Instruction

Z-Ware SDK 7.18.x Web User Guide

Document No.:	INS14428
Version:	22
Description:	Z-Ware is a Z-Wave Plus v2 SmartStart Web Gateway over ZIPGW. It comes with sample web pages for UI
Written By:	KAJAROSZ;MIKOZIK;ADGIELNI;JFR;PINOWOBI;MASZPIEC
Date:	2022-05-30
Reviewed By:	NTJ;TRBOYD;SCBROWNI;JCC;ABUENDIA;JFR
Restrictions:	Public

Approved by:				
Date	CET	Initials	Name	Justification
2022-05-30	06:14:58	NTJ	Niels Johansen	

REVISION RECORD

Doc. Ver.	Date	By	Pages affected	Brief description of changes
1	20180726	SNA	ALL	SDK v7.00.00: Cloned from SDK v1.11
2	20181011	SNA	3, 33	Clarified role, n/w ops & CC support; Clarified portal registration Tab UI Dimmer, Door Lock; Eng UI Configuration CC
3	20181024	SNA	3	Updated ZIP CC support; Added Tab UI Maintenance (Device) Network Health
4	20181122	SNA	3	v7.00.02 beta: removed older ZIPGW info, Corrected mailbox CC support version
5	20181122	SNA	1	Removed BBB reference
6	20190215 20190220	SNA	ALL	SDK v7.11.0: RPi3B+, Control CC: Window Covering; N/W IMA v2, User Code v2; updated apps URLs; Tab UI: added Windows Covering, Firmware Backup, User Code v2 Eng UI: added Windows Covering, Firmware Backup; updated About Page Removed Lib info, Added reference to Lib Tab/Eng UI: Binary Switch duration; Grant Key reject Eng UI: multilevel switch duration
7	20190318	SNA	2, 3	Corrected controlled & supported CC table, reference in Update Node/Network
8	20190531	SNA	ALL	v7.11.1:CC control, CC support, Scenes Sound switch action, ZIPGW Portal Config, Tab UI: About, Firmware Update, Device page ZIP GW & Portal settings Eng UI: Firmware Update, Binary Sensor, User Code
9	20190913	SNA	ALL	V7.11.2: CC Control, Scenes Action Window Covering Tab UI: Battery, Indicator, Firmware Eng UI: Feature, Battery, Indicator, Firmware
10	20191115 20191205	SNA	ALL	v7.13.0: CC Control - Protection, DoorLock Logging; CC Support - ZIP v5 removed Tab/Phone UI restrictions, Eng UI – Identify, Protection & Doorlock Logging Tab/Phone UI – Identify, Protection & Doorlock Logging Removed Eng UI: Command Queueing Added techpub edits, Moved Multi CMD CC support to ZIPGW, NW MGMT PROXY v3
11	20191226 20200107	SNA	ALL	CC Control: Updated NWMG_PROXY to v2, removed duplicate SENSOR_ALARM, added ZIPGW; CC Support: Overhauled table to show security requirements Tab UI: Maintenance – added ZIPGW tab and Set Learn Mode button CC Support:: corrected Node Provisioning CC details
12	20200110	SNA	ALL	v7.13.1 – clarified Set Learn Mode for cert
13	20200325	SNA	ALL	Removed Web UI & Portal section & updated Eng UI with same info
14	20200417	ADGIELNI	2, 8, 24	Eng UI: Battery CC v3.
14	20200610	PINOWOBI	11-15	Eng UI: Added Network Manager, Settings description
15	20200618	MIKOZIK	Iv, 3	- Removed old version ”7.13” from table 5 description. - Update Required Security class for: FIRMAWRE_UPDATE_MD, NW_MGMT_BASIC, NW_MGMT_INCLUSION, NW_MGMT_IMA, NW_MGMT_PROXY in table 5
16	20200629	SCBROWNI	ALL	Tech Pubs review
16	20200702	MIKOZIK	ALL	Changed title to 7.14.x
17	20201124	ADGIELNI	2, 3 7, 8, 9 10 16 29	CC Control/CC Support: Added ANTITHEFT_UNLOCK v1, updated NW_MGMT_INSTALLATION_MAINTENANCE to v4, updated NW_MGMT_PROXY to v4, updated NW_MGMT_INCLUSION to v4, updated ZIP_ND to v2. Update Eng UI screenshots. Update Network Manager Node List description Added Z-Wave Long Range Channel Configuration to Network Manager section Added Anti-theft Unlock Interface
17	20201124	MIKOZIK	4.4.1, 4.6	Add info on adding a Long Range node Update Figure 21: SmartStart Add/Edit Device
18	20201130	SCBROWNI	All	Tech Pubs review on new/revised content since last Tech Pubs review
19	20201222	KAJAROSZ	4.4.8	Add more details to Node Identify
19	20210115	MASZPIEC	4.4.10	Update figure
19	20210118	MIKOZIK	4.4.8	Update Node Identification description
20	20210518	MIKOZIK	Cover	Update version to 7.16.x
20	20210518	KAJAROSZ	4.8.26	Explanations regarding portal removal
20	20210519	MIKOZIK	4.4.8.1	Update Node Identification procedure
21	20211122	KAJAROSZ	Cover	Bump version to 7.17.x
22	20220525	KAJAROSZ	1	Change version to 7.18.x

Table of Contents

Table of Tables

Table of Figures

1 Introduction

1.1 Purpose

Z-Ware is a Z-Wave controller middleware running over a Z-Wave over IP (Z/IP) Gateway (ZIPGW) as a Web Gateway. Web pages are built into the Z-Ware Web Server providing a simple web UI. Z-Ware is run on a RPi3B+ (Raspberry Pi 3 – see https://www.raspberrypi.org/products/raspberry-pi-3-model-b-plus/) platform.

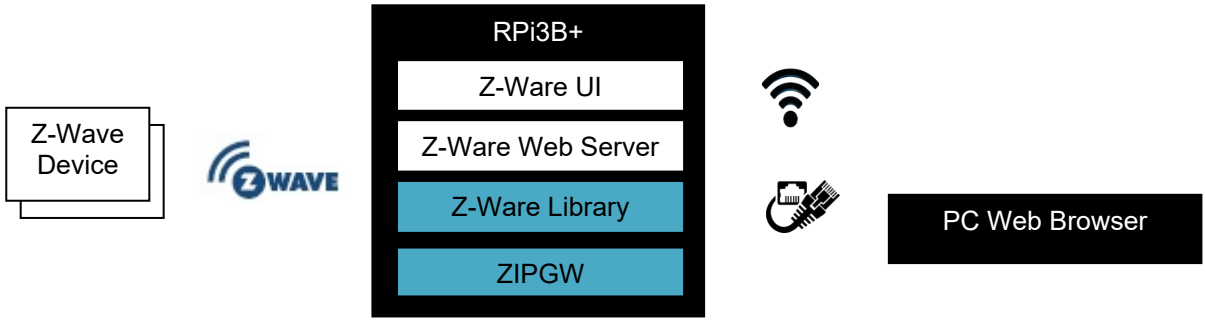


Figure 1: Z-Ware on RPi3B+

This document covers the usage of Z-Ware Web Server.

The diagrams shown in this guide are for Windows® OS with Internet Explorer 8 unless otherwise specified. Your experience may vary slightly depending on your platform configuration.

1.2 Audience and Requirements

Z-Wave Web users

2 Overview

2.1 Z-Ware Library

The Z-Ware Library, which abstracts the ZIPGW, provides Z-Wave Command Class (CC) level APIs and discovery of device capability and state. It is statically linked into the Z-Ware Web Server and provides the following features. Please see [2] Silicon Labs, INS14606, INS, Z-Ware Library User Guide for details on the Library behavior that affects the Web Server.

2.2 CC Control

Z-Ware controls the following CCs and versions:

Table 1: UI-Controlled Z-Wave CCs

CC	Ver	CC	Ver
ANTITHEFT_UNLOCK	1	PROTECTION	2
ASSOCIATION	3	SECURITY	1
ASSOCIATION_GRP_INFO	3	SECURITY 2	1
BARRIER_OPERATOR	1	SENSOR_BINARY	2
BASIC	2	SENSOR_MULTILEVEL	11
BATTERY	3	SOUND_SWITCH	2
CENTRAL_SCENE	3	SWITCH_BINARY	2
CONFIGURATION	4	SWITCH_COLOR	3
DOOR_LOCK	4	SWITCH_MULTILEVEL	4
DOOR_LOCK_LOGGING	1	THERMOSTAT_FAN_MODE	5
FIRMWARE_UPDATE_MD	7	THERMOSTAT_FAN_STATE	2
INDICATOR	3	THERMOSTAT_MODE	3
MANUFACTURER_SPECIFIC	2	THERMOSTAT_OPERATING_STATE	2
METER	5	THERMOSTAT_SETPOINT	3
MULTI_CHANNEL	4	TIME	2
MULTI_CHANNEL_ASSOCIATION	4	USER_CODE	2
NW_MGMT_BASIC	2	VERSION	3
NW_MGMT_INCLUSION	4	WAKE_UP	2
NW_MGMT_INSTALLATION_MAINTENANCE	4	WINDOW_COVERING	1
NW_MGMT_PROXY	4	ZIP_GATEWAY	1
NODE_NAMING	1	ZIP_PORTAL	1
NODE_PROVISIONING	1	ZWAVEPLUS_INFO	2
NOTIFICATION/ALARM	8		

Table 2: Controlled Z-Wave CCs Inherited through Library

CC	Ver	CC	Ver
SENSOR_ALARM	1	NO_OPERATION	1
APPLICATION_STATUS	1	POWERLEVEL	1
CRC_16_ENCAP	1	SUPERVISION	1
DEVICE_RESET_LOCALLY	1	ZIP	5
MULTI_CMD	1	ZIP_ND	2

Table 3: Controlled Z-Wave CCs inherited from ZIPGW

CC	Ver	CC	Ver
INCLUSION CONTROLLER	1	TRANSPORT_SERVICE	2

NODE_PROVISIONING CC is only present when Z-Ware is operating as a Z-Wave SIS.

2.3 CC Support

For easier reference during certification, supported CCs (including those inherited from ZIPGW) are shown below.

Table 4: Supported Z-Wave CCs Pushed down from Z-Ware (No Security Requirements)

CC	Ver
ASSOCIATION	3
ASSOCIATION_GRP_INFO	3
DEVICE_RESET_LOCALLY	1
MULTICHANNEL_ASSOCIATION	4

Table 5: ZIPGW SDK Supported Z-Wave CCs

CC	Ver	Not Added	Required Security classes when added	On Secure Inclusion Failure
APPLICATION_STATUS	1	X	None	X
CRC_16_ENCAP	1	X	None	X
FIRMWARE_UPDATE_MD	5		Highest granted security class - not supported when included non-securely	
INCLUSION_CONTROLLER	1	X	None	X
INDICATOR	3	X	Highest granted security class	X
MAILBOX	2		LAN-side only	
MANUFACTURER_SPECIFIC	2	X	Highest granted security class	X
MULTI_CMD	1	X	None	X
NODE_PROVISIONING	1		Access Control, only when SIS	
NW_MGMT_BASIC	2		Highest granted security class - not supported when included non-securely	
NW_MGMT_INCLUSION	4		Highest granted security class - not supported when included non-securely	

NW_MGMT_IMA	4		Highest granted security class - not supported when included non-securely	
NW_MGMT_PROXY	4		Highest granted security class - not supported when included non-securely	
POWERLEVEL	1	X	Highest granted security class	X
SECURITY	1	X	None	
SECURITY_2	1	X	None	X
SUPERVISION	1	X	None	X
TRANSPORT_SERVICE	2	X	None	X
TIME	1	X	None	X
VERSION	3	X	Highest granted security class	X
ZIP	4		LAN-side only	
ZIP GATEWAY	1		LAN-side only	
ZIP_ND	2		LAN-side only	
ZIP NAMING	1		LAN-side only	
ZIP PORTAL	1		LAN-side only	
ZWAVEPLUS_INFO	2	X	None	X

Z-Ware does nothing on receiving Basic CC Set or Get, unless the Basic Set from any particular node or endpoint is used as a Scene trigger. Z-Ware supports only 1 Association group supporting 1 node for Lifeline. This node will receive the Device Reset Locally command.

2.4 Scenes

A Z-Ware Scene is a set of actions that may be activated by triggers. An action is a Z-Wave SET command, such as turning on a switch. A trigger may be a user request through a UI element, by schedule, or on an event. A schedule can be set to execute a Scene on any or every day of the week at a preset time. A schedule remains active until it is disabled or deleted. An event refers to the receipt of a Z-Wave report, typically a sensor report, such as motion sensed. The scene state, i.e., whether it is completely activated, can also be monitored.
A Z-Ware Security Scene is a special Scene that can be armed or disarmed by an event trigger or through the UI. It can only be alarmed when it is armed. When alarmed, it can send out alerts using email and/or SMS. Arming, disarming, and alarming can also be configured to activate normal scenes.
The CCs and commands supported for Scenes actions and triggers are shown below. For Central Scene CC, only the Key Pressed attribute is used.

Table 6: Scenes Actions Supported

CC	Command(s)
BASIC	SET
SWITCH_BINARY	SET
SWITCH_MULTILEVEL	SET, START_LEVEL_CHANGE
SWITCH_COLOR	SET
DOOR_LOCK	OPERATION_SET
BARRIER_OPERATOR	SET
THERMOSTAT_SETPOINT	SET
THERMOSTAT_MODE	SET
SOUND_SWITCH	TONE_PLAY_SET
WINDOW_COVERING	SET, START_LEVEL_CHANGE

Table 7: Scenes Event Triggers Supported

CC	Command	Scene	Security Arm/Disarm	Security Alarm
BASIC	SET	Y		Y
SENSOR_BINARY	REPORT	Y		Y
SENSOR_MULTILEVEL	REPORT	Y		
NOTIFICATION	REPORT	Y		Y
DOOR_LOCK	REPORT	Y	Y	
CENTRAL_SCENE	NOTIFICATION	Y	Y	

3 Access

Figure 2: Login Page

Users access their accounts on the machine they have installed at https://<machine IP address>. The default username and password are ‘user’ and ‘smarthome’ respectively.

4 UI

4.1 Home

After successful login, the user can view on the Home page whether or not the controller is already initialized. All Web pages have a navigation menu on the left. The home page shows the details of the local controller.

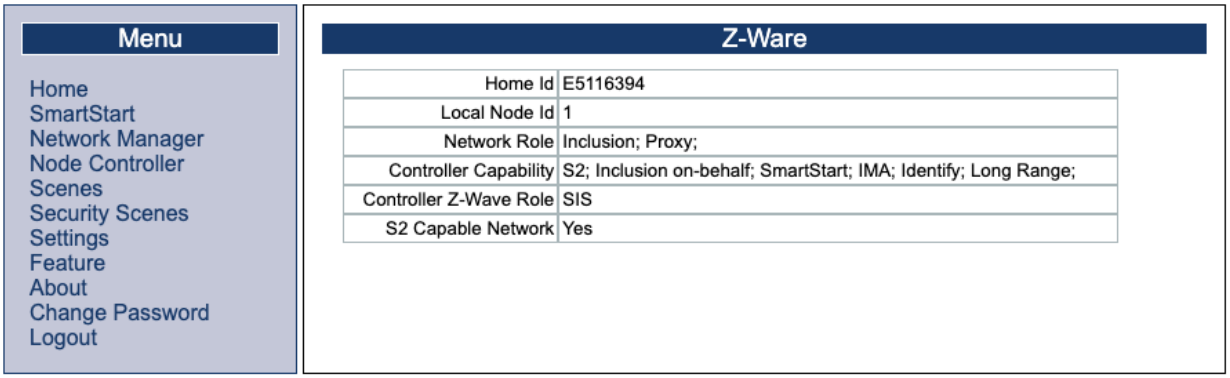


Figure 3: Home Page

The menu bar on the left is used to navigate to other pages described in the subsequent chapters. The user may log out anytime by clicking the “Logout” Menu option. “Change Password” Menu option can be used to change the password which has to be 8 to 16 UTF-8 characters. Resetting the password is done by the start menu item in Windows OS, or a script in Linux OS, or an application in OS X.

4.2 About

The About page displays the information obtained from the server by using zw_info API. The information is categorised into two different tables, namely General and Version information as shown below.

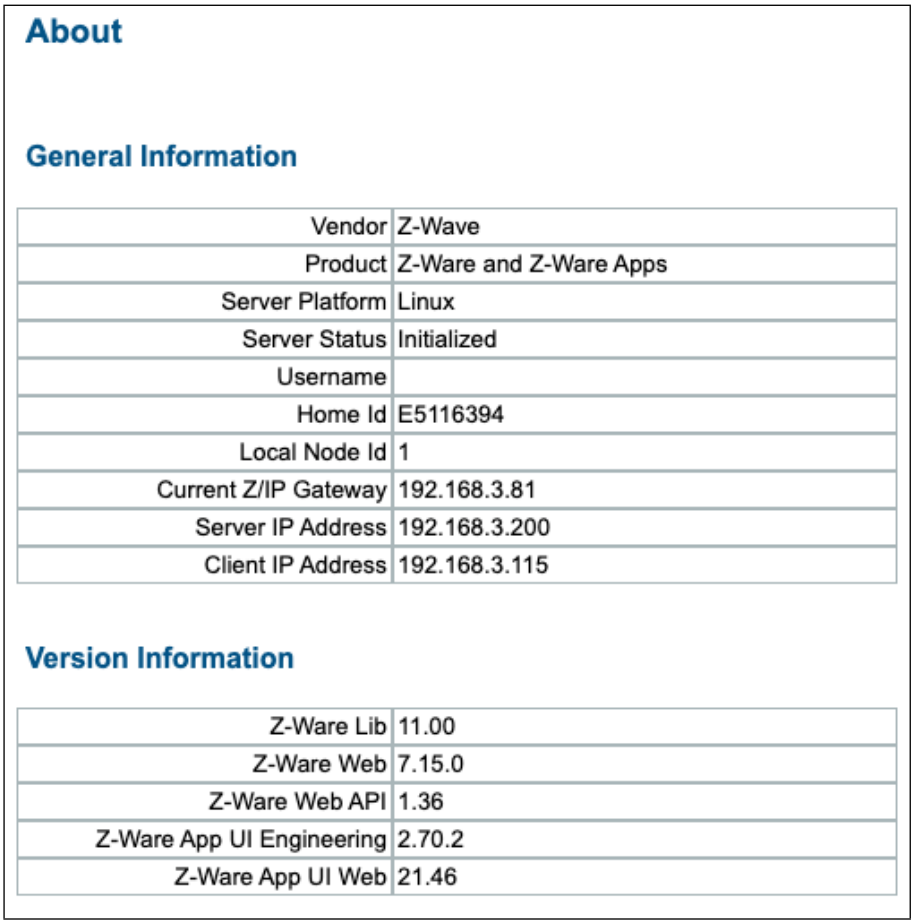


Figure 4: About Page

4.3 Features

This page lists the features – CCs, interfaces, and versions.

Command Class	Command	Web API
Command Class Alarm	8	1
Command Class Anti-theft Unlock	1	1
Command Class Association	3	1
Command Class Association	3	1
Command Class Barrier Operator	1	1
Command Class Basic	2	1
Command Class Battery	3	1
Command Class Central Scene	3	1
Command Class Configuration	4	1
Command Class Door Lock	4	1
Command Class Door Lock	1	1
Command Class Firmware Update	7	1
Command Class Indicator	3	1
Command Class Meter	5	1
Command Class Multi Channel	4	1
Command Class Node Naming	1	1
Command Class Protection	2	1
Command Class Sensor Binary	2	1
Command Class Sensor Multilevel	11	1
Command Class Sound Switch	2	1
Command Class Switch Binary	2	1
Command Class Switch Color	3	1
Command Class Switch Multilevel	4	1
Command Class Thermostat Fan	5	1
Command Class Thermostat Fan	2	1
Command Class Thermostat	3	1
Command Class Thermostat	2	1
Command Class Thermostat	3	1
Command Class Time	2	1
Command Class User Code	2	1
Command Class Version	3	1
Command Class Wake Up	2	1
Command Class Window	1	1
Command Class Z/IP Gateway	1	1
Command Class Z/IP Portal	1	1
Command Class Z-Wave+ Info	2	1

Figure 5: Eng UI – Features

Scene Action Feature

Command Class	Command Class	Web API Command	Web API version
Command Class Barrier Operator	1	BARRIER_OP_SET	1
Command Class Basic	2	BASIC_SET	1
Command Class Door Lock	4	DLOCK_OP_SET	1
Command Class Sound Switch	1	SOUND_SWITCH_TONE_PLAY_SET	1
Command Class Switch Binary	2	BINARY_SWITCH_SET	1
Command Class Switch Color	3	COLOR_SWITCH_SET	1
Command Class Switch Multilevel	4	MULTILEVEL_SWITCH_SET MULTILEVEL_SWITCH_LVL_CHG_SET	1
Command Class Thermostat Mode	3	THRMO_MODE_SET	1
Command Class Thermostat Setpoint	3	THRMO_SETPT_SET	1
Command Class Window Covering	1	WINDOW_COVERING_SET WINDOW_COVERING_LEVEL_CHANGE_SET	1

Scene Event Feature

Command Class	Command Class	Web API Command	Web API version
Command Class Alarm	8	ALARM_GET	1
Command Class Basic	2	BASIC_EVENT	1
Command Class Central Scene	3	CENTRAL_SCENE_REPORT	1
Command Class Door Lock	4	DLOCK_OP_GET	1
Command Class Sensor Binary	2	BINARY_SENSOR_GET	1
Command Class Sensor Multilevel	11	MULTILEVEL_SENSOR_GET	1

Figure 6: Scene Features

Security Scene Arm Feature

Command Class	Command Class	Web API Command	Web API version
Command Class Central Scene	3	CENTRAL_SCENE_REPORT	1
Command Class Door Lock	4	DLOCK_OP_GET	1

Security Scene Disarm Feature

Command Class	Command Class	Web API Command	Web API version
Command Class Central Scene	3	CENTRAL_SCENE_REPORT	1
Command Class Door Lock	4	DLOCK_OP_GET	1

Security Scene Alarm Feature

Command Class	Command Class	Web API Command	Web API version
Command Class Alarm	8	ALARM_GET	1
Command Class Basic	2	BASIC_EVENT	1
Command Class Sensor Binary	2	BINARY_SENSOR_GET	1

Figure 7: Security Scene Features

4.4 Network Manager

The Network Manager menu lists nodes in the network and allows network operations, such as include/exclude.
The Z-Wave node/vendor/product ID, product types, and categories are shown. Further:

- Nodes with a lock icon contain at least one secure interface
- Non-listening nodes have a ‘zz’ superscript sleep indicator
- Nodes with a ‘R’ icon are running in restricted mode
- Nodes with a ‘LR’ icon are included as Z-Wave Long Range node
- Failed nodes are shown in red and can be selected for replace/remove failed node operations.

Z-Wave+ information and version information from the node is also displayed at the bottom when the “>>” icon in the node entry is clicked.

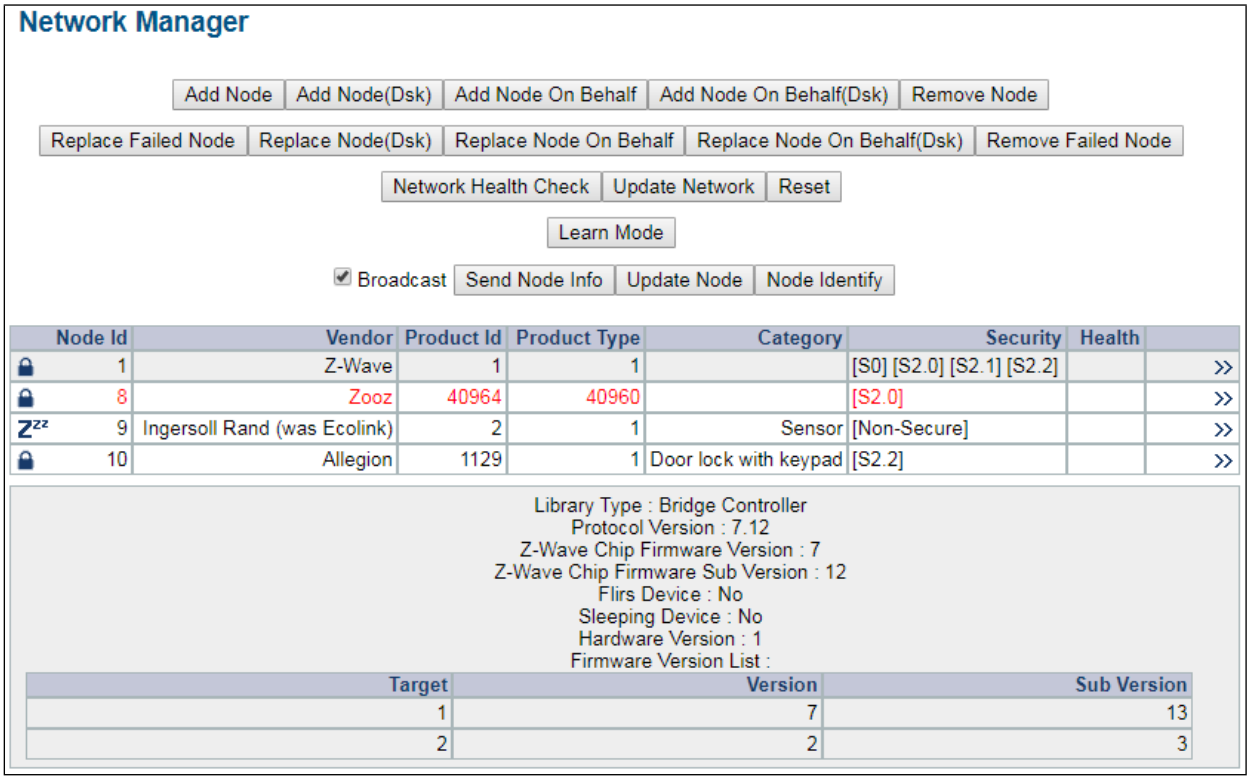


Figure 8: Network Manager Page

Progress information for all operations is shown to give immediate feedback to the user.

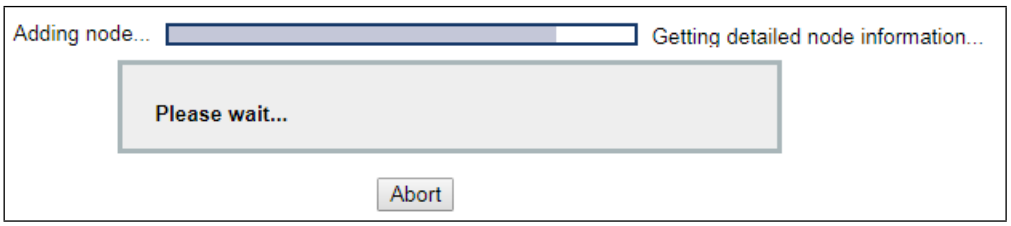


Figure 9: Network Operation Progress

The network operations are similar to the PC Controller software and will not be elaborated here. A quick map of operations to buttons is provided below.

Table 8: Z-Wave Network Buttons Mapping

Z-Wave Network Operation	Button(s)
Include nodes	Add Node
Exclude nodes	Remove Node
Include into an existing network	Learn Mode
Factory Reset	Reset

Network operation buttons are shown based on the role of the attached controller, for example, Add Node will not show a secondary controller. Node Identify button is enabled for nodes that support Indicator CC Identify ID.

4.4.1 Add/Remove Node (Optionally On Behalf)

This is a Z-Wave include/exclude network operation for non-SmartStart devices. Devices are automatically named if not previously named in the Node Naming CC. ZIPGW will always try classic inclusion first, then automatically proceed to Network Wide Inclusion (NWI) when it fails.

Note: While this operation can be aborted at any time with 'Abort' button, it is a compound operation that may perform secure bootstrapping and elaborate device discovery after a normal Z-Wave inclusion. Therefore, after abort, the device may still be included but insecurely or with interfaces undiscovered.

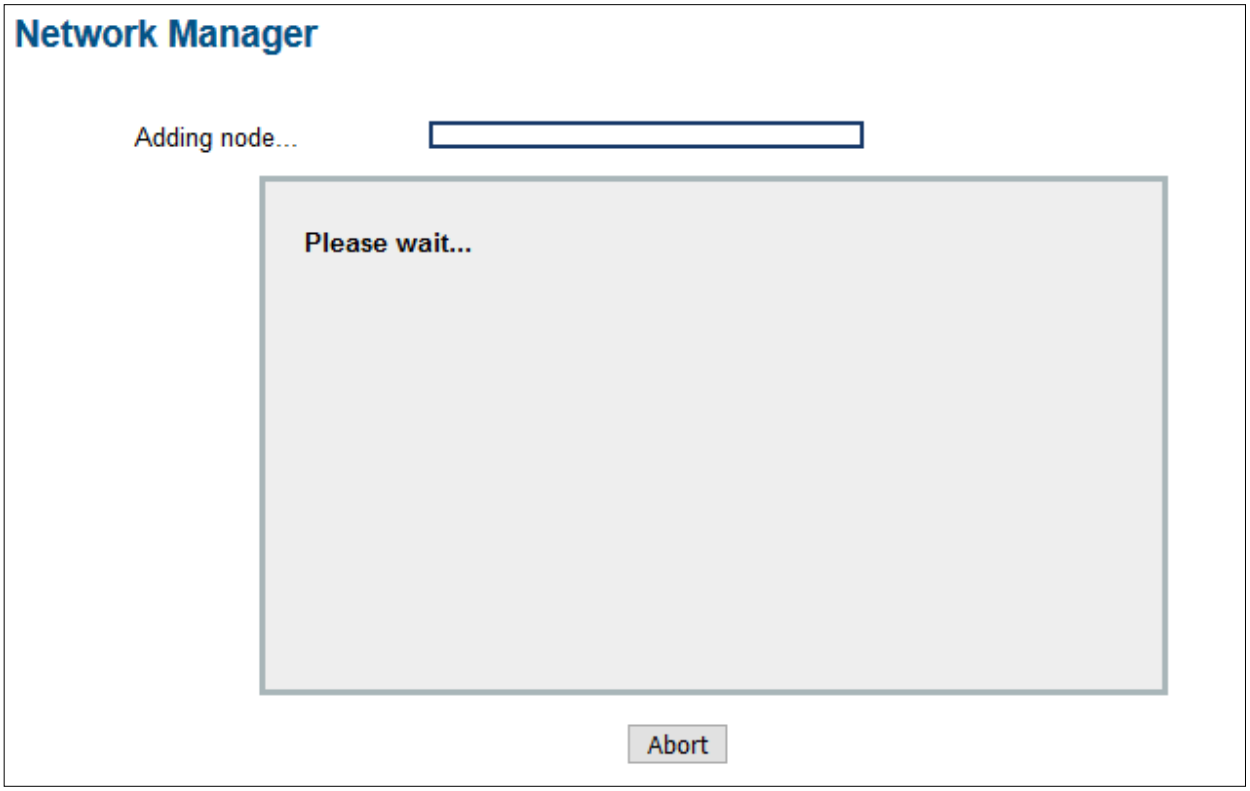


Figure 10: Adding node

With Security 2, DSK information may need to be entered and security keys granted/accepted.

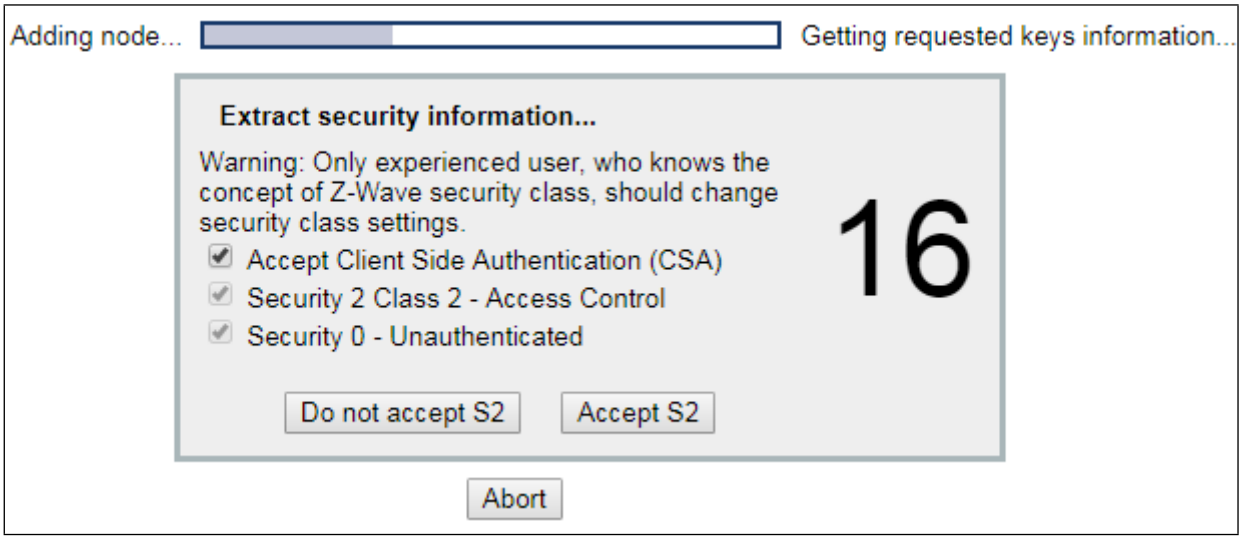


Figure 11: S2 Accepting Security Keys

Figure 12: S2 Entering DSK

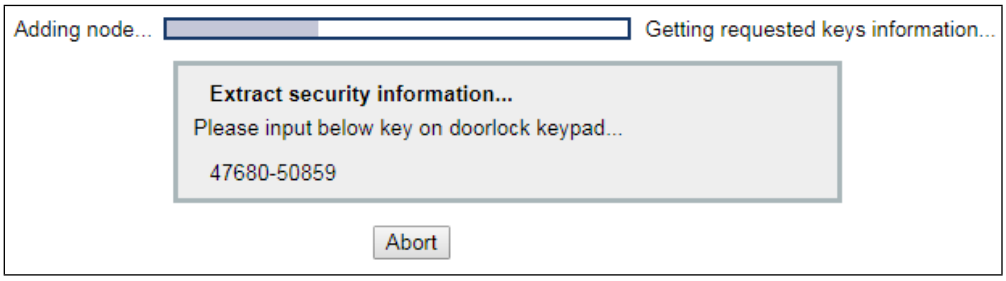


Figure 13: S2 CSA

Note: To add a Long Range node, the user needs to add an entry to a Smart Start provisioning list with Long Range SmartStart Bootstraping mode enabled.

4.4.2 Remove/Replace Failed Node (Optionally On Behalf)

This is a Z-Wave network function on failed devices. As with most network operations, it can be aborted. For Replace Failed node on Security 2 devices, additional pop ups, will appear.

4.4.3 Update Node

It rediscovers and updates the device – see [2].

4.4.4 Reset

This is the Z-Wave Set Default network operation.

4.4.5 Update Network

The rediscovers and updates all devices in the network – see [2] for details.

4.4.6 Learn Mode

This performs the Z-Wave Set Learn Mode network operation to allow this controller to join or be removed from a network. The corresponding including or removing controller needs to start Add or Remove node operation accordingly. To complete an S2 inclusion, the DSK may need to be entered on the including Controller.

Figure 14: S2 Set Learn Mode

4.4.7 Send Node Info

This sends the attached controller's Z-Wave Node Information Frame to the device.

4.4.8 Node Identify

This sends a command to chosen node to identify itself. The command parameters are as follows (see Indicator Command Class in [8]):

- On/Off Period 800ms,
- On/Off Cycles 3,
- On time within an On/Off period 600ms.

4.4.8.1 Identifying Z/IP Gateway/Z-Ware node

To identify the Z/IP Gateway/Z-Ware node one may:

- Using Z-Ware UI:
    1. Go to the Network Manager tab
    2. Select the Z/IP Gateway/Z-Ware row
        i. *Hint: The Z/IP Gateway Node Id can be read in the About tab (Local Node Id field)*
    3. Click the Node Identity button
- Or using another Controller:
    1. Send to Z/IP Gateway Node the Node Identify command (Indicator CC, INDICATOR_SET, Indicator ID: 0x50).

As a result, the Raspberry Pi hosting the Z/IP Gateway will blink the LED onboard as described in 4.4.8.

Figure 15. Node identification: the UI with Node Identity button highlighted; Raspberry Pi3B+ hosting Z/IP Gateway and Z-Ware with LED blinking

4.4.9 Network Health Check

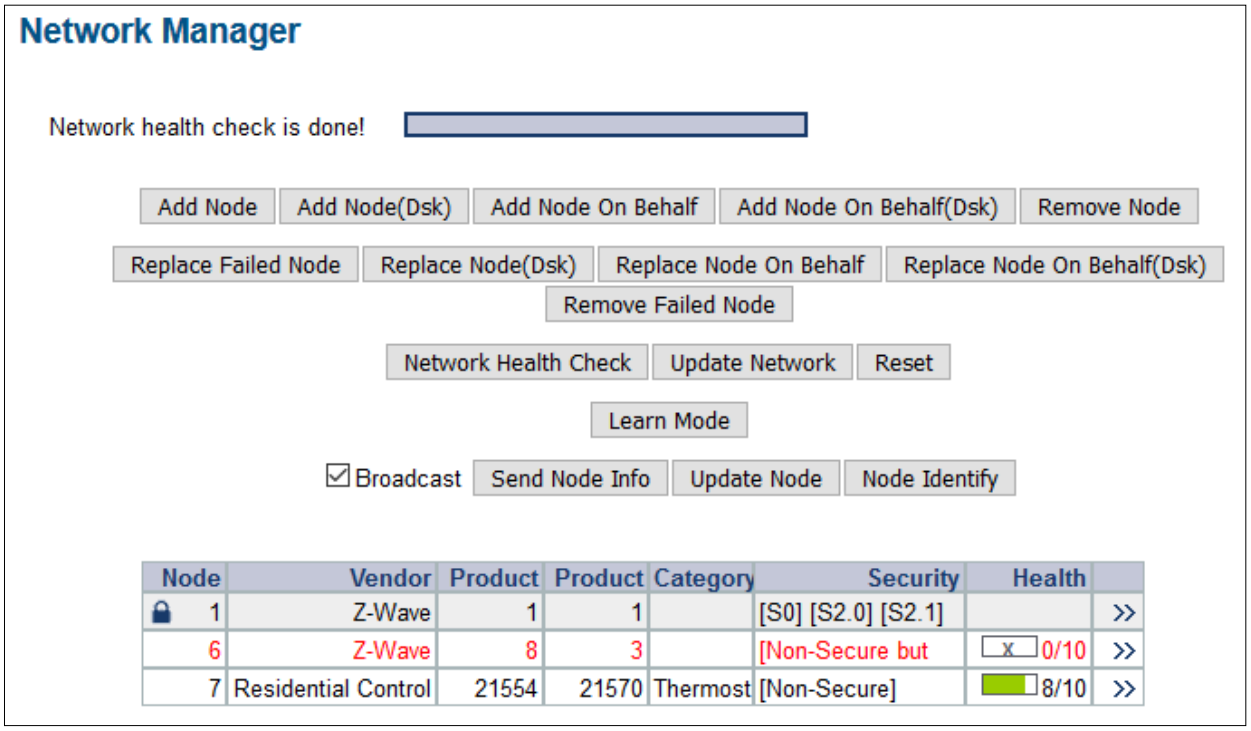


Figure 16: Network Health Check

4.4.10 Z-Wave Long Range Channel Configuration

Allows one to configure channel used by Z-Wave Long Range. Two channels are supported: Primary and Secondary.

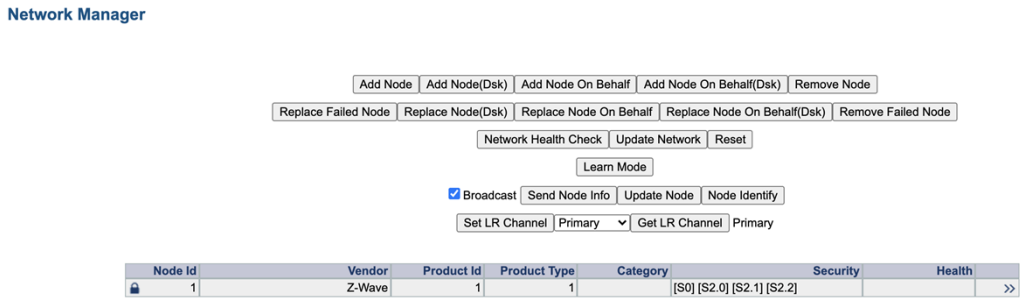


Figure 17: Z-Wave Long Range Channel

4.5 Settings

This page allows configuring the connected ZIP GATEWAY.

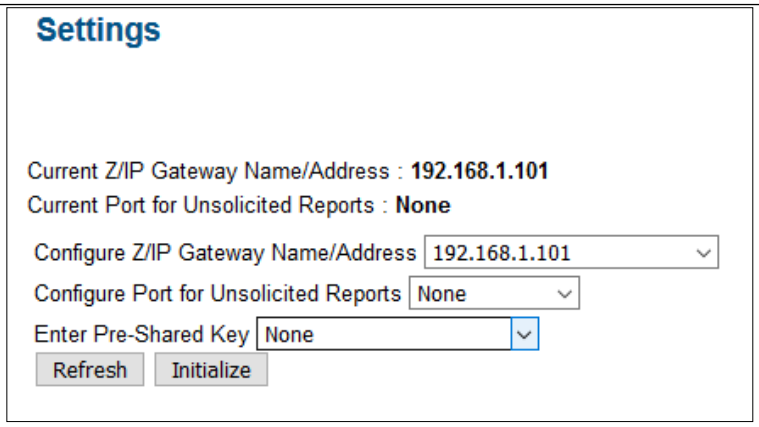


Figure 18: ZIP Gateway Settings

Detailed configuration of ZIP GATEWAY and ZIP PORTAL is accessible under Node Controller page.

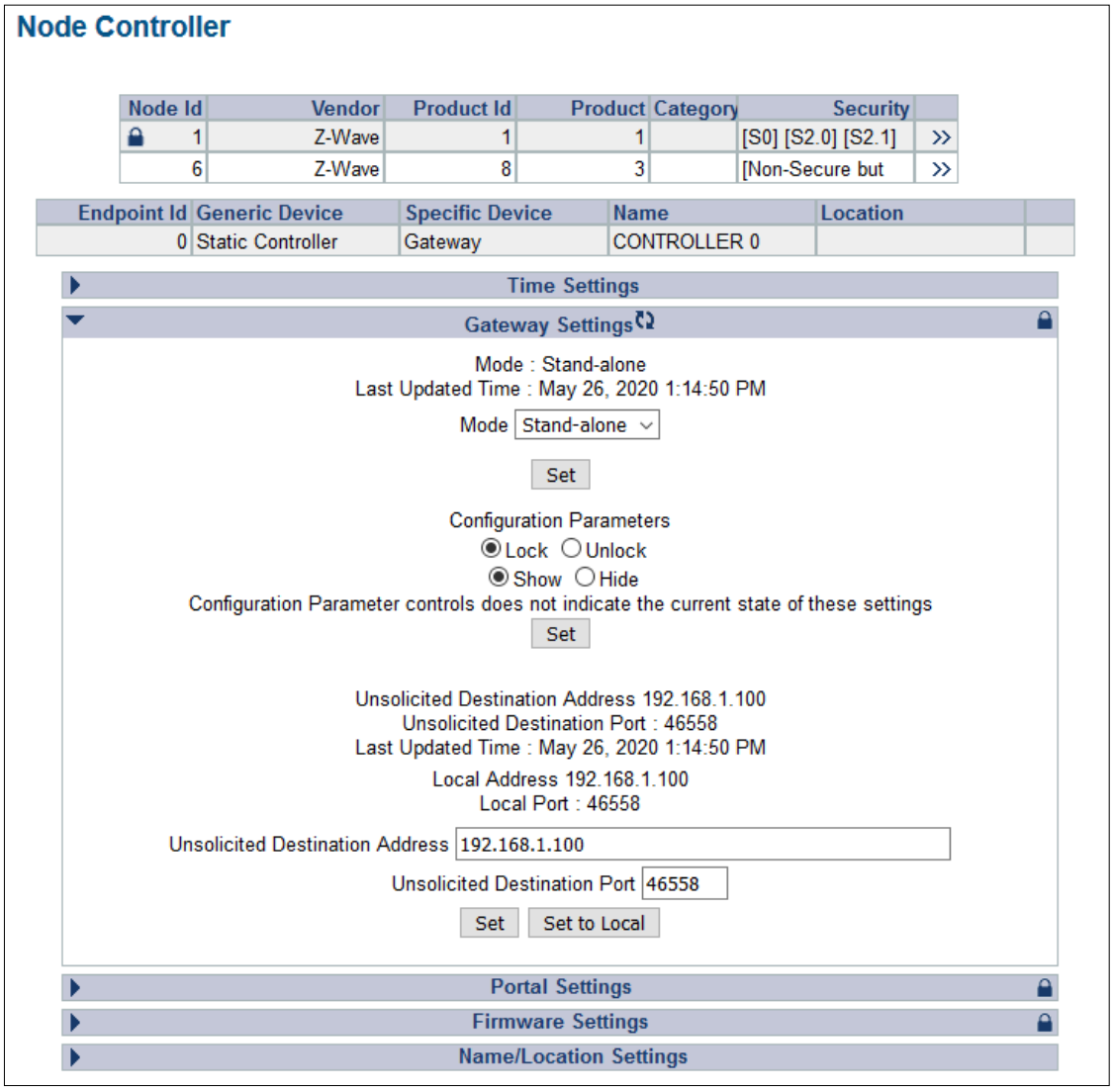


Figure 19: Detailed ZIP Gateway settings

4.6 SmartStart

On entry, the current provisioning list is shown. Each node has its status shown on the right. If a device added to the list is not SmartStart-capable, this is indicated with a '!' icon next to the status and normal Z-Wave inclusion, i.e., 'Add Device', has to be used.

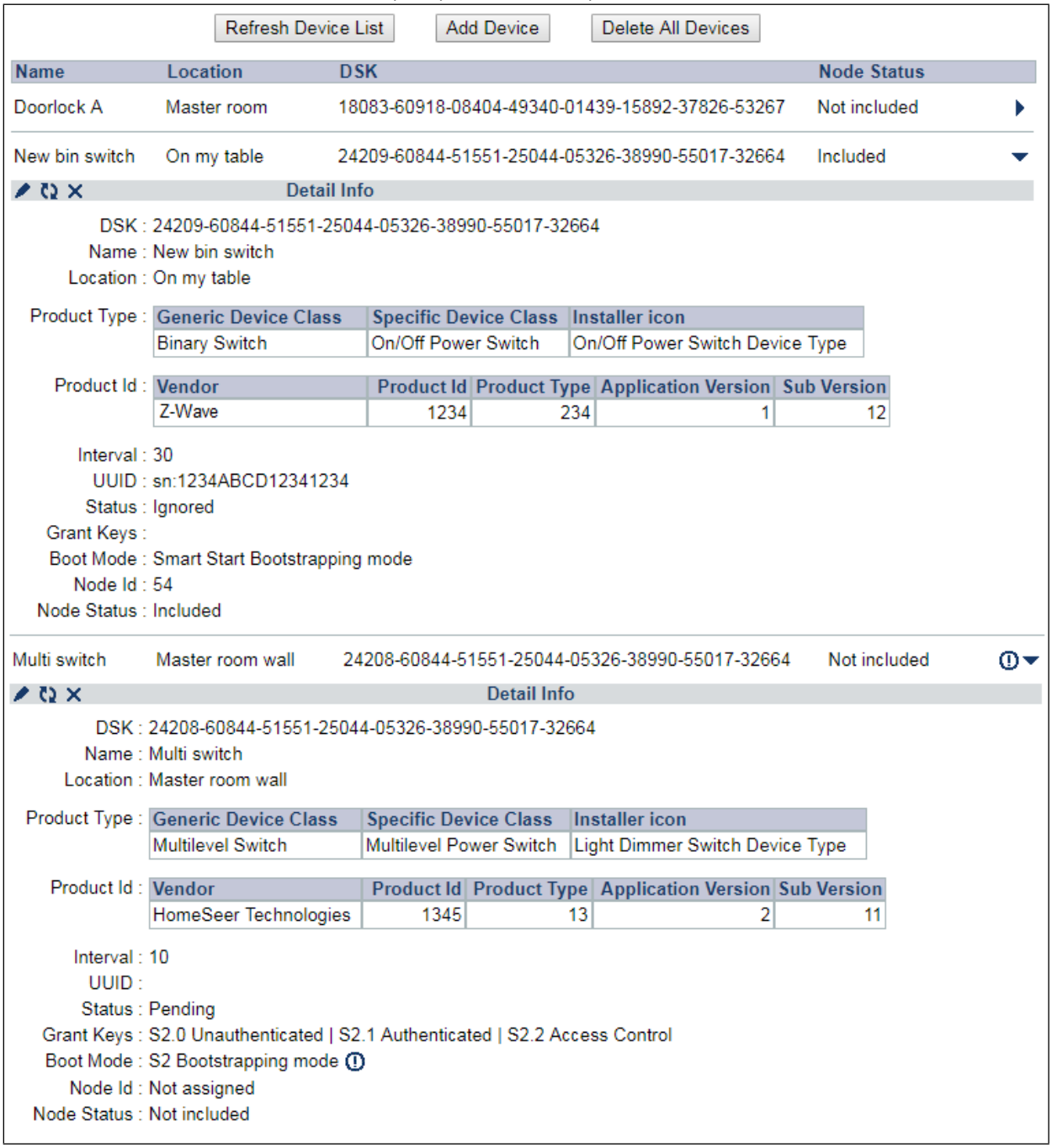


Figure 20: SmartStart List

Nodes can be added to this list using the 'Add Device' button on top. Clicking on the right arrow at the right of each node allows viewing the details. In the detailed view, the node can be refreshed, deleted, or edited. Adding a node and editing a node lead to the same page. In the edit page, a node in pending status can be ignored by selecting the 'ignore' radio button.

SmartStart nodes in the list that have already joined other networks when detected will cause a ‘device joined other network’ popup.

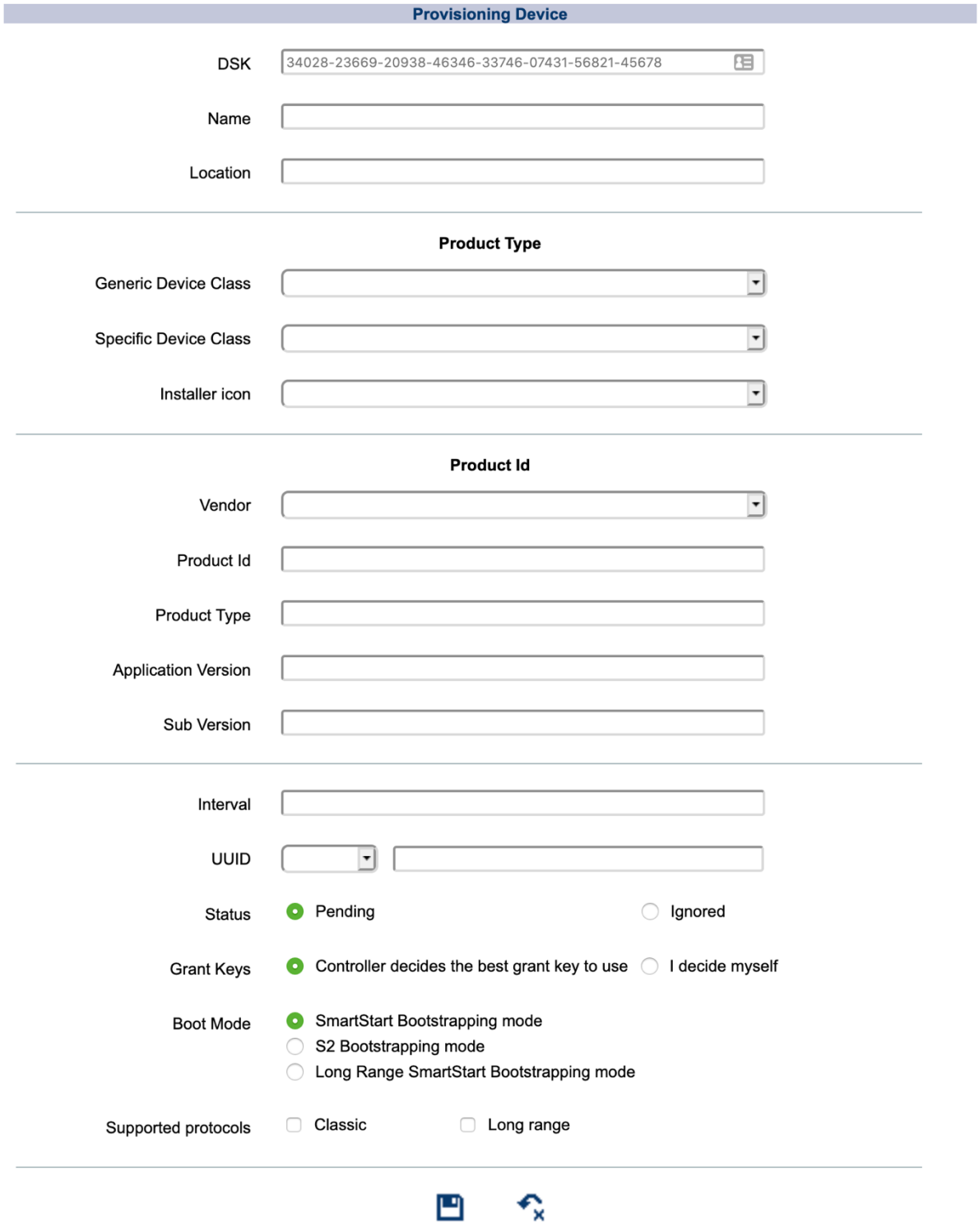


Figure 21: SmartStart Add/Edit Device

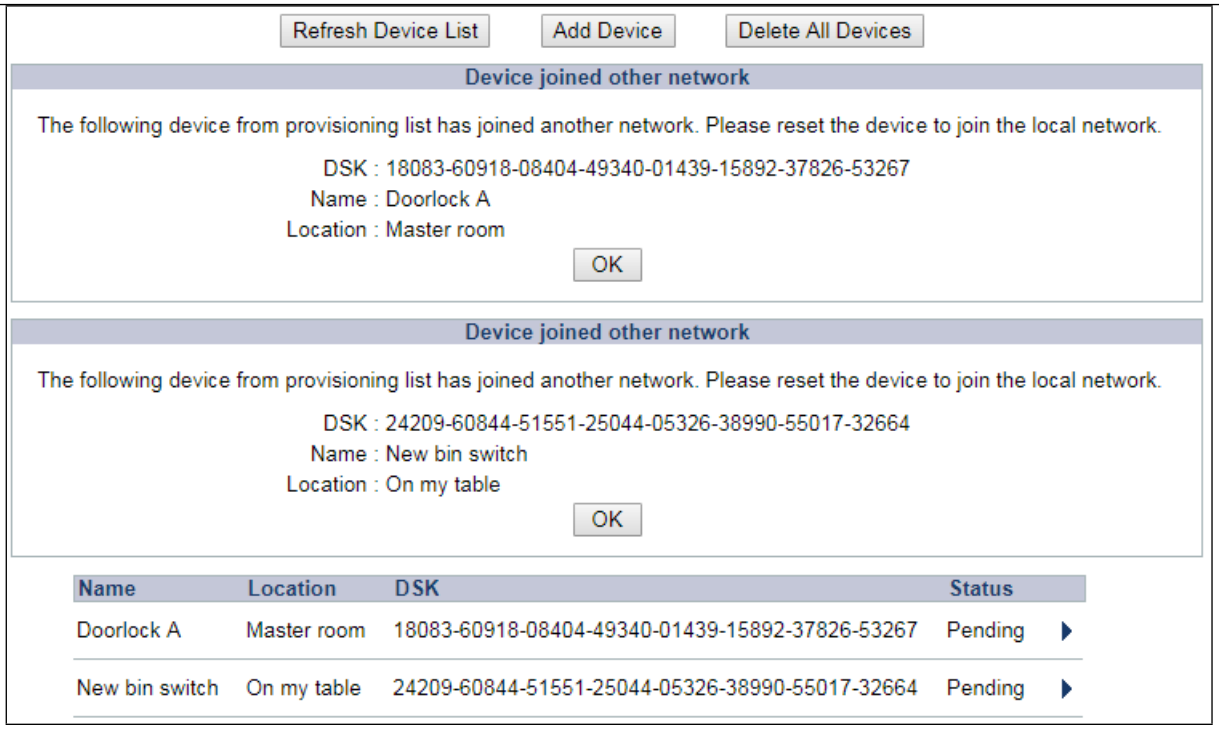


Figure 22: SmartStart Z-Wave Reset Required Detection

4.7 Node Controller

This page also lists all nodes in the network. The selected node's endpoints and device classes and the selected endpoint's interfaces are shown. Endpoints that support Z-Wave Plus are shown with a 'Z+' icon. Secure interfaces are shown with a lock icon. Clicking the arrow on the interface tab reveals the elements within for specific control or monitoring.

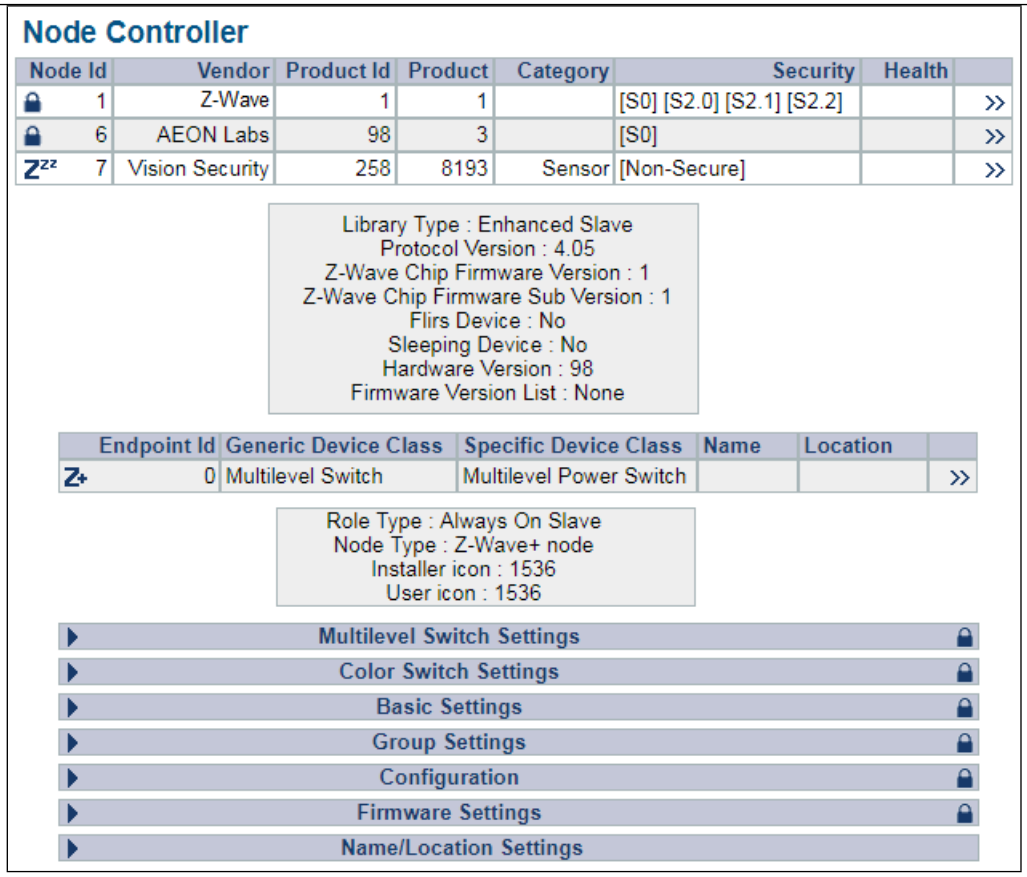


Figure 23: Node Controller Page

Clicking on the ">>" icon on the right of a node provides version information on the firmware and whether or not it is an FLIRS or a Sleeping Device. Clicking on the ">>" icon on the right of an endpoint provides Z-Wave Plus information.

4.8 Interfaces

Most of the interface panels have a cycle icon in the middle of the header to refresh the time-stamped state by soliciting data from the node/endpoint. For more information about each interface, see [7] to [10].

4.8.1 Basic

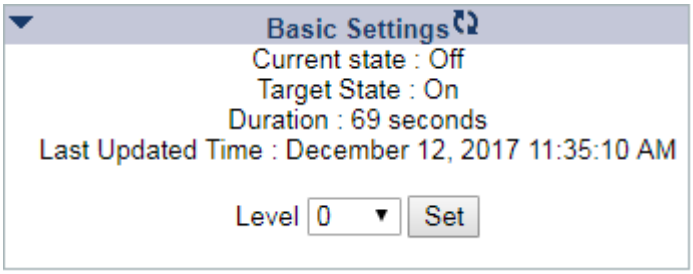


Figure 24: Basic Interface

Basic CC is device-specific and should be documented in the device's product manual. Target State and Duration are shown only if the device supports them.

4.8.2 Binary Sensor

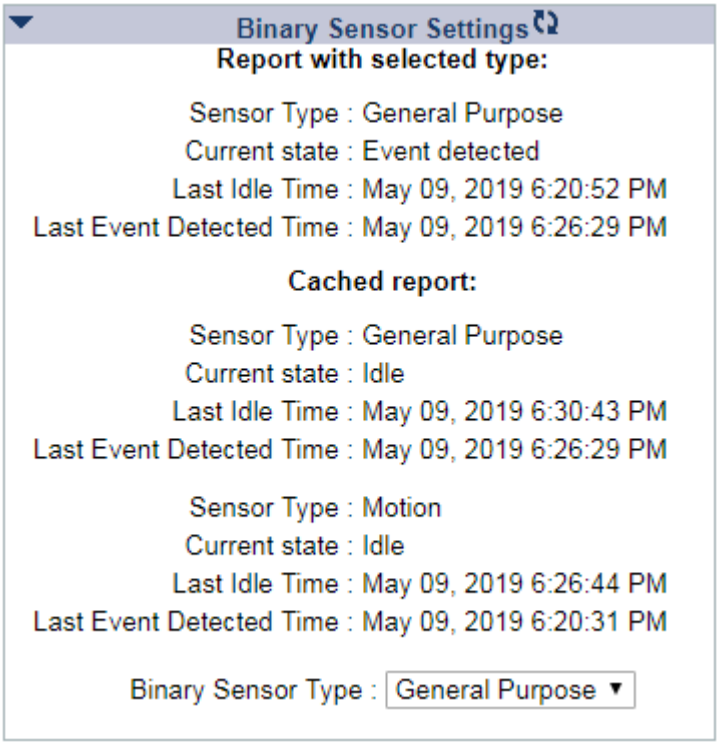


Figure 25: Binary Sensor Interface

4.8.3 Multi-Level Sensor

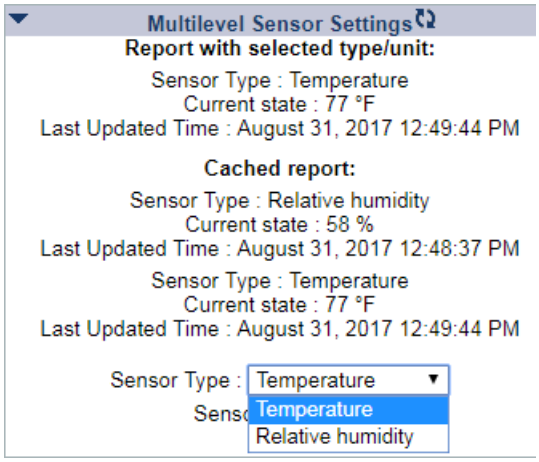


Figure 26: Multilevel Sensor Interface

4.8.4 Alarm/Notification

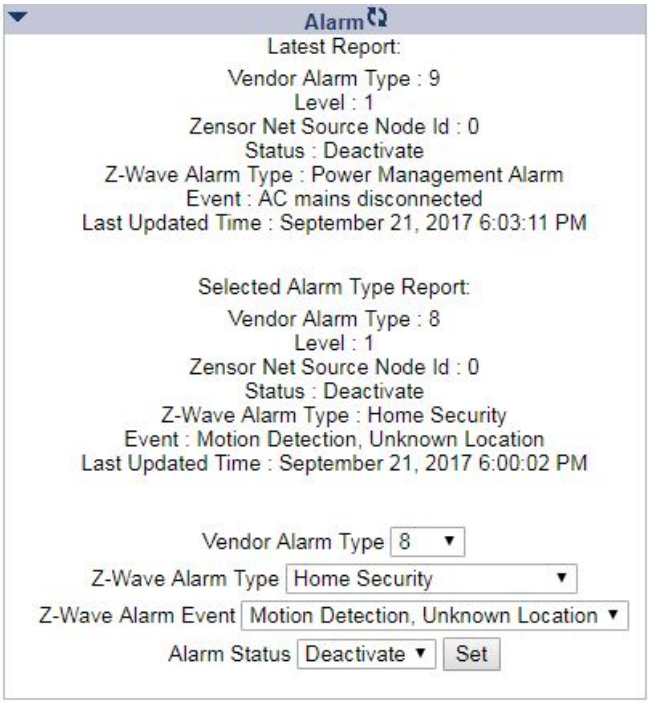


Figure 27: Alarm/Notification Interface

4.8.5 Meter

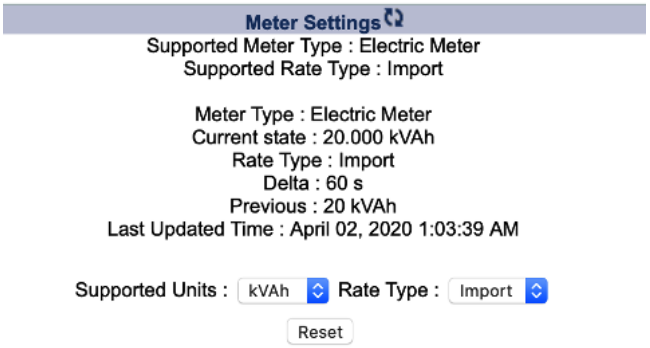


Figure 28: Meter Interface

4.8.6 Battery

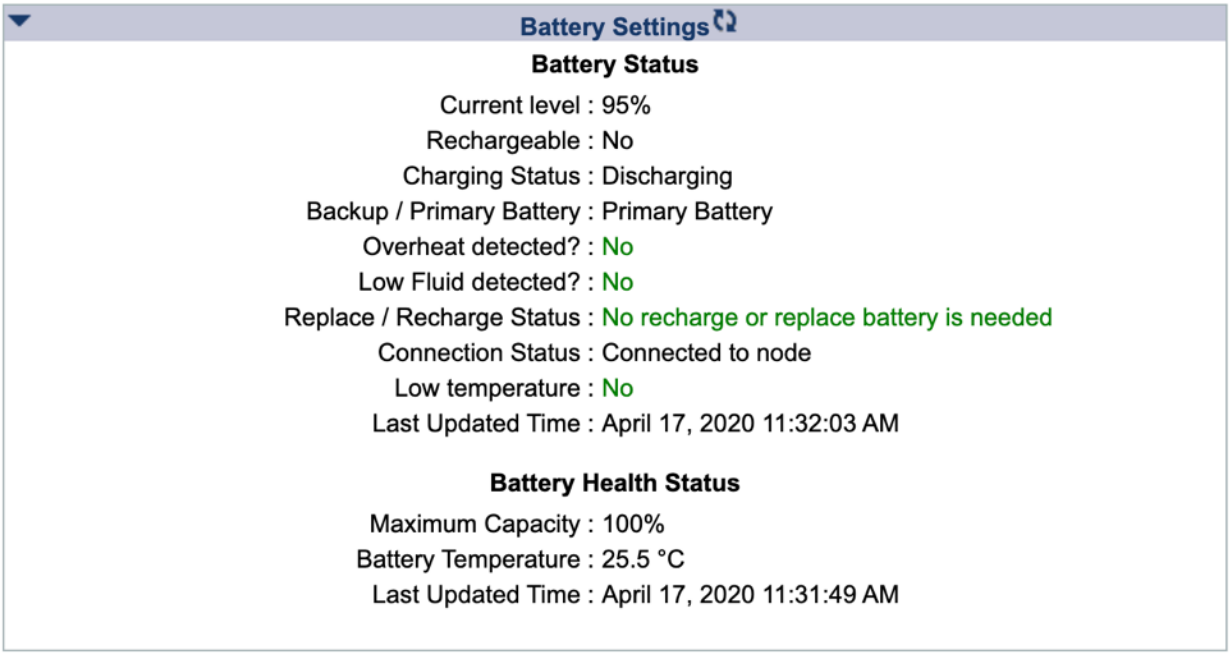


Figure 29: Battery Interface

4.8.7 Binary Switch

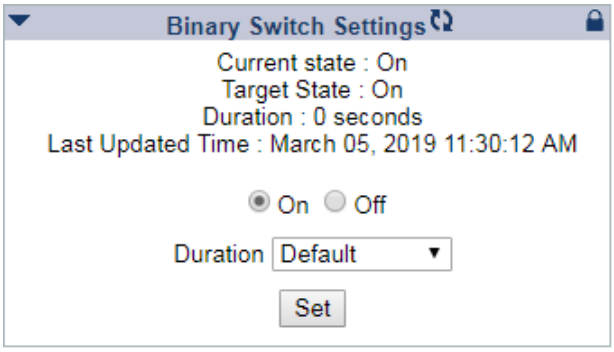


Figure 30: Binary Switch Interface

4.8.8 Multi-Level Switch

Depending on the CC version, the control elements may vary.

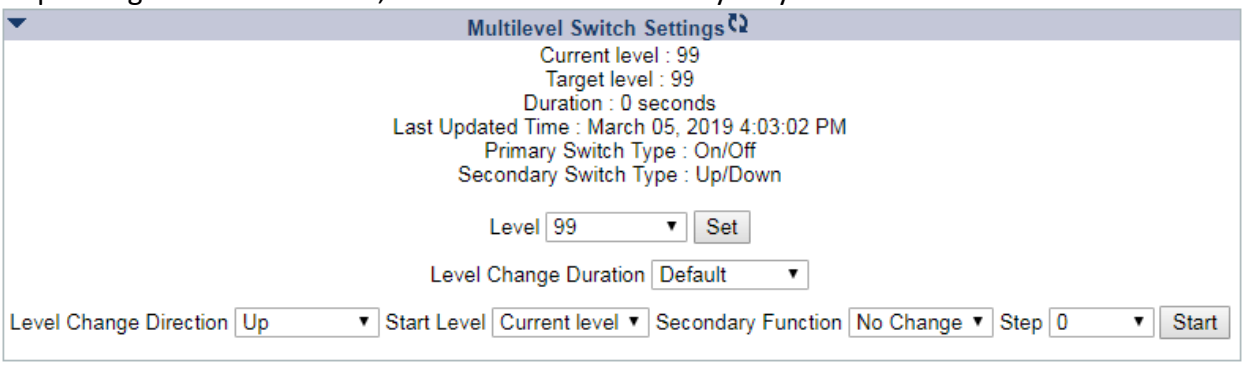


Figure 31: Multilevel Switch Interface

4.8.9 Color Switch Interface

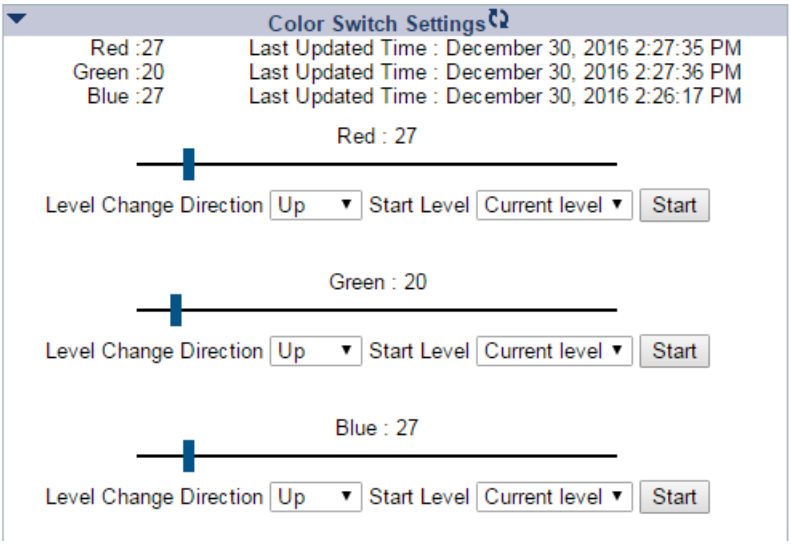


Figure 32: Color Switch Interface

4.8.10 Central Scene Controller

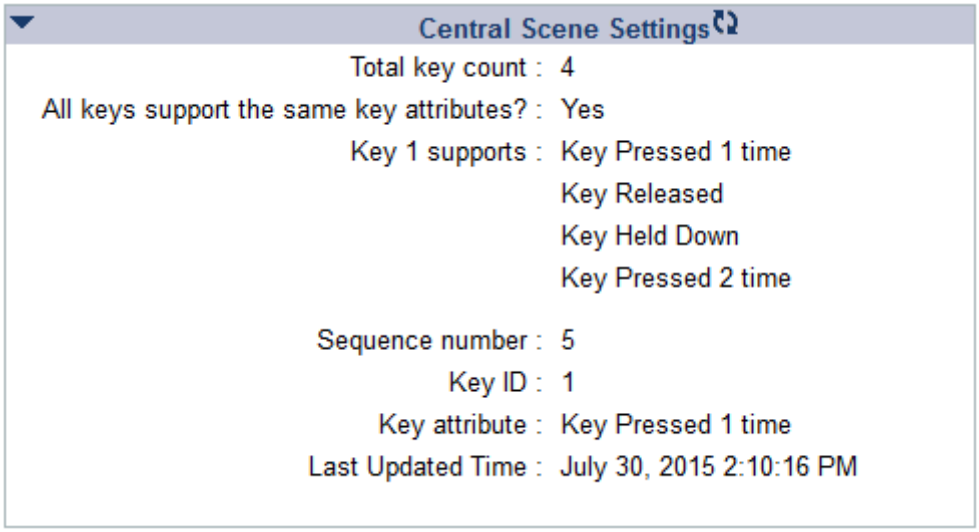


Figure 33: Central Scene Controller Interface

4.8.11 Door Lock

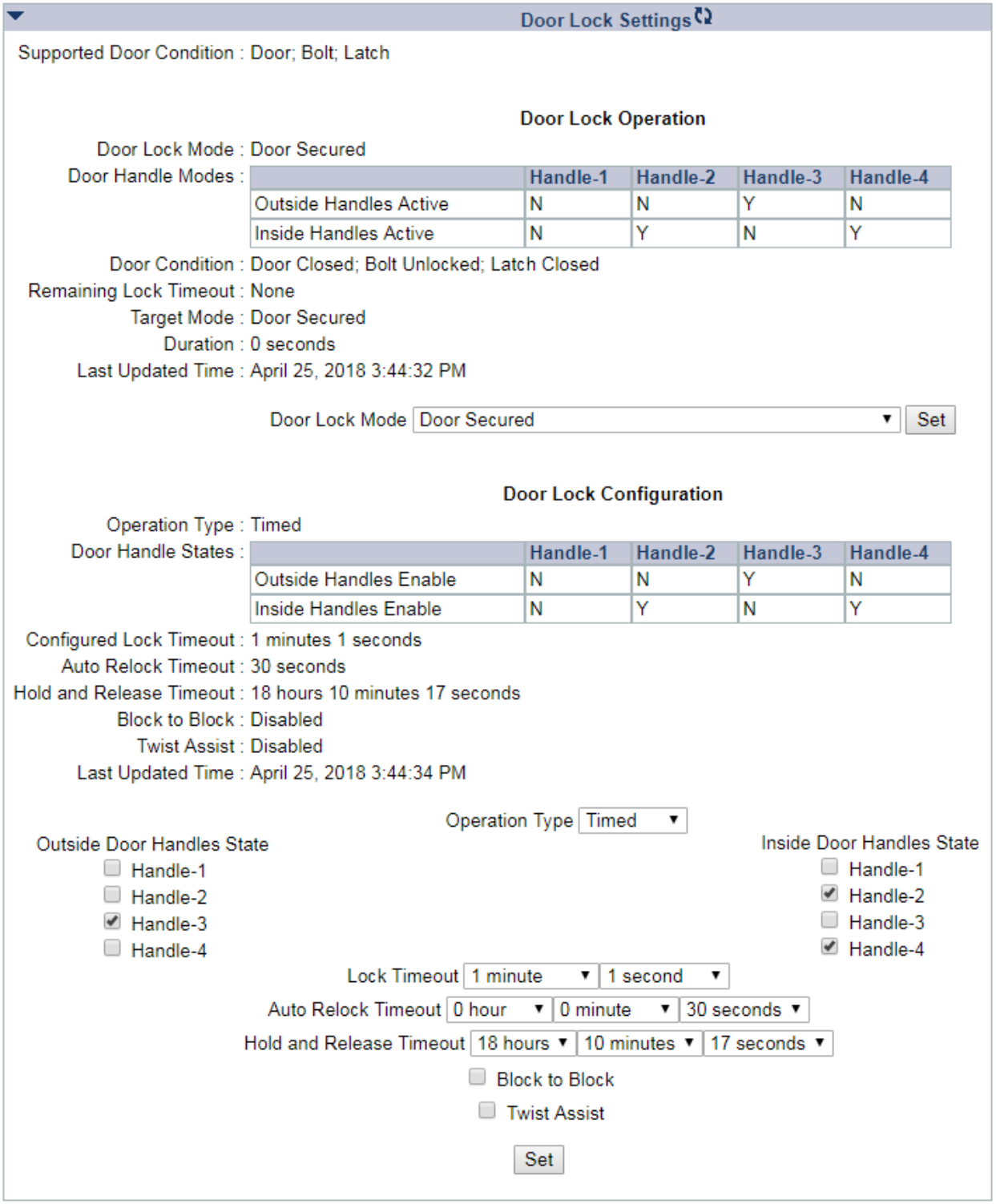


Figure 34: Door Lock Interface

4.8.12 User Code

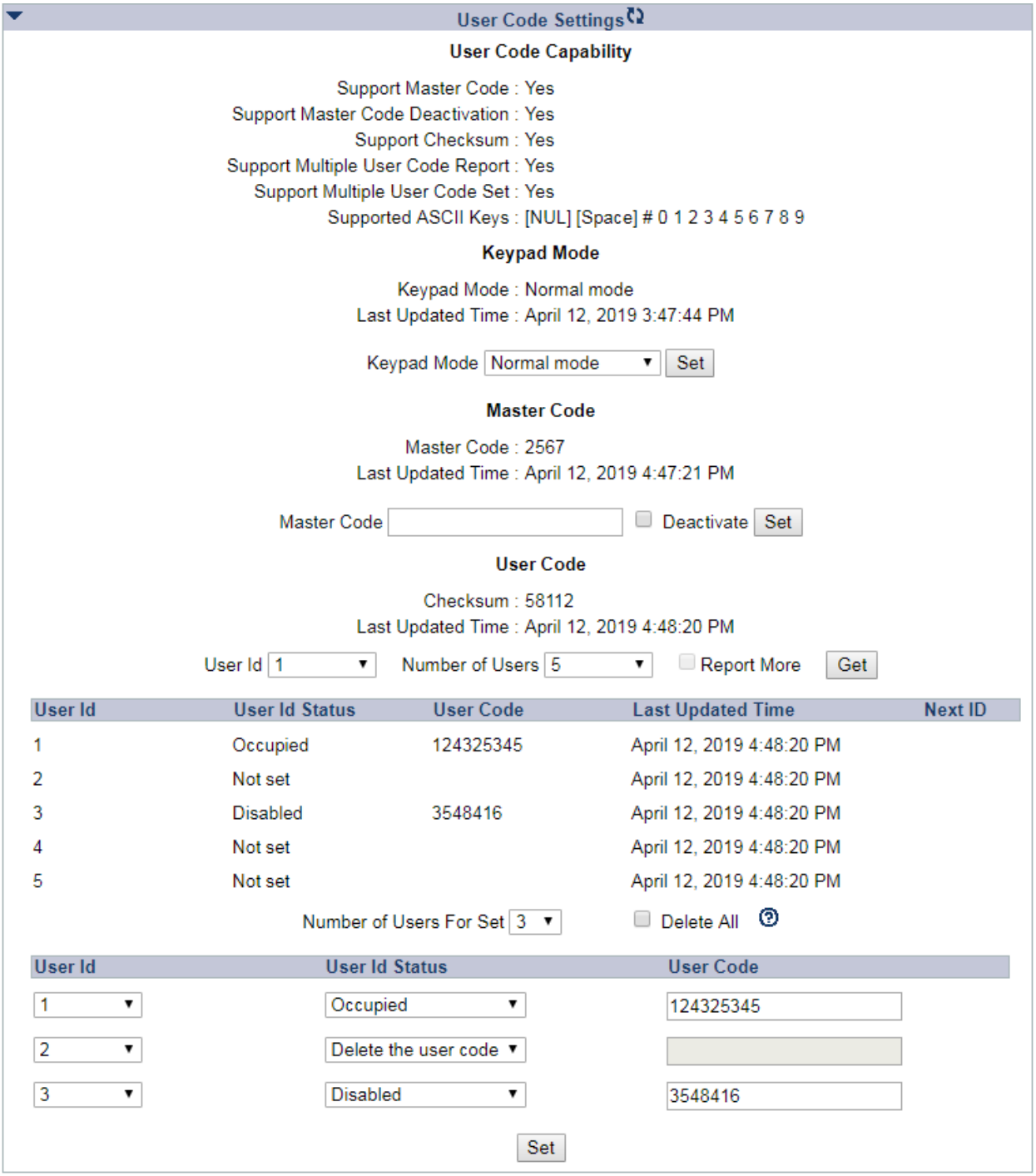
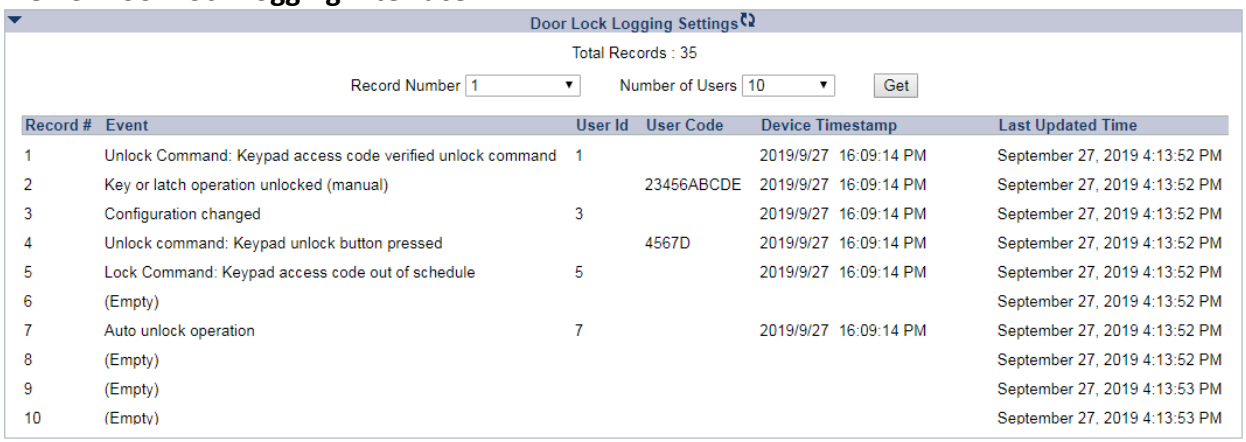


Figure 35: User Code Interface

4.8.13 Door Lock Logging Interface



Record #	Event	User Id	User Code	Device Timestamp	Last Updated Time
1	Unlock Command: Keypad access code verified unlock command	1		2019/9/27 16:09:14 PM	September 27, 2019 4:13:52 PM
2	Key or latch operation unlocked (manual)		23456ABCDE	2019/9/27 16:09:14 PM	September 27, 2019 4:13:52 PM
3	Configuration changed	3		2019/9/27 16:09:14 PM	September 27, 2019 4:13:52 PM
4	Unlock command: Keypad unlock button pressed		4567D	2019/9/27 16:09:14 PM	September 27, 2019 4:13:52 PM
5	Lock Command: Keypad access code out of schedule	5		2019/9/27 16:09:14 PM	September 27, 2019 4:13:52 PM
6	(Empty)				September 27, 2019 4:13:52 PM
7	Auto unlock operation	7		2019/9/27 16:09:14 PM	September 27, 2019 4:13:52 PM
8	(Empty)				September 27, 2019 4:13:52 PM
9	(Empty)				September 27, 2019 4:13:53 PM
10	(Empty)				September 27, 2019 4:13:53 PM

Figure 36: Door Lock Logging Interface

4.8.14 Barrier Operator Interface

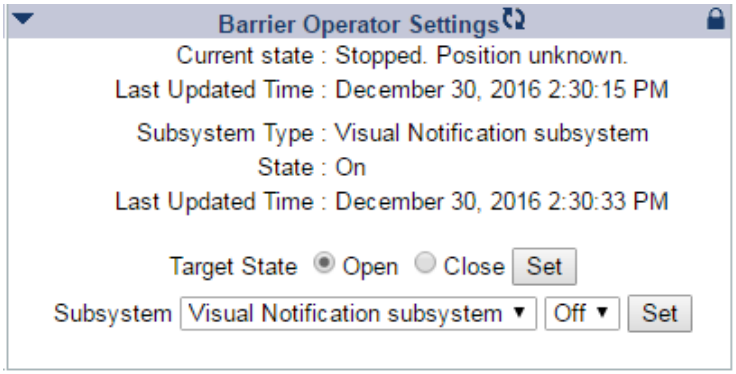


Figure 37: Barrier Operator Interface

4.8.15 Window Covering Interface

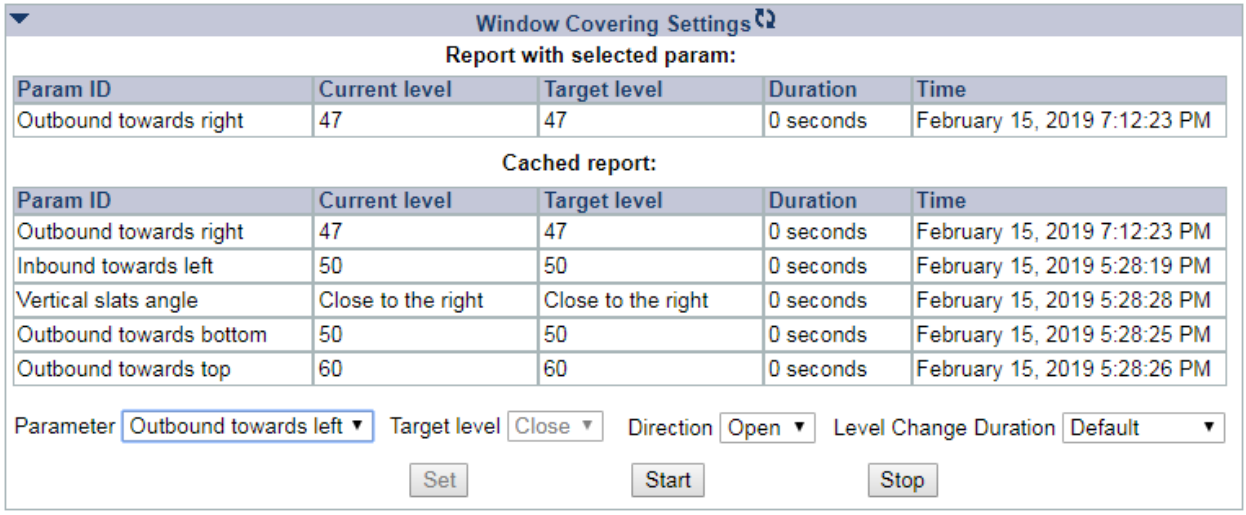


Figure 38: Window Covering Interface

4.8.16 Anti-theft Unlock Interface

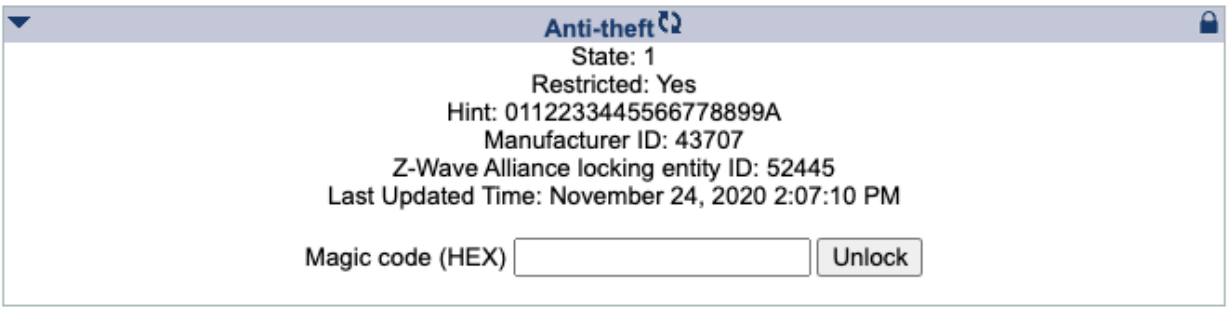


Figure 39: Anti-theft Unlock Interface

4.8.17 Thermostat-Related Interfaces

4.8.17.1 Thermostat Fan

If both Fan Mode and State interfaces are available in the endpoint, they will be shown combined in a single frame. Otherwise, they will be shown separately.

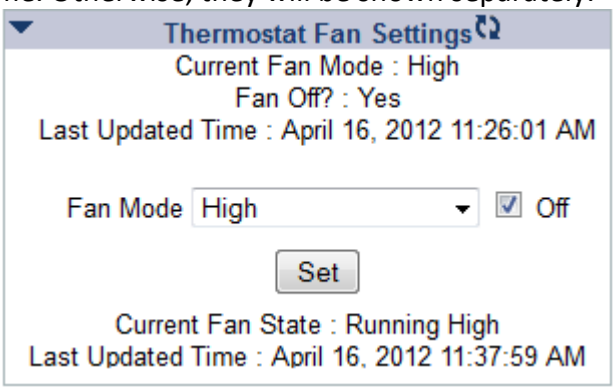


Figure 40: Thermostat Fan Interface

4.8.17.2 Thermostat Mode and Operating State

If both Mode and State interfaces are available in the endpoint, they will be shown combined in a single frame. Otherwise, they will be shown separately.

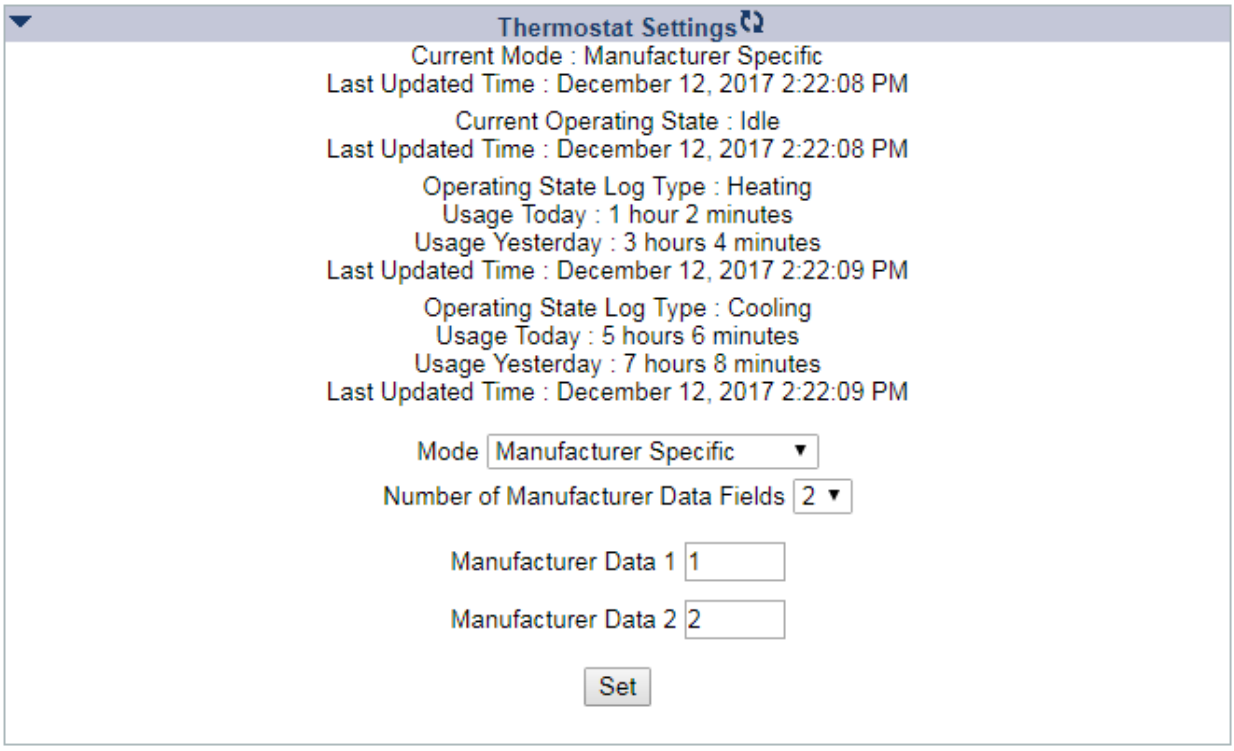


Figure 41: Thermostat Mode and State Interface

4.8.17.3 Thermostat SetPoint

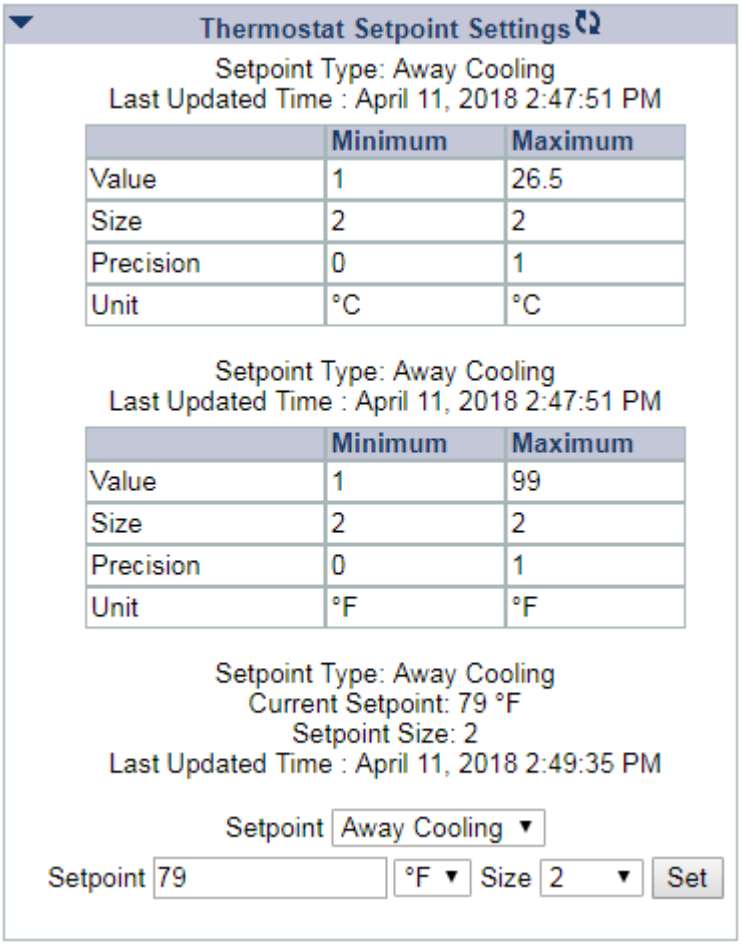


Figure 42: Thermostat Setpoint Interface

4.8.18 Sound Switch

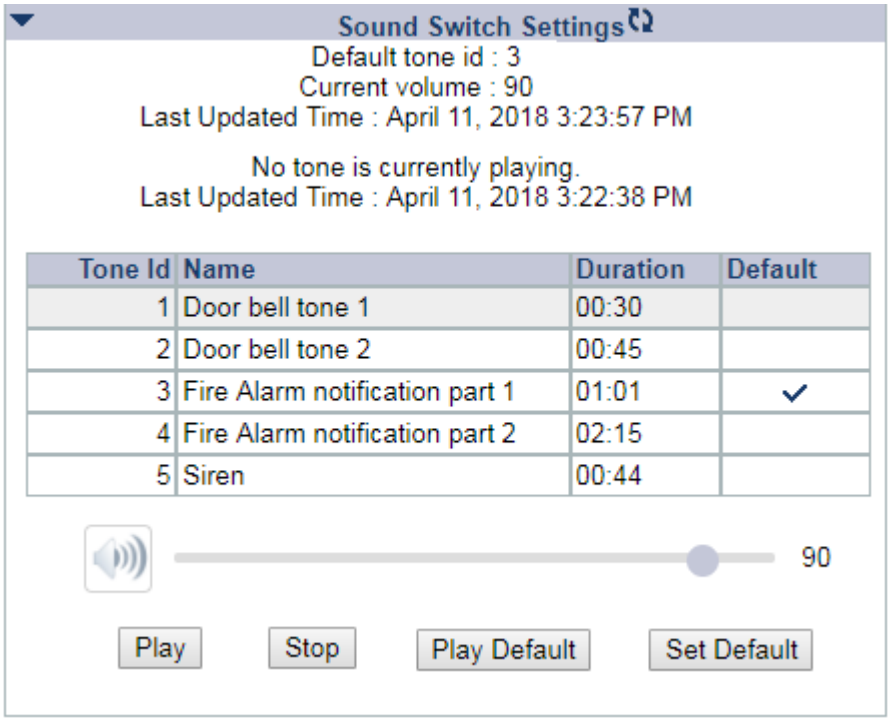


Figure 43: Sound Switch Interface

4.8.19 Indicator

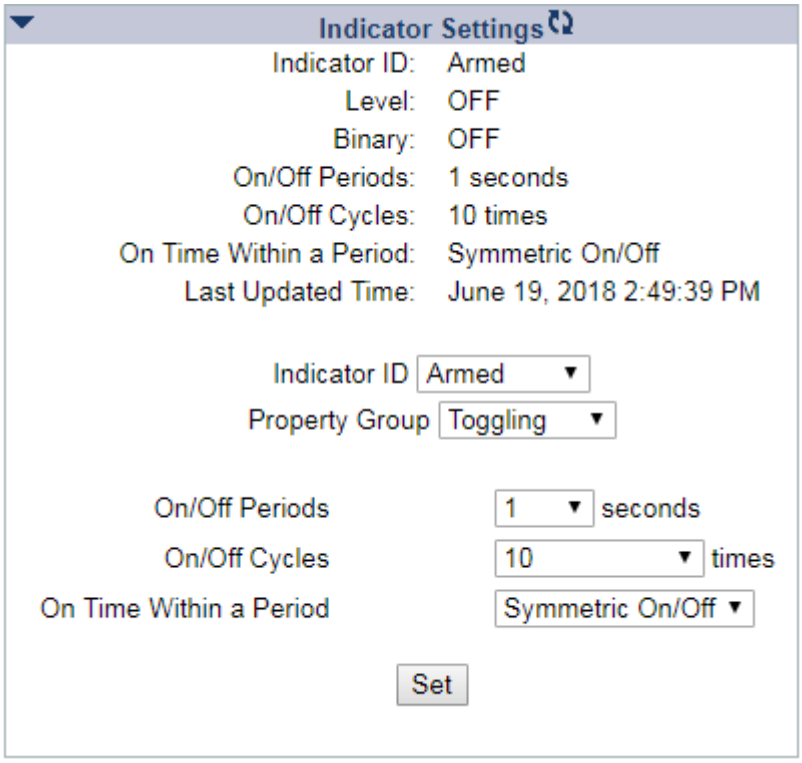


Figure 44: Indicator Interface

4.8.20 Naming/Location

The name/location interface always exists, at least on the local machine, even if the device does not support the corresponding CC. The name/location is used to set the name/location strings for easier identification. If the device supports the CC, the name is initialized from the device during inclusion and is only refreshed after a node update and setting will set to the device as well.

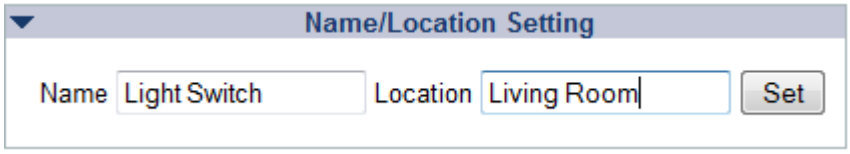


Figure 45: Name/Location Interface

4.8.21 Association

The user can add or remove node or endpoints (depending on interface support) to any group supported by the interface limited by its storage. Association, Multichannel Association, and Association Group Information (AGI) details are shown in this interface.

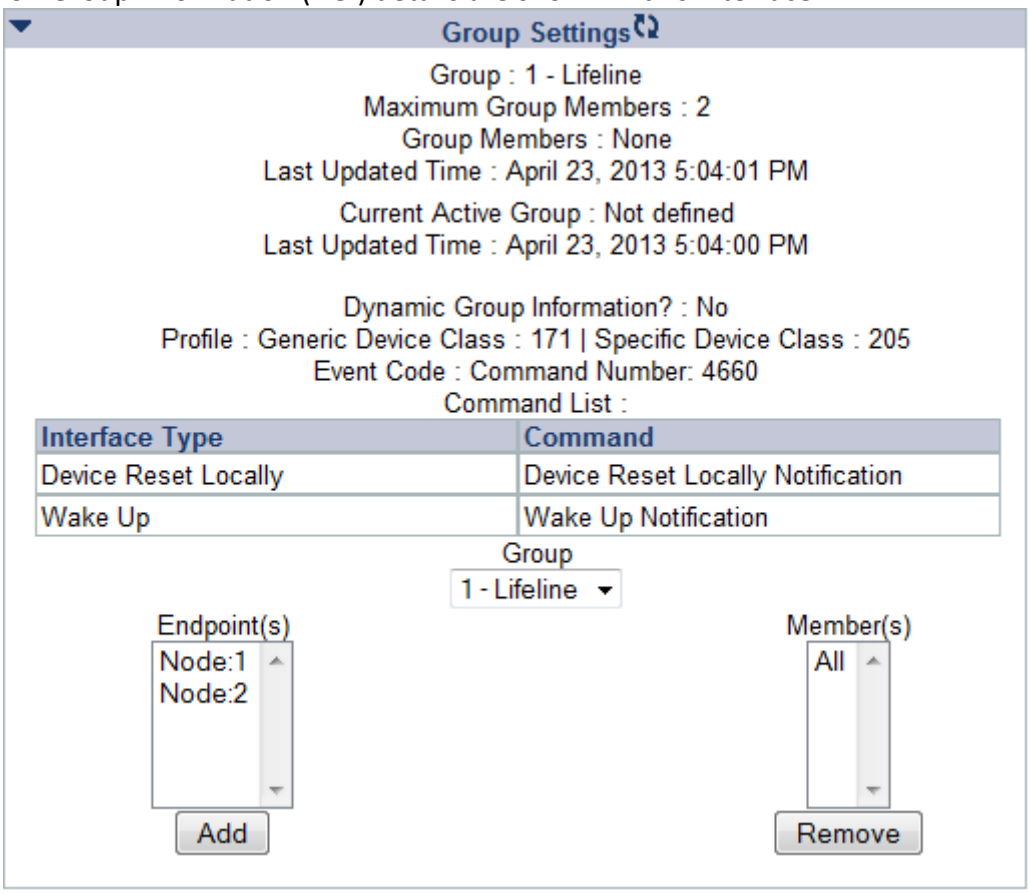


Figure 46: Group Interface

4.8.22 Configuration

Configuration is a manufacturer-specific setting which requires referring to the product manual. ‘Size’ can be specified explicitly or as the minimum size needed for the given value. Enabling ‘Default’ ignores the ‘Value’ and resets the configuration parameter after ‘Set’. ‘Number of parameters’, available only if the device supports it, allows setting multiple

parameters and as many ‘Value’ fields will appear. Enabling ‘Handshake’, available only if the device supports it, returns a report after ‘Set’.

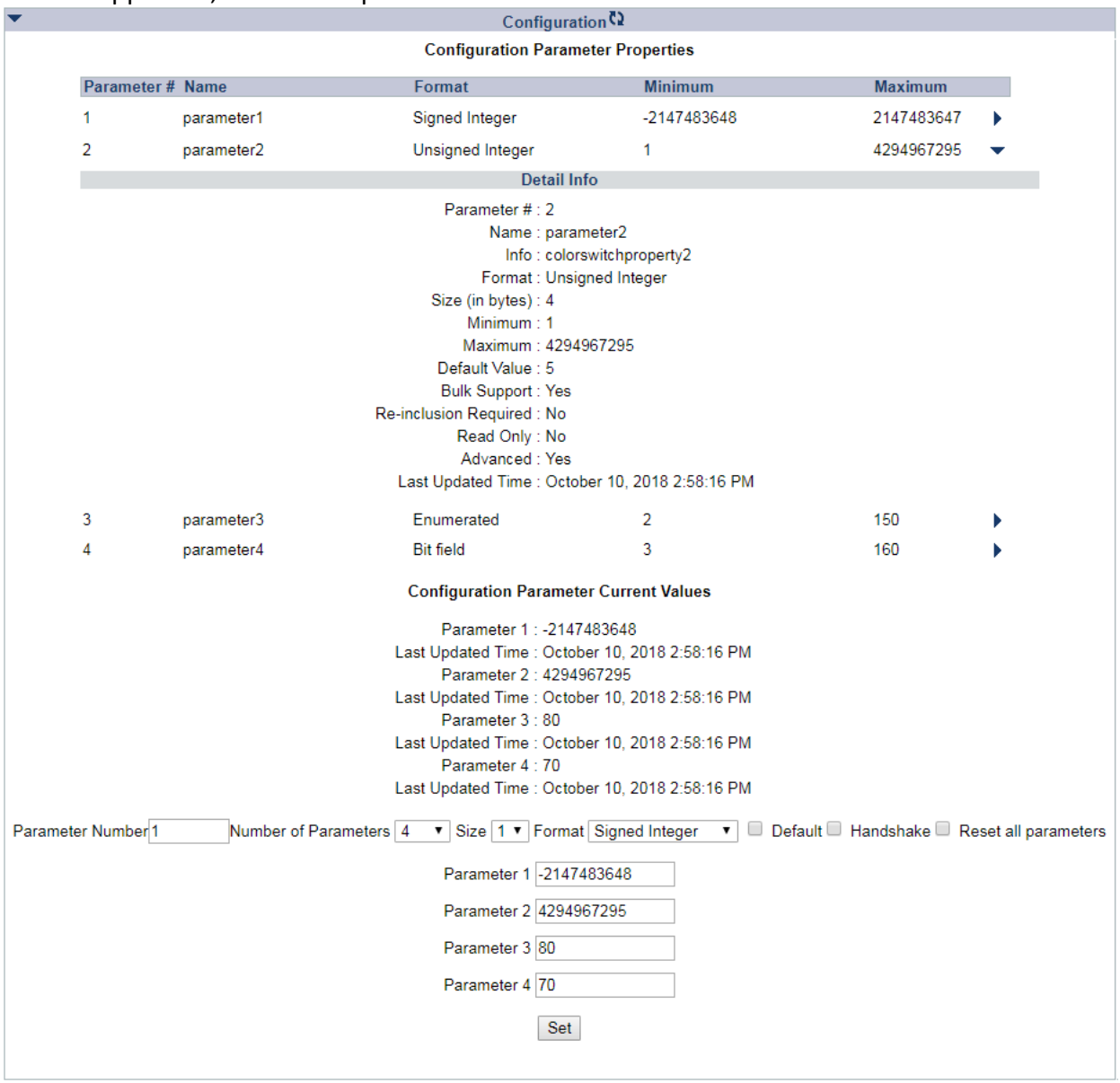


Figure 47: Configuration Interface

4.8.23 Wakeup

Set the controller as the notified node. Otherwise, it will not be able to de-queue commands for this node. This is automatically done by Z-Ware. Users should not change anything on this interface because the newer versions of the underlying ZIPGW expect the current settings for its mailbox service.

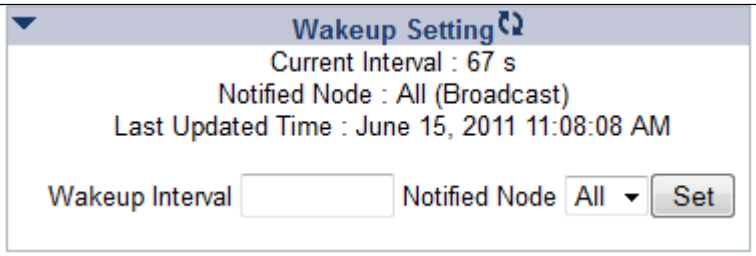


Figure 48: Wakeup Interface

4.8.24 Firmware Update

Use this interface to upgrade firmware (Z-Wave chip or others, such as a host controller) in the node. This can also be used to push security certificates and network configurations to the node. The usage of multiple firmware/targets and checksum are manufacturer-dependent and should be found in the relevant production manual or upgrade documentation.

Limitation: Instead of uploading the firmware files from the a web client (browser), these files must be placed under a 'data' folder at the (platform-specific) application data area shown.

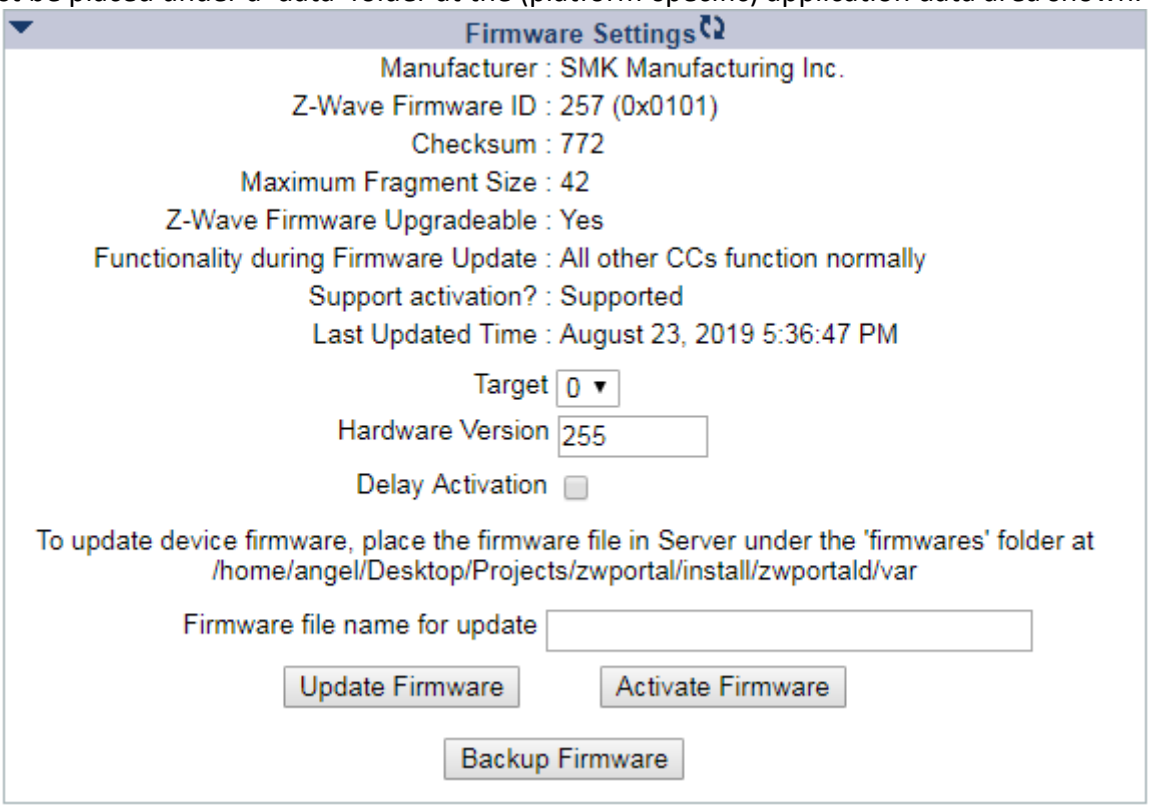


Figure 49: Firmware Update Interface

4.8.25 Protection

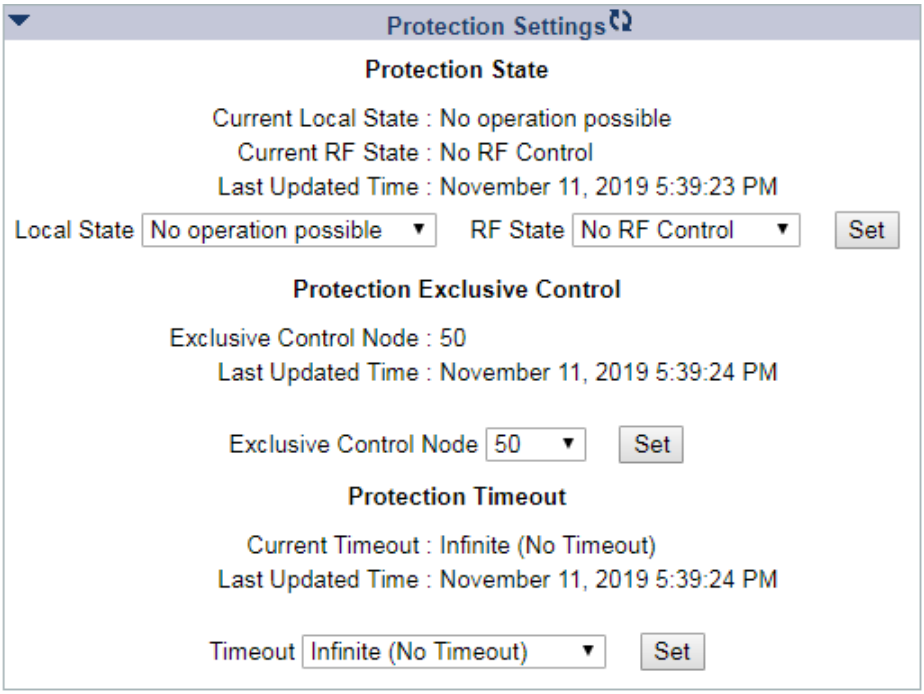


Figure 50: Protection Interface

4.8.26 Z/IP Gateway

Z/IP Gateway is an interface to configure the ZIPGW with a peer name, peer IP address, and peer port number. Unsolicited destination addresses and port numbers can also be configured. 'Set to Local' button allows to set the locally reachable IP address and local listening port number as unsolicited destination. Despite the fact, the Portal mode has been removed from Z-Ware, the Engineering UI still has functions to configure the Gateway for the Portal mode.

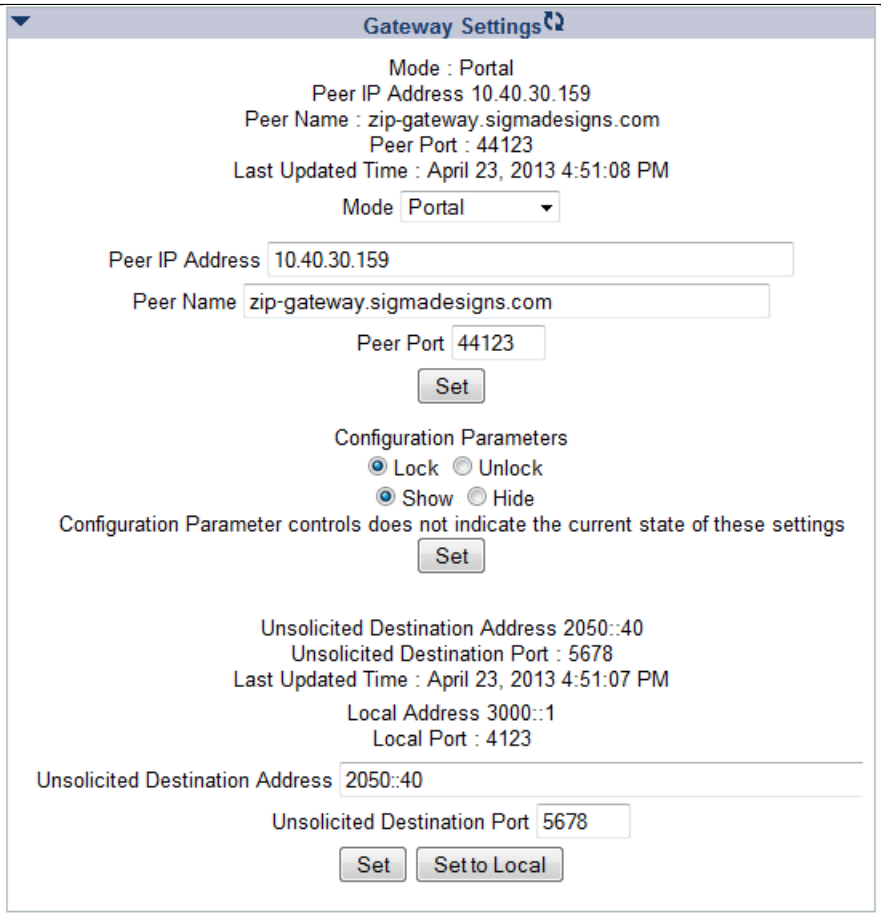


Figure 51: ZIPGW Interface Portal Mode

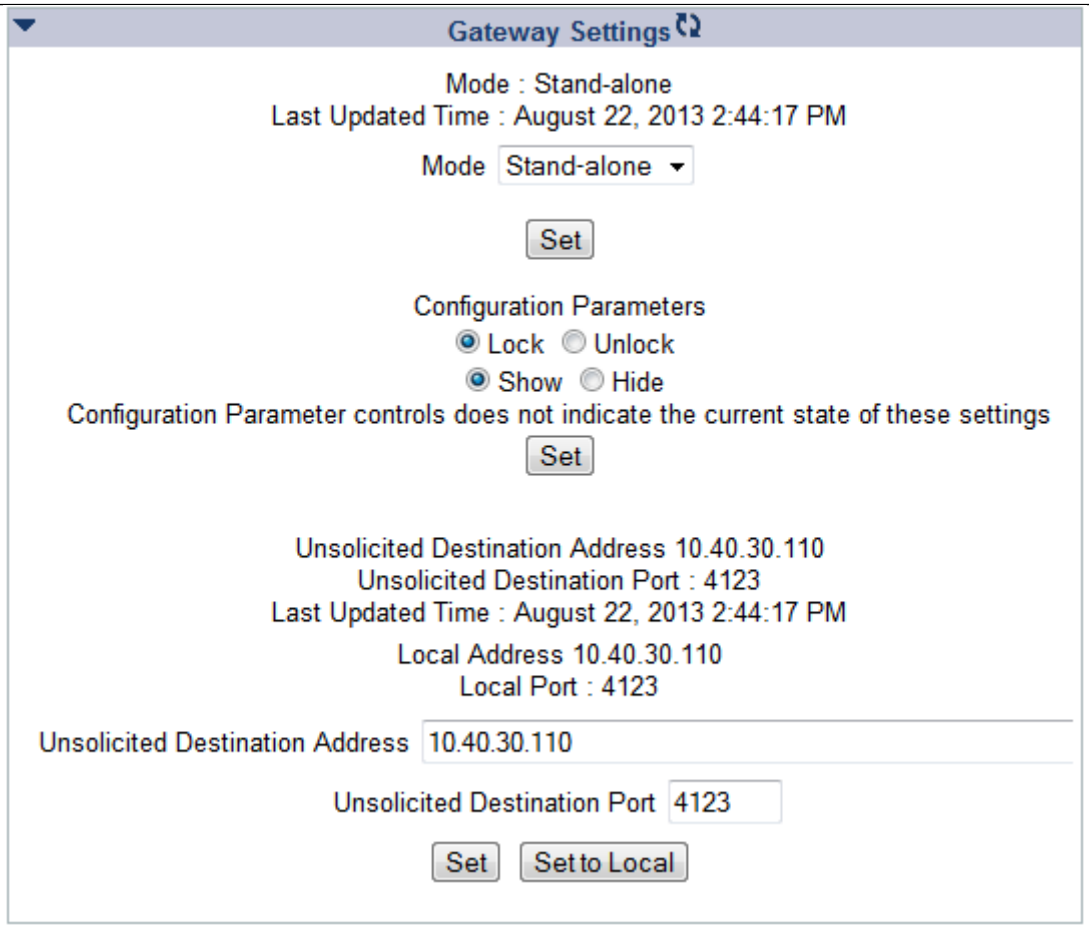


Figure 52: ZIPGW Interface Standalone Mode

4.9 Scenes

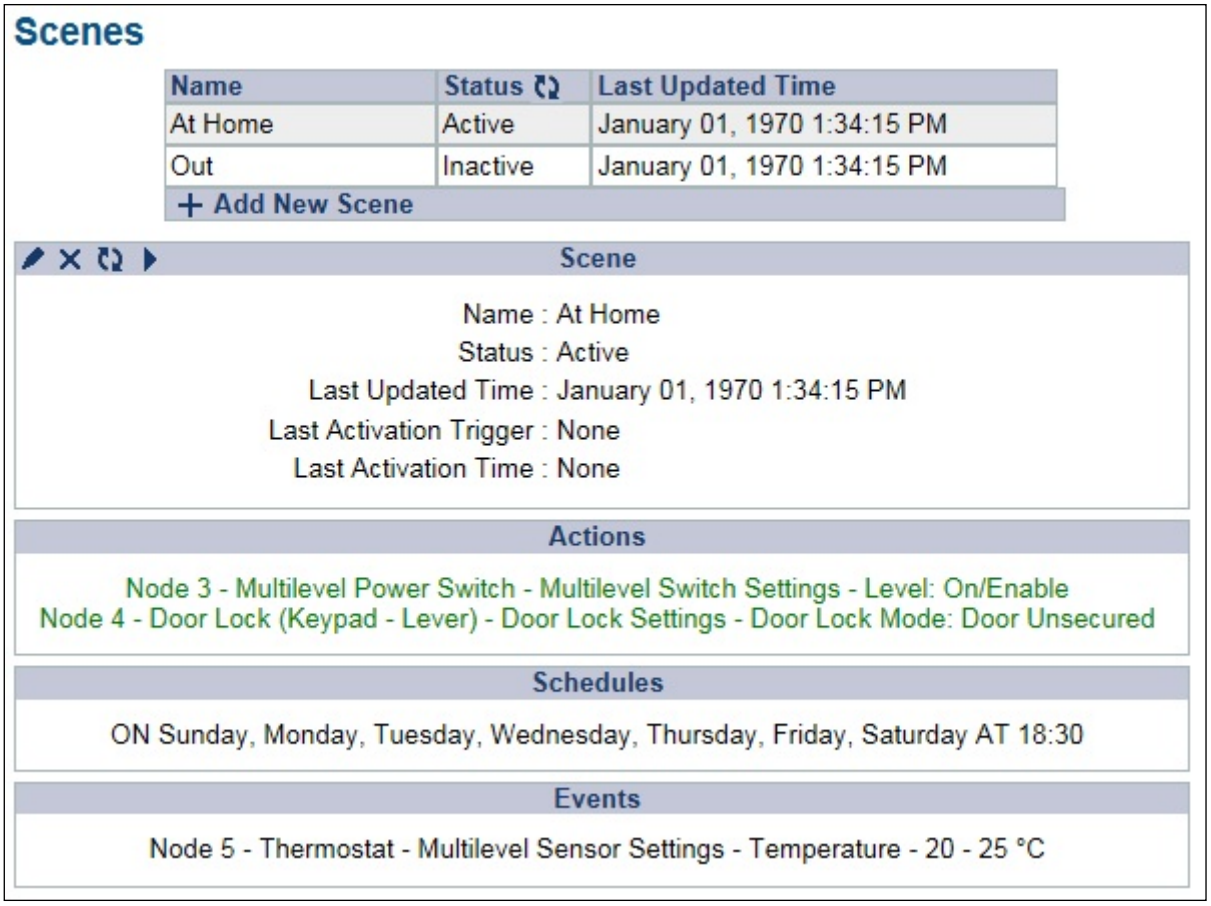


Figure 53: Scenes Page

A list of scenes is shown with their activity information. Status can be Active, Inactive, or Unknown. To update the scene status, use the cycle icon next to the Status header. To add a scene addition, use “+ Add New Scene” at the foot of the list. To select a scene, click on it.

The selected scene is shown in a panel below the list. To edit, use the pen icon at the top left of this panel. To delete, use the cross icon. To refresh status, use the cycle icon. To execute the scene, use the play icon.

Actions, Schedules, and Events are listed in this panel. Actions that match the current state of the device are shown in Green while others are shown in Orange. Actions with unknown states are shown in default black.

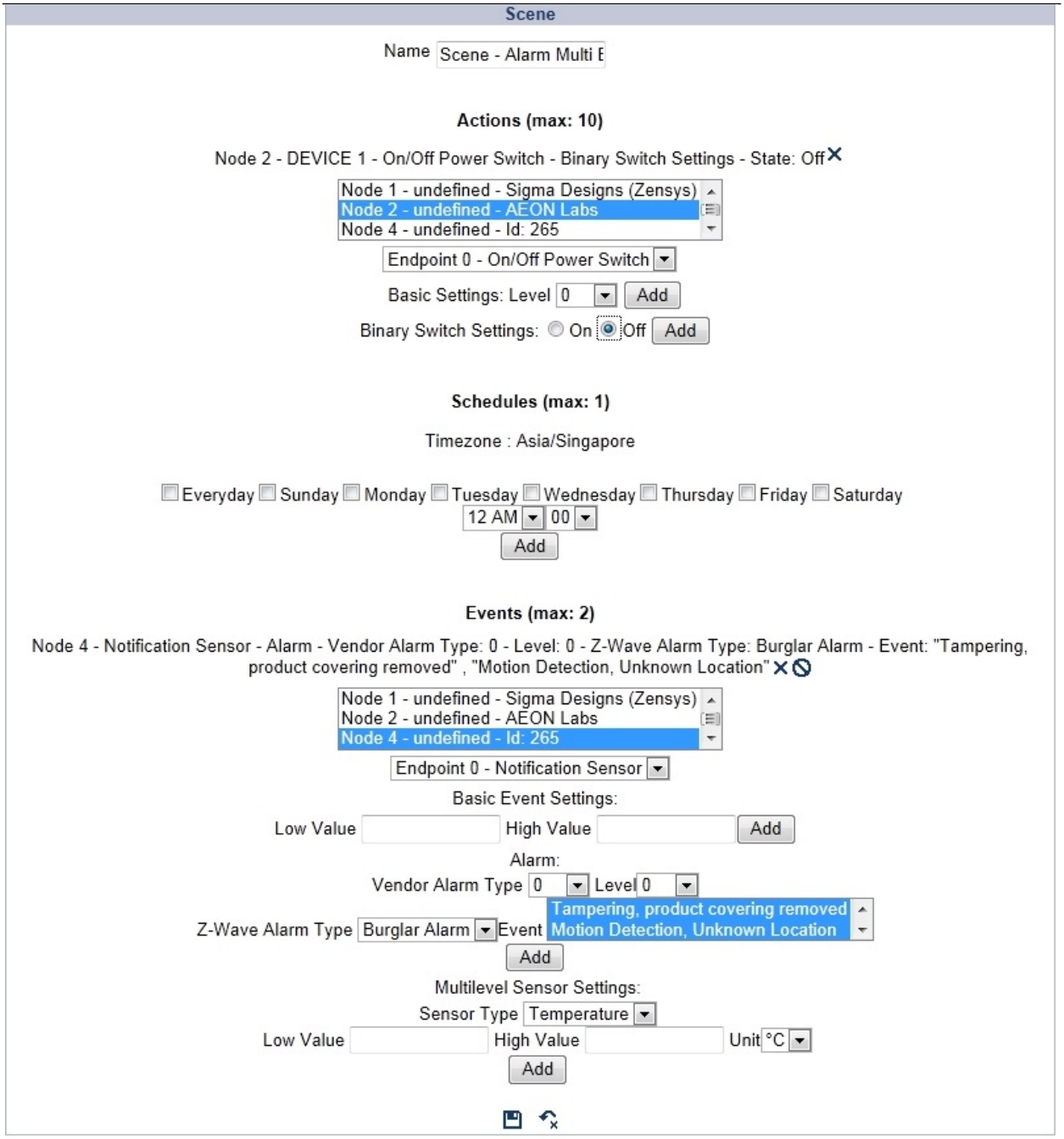


Figure 54: Scene Edit

The Scene Edit screen looks exactly like the "Add New Scene" screen except that the Scene information (e.g., Scene name, Actions, Schedules and Events) is already populated.
Any Scene information (including its name) may be changed. The maximum number of actions, schedules and events allowed are displayed. The Save and Cancel buttons are at the bottom.
At least 1 action is necessary for a valid scene. On the right of every added action is a delete button. When an endpoint is chosen in the action endpoint list, the candidate interfaces within are listed below for a SET operation. These include the Basic, Binary/Multi-Level Switch, Door Lock, and Thermostat SetPoint CCs.
On the right of every added schedule and event are delete and disable buttons. The disable button turns into an enable (tick) button when an item is disabled. Disabled schedules and

events are shown in orange and do not trigger a scene even when the conditions specified are met. When an endpoint is chosen in the event endpoint list, the candidate interfaces within are listed below to respond to a Binary/Multi-Level Sensor, Door Lock, or Alarm/Notification CC report, or a Basic Set command. Other than Door Lock, these CCs can support multiple types, and these types are listed for selection as well.

4.10 Security Scenes

Figure 55: Security Scenes Page

A list of security scenes is shown with their arm status, time of change, and last triggered time. The play icon on the arm and disarm compartments can be used to manually arm or disarm the scene. The pen and cross icons on the security scene compartment allow editing and deletingof the scene.

When editing or creating a security scene, disarm/arm/alarm triggers/scenes can be chosen.

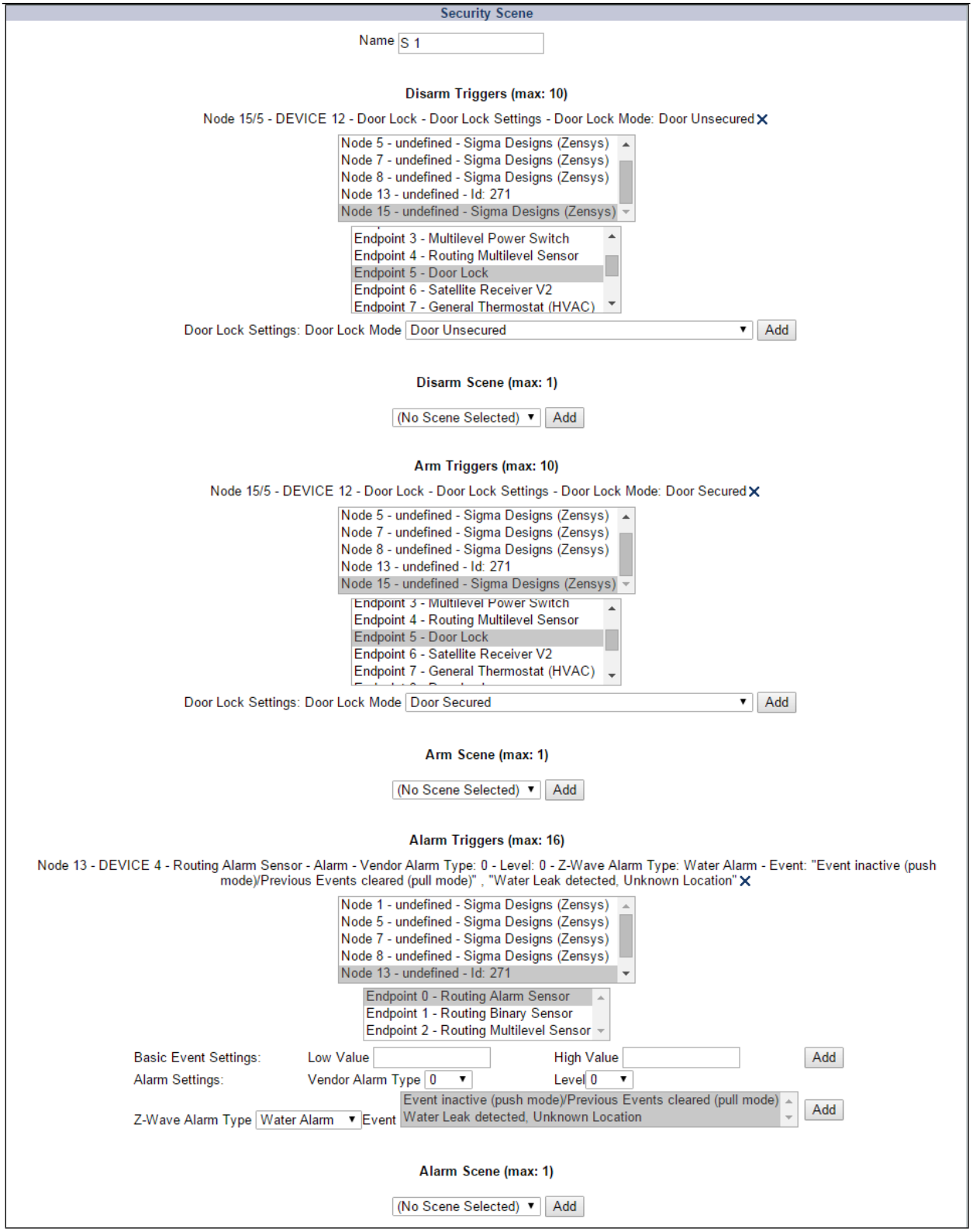


Figure 56: Security Scene Edit

At the bottom of the page is the notification section where email and/or SMS can be used.

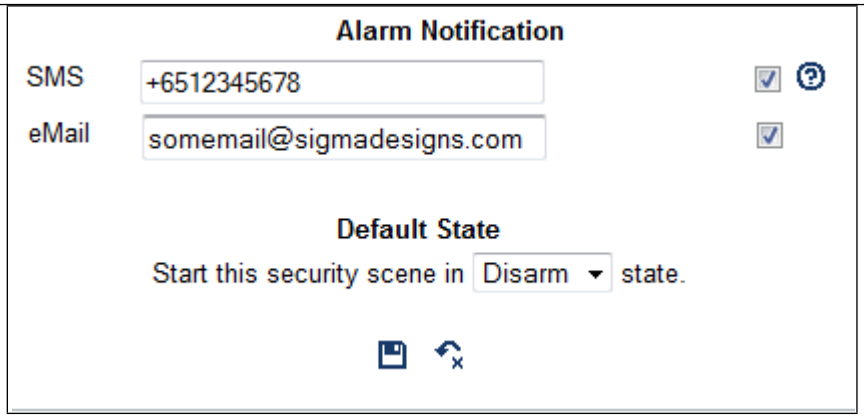


Figure 57: Security Scene Notification Edit

References

[1] Silicon Labs, INS14167, INS, Z-Ware Web Developer's Guide
[2] Silicon Labs, INS14606, INS, Z-Ware Library User Guide
[3] Silicon Labs, INS14416, INS, Z-Ware Library C API Reference Manual
[4] Silicon Labs, SDS12089, SDS, Z/IP Gateway Bootstrapping
[5] Silicon Labs, APL13031, APL, Z-Wave Networking Basics
[6] Silicon Labs, SDS10242, SDS, Z-Wave Device Class
[7] Silicon Labs, SDS13781, SDS, Z-Wave Application CC
[8] Silicon Labs, SDS13782, SDS, Z-Wave Management CC
[9] Silicon Labs, SDS13783, SDS, Z-Wave Transport-Encapsulation CC
[10] Silicon Labs, SDS13784, SDS, Z-Wave N/W Protocol CC