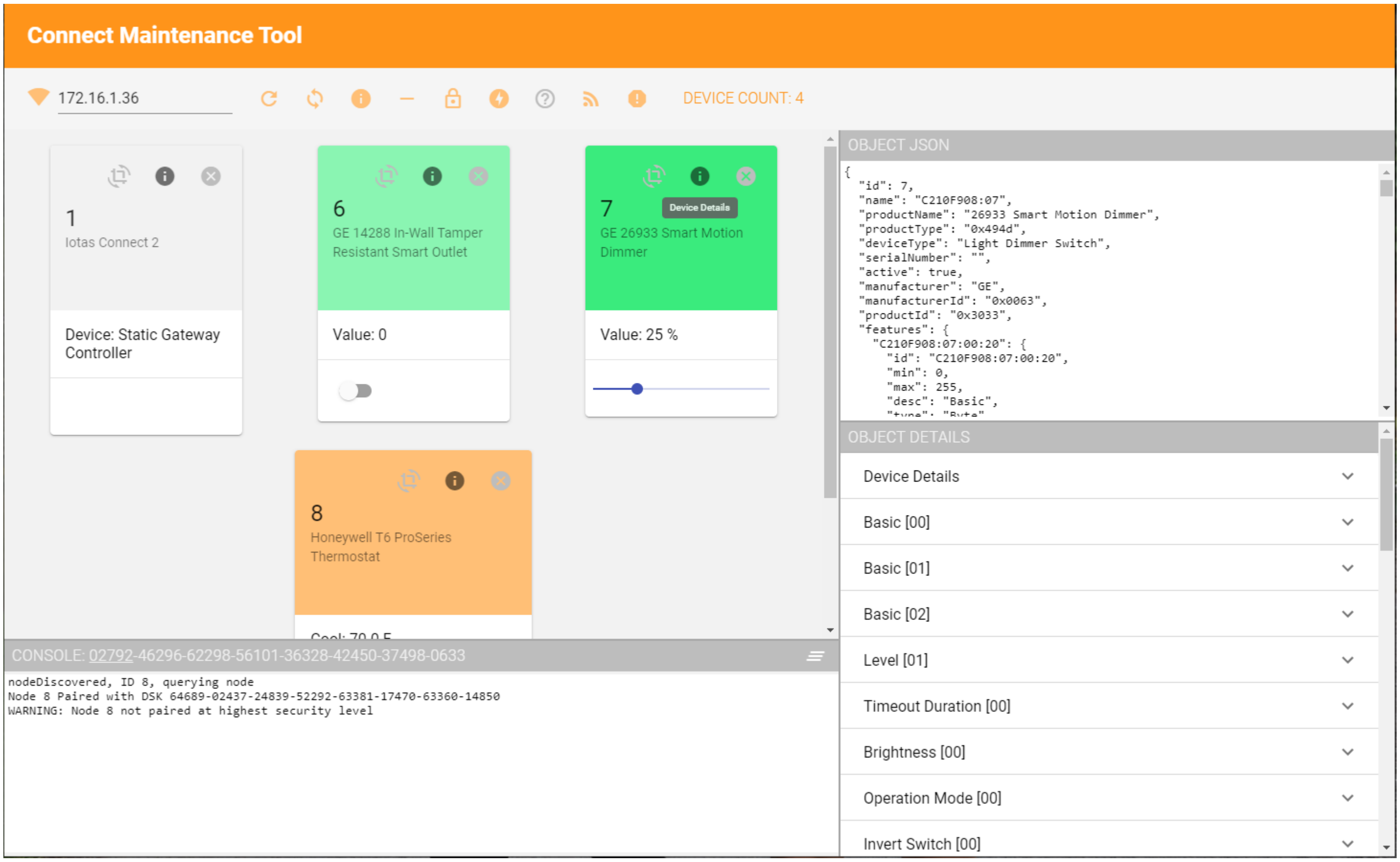
IOTAS Connect Maintenance Tool



```
{
  "id": 7,
  "name": "C210F908:07",
  "productName": "26933 Smart Motion Dimmer",
  "productType": "0x494d",
  "deviceType": "Light Dimmer Switch",
  "serialNumber": "",
  "active": true,
  "manufacturer": "GE",
  "manufacturerId": "0x0063",
  "productId": "0x3033",
  "features": {
    "C210F908:07:00:20": {
      "id": "C210F908:07:00:20",
      "min": 0,
      "max": 255,
      "desc": "Basic",
      "type": "Byte"
```

```
nodeDiscovered, ID 8, querying node
Node 8 Paired with DSK 64689-02437-24839-52292-63381-17470-63360-14850
WARNING: Node 8 not paired at highest security level
```

Table of Contents

Supported Browsers

By default, the generated project supports all modern browsers.

Support for Internet Explorer 9, 10, and 11 requires polyfills.

Loading the Connect Maintenance Tool Interface

This application is accessed, using a modern browser, through a dedicated port on the Connect Hub

- To access the maintenance app, use the following url, replacing <hub address> with the actual address
- http://<hub address>:3000

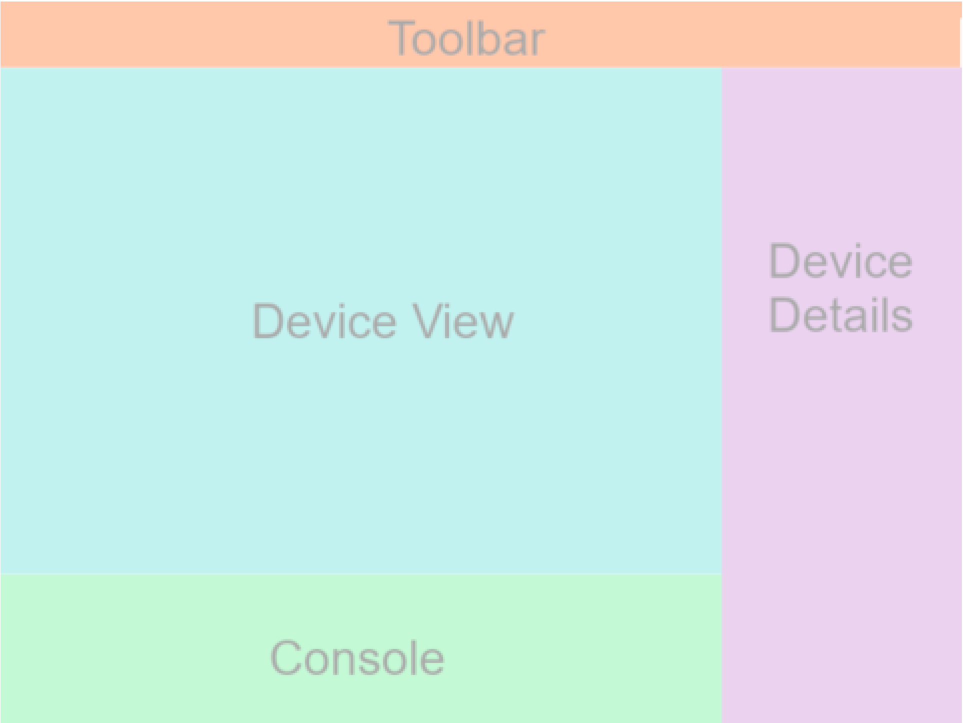
Using the IOTAS Connect Maintenance Application

Terminology

- **Inclusion**: 'Add' a device
- **Exclusion**: 'Remove' a device
- **Replication**: 'Copy' a Z-Wave™ controller to another Z-Wave controller

Introduction

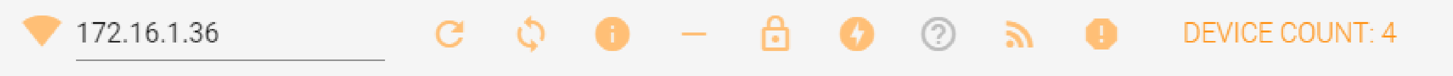
The IOTAS Connect Maintenance application allows the user to include/exclude, control and examine devices connected to the IOTAS hub. The user interface consists of four main informational panels:



What follows is an explanation of each of the above panels as well as other capabilities of the application.

Toolbar

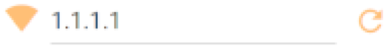
The key to interacting with the Z-Wave controller and its devices/nodes is the application toolbar. As can be seen in the screen shot below the toolbar consists of the connection text box and a series of buttons:



172.16.1.36

DEVICE COUNT: 4

Connecting



1.1.1.1

In order to interact with any IOTAS hub you are first required to connect to it. Connecting is as simple as typing in the IP address or device name of the hub that you would like to connect to and pressing 'Enter' (if you are on a tablet style device you can use the refresh icon next to the IP address to submit the information).

Node Status

ⓘ

This button interrogates the Z-Wave layer for the usage state of each node and displays the results in the console view. This will also refresh failed node status on each device card.

Exclusion

—

Use this button to remove (exclude) an existing device from the hub. Click the button, then trigger the Z-Wave exclusion process on the device to be removed. When the device is successfully removed the device view will automatically refresh.

Secure Inclusion

🔒

Use this button to perform up to, and including an 'S2 Authenticated Security' pairing request using the DSK to include the new device. Click the button and you will be presented with a dialog requesting the secure pairing code (first 5 characters of DSK). Type in the code if available, otherwise leave empty, and click the 'pair' option, at this point you need to trigger the Z-Wave inclusion process on the device to be added. When the device is successfully included the device view will automatically refresh and display the high level device information. If the pairing does not result in the highest level available, the console will display the final status of the pairing.

Stop Command

⚡

Use this button to stop the last command sent to the hub.

Learn

?

Use this button to allow the hub to join or leave an existing Z-Wave network.

Hard Reset

!

This button enables the user to reset the state of the hub, clearing all network information.

Device View

The device view displays a 'device card' for all devices discovered by the hub. If a device is 'unknown' to IOTAS it will still be shown, but no detail information will be displayed as the maintenance tool does not know how to map it to a specific device card. The mappings for known devices are maintained in the devices.json file located in the data path. This file can be modified when new devices are added to the system in order to render the appropriate card type. An entry in the devices.json file is made up as follows:

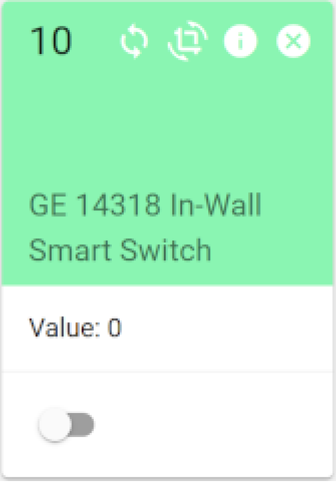
```
"0x0086-0x0102-0x0064": "GenericSensorDeviceCard"
```

This format represents the `manufacturerid-producttype-productid` followed by the type of card to display. Card types supported at this time include:

- BlindsDeviceCard
- DimmerDeviceCard
- EnergyMonitoringDeviceCard
- GenericSensorDeviceCard
- LeakSensorDeviceCard
- LockDeviceCard
- MotionDeviceCard
- OnOffDeviceCard

- OpenCloseDeviceCard
- RGBDeviceCard
- ThermostatDeviceCard
- UnknownDeviceCard for all others or unknown devices

Card Details



10

GE 14318 In-Wall Smart Switch

Value: 0

As can be seen in the above image a number of different elements make up a device card.

Device ID

The top left number of the card header is the device id

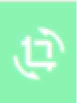
Description

The text in the card header is a description scraped from combining the `deviceManufacturer` and `productName` fields of the device data.

Menu Bar

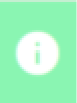
The card header toolbar consists of 4 options:

Secure Replace Failed Device



Secure replace will request the secure code of the new device before trying replace the old device.

Device Details



Populates the device details panel with 2 views of the devices details:

- The top panel will contain the JSON object view of the device data.
- The bottom panel will contain an individual breakdown of each feature of the device and the ability to edit the feature value when applicable.

Force Remove Failed Device

⊗

Provides the ability to force the removal of a device from the Z-Wave table on the hub when the device has been disconnected without using the exclusion solution provided through the Z-Wave libraries.

Device Detail View

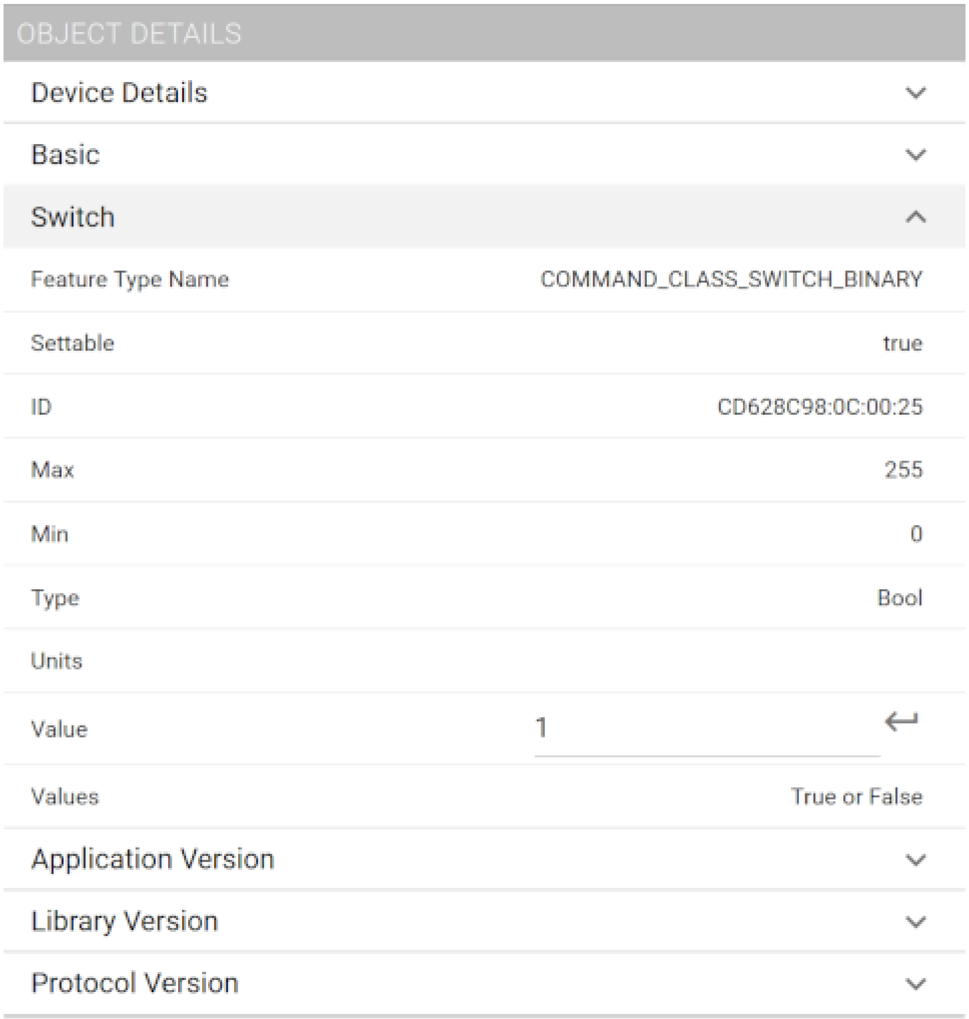
The device detail view is broken into two views:

- The first is the JSON view of the device meta data
- The second is an interactive view of the device features

JSON View

The json view renders the device metadata (in json) exactly as it formatted from the IOTAS Interconnect layer.

Feature Detail View



OBJECT DETAILS

Device Details

Basic

Switch

Feature Type Name	COMMAND_CLASS_SWITCH_BINARY
Settable	true
ID	CD628C98:0C:00:25
Max	255
Min	0
Type	Bool
Units	
Value	1
Values	True or False

Application Version

Library Version

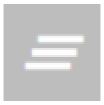
Protocol Version

Every device is fully described in the detail view, this includes information not available on the primary card of the device.

The device detail view lists (in collapsible panel form) all of the features of a device. The endpoint of each feature of a device is appended to the feature within [] brackets. This allows the user to view specifics about each of the features and in cases where a feature is editable (see 'settable' value in feature details) the user can set a new value simply by entering (text field) or selecting (combo box) the new value. As can be seen in the image above the features detail for a free form text field includes information about the type of value, and options for what can be input. When the value is changed the change and the enter button pressed the information is sent to the Z-Wave layer causing both the UI and the device to respond accordingly.

Console View

The console view shows an ongoing stream of messages that the maintenance too presents to the operator, including extra status from the Z-Wave layer.

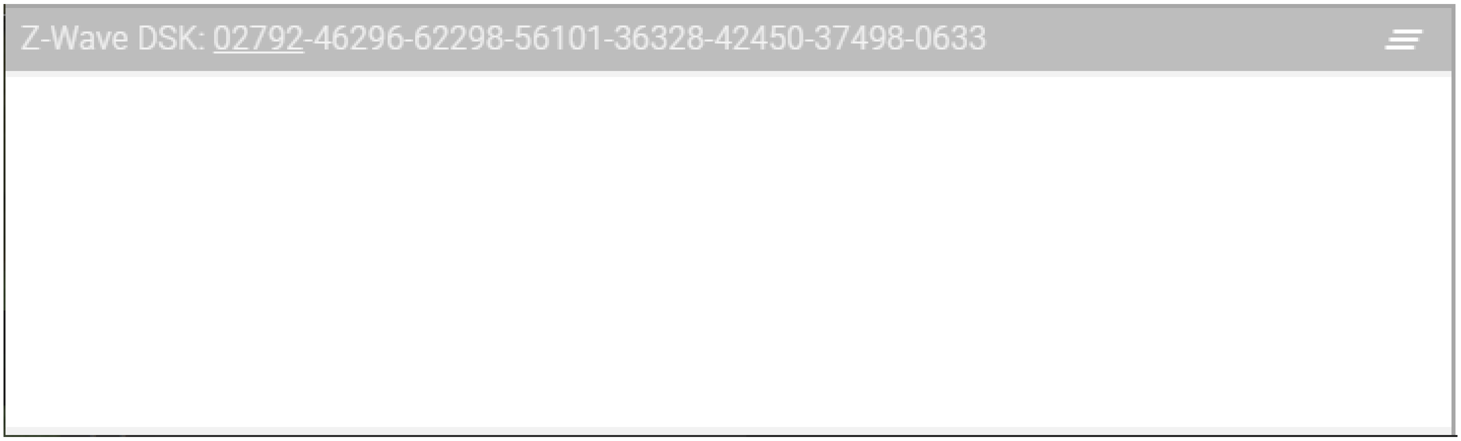


The 'Clear Text' button on the console navigation bar clears all the text from the console, this information is not stored or logged anywhere so be careful to copy and paste any text you may need before clicking.

Additional Z-Wave Maintenance Information

Replicating, Including the hub in an existing network

When including the hub in an existing network, activate the "Add Node" button on the primary controller, and then activate the Learn button on the hub's Connect Maintenance Tool interface (the sequence of these two steps is not vital). This will include the Hub into the Z-Wave network and transfer the complete network topology. The hub will request S2 Access control. The primary controller will display all digits in your DSK with the exception of the first five digits (the DSK's PIN). When prompted by the primary controller, verify that the visible digits in the DSK match your controller's DSK and then enter 5 missing digits.



Z-Wave DSK: 02792-46296-62298-56101-36328-42450-37498-0633

Including a Device

See Secure Inclusion for details

Basic Documentation

Basic command

The basic command class is controlled but not supported by this controller. The basic command class is not mapped to any other Z-Wave Command Class.

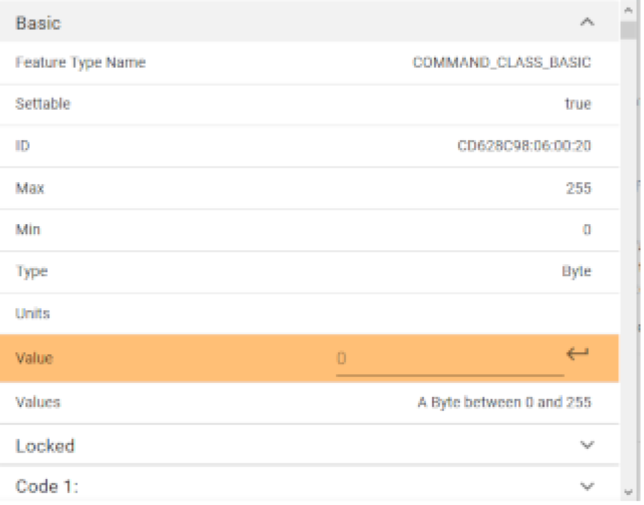
Association Command Class

The Connect 2 hub supports only 1 Association group supporting 1 node for Lifeline. This node will receive the Device Reset Locally command.

Devices from multiple manufacturers

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

Basic Command Control



Basic

Feature Type Name	COMMAND_CLASS_BASIC
Settable	true
ID	CD628C98:06:00:20
Max	255
Min	0
Type	Byte
Units	
Value	0
Values	A Byte between 0 and 255

Locked

Code 1:

The hub is able to control any device that supports the basic command class. Such a device will list "Basic" as one of the drop down's in the Feature Detail View. Enter a digit between 0-255 in the "Value" field and press the "return" button to the right of the value field to commit.
Refer to the device's documentation to get futher information on valid input values for the basic command class of the remote device. eg 0, non-zero for on off switches, values between 0 & 99 for level control etc.

Factory Default Reset

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.

The Hard Reset button described in the Toolbar section is how the test tool allows the user to factory reset a hub.

S2 Security CC

Inclusion - Will secure to highest level provided by the node (if no code is required)
Secure inclusion - Needs DSK of the device the code must be provided will secure to highest level provided by the node

The Connect 2 hub supports the following security levels:

- S0
- S2 Unauthenticated
- S2 Authenticated
- S2 Access

Supported Command Classes

Following is a list of supported command classes and their security levels.

Inclusion NIF:

- 0x5E - COMMAND_CLASS_ZWAVEPLUS_INFO
- 0x55 - COMMAND_CLASS_TRANSPORT_SERVICE
- 0x56 - COMMAND_CLASS_CRC_16_ENCAP
- 0x22 - COMMAND_CLASS_APPLICATION_STATUS
- 0x9F - COMMAND_CLASS_SECURITY_2
- 0x98 - COMMAND_CLASS_SECURITY
- 0x74 - COMMAND_CLASS_INCLUSION_CONTROLLER
- 0x73 - COMMAND_CLASS_POWERLEVEL
- 0x72 - COMMAND_CLASS_MANUFACTURER_SPECIFIC
- 0x86 - COMMAND_CLASS_VERSION
- 0x6C - COMMAND_CLASS_SUPERVISION
- 0x8F - COMMAND_CLASS_MULTI_CMD
- 0x85 - COMMAND_CLASS_ASSOCIATION
- 0x59 - COMMAND_CLASS_ASSOCIATION_GRP_INFO
- 0x5A - COMMAND_CLASS_DEVICE_RESET_LOCALLY

Insecure:

- 0x5E - COMMAND_CLASS_ZWAVEPLUS_INFO
- 0x55 - COMMAND_CLASS_TRANSPORT_SERVICE
- 0x56 - COMMAND_CLASS_CRC_16_ENCAP

- 0x22 - COMMAND_CLASS_APPLICATION_STATUS
- 0x9F - COMMAND_CLASS_SECURITY_2
- 0x98 - COMMAND_CLASS_SECURITY
- 0x74 - COMMAND_CLASS_INCLUSION_CONTROLLER
- 0x6C - COMMAND_CLASS_SUPERVISION
- 0x8F - COMMAND_CLASS_MULTI_CMD

Secure S2 Access:

- 0x86 - COMMAND_CLASS_VERSION
- 0x72 - COMMAND_CLASS_MANUFACTURER_SPECIFIC
- 0x73 - COMMAND_CLASS_POWERLEVEL
- 0x59 - COMMAND_CLASS_ASSOCIATION_GRP_INFO
- 0x85 - COMMAND_CLASS_ASSOCIATION
- 0x7A - COMMAND_CLASS_FIRMWARE_UPDATE_MD

How to Activate Device Functionality Related to Z-Wave Behavior

The following links outline the interactions available to the user in the test application:

- Toolbar
  - Connecting
  - Node Status
  - Exclusion
  - Secure Inclusion
  - Stop Command
  - Learn
  - Hard Reset

Special Procedures

The Z-Wave Plus™ CTT test requires extra steps for verification, the IOTAS hub expects key exchange prior to pairing where ad the CTT is expecting key exchange during pairing
Steps are:

- Run the test per the CTT test instructions
- Take note of the first 5 characters of the DSK provided by the CTT during the test
- Allow test to complete to failure

- Rerun the pairing sequence using the lock symbol on the Z-Wave maintenance app and when prompted enter the previously noted 5 characters of the DSK
- Let test continue
- Test should now pass

How to Send any Controlled Command from the Controller

The following links outline the interactions available to the user in the maintenance application:

- Toolbar
  - Connecting
  - Node Status
  - Exclusion
  - Secure Inclusion
  - Stop Command
  - Learn
  - Hard Reset
  - Replace Device
  - Secure Replace Device
  - Force node removal