- 3) Add another device
- 4) Go into view of all the devices

4.1.3 SmartStart device

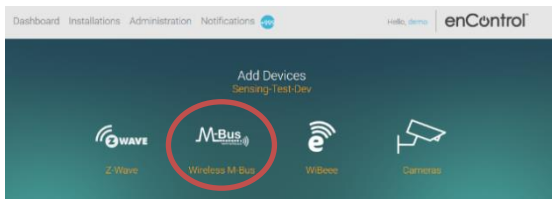
SmartStart is designed to facilitate the inclusion of multiple devices simultaneously by storing unique Device Security Keys (DSK) in the hub. This ensures that the Gateway is ready for error-free, and uniform inclusion

across all device types and brands with secure S2 security framework before the device is even powered on for the first time.

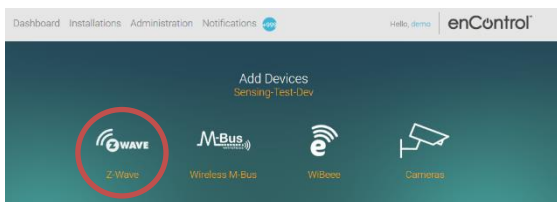
The automatic inclusion will be enabled when added the device DSK in the DSK provisioning list of the GW. The procedure is explained in section 6.2

4.2 Exclusion of Z-Wave Device

In order to remove a Z-Wave device from your network navigate to “Administration”->”Installations” menu option.



Click in the “Add Device” Icon, a screen shown different protocols will appear.



Click Z-Wave



To start removing devices, click the “-” icon. After that just set your Z-Wave device in exclusion mode (see device’s user manual, sometimes it’s also called learn mode).

The System will guide you through the process, please follow the instructions online.



When the process completes the timer will disappear and a message will confirm successful removal (only if the device previously belonged to your Z-Wave network).

4.2.1 SmartStart device

Before removing a SmartStart device, you should consider whether the device is in the DSK provisioning list of the GW. Having the device in the DSK provisioning list, upon removing from Z-Wave network (following procedure explain in section 4.2), the device may be included automatically back to the Z-Wave Network.

Section 6.2 explains how to manage the gateway device DSK provisioning list.

4.3 Remove failed device

To make it easier for the user, the “delete” action for failed devices is only shown when the device has been detected as failing (so it will have the “offline” status). To access the feature from the “Devices” section, just click on an item (if they belong to the same Z-Wave device it’s not important which one you choose), a menu with some options will appear, one of them being a paper bin (only if the sensor is detected as failing), use it to trigger the “Remove failed” Z-Wave functionality.

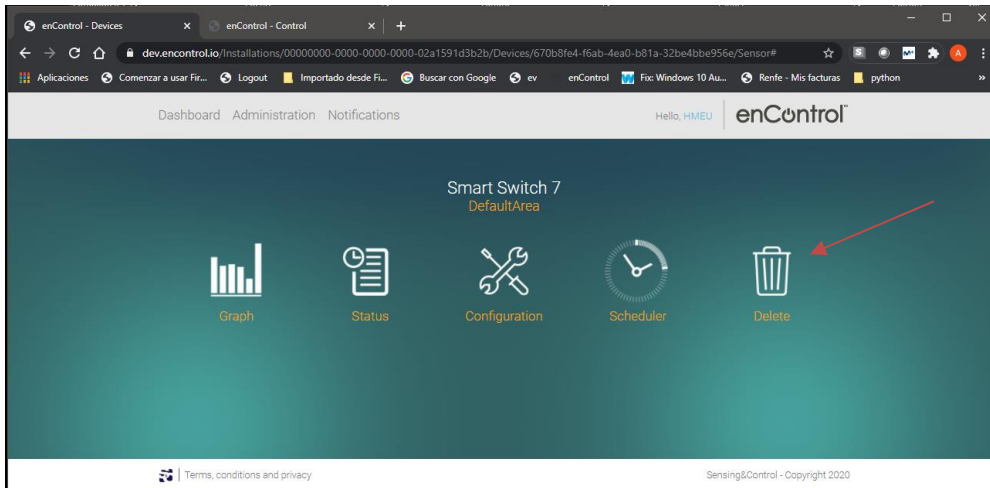


Figure 11: Removing failing device

If the tester prefers not to wait for the item to be detected as failed, the same command can be triggered from the view (even if the paper bin does not appear), just open the JavaScript developer console and type “deleteSensor();” and press enter.

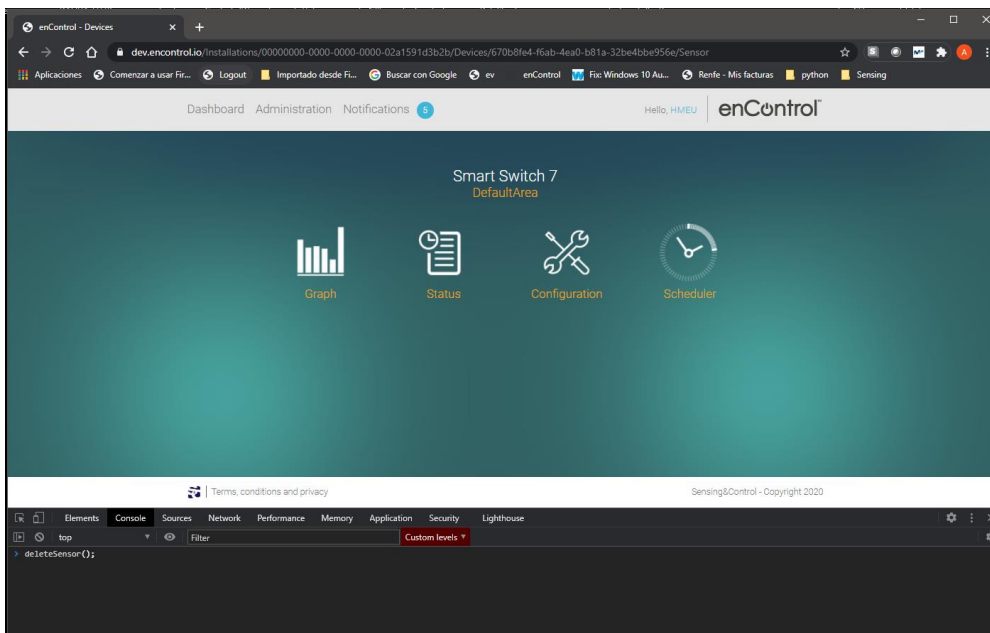
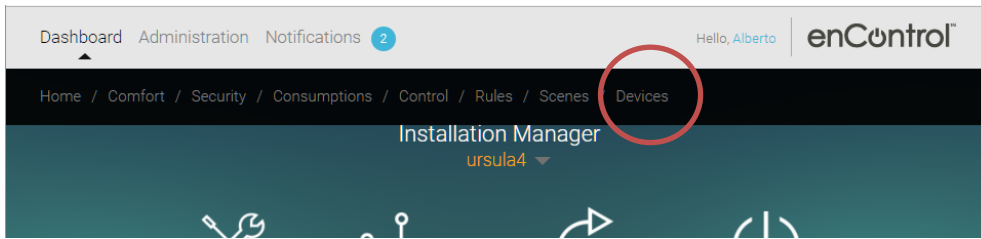


Figure 12: Removing non failing (online) device

5. Device Configuration

The device configuration through device option in the main menu.



The system will redirect you to the next screen, where all devices will be shown.

For each device, you can:



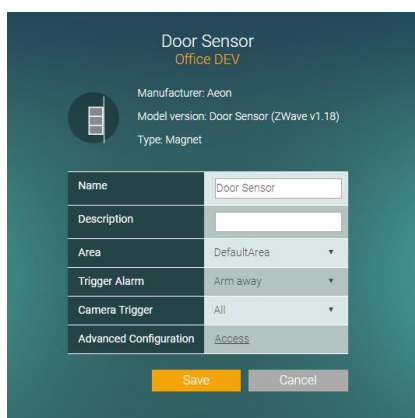
1. Know whether the device is online or offline (the device that does not communicate is labeled "offline").
2. You can know the date of last communication between the gateway and the sensor.
3. Clicking on it you will be directed to the configuration view as next figure



You will be able to:

1. Plot graphs of historical values
2. See history of sensors (on, off, detect, offline, etc....)
3. Configure the device
4. Delete (this icon only appears if it is marked offline). IP-connected devices (such as cameras) can be deleted from the add devices screen.

By clicking “Configuration” you will be able to access the configuration view for this device. For instance, for a magnetic sensor you will have following options:



- 1) Change name
- 2) Change area
- 3) Access advanced configuration

The platform preconfigures the devices automatically, so you don't need to worry about configurations. However, you may need sometimes to adjust some parameters. To do so just click on “Access” link on the Advanced Configuration row.

Depending on the device, the view can show up more or less rows.

5.1 Configuration parameters for security devices.

For a security device, you will be able to configure:

- 1) Alarm trigger

- a. Magnets, movement type: You can choose if an alarm is raised upon detection by device (movement or door/windows opens) when the system is in: Arm, Partial or Disarm state. By default, this type of devices is set to trigger an alarm when the system is in Arm state.
 - b. CO, Smoke, Water leakage type: Same as before, but these devices will trigger an alarm when the system is disarmed by default.
- 2) Alarm delay: allows you to delay the trigger of an alarm. Upon completion of this delay, if the sensor has return to OK status (from DETECT status) the gateway will not send the alarm to the service.
- 3) Decide if an alarm of this sensor will active your siren(s) installed. By default, yes.

Particular options for different devices can be found under “Advanced Configuration”. For instance, Fibaro’s smoke sensor allows you to select the sensitivity of the device.

5.2 Configuration parameters for energy meter devices.

For meter devices, you will be able to configure:

- 1) Electricity
 - a. Consumption category
 - i. Decide if the device is the main meter of the installation.
- 2) Gas, water
 - a. Decide if the device is the main meter of the installation.

5.3 Configuration parameters for comfort devices

For comfort devices, you will be able to configure:

- 1) Thermostat
 - a. Select type and/or configure control codes (for AC IR Remotec)
 - b. Select device as main Thermostat.
- 2) Temperature sensors
 - a. Temperature compensation

5.4 Configuration parameters for control devices.

For a control device, you will be able to configure:

- 1) Lights
 - a. Type of switch
- 2) Curtains/shadows
 - a. Type (normal, venetian)
 - b. Calibration

6. Z-Wave advance actions

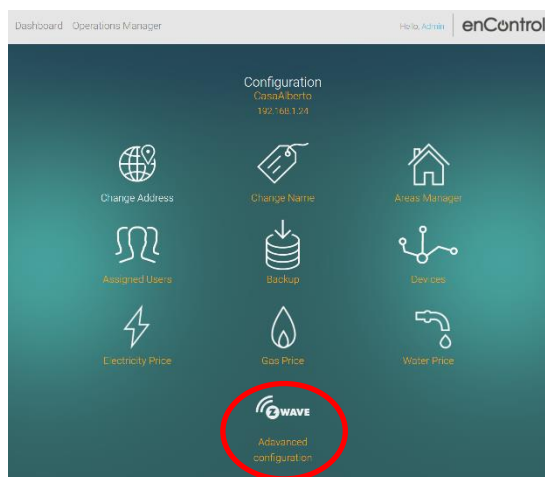
Click on the Administration menu, then installations.



Once inside installations, select configuration.



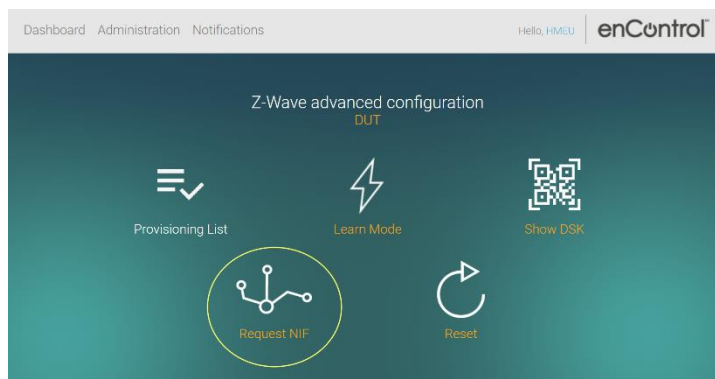
From Configuration view you will be able to access Z-Wave advance configuration options.



From where you will be able to:

- 1) Deal with learn mode
- 2) Manage Provisioning list
- 3) Show DSK
- 4) Request NIF
- 5) Default RESET of the GW.

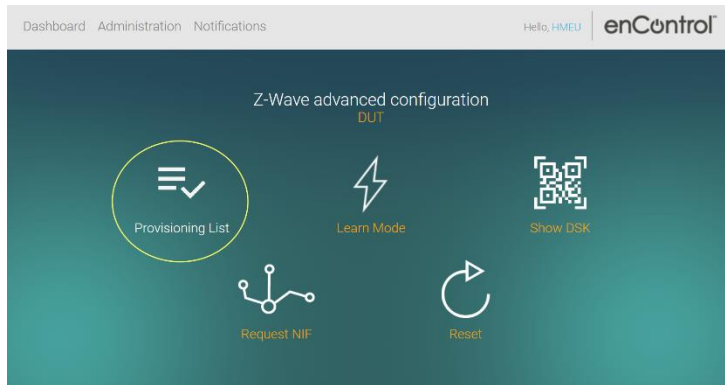
6.1 Send NIF



A send NIF action can be triggered on demand. When logged, navigate to Administration / Installations in the top-level menu and click on Configuration. Once in the configuration menu, click on Z-Wave advanced configuration. Select “Request NIF”, this will trigger a report from the Z-Wave controller (unless it’s already performing some other network management action, since we’re using Z/IP Gateway which only allows one network management action at a time).

Figure 13: request NF

6.2 Node provisioning for smart start



Smart Start is designed to facilitate the inclusion of multiple devices simultaneously by storing unique Device Security Keys (DSK) in the hub. This ensures that the Gateway is ready for error-free, and uniform inclusion across all device types and brands with secure S2 security framework before the device is even powered on for the first time.

Figure 14: Provisioning List

A pop-up window will appear (in the example with some DSK already included in a gateway) for Provisioning List management:

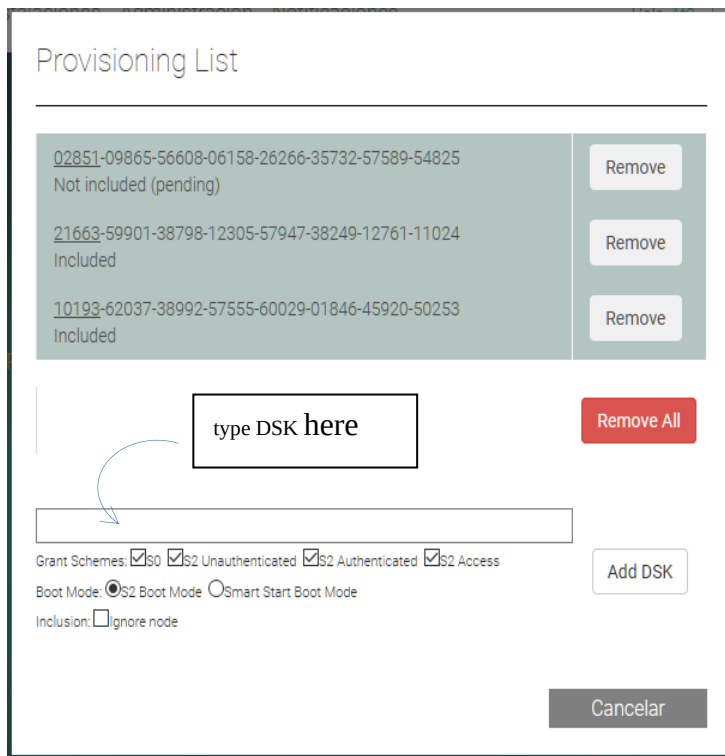


Figure 15: Provisioning list management

A DSK will be added into the provisioning list typing the DSK then by clicking “Add DSK” button. You should specify which security schemes would like to be used for the device (we recommend leaving as default) and whether the device is SmartStart capable or not (consult manufacturer documentation).

For SmartStart capable device ensure you do not unselect the SmartStart Boot Mode button (default option).

For S2 compatible devices without SmartStart, consult the original manufacturer documentation.

When adding a DSK of a non SmartStart device, the GW will inform you that you must proceed with manual inclusion (as explained in section 4.1.2). A smart start device will be added automatically into Controllers Z-Wave network upon power up.

After adding a DSK. The DSK will appear in green area, and the gateway will inform about the status of the device in the Z-Wave network as following.

- Not included (pending) - The node will be added when it issues SmartStart Inclusion requests or is added manually following manufacturer inclusion procedure.
- Included – The node has been already included in the Z-Wave network.
- Not included (pending) Ignored - SmartStart Inclusion requests are ignored unless changed by controller.

“Remove” button will remove the device from the provisioning list, while “Remove all” will remove all devices from provisioning list. Removing the device (or devices) from the provisioning list does not mean the device is removed from the Z-Wave network. You must follow manufacturer instructions to manually exclude the device (section 4.2 explains how to exclude devices from the Z-Wave Network)-

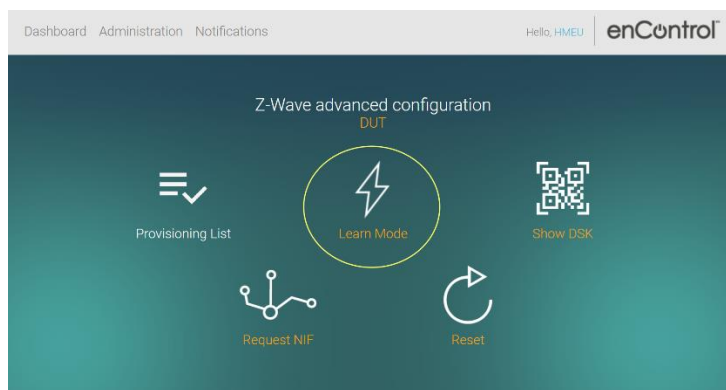
Keeping devices in the provisioning list allows them to be factory reset or excluded. They will automatically be included in the Z-Wave network again if they have power.

6.3 Learn mode

This performs the Z-Wave Set Learn Mode network operation. This can be performed when; (i) the gateway is not in a network and will typically make the gateway an Inclusion or Secondary Controller, in which case, some of its facilities will not be available, and (ii) when the DUT is part of a network (for exclusion of the DUT if it is not SIS).

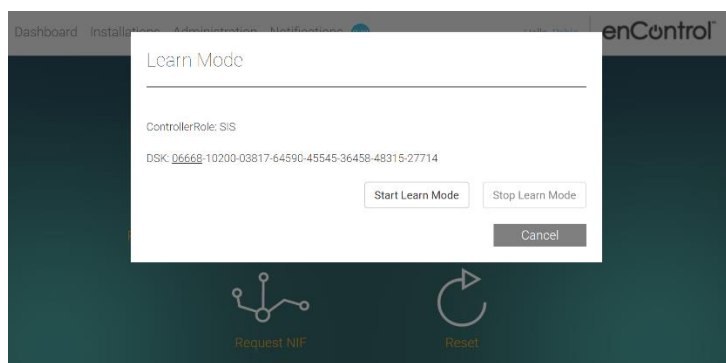
6.3.1 Inclusion of controller into an existing network

To include this controller into a Z-Wave Plus™ S2 primary controller. You will need to follow next steps. First, you have to enable Z-Wave Inclusion mode on the Z-Wave Plus S2 primary controller, so devices may be added its network.



Then click Learn Mode on Z-Wave advance configuration view.

Figure 16: Learn mode



Click “Start Learn Mode” to initiate the inclusion.

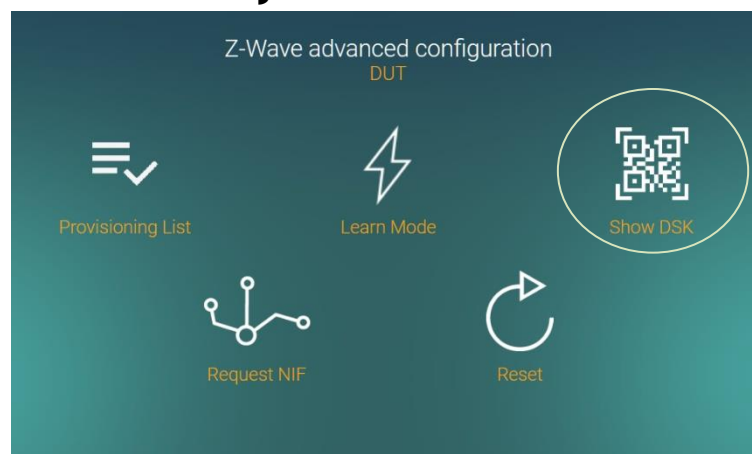
Leave all security modes enabled on the primary Z-Wave Plus S2 Controller. To complete an S2 inclusion, type the first segment of the DSK shown when prompted from the including Controller.

Figure 17: Learn mode interface

When successfully added, network information from the primary controller will be replicated on this controller.

To include this controller into a Z-Wave Plus no capable S2 primary controller, the procedure is the same, but you will not need to enter DSK information as you will not be prompted to do so.

6.4 Gateway's DSK



This will show the unique Device Security Key of the gateway.

Figure 18: Show GW dsk

6.5 Reset

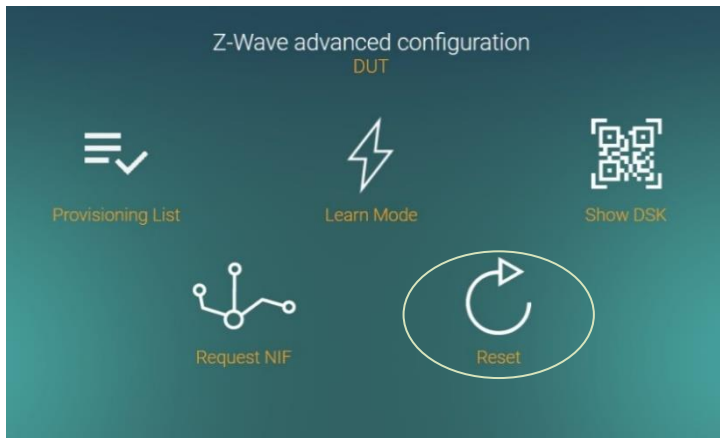


Figure 19: GW default reset

This factory resets the gateway:

- 1) Removes all Z-Wave device
 - a. from the Gateway
 - b. from the installation.
- 2) Resets Z-Wave Module

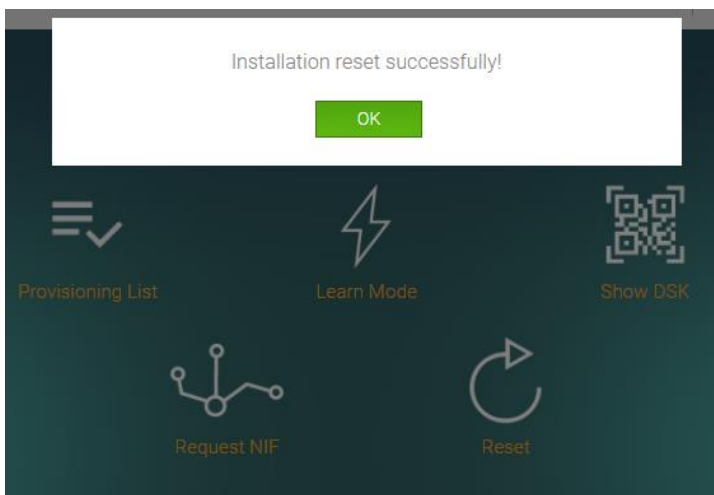


Figure 20: Notification of finalisation of reset procedure.

The UI will notify a successful reset by a pop-up window when this procedure is finished by the GW.

The gateway will reboot and will be ready for new interactions after a side message is shown in the UI (independently of the view) as following: **“InstallationName is initialised”**

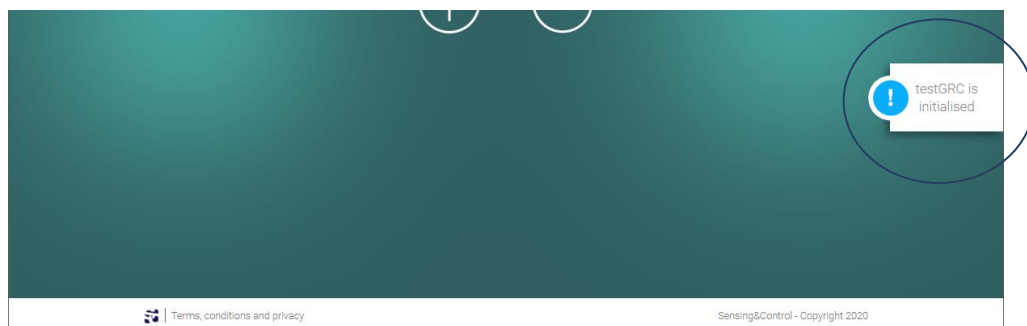


Figure 21: GW connected to service and ready for interaction.

May you find UI is not responsive right after this message. Just wait around 5 to 10 seconds afterwards.

7. Z-Wave Network

7.1 Devices and manufacturers

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

7.2 Associations

There is only 1 Association group, supporting 1 node for Lifeline. This node will receive the Device Reset Locally Notification command when the device is reset to default.

7.3 Devices support and S2 Security.

This product can control/monitor Z-Wave-certified devices of different categories from various vendors through their CCs. CCs that are automatically handled are not exposed to the user.

The Gateway supports the following CCs:

Table 1: CCs supported

Command Class	Version	Required Security Class
APPLICATION_STATUS	1	None
ASSOCIATION	2	Highest granted
ASSOCIATION_GRP_INFO	3	Highest granted
CRC_16_ENCAP	1	None
DEVICE_RESET_LOCALLY	1	Highest granted
FIRMWARE_UPDATE_MD	5	Highest granted
INCLUSION_CONTROLLER *	1	None
INDICATOR	3	Highest granted
MANUFACTURER_SPECIFIC	2	Highest granted
MULTI_CHANNEL_ASSOCIATION	3	Highest granted
MULTI_CMD	1	None
NODE PROVISIONING	1	Highest granted
NW_MGMT_BASIC	2	Highest granted
NW_MGMT_INCLUSION *	3	Highest granted
NW_MGMT_INSTALLATION_MAINTENANCE	2	Highest granted

NW_MGMT_PROXY	3	Highest granted
POWERLEVEL	1	Highest granted
SECURITY	1	None
SECURITY_2	1	None
SUPERVISION	1	None
TIME	1	None
TRANSPORT_SERVICE	2	None
VERSION	3	Highest granted
ZWAVEPLUS_INFO	2	None

* INCLUSION_CONTROLLER & NW_MGMT_INCLUSION CCs are only present if the Gateway role is inclusion controller.

7.4 Basic command class

This product does nothing on receiving Basic CC Set or Get.

This product controls “unknown” devices using Basic CC Set and Get through controls provided in the user interface (through ‘Control’ interface, section 3.2).

7.5 Controller replication

Controller Replication is the process of updating network information from a primary controller to secondary controllers, such as node list and routing information. These steps are usually not required unless you have a multiple controller network. To initiate this process, start the Add Mode on the primary controller and the Learn Mode on the secondary controller. All Z-Wave network relevant information will be updated for the secondary controller.

8. Trouble Shooting

Ensure the GW is connected to service, i.e., the only BLUE led is on. If other leds are ON, the GW may be busy or unconnected from/to cloud the service. Figure 1 provides information about its current state, and will help you to fix problem related. In any case, product support will inquire you about which leds status if not possible to connect to gateway remotely.

May you find UI is not responsive after power up, reboot or reset? Just wait around 5 to 10 seconds when GREEN led switches off.

If you have a problem with a device, locate the problem in the troubleshooting list below and take the corrective actions indicated. If the problem persists, contact your dealer.

Table 2: troubleshooting

PROBLEM	POSSIBLE CAUSES	SOLUTION
The gateway does not work	No electric current	Check the connections to the network. Check that the power LED (blue) is lit.
	Not connected to the network	Verify that the gateway is on your local network Verify that the green led of the Ethernet cable flashes
	There is no Internet	Using a computer, tablet or phone, verify that you have internet access by connecting to the same router that your gateway is connected to
I cannot include / exclude Z-Wave devices.	The device is away from the Gateway	Try as close to the gateway as possible
	The device has no batteries	Check the batteries and replace if necessary. Try again with charged batteries.
	The device is not recognized	Contact your service provider by sending details of the device you want to add