SNP-C19033

Z-Wave™ Mini Gateway User Manual

Document Revision v1.2

This document is property of VISION AUTOMOBILE ELECTRONICS INDUSTRIAL

Content

SNP-C19033 1

Z-Wave Mini Gateway User Manual 1

1. Introduction 3

2. Quick Install 5

2.1 Setting Mini Gateway network configuration 5

2.2 IP address of Mini Gateway detection 6

3. Website Introduction 7

4. System Functions 7

4.1 Change Password 7

4.2 Change Time zone 8

4.3 Upgrade System Firmware 9

5. Scenes Functions 10

5.1 Add Scene Rule 10

5.2 Delete Scene Rule 12

5.3 Enable/Disable scene rule 12

5.4 Scene schedule 13

5.5 Scene task implement directly 14

6. Z-Wave Functions 15

6.1 Adding Device (Inclusion) 15

6.2 Remove Device (Exclusion) 17

6.3 Network Replication (Copy) 18

6.4 Network Update 18

6.5 Check a Z-Wave device 18

6.6 Replace a failed Z-Wave device 20

6.7 Remove a failed Z-Wave device 20

6.8 Request capability rediscovery 22

6.9 Including the Mini Gateway to an existing network (Learn mode) 23

6.10 Factory Default Reset 23

6.11 Device Event History 25

6.12 Add/Remove node to SmartStart List 26

6.13 Additional Information 27

7. Security Functionality 38

7.1 Setting Security Mode 38

7.2 Disable Security Mode 38
7.3 Setting the security mode detection devices 38
7.4 Turn off all sirens 39
8. Supported Z-Wave Device Classes 39
9. Supported Z-Wave Command Classes 40

1. Introduction

Thanks for choosing Mini Gateway. The product is designed primarily as a Z-Wave Gateway / Controller to work with other Z-Wave enabled devices.

This product can be operated in any Z-Wave network with other 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. It is suggested to place the product near your home Internet router. Before installing, please check that you have an available Wi-Fi and power socket in the desired location.

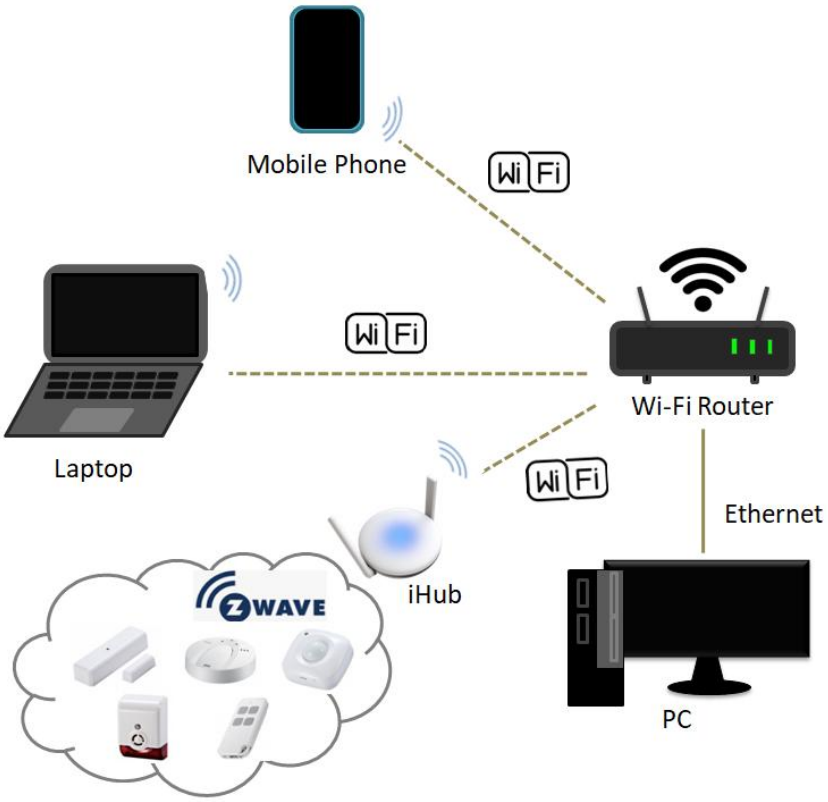


Figure 1: Network Diagram

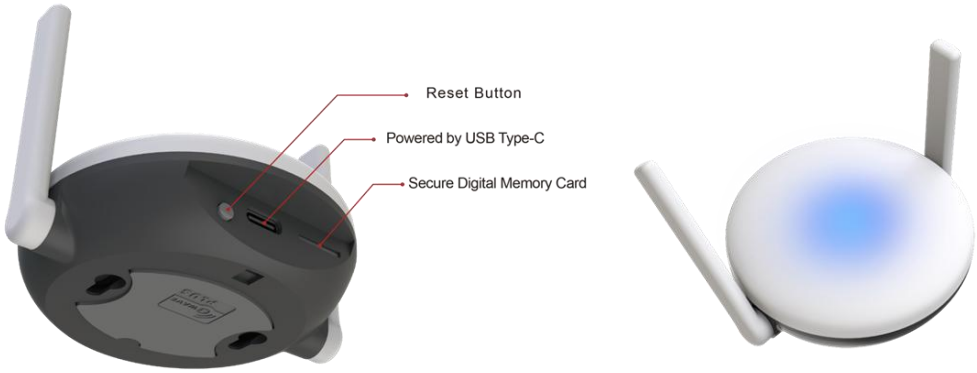


Figure 2: Mini Gateway Hardware Overview

Color	Status
Flashes green and blue	System is ready and the network is connected.
Flashes red and purple	Extranet is unable to connect.
Flashes blue	System is ready.
Flashes green	Extranet is connected.
Flashes red 2 times	System is restored to default WIFI setting .
Flashes red 5 times and then flashes yellow.	System is restored to factory default setting.

Table 1: Status of LED

2. Quick Install

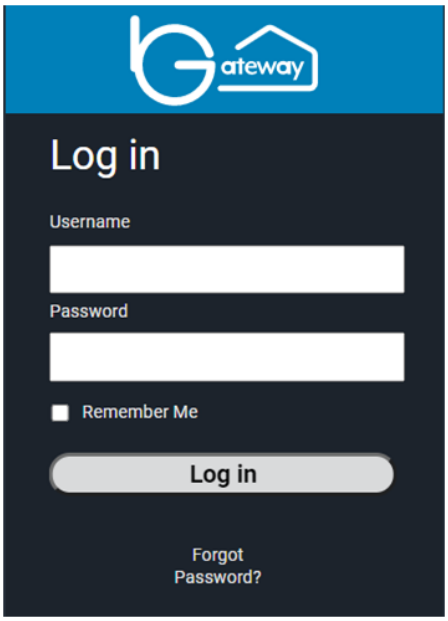
Before installing your Z-Wave network Mini Gateway please follow these steps to install your Mini Gateway:

Step 1: Plug in USB Type-C power to Mini Gateway.

Step 2: Connect the Mini Gateway Wi-Fi "VisionSensorHub_XXXXXX" via your laptop or mobile phone, the Wi-Fi password is **12345678**.

Step 3: Visit https://VisionSensorhub/index.html or https://192.168.109.1/index.html in your browser (Google Chrome/ Microsoft Edge).

Step 4: Log in the website of Mini Gateway, the default username is **root** and password is **1234**.



2.1 Setting Mini Gateway network configuration

If logging in the website successfully, please follow the steps to set up Wi-Fi for Mini Gateway.

Step 1: Select "**Network Configuration**" page.

Step 2: Choose "**Enable**" in SSID setting.

Step 3: Use to scan available owned Wi-Fi SSID and then key-in password to connect network.

Step 4: Confirm router information if correct and then click "Save" button. The system will be restarted, please wait a moment.

Step 5: If the network is connected successfully, the light of Mini Gateway will be blue and green.

Step 6: If the network is failed to connect, the light will be blue, please presses the reset button 6~10 seconds up to restore default configurations of Wi-Fi.

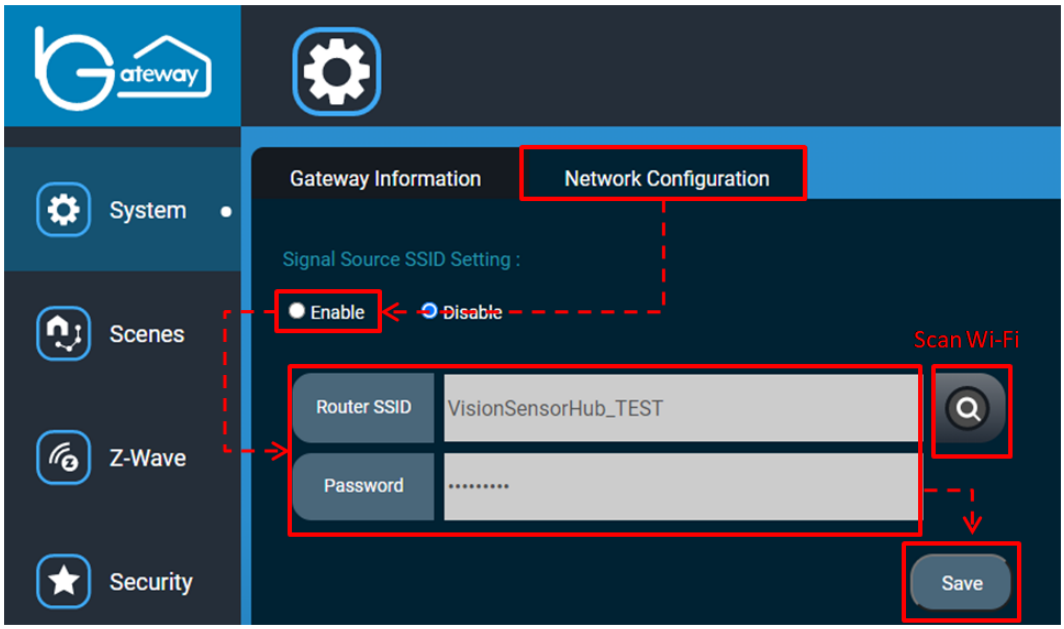
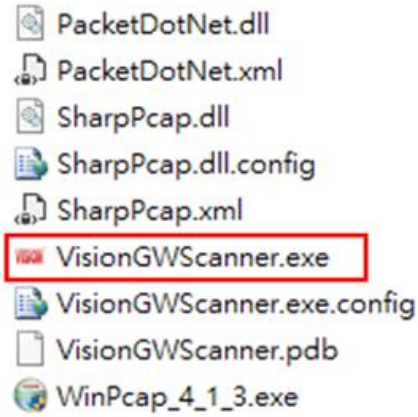


Figure 3: Setting Mini Gateway network steps

2.2 IP address of Mini Gateway detection

Please download GWScanner from http://www.visionsecurity.com.tw .

Step 1: Please lunch the GWScanner.exe in Windows environment of your computer..

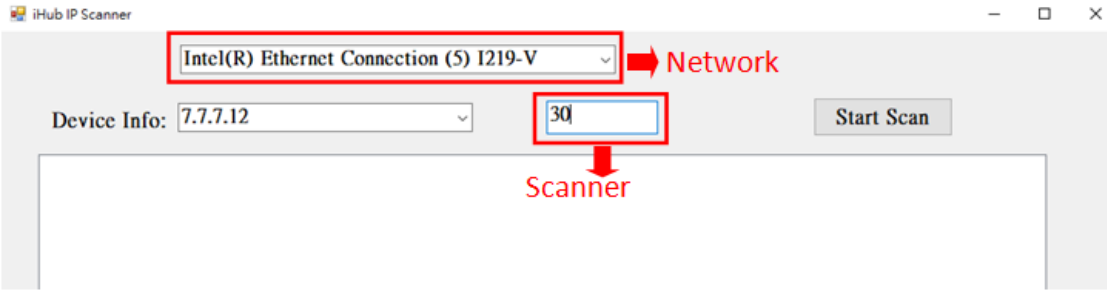


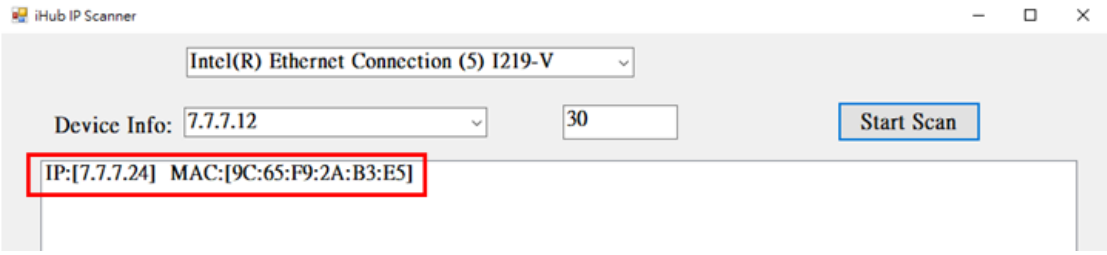
Step 2: Select your network interface.

Step 3: Select your device information and enter scanner range value.

Step 4: Click **"Start Scan"** button to detect the IP address of Mini Gateway.

Step 5: Visit the website of detected IP of Mini Gateway in your browser.





3. Website Introduction

The website has four main menus： “System”, “Scenes”, “Z-Wave” and “Security”.

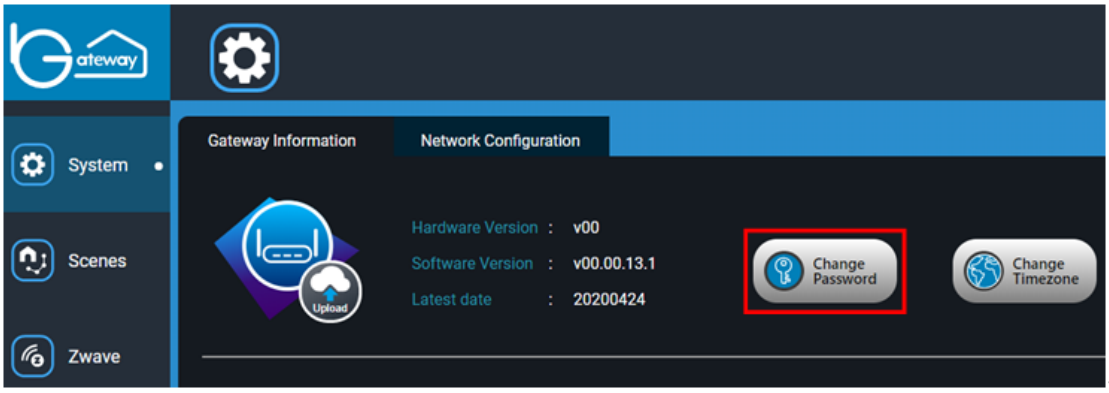
- “**System**”: displaying version of Mini Gateway, network information, time zone setting, and password change.
- “**Scenes**”: Users can customize the linkage between different devices.
- “**Z-Wave**”: displaying Z-Wave devices. User can control all devices.
- “**Security**”: Provides home security configuration.

4. System Functions

You can upgrade firmware, change password, change time zone and setting network.

4.1 Change Password

Step 1: Click the icon “**Change Password**”.



Step 2: Enter the current password in the first line.

Step 3: Enter the new password in the second line.

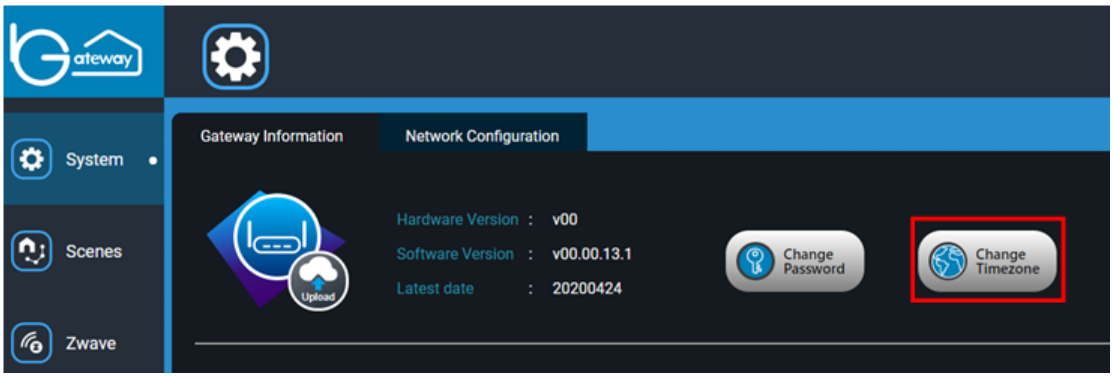
Step 4: Enter the new password again in the third line.

Step 5: Click "**Change**" button to save setting.

Step 6: If setting up successful, and then website will log out automatically.

4.2 Change Time zone

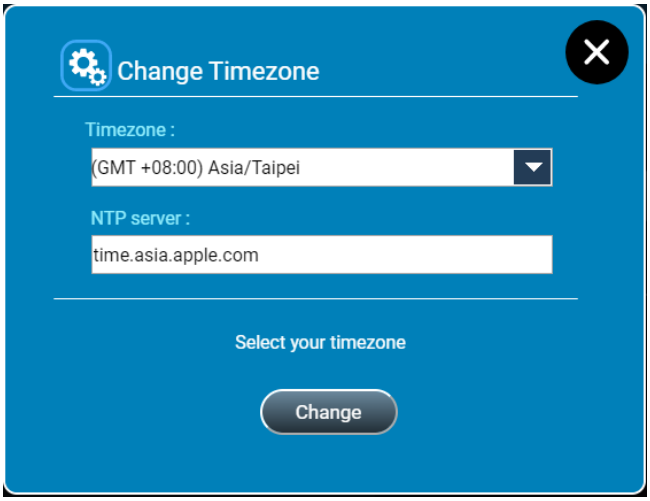
Step 1: Click "**Change Time zone**" button.



Step 2: Select your time zone.

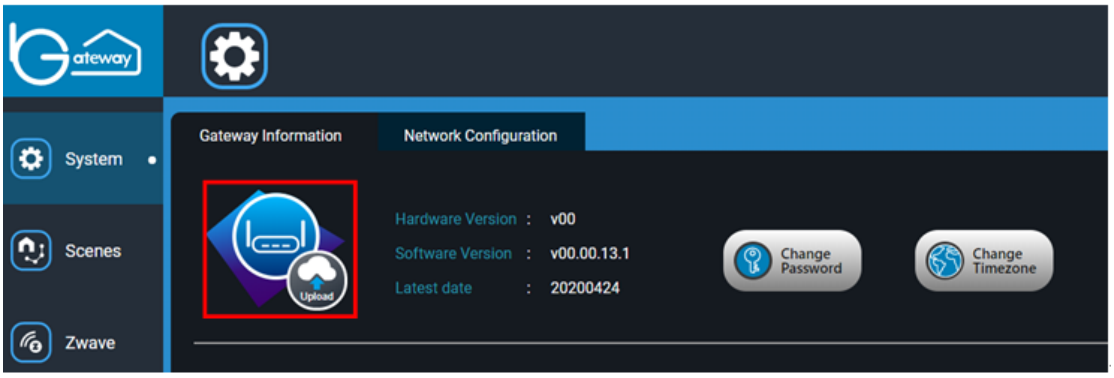
Step 3: Input the Network Time Protocol (NTP) Server if you want to calibrate the system time from network.

Step 4: Click "**Change**" button for save setting.



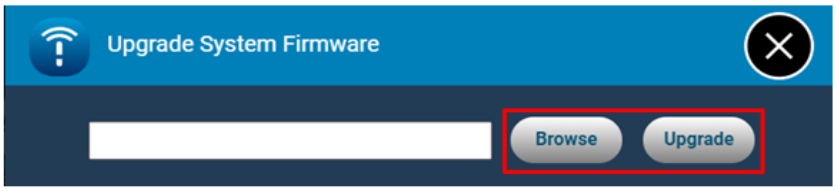
4.3 Upgrade System Firmware

Step 1: Click the "**Upload**" icon.

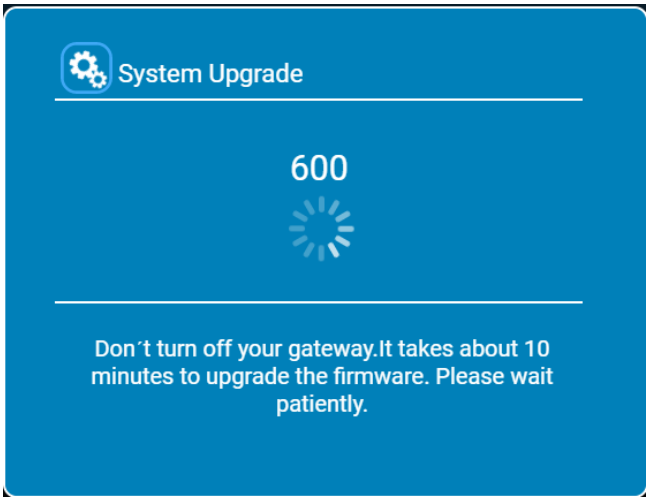


Step 2: Click the "Browse" button to select the firmware file (filename.bin).

Step 3: Click the "Upgrade" button to start upgrading firmware.



Step 4: Wait 600 seconds until upgrade finished.



If upgrading failed, please refresh the web page, and then back to the step 1.

5. Scenes Functions

You can integrate numbers of Z-Wave devices which can be executed by any of the following triggers:

- Events

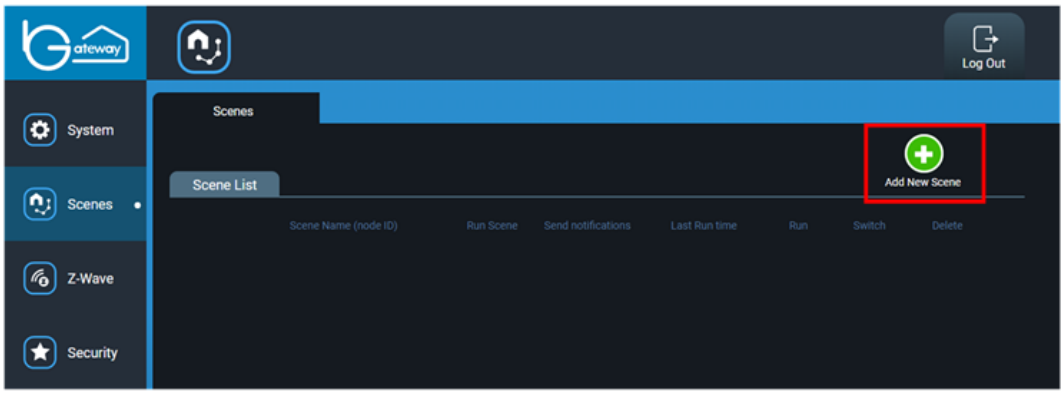
  The designated devices can be triggered by notification of another device.
- Schedule

  The designated devices can be triggered by preset time.
- Manual

  A user can manually execute a Scene by clicking “Run”.

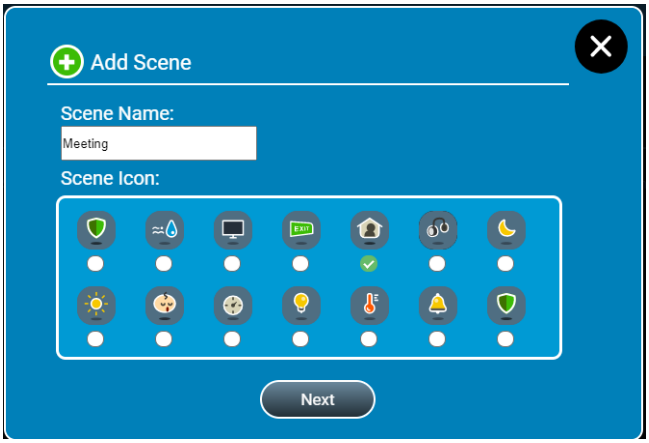
5.1 Add Scene Rule

Step 1: Click “**Add New Scene**” button.



Step 2: Enter scene name.

Step 3: Select scene icon and then click “**Next**” button.

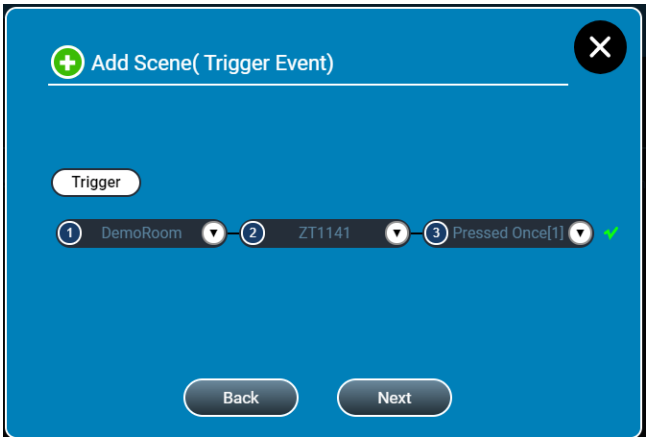


Step 4: Select location of trigger device.

Step 5: Select device of trigger event.

Step 6: Select event of trigger device.

Step 7: Click the "**Next**" button.

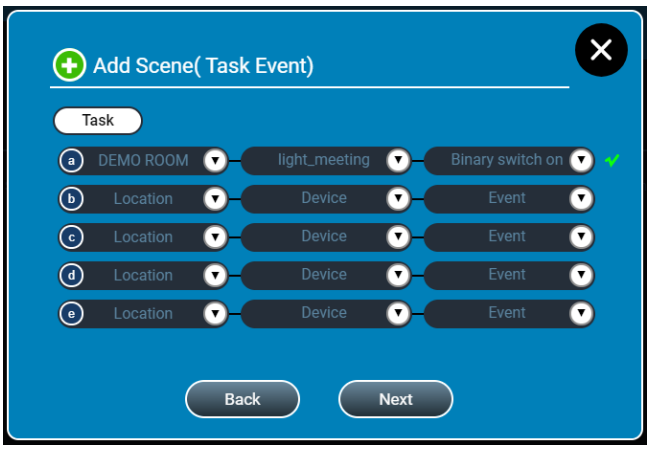


Step 8: Select location of task device.

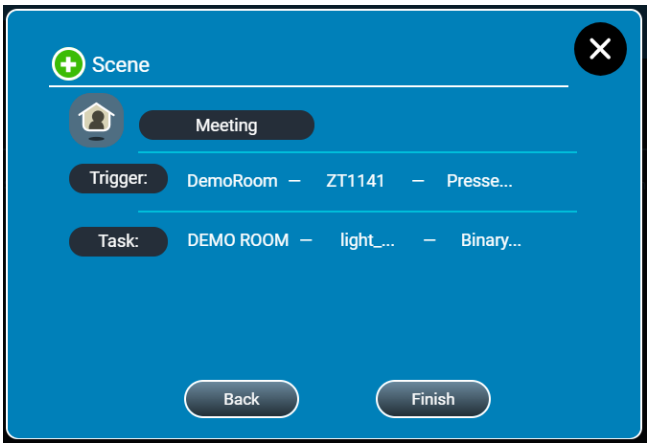
Step 9: Select device of task event.

Step 10: Select event of task device.

Step 11: Click the "**Next**" button.

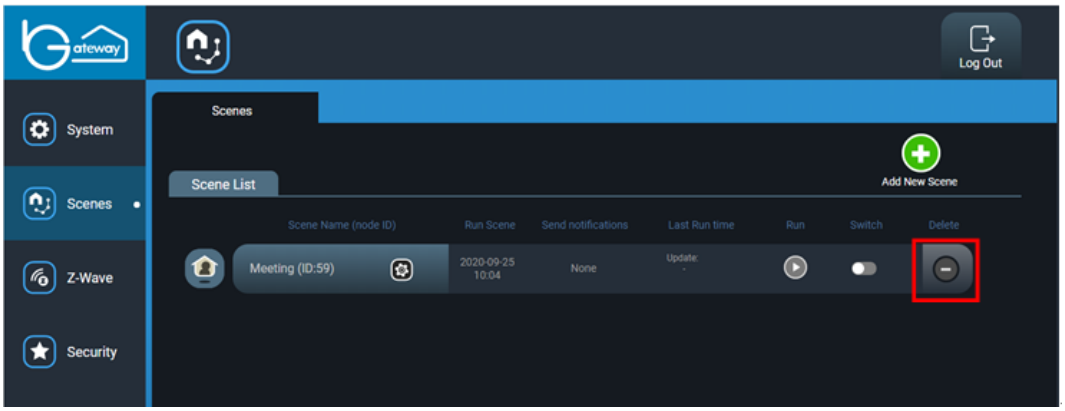


Step 12: Check information and then click the “**Finish**” button.

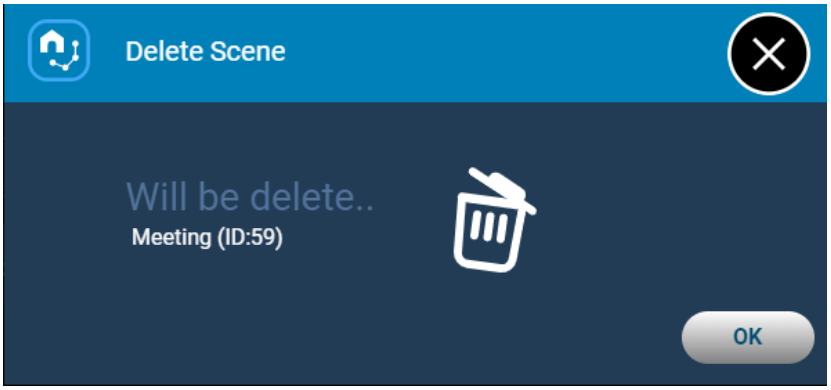


5.2 Delete Scene Rule

Step 1: Click the scene delete button.

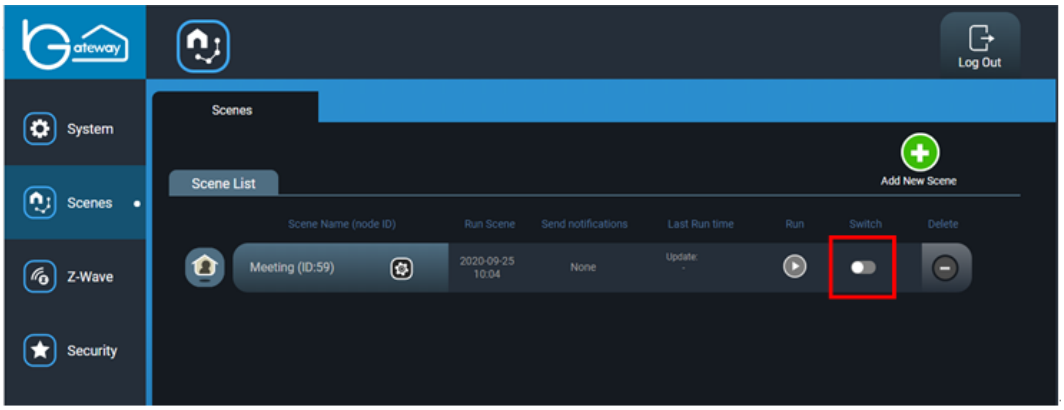


Step 2: Click the “OK” button.



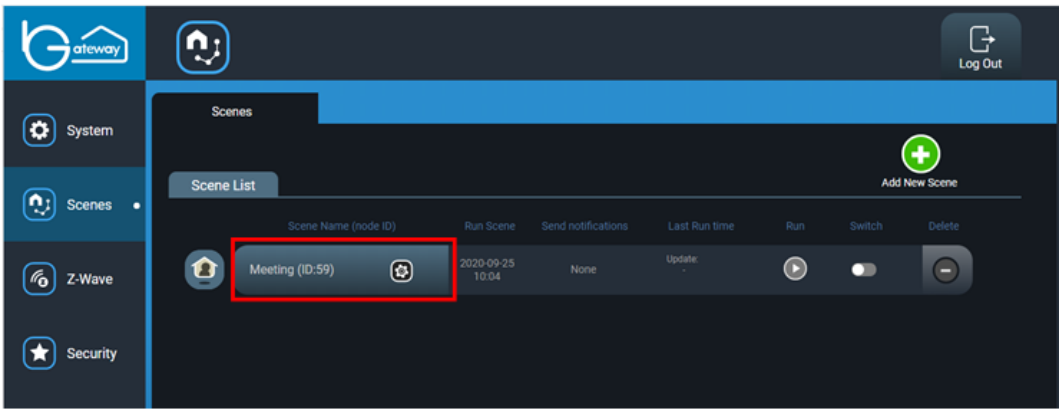
5.3 Enable/Disable scene rule

Step 1: Click the scene switch button.

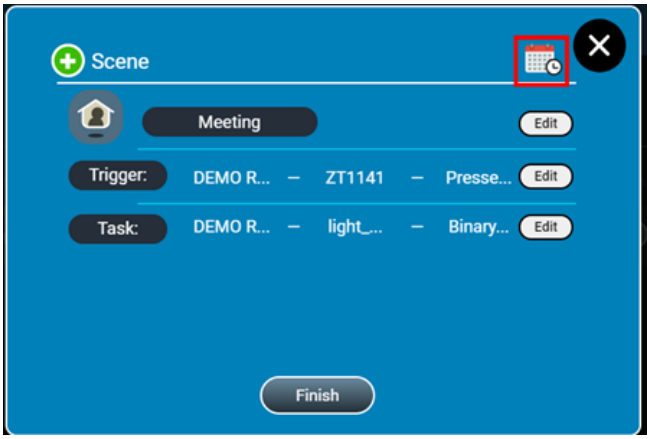


5.4 Scene schedule

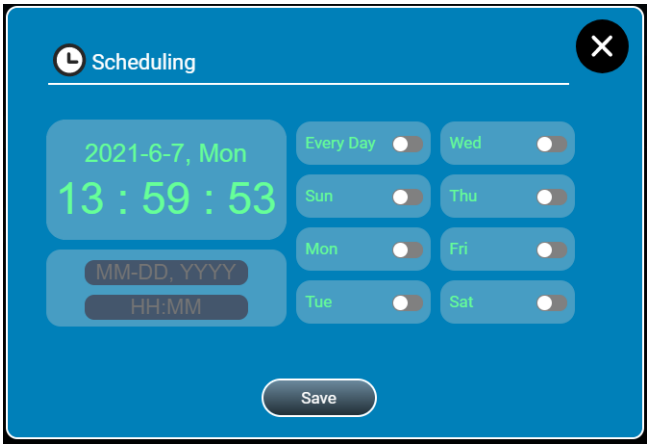
Step 1: Click the scene setting.



Step 2: Click the “schedule” icon.



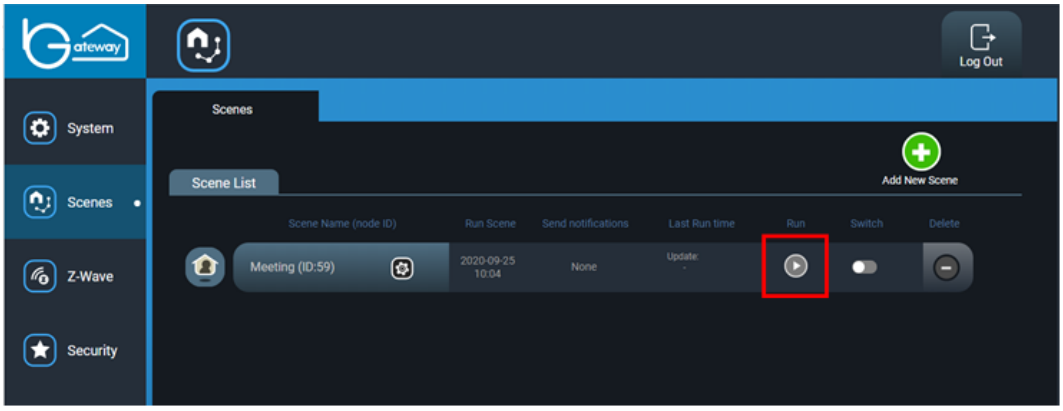
Step 3: Select date, time and repeat days.



Step 4: Click the "**Save**" button.

5.5 Scene task implement directly

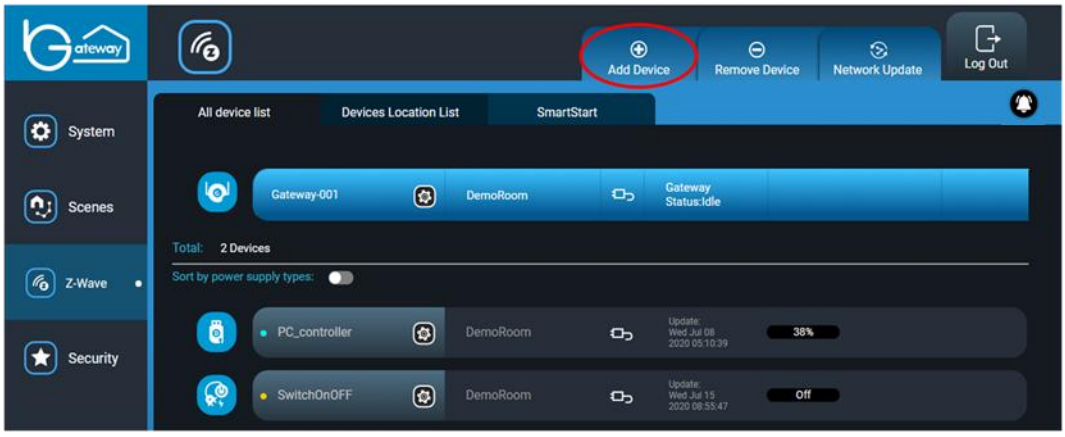
Step 1: Click the scene Run button.



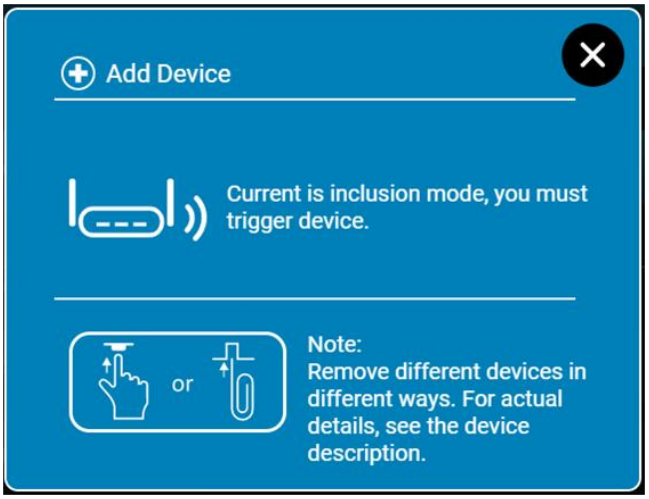
6. Z-Wave Functions

6.1 Adding Device (Inclusion)

Step 1: Click button "**Add Device**" on the website.

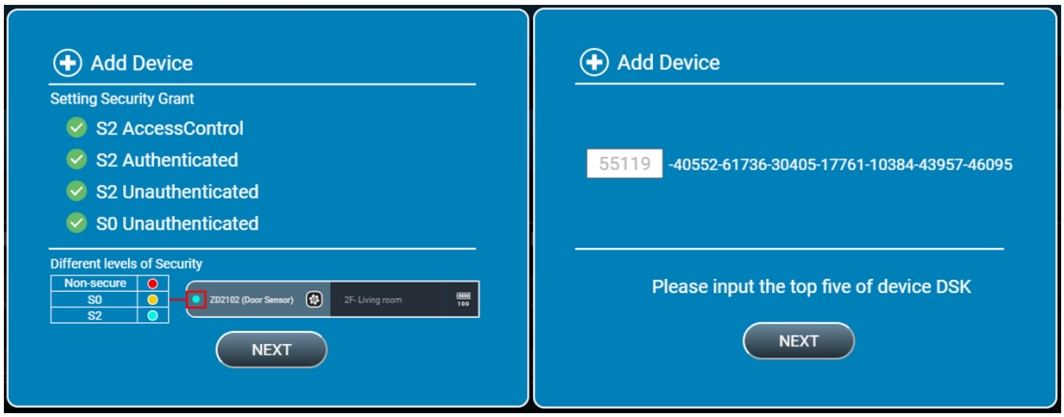


Step 2: System is on inclusion mode and waiting for user to trigger inclusion mode of device. If you would like to stop this action, just taps Exit button.



Step 3: After triggering device, the gateway will show **"Setting Security Grant".** If the device supports S2 Security, please choose the security level for the device. If the selection is **"S2 Access Control"** or **"S2 Authenticated"**, the system will prompt user to input the device first 5 digit of the DSK.

If device only supports S0, the gateway will automatically skip "Setting Security Grant" step.



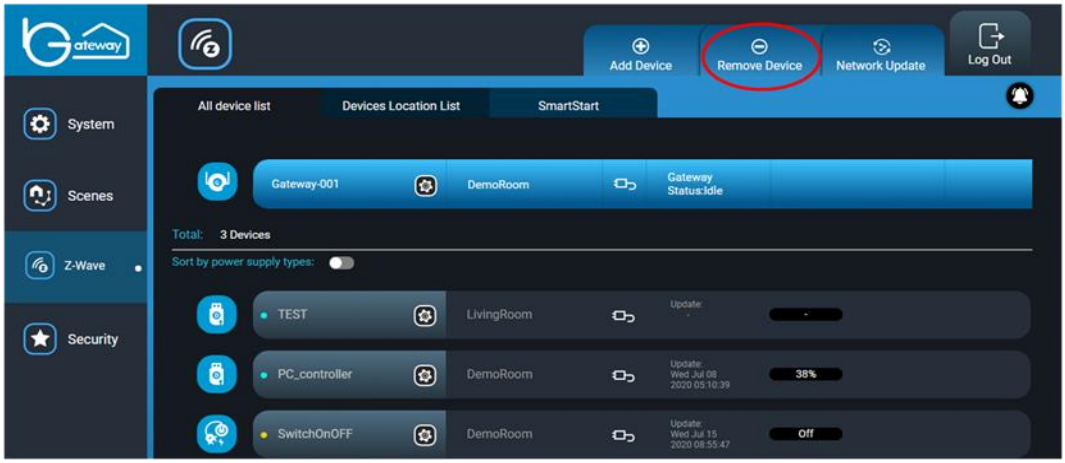
Step 4: Wait for the whole inclusion process to finish; it may take up to 1-2 minutes depending on the device.

Step 5: If the inclusion is successful, the system will show “device included successfully”. Otherwise, a failure message will appear.

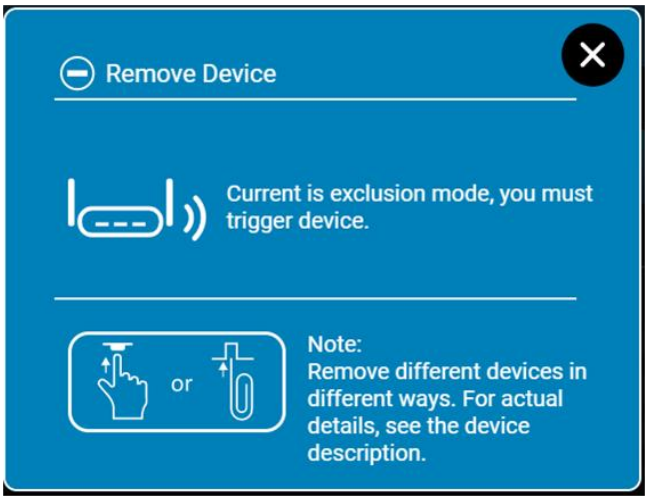
Step 6: If the inclusion is successful, you will be asked to name the device and set up a location of the device.

6.2 Remove Device (Exclusion)

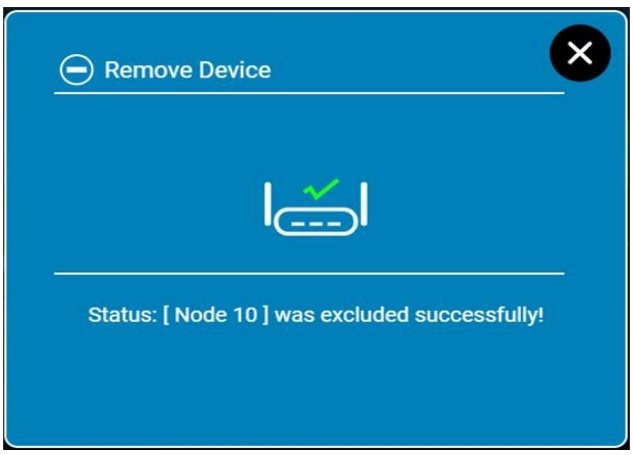
Step 1: Click button "**Remove Device**".



Step 2: System is on exclusion mode and waiting for user to trigger the intended device to removal mode. If you would like to stop this action, just taps Exit button.



Step 3: If the exclusion is successful, system will show the excluded node ID on the pop-up window.



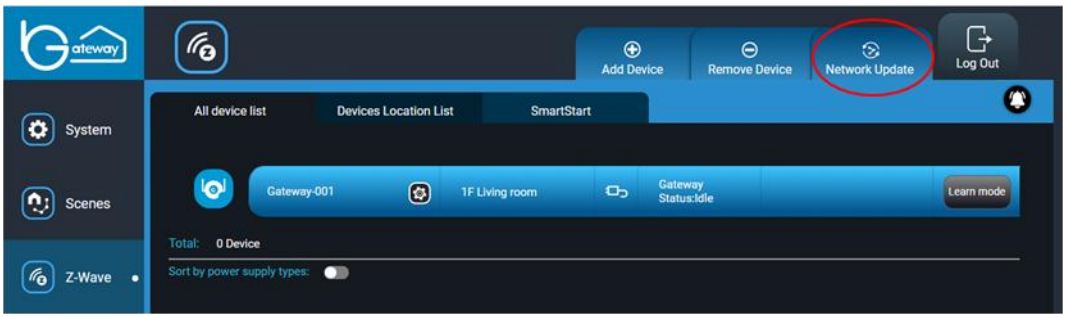
6.3 Network Replication (Copy)

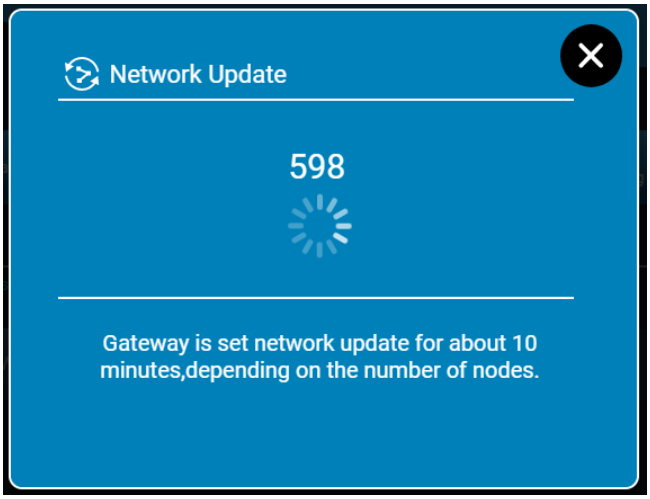
Initiate a replication to copy network information from your gateway to another controller.

1) Start the add device process in Adding Device.
2) Follow the manufacturer's instructions of the other **controller** to enable it to go into learn mode.
3) Enter DSK code if necessary, and await the whole process to finish.

6.4 Network Update

Update your Z-Wave network for maintenance and optimization routine, which includes checking and repairing node return routes and checking node neighbors. This operation will also be performed at least 10 minutes.



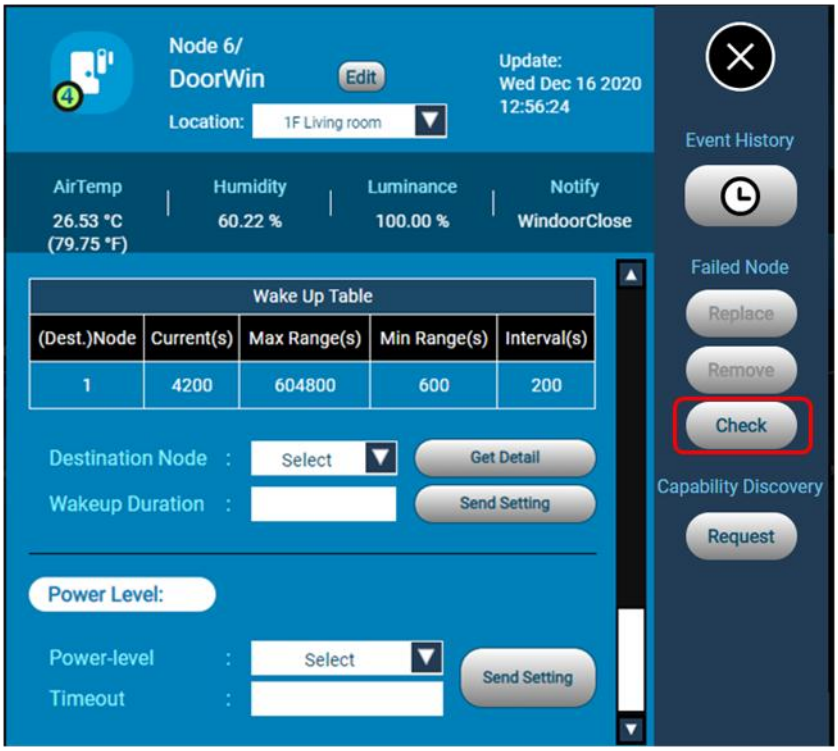


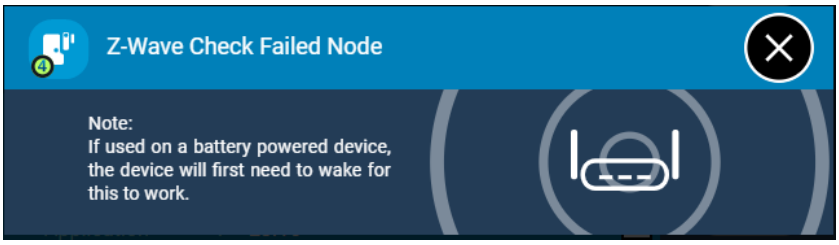
6.5 Check a Z-Wave device

Check and attempt to locate missing or out of range devices, if icon turns gray, the device loses connection. Note if device is a battery type, the battery maybe is out of power.

Step 1: Click "Check" button.

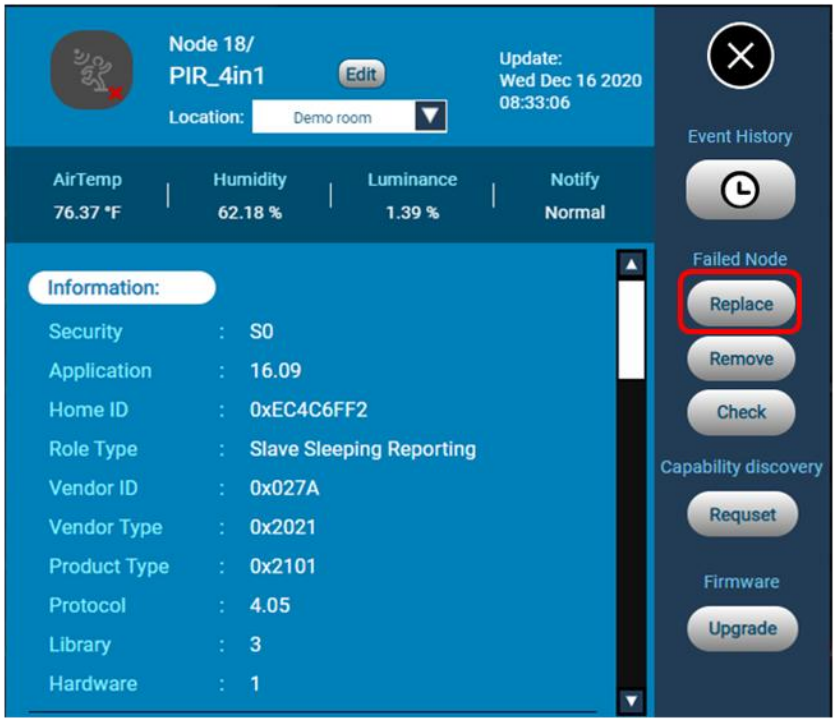
Step 2: Wait gateway for looking for missing device.



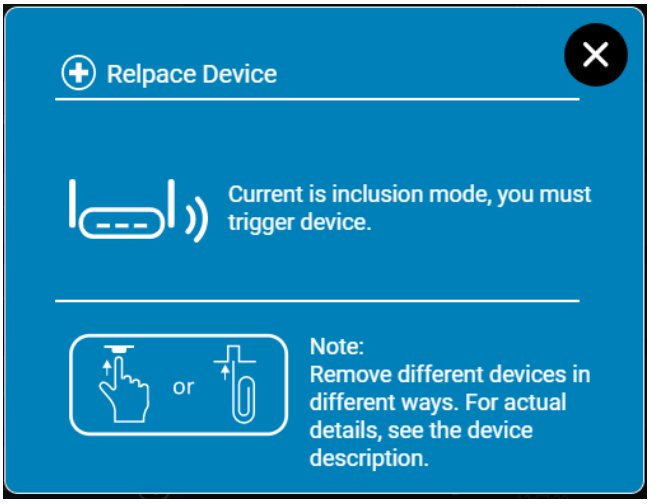


6.6 Replace a failed Z-Wave device

Step 1: Click "**Replace**" button.



Step 2: Start the add device process in Adding Device.

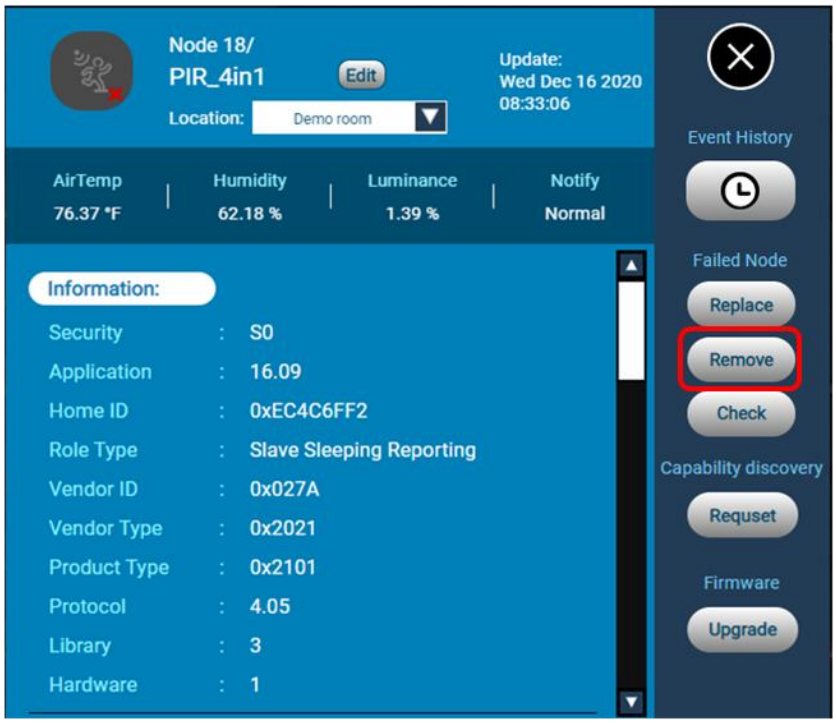


Step 3: Follow the manufacturers instructions of the other controller to enable it to go into learn mode.

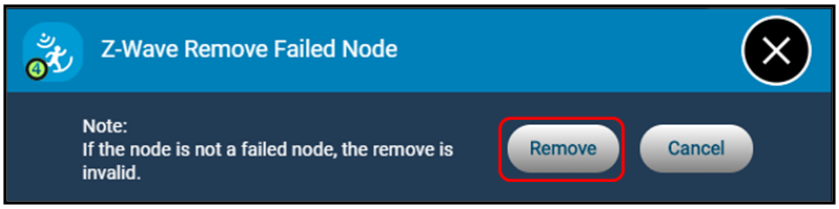
Step 4: Enter DSK code if necessary, and await the whole process to finish.

6.7 Remove a failed Z-Wave device

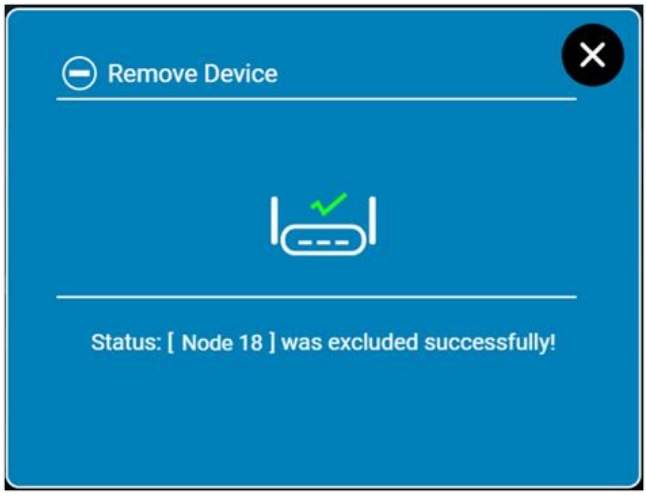
Step 1: Click "Remove" button, if the device is failed node.



Step 2: Click "**Remove**" button would force remove the device.

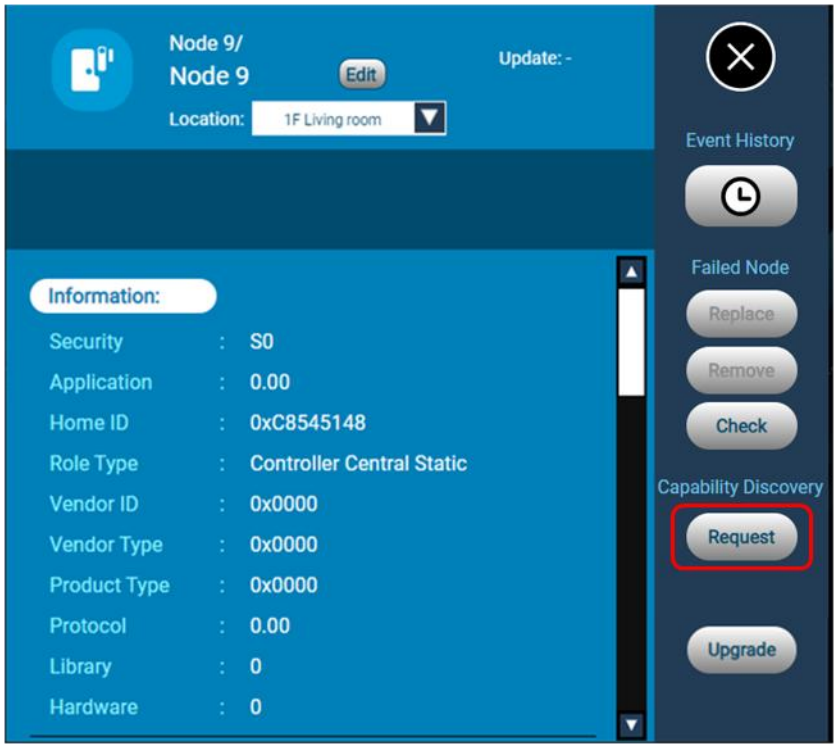


Step 3: If the exclusion is successful, system will show the exclude node ID on the pop-up window.

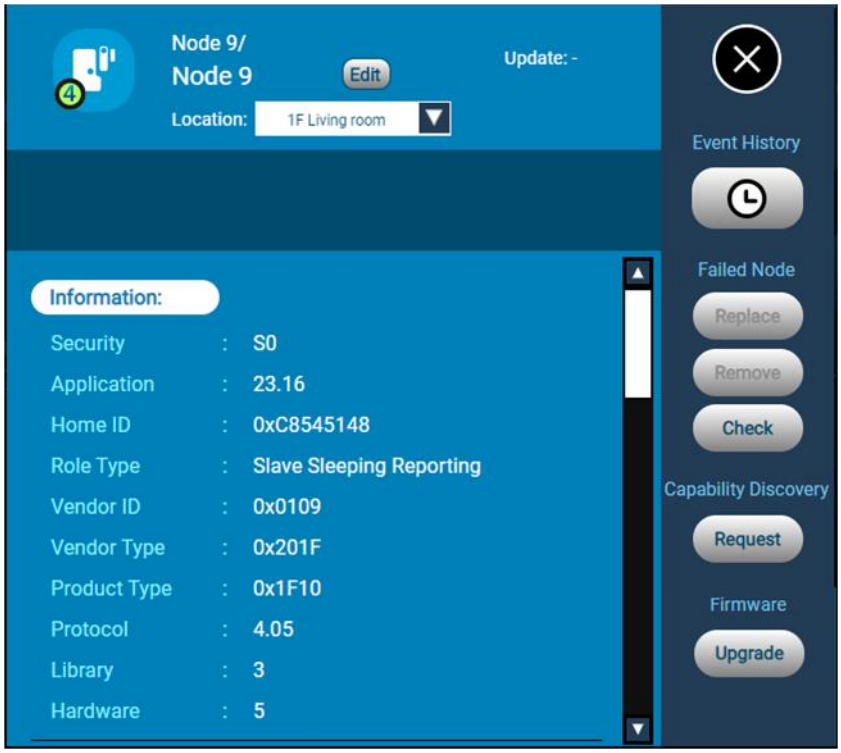


6.8 Request capability rediscovery

Step 1: Click “Request” button, the Mini Gateway would rediscovery the device capability.



Step 2: If successful, the device information would update correctly.

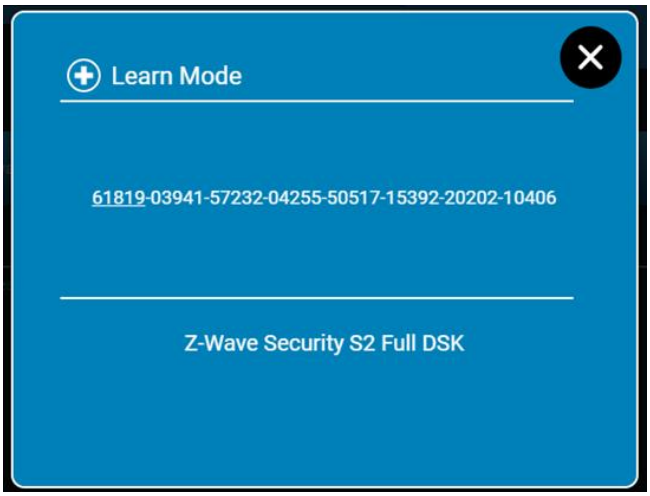


6.9 Including the Mini Gateway to an existing network (Learn mode)

The Z-Wave gateway can also function as an Inclusion / Secondary Controller in the existing Z-Wave network.

Step 1: Follow the manufacturer's instructions of the other controller to enable it into Add mode.

Step 2: Click "**Learn Mode**" button. If it is a S2 Controller, the DSK of the Gateway will appear. Please key in the DSK to the other Controller UI when prompted.

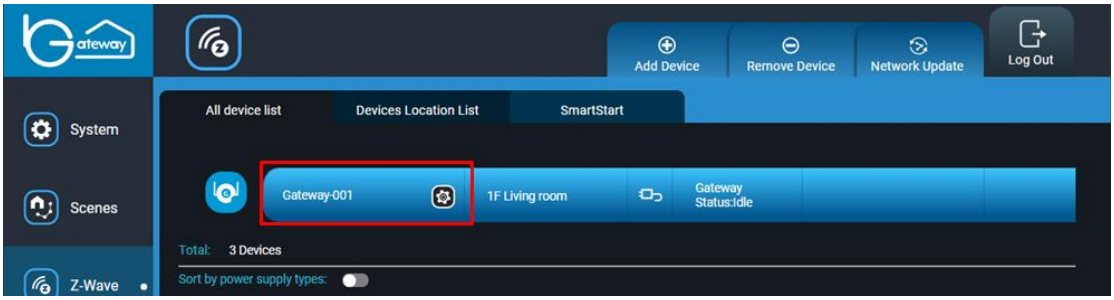


Step 3: When completed, the UI will show the existing Controller and device(s) in the network.

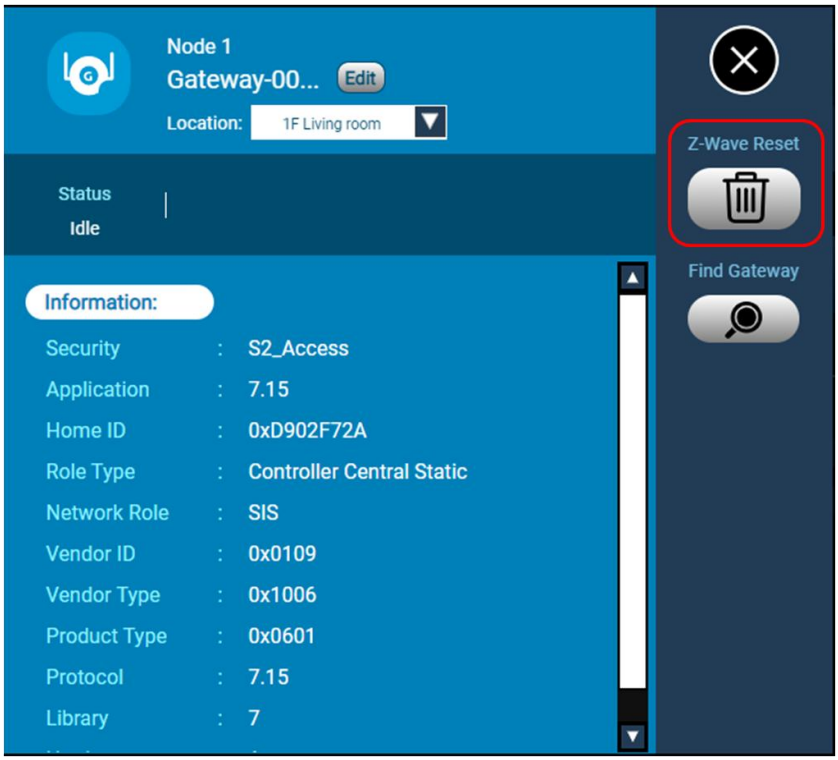
6.10 Factory Default Reset

Factory resets of Z-Wave controller. Do note that once this is done, any device in the Z-Wave network will not be accessible. Hence proceed with caution when doing reset as it is irreversible. If this controller is the primary controller for your network, resetting it will result in the nodes in your network being orphaned and it will be necessary after the reset to exclude and re-include all of the nodes in the network. If this controller is being used as a secondary controller in the network, use this procedure to reset this controller only in the event that the network primary controller is missing or otherwise inoperable.

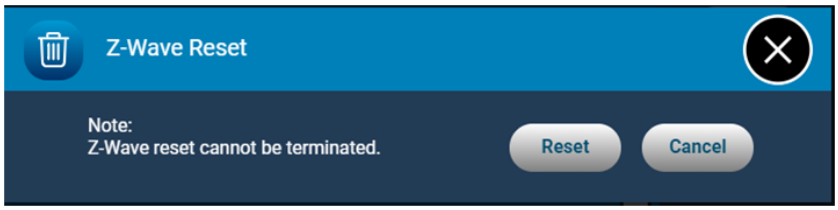
Step 1: Click Gateway setting button.

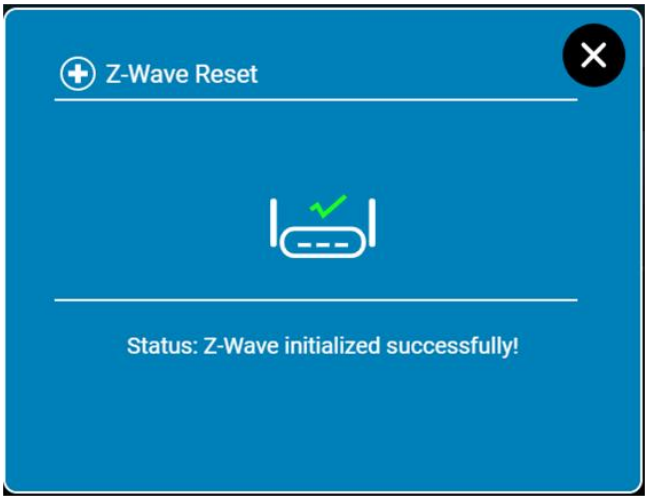


Step 2: Select “Z-Wave Reset” button.



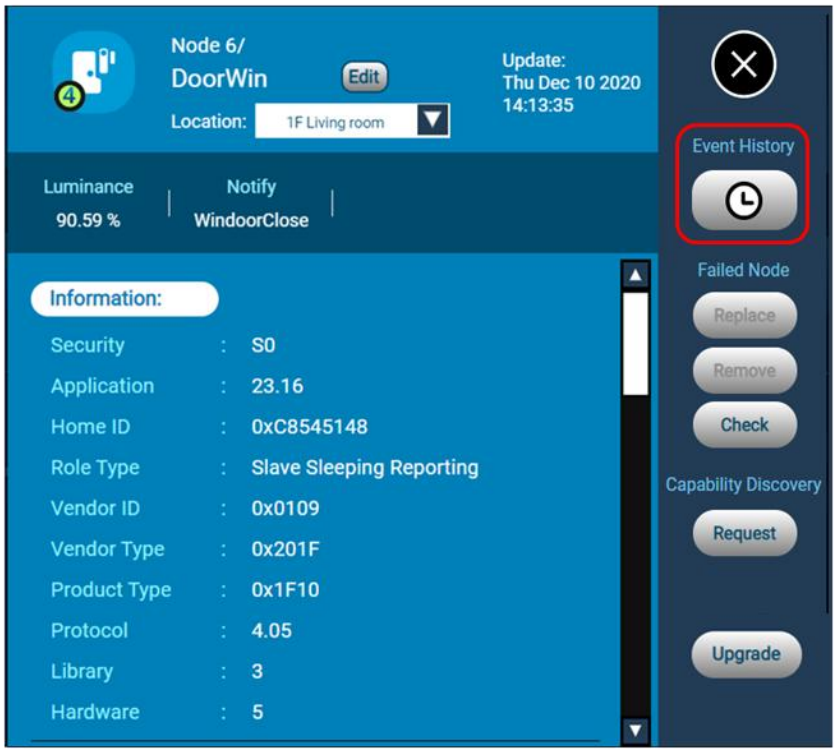
Step 3: Confirm the dialog. Click “Reset” button will perform a factory reset to the Gateway.

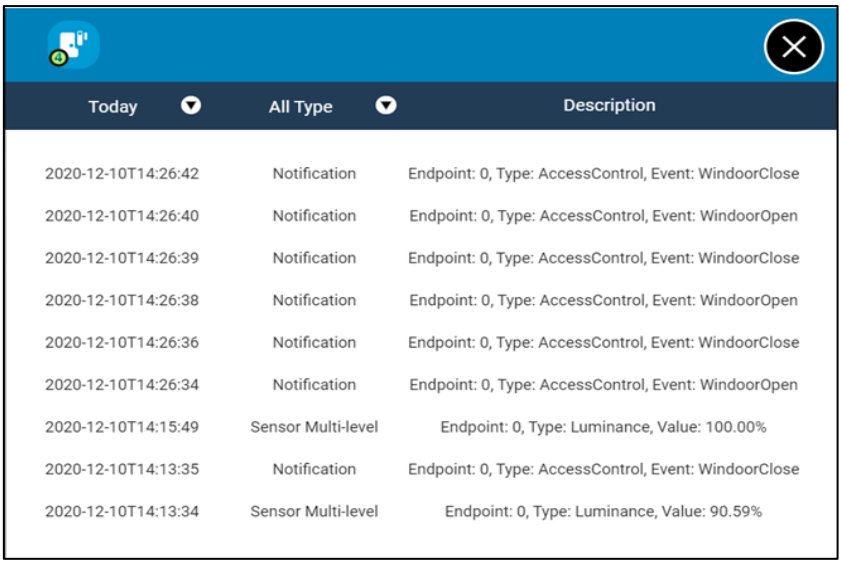




6.11 Device Event History

Click the icon to show history of device.



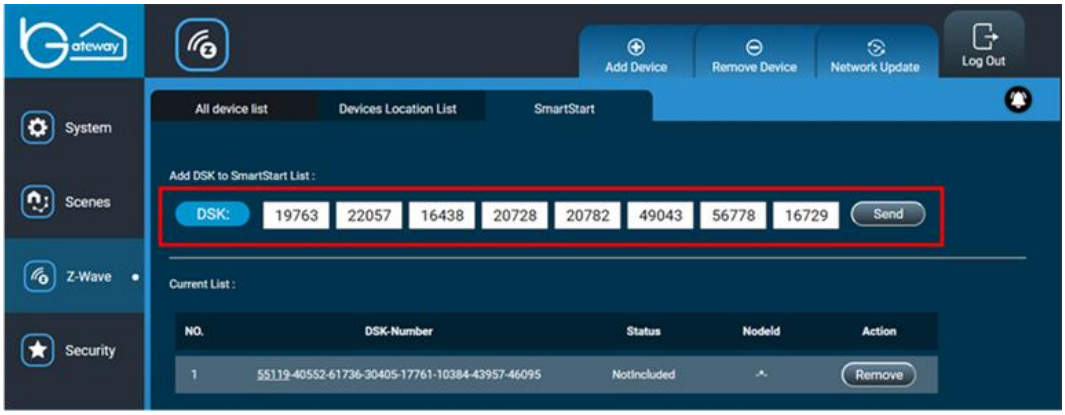


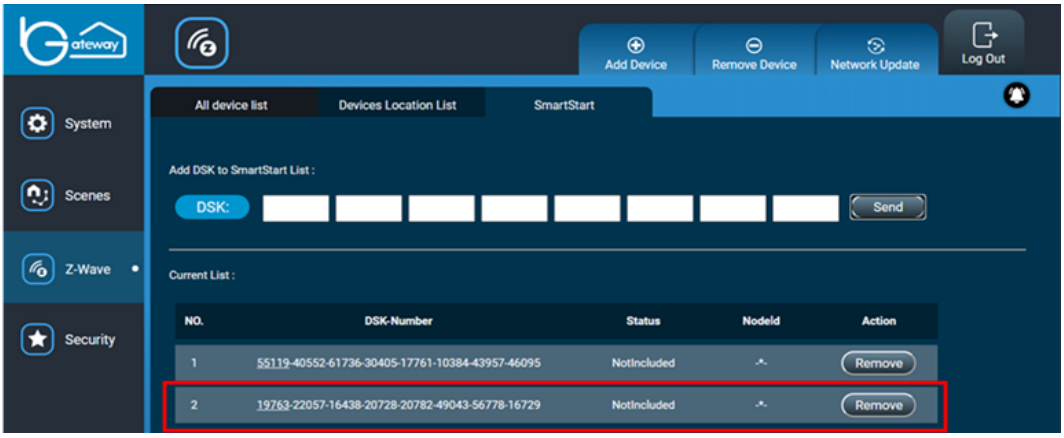
6.12 Add/Remove node to SmartStart List

Step 1: Click "**SmartStart**" from Z-Wave menu.

Step 2: Type in 40 decimals S2 DSK number of the device which user wants to add in using SmartStart and presses "Send".

No further action is required and the SmartStart product will be added automatically.



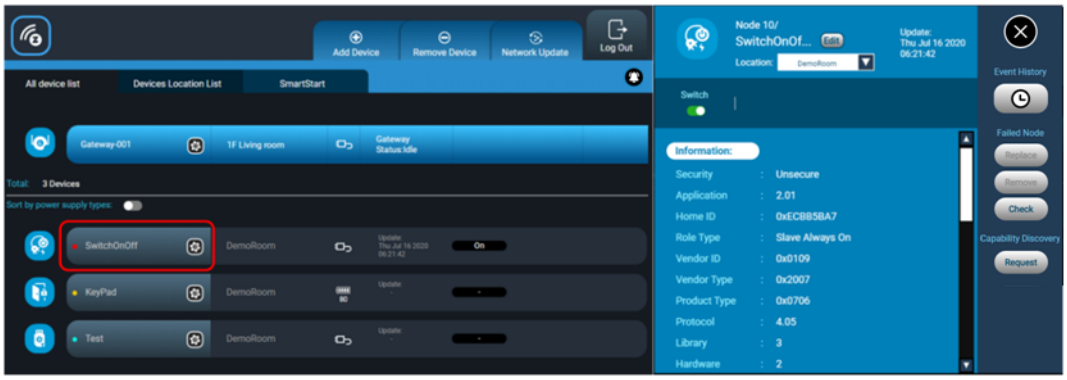


Step 3: You can use "**Remove**" button to remove the specified DSK.

6.13 Additional Information

6.13.1 Controlled Command Classes

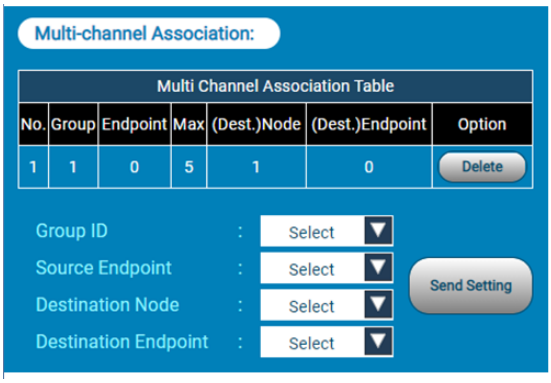
Our product has two ways to control device. End user could quickly switch status from node table (such as switch on/off, lock/unlock, multi level switch, etc.) or click configuration icon to enter detail setting of the node.

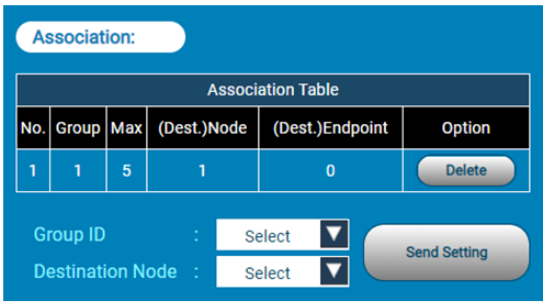


6.13.2 Association Command Class and Multi Channel Association Command Class

The gateway supports Association Command Class. It has one association group 1("Lifeline" group); only one device can be associated to this group. The Gateway will send reset notifications to the associated device when the factory reset is performed on the Gateway.

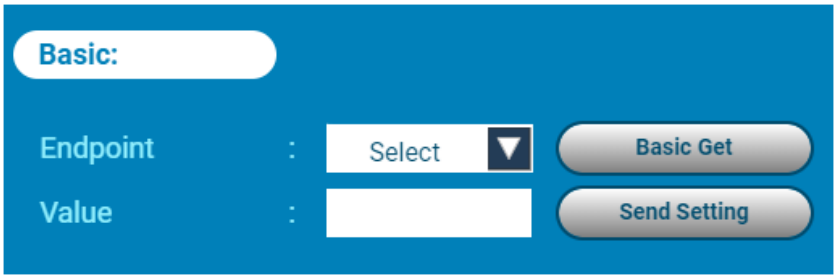
End user could control Association Command and Multi Channel Command from detail setting interface. If device supports Association Command Class and Multi Channel Association Command Class at same time the gateway only show Multi Channel Association Command Class in the detail setting.





6.13.3 Basic Command Class

The gateway is able to controlled Basic Set/Get CC to devices but not supported. It's going to ignores requests when others controller send Basic Set/Get CC to Gateway. This command must to enter detail setting interface.

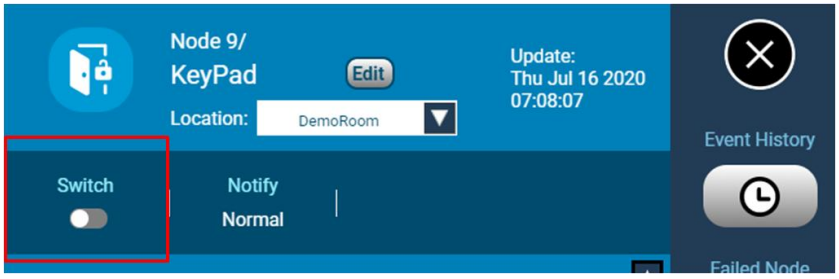


6.13.4 Battery Command Class

The gateway display battery level on node table when device support Battery Command Class. Or send battery get command from detail setting interface manually.

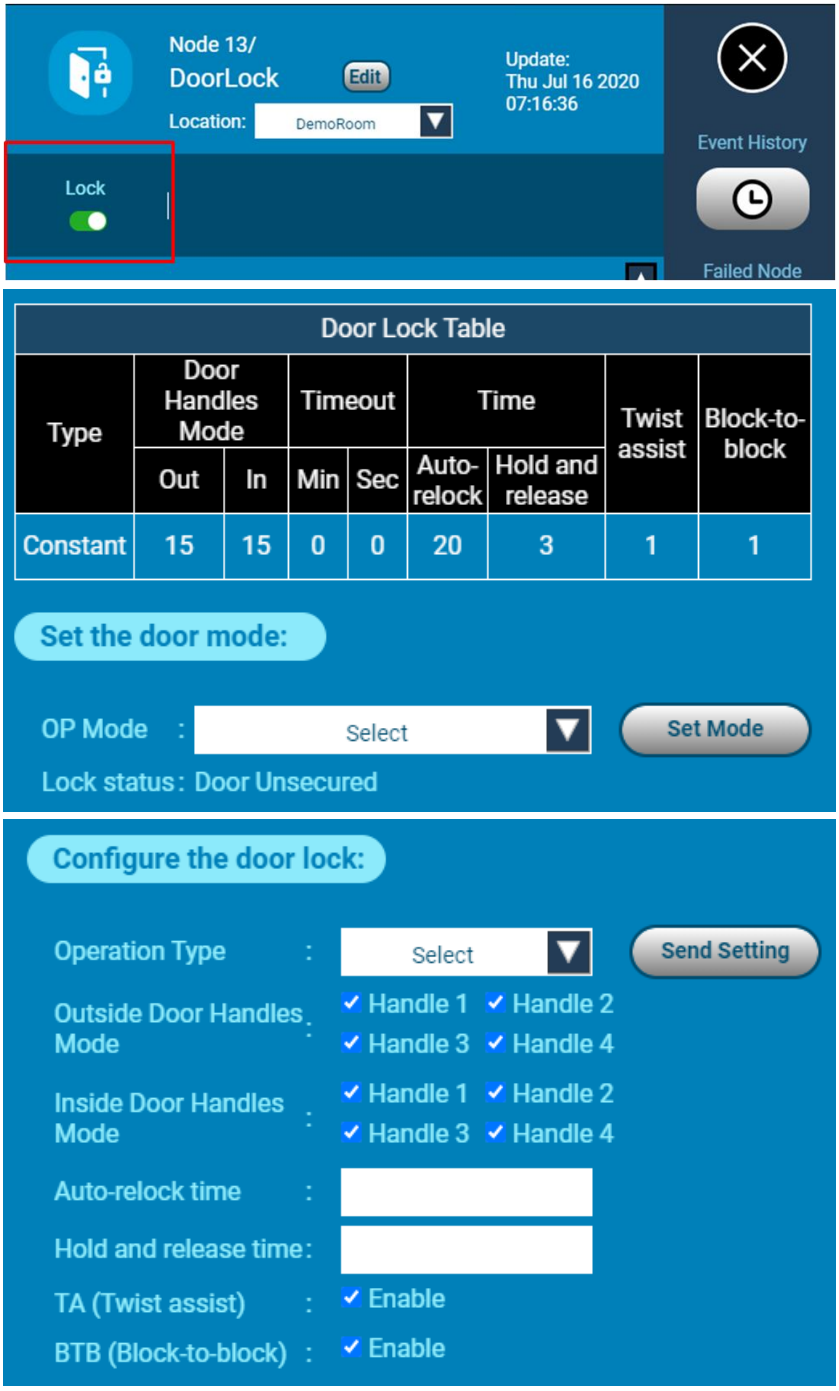
6.13.5 Binary Switch Command Class

End user could switch status from detail setting of the node.



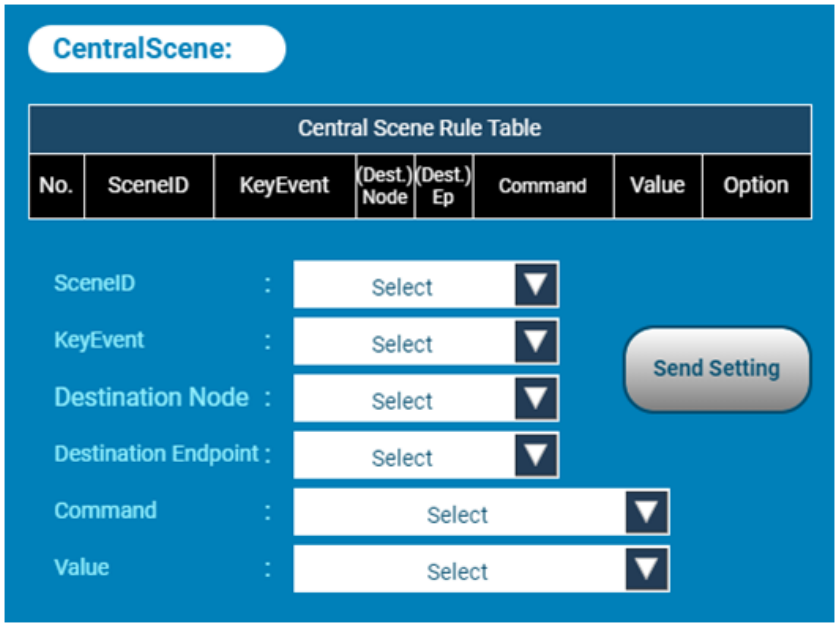
6.13.6 Door Lock Command Class

End user could switch lock and unlock from detail setting of the node.



6.13.7 Central Scene Command Class

The gateway provide setting scene in the detailed setting.



If you want to test your scenes, you must trigger central scene device.

•Pressing shortly the key can be used as trigger for scenes.

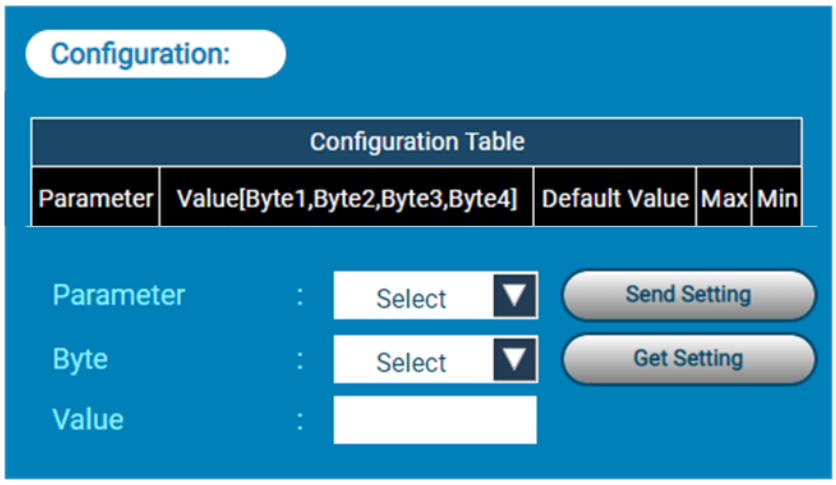
• Holding the key does nothing.

• Releasing the key (after long press) can be used as trigger for scenes.

• Holding and releasing are both shown as "Long Pressed" each.

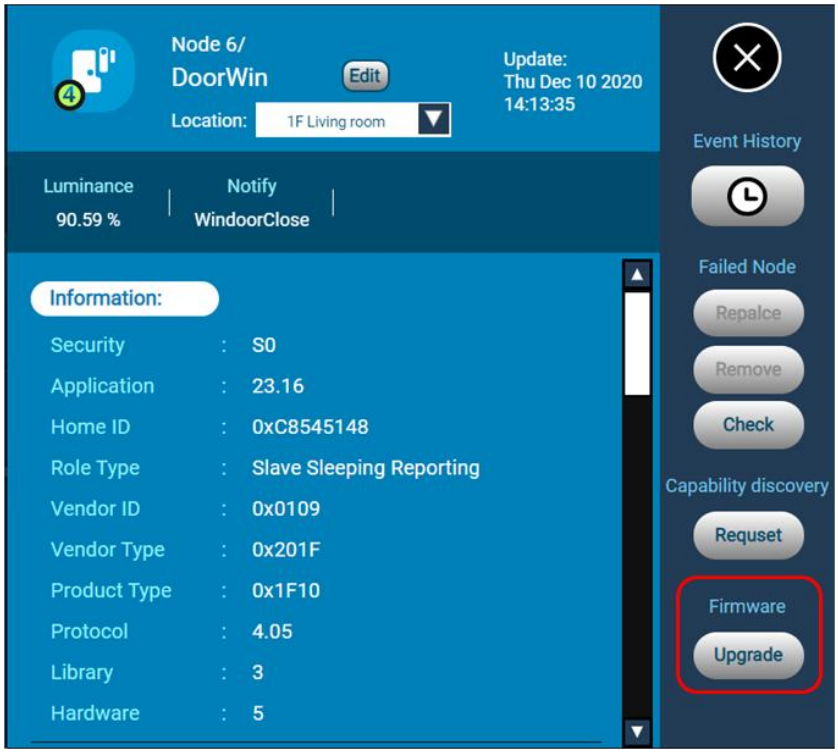
6.13.8 Configuration Command Class

End user could control this command from the detailed setting interface. Set and Get must refer device user manual.

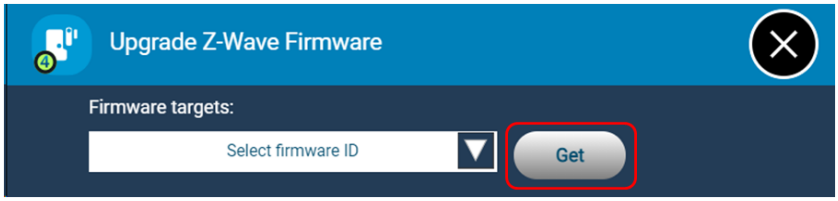


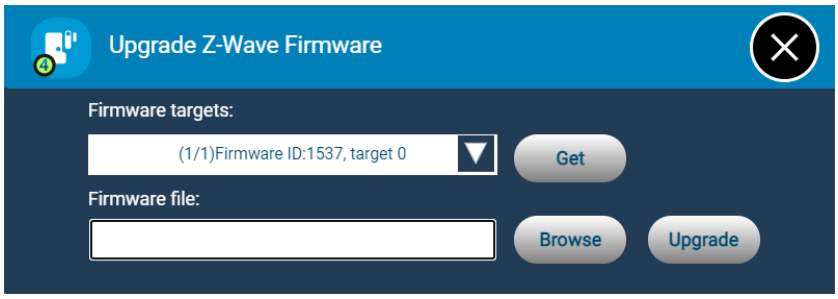
6.13.9 Firmware Update MD Command Class

This command must enter the detailed setting interface and click button **"Upgrade"**.



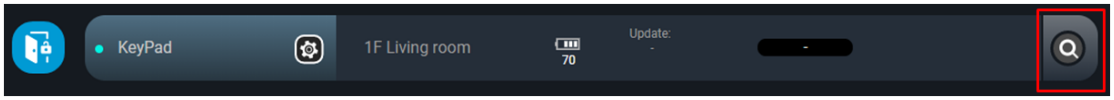
Some devices have several firmware targets. End user must click the **"Get"** button to get firmware targets information and select targets before firmware update.

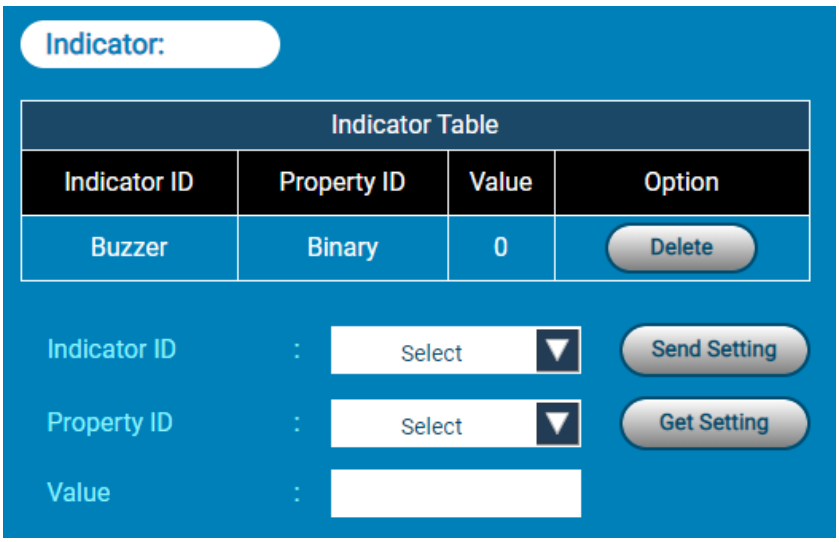




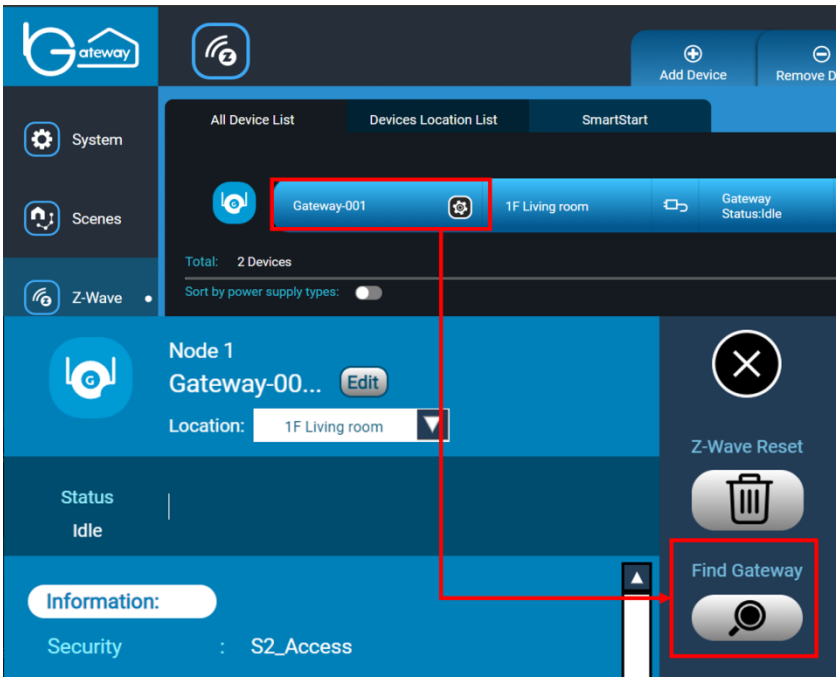
6.13.10 Indicator Command Class

End users could control this command from the detailed setting interface or click the icon to identify itself. The supporting node will be switched on 600ms and switched off 200ms three times.



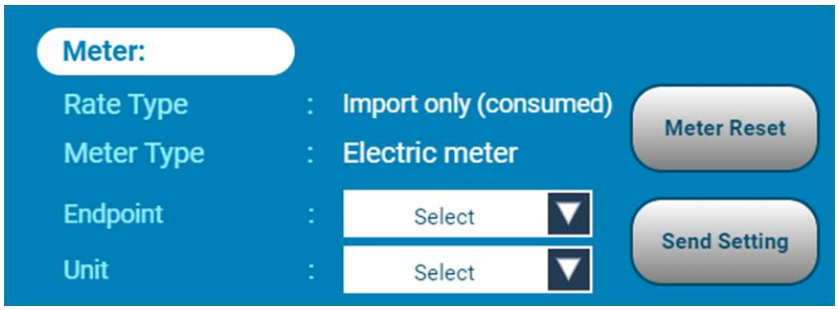


End user could click "**Find Gateway**" button to find gateway, the gateway will be blinks with red light.



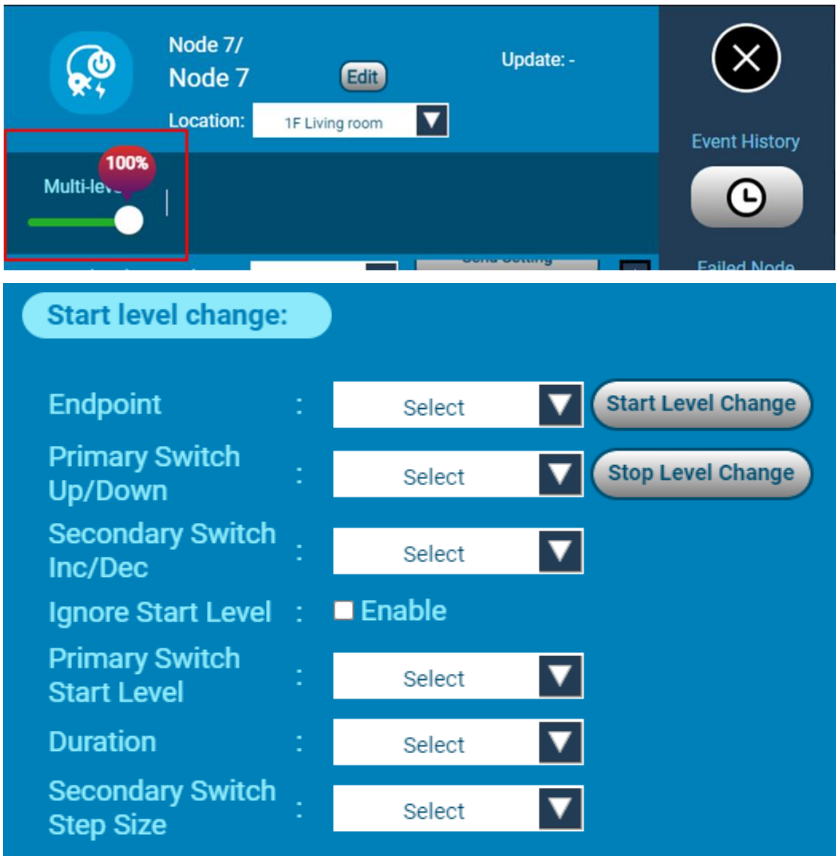
6.13.11 Meter Command Class

End users could get different unit from the detailed setting interface.



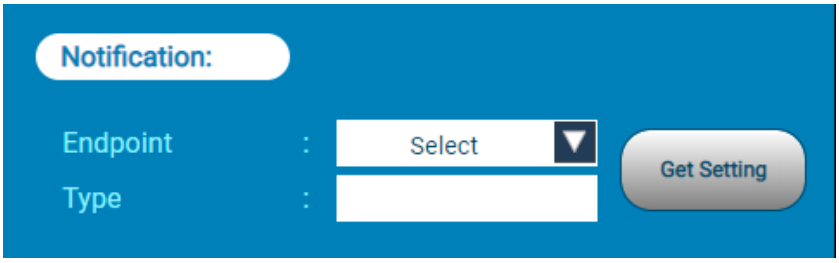
6.13.12 Multilevel Switch Command Class

End users could switch level 0 to 100 from node table. If you want to confirm the current level, you must enter the detailed setting.



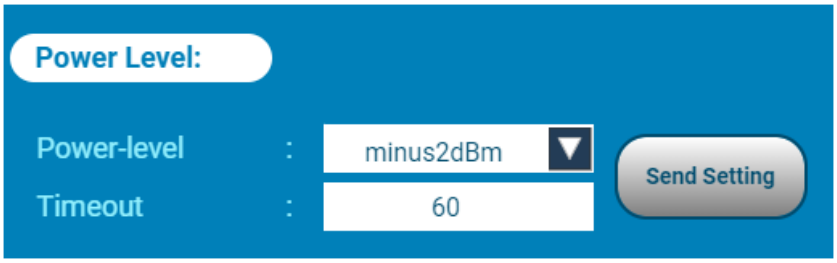
6.13.13 Notification Command Class

When gateway has received a Notification Command Report, it displays on node table.



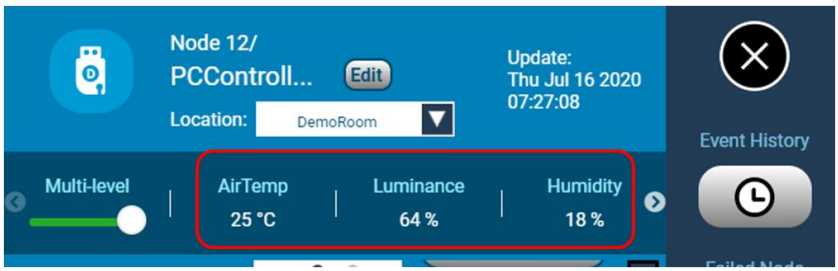
4.12.14 Power Level Command Class

End users could control this command from the detailed setting interface.



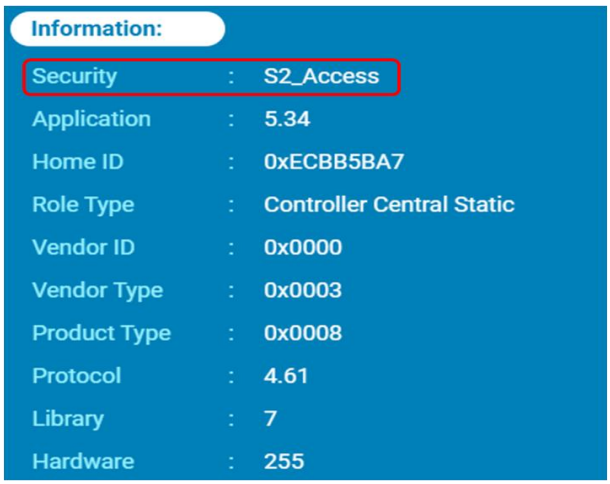
6.13.15 Sensor Multilevel Command Class

When gateway received Sensor Multilevel Command Report it display on node table. The gateway doesn't provide end user send this command.



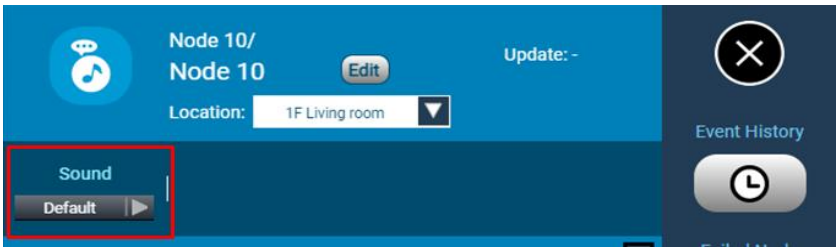
6.13.16 Security Command Class

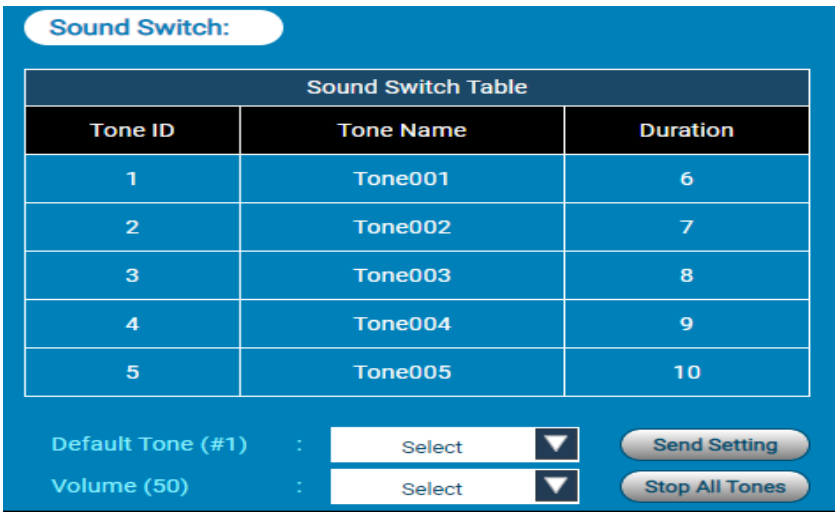
The gateway is a security-enabled device. When a security-enabled Z-Wave device is added to the Gateway's network, its secure communication will be 128-bit AES encrypted. Whether S0 or S2 is used, they will depend on the included device. End users could view security level from the detailed setting interface.



6.13.17 Sound Switch Command Class

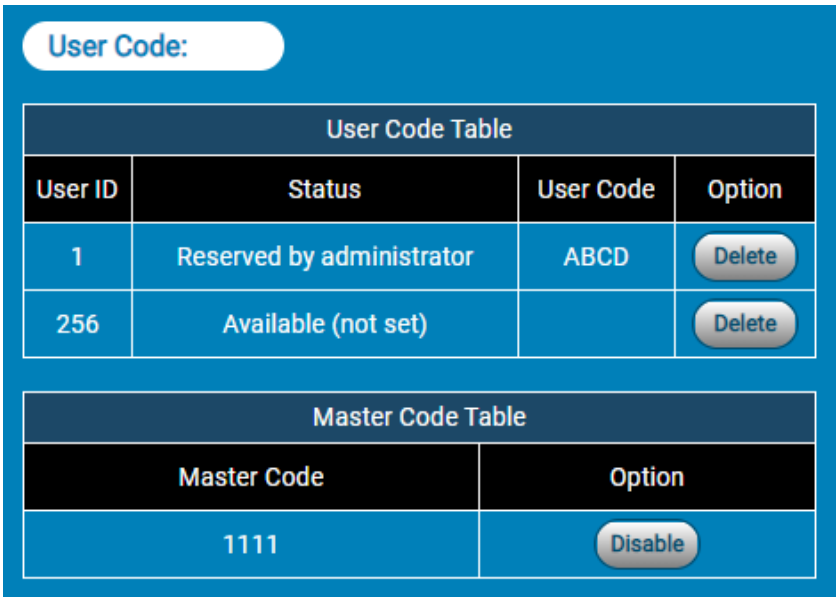
End users could switch sound tone and volume from the detailed setting interface.

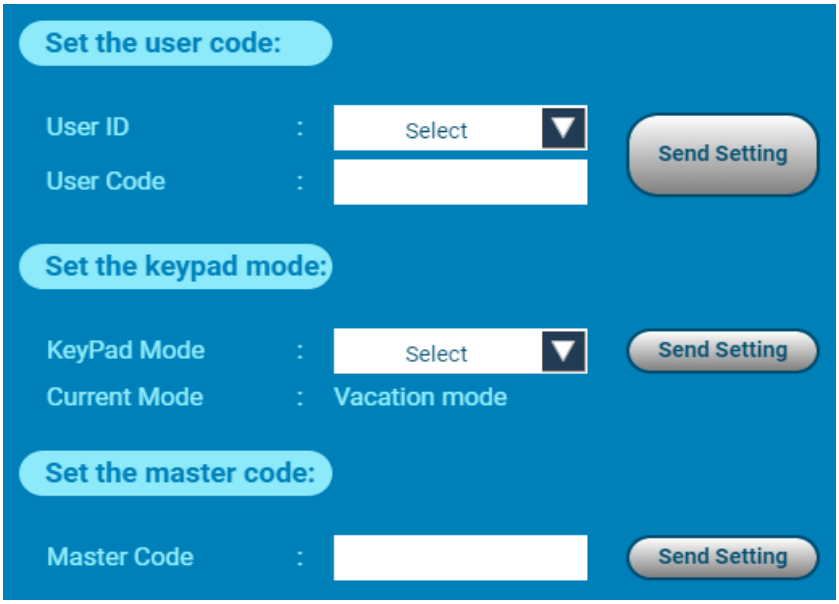




6.13.18 User Code Command Class

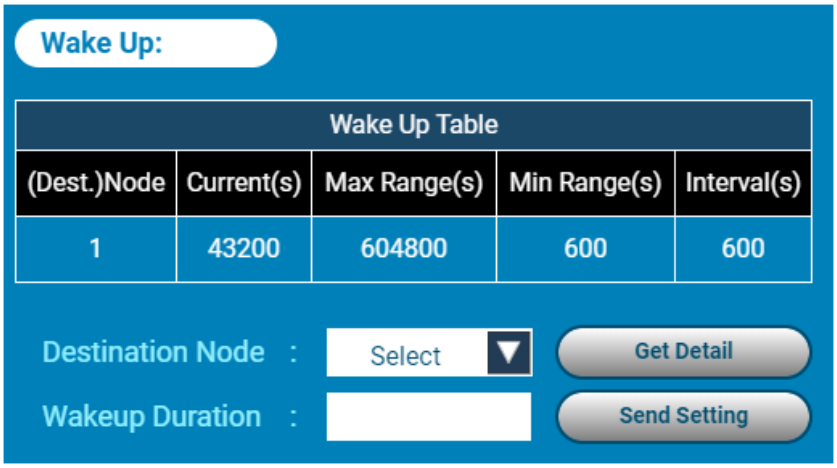
End users could control this command from the detailed setting interface.





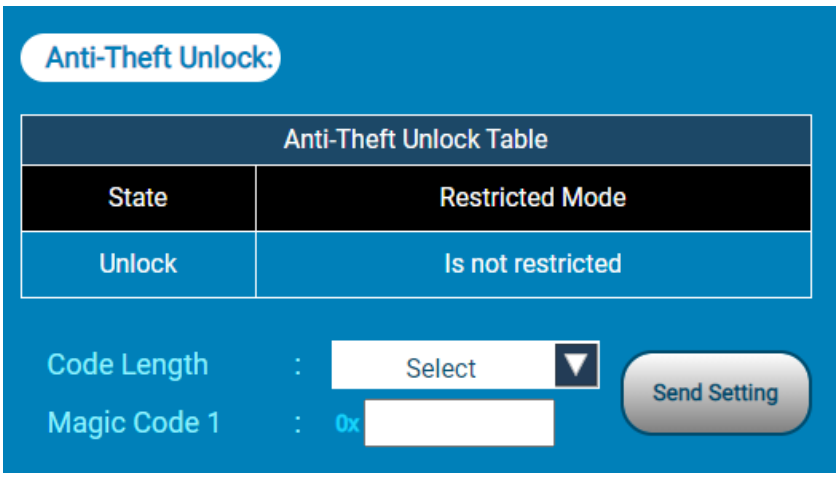
6.13.19 Wake Up Command Class

End users could control this command from the detailed setting interface.



6.13.20 Anti-Theft Unlock Command Class

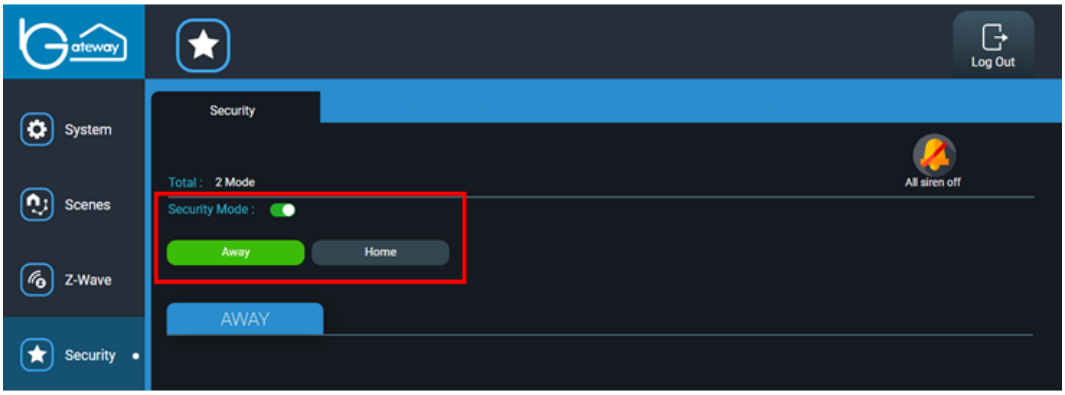
End users could control this command from the detailed setting interface.



7. Security Functionality

7.1 Setting Security Mode

Step 1: Switch your security mode.

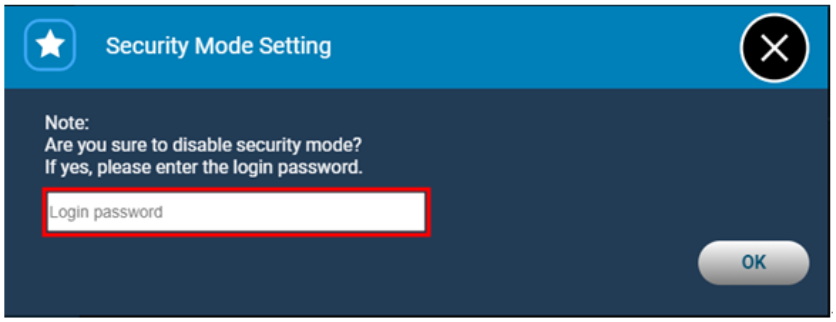


Step 2: If setting successfully, the background of security mode will become green color.

7.2 Disable Security Mode

Step 1: If you want to disable security mode, please click toggle button of **"Security Mode"** side.

Step 2: Enter website to log in and then click **"OK"** button.

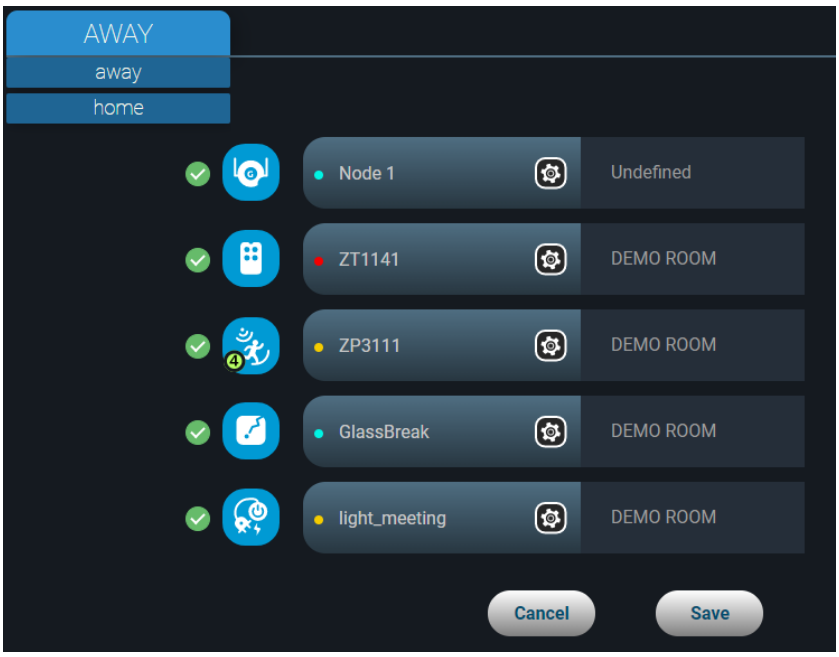


7.3 Setting the security mode detection devices

Step 1: Select the security mode

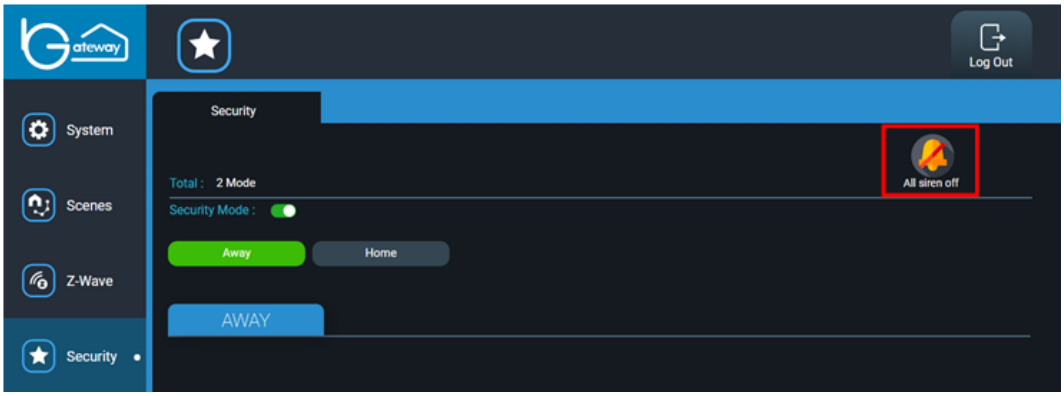
Step 2: Select the devices to detect in the security mode.

Step 3: Click **"Save"** button.



7.4 Turn off all sirens

Step 1: Click the **"All sirens off"** button for turning off all sirens.



8. Supported Z-Wave Device Classes

Device Class	Value	Type
GENERIC_TYPE_STATIC_CONTROLLER	02	Generic
SPECIFIC_TYPE_GATEWAY	07	Specific

9. Supported Z-Wave Command Classes

Command Class	Version	Security level
APPLICATION_STATUS	1	none
ASSOCIATION	3	highest granted
ASSOCITAION_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	none
MANUFACTURER_SPECIFIC	2	This command class is supported secure only if DUT is included on S2 security level.
MULTI_CMD	1	none
MULTI_CHANNEL_ASSOCIATION	4	highest granted
NETWORK_MANAGEMENT_BASIC	2	highest granted
NETWORK_MANAGEMENT_PROXY	4	highest granted
NETWORK_MANAGEMENT_INCLUSION	4	highest granted
NETWORK_MANAGEMENT_INSTALLATION_MAINTENANCE	4	highest granted
NODE_PROVISIONING	1	This command class only supported if DUT is SIS and works on S2 Access security level
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