Inspextor UI Guide

Version v.0.1.2245

Prepared By:

Broc Christensen

Senior Field Engineer

Document Contents

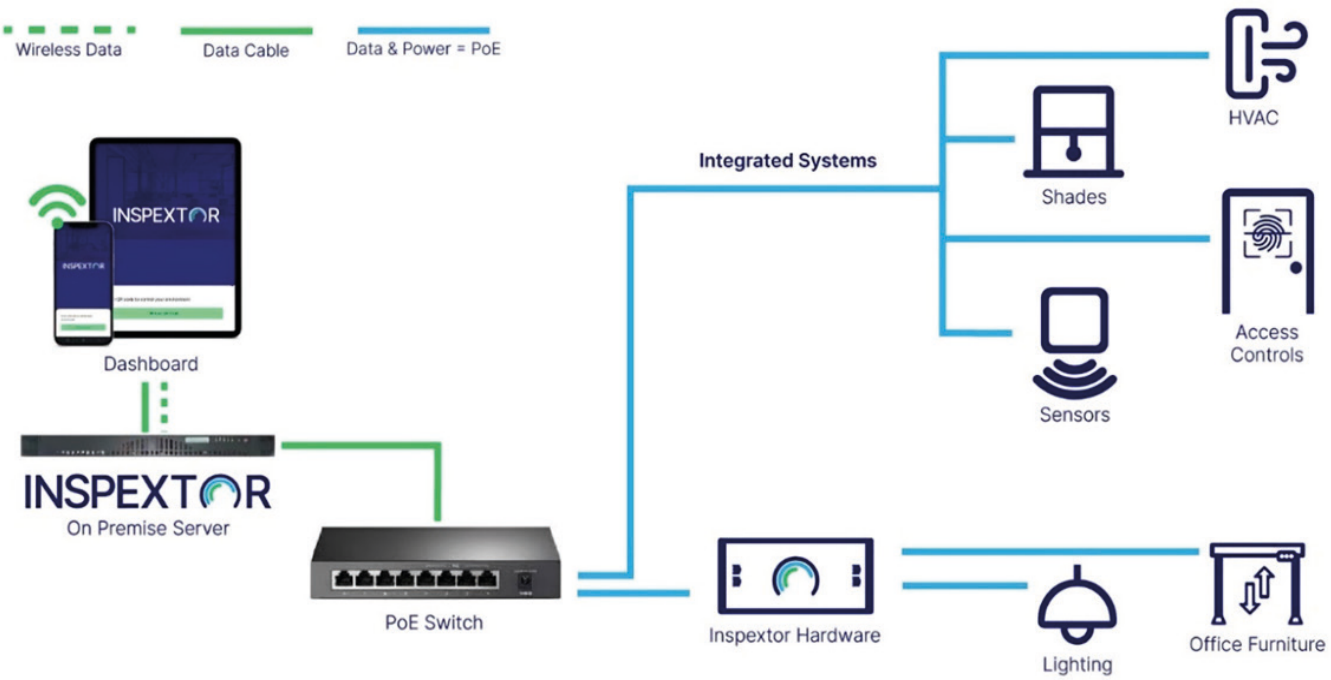
Document Purpose

This document is designed to help with allowing Users to understand the base configuration of the Inspextor Server. The goals listed below will provide an overview of the rest of the document.

- Accessing Inspextor Web Interface
- Inspextor Page structures and vocabulary
- Inspextor Dashboard
- Inspextor Controls and Floor Plan
- Inspextor Settings
- Inspextor User Management
- Inspextor Management
- Inspextor Commissioning
- Inspextor Support

Inspextor Solution

The figure below shows the general Inspextor Solution with a broad overview of the structure of the system. The Inspextor system utilizes the latest in POE technology to deliver 90 Watts of power to the MHTi Node. Where it utilizes both server side and Node end code to deliver reliable and accurate monitoring and system controls. The use of COAP messaging allows the system to communicate information effectively. The nodes built in RS485 capability expands the features to allowing VAV controls and future expansion into the building controls market. The Inspextor software also offers a robust API that has allowed MHT to form integrations with multiple leaders in the IoT industry.



Inspextor Physical Infrastructure Vocabulary

Power Sourcing Equipment or (PSE)

Are the devices that provide power PoE to the components in the Inspextor Solution. In most situation these are Managed Network Switches in rare instances they are Unmanaged Network Switches or Power Injectors. For Further reading on PSE's please see the IEE 802.3bt Standards. A PSE in the Inspextor System provides power for multiple PoE Circuits.

Power Device(PD)

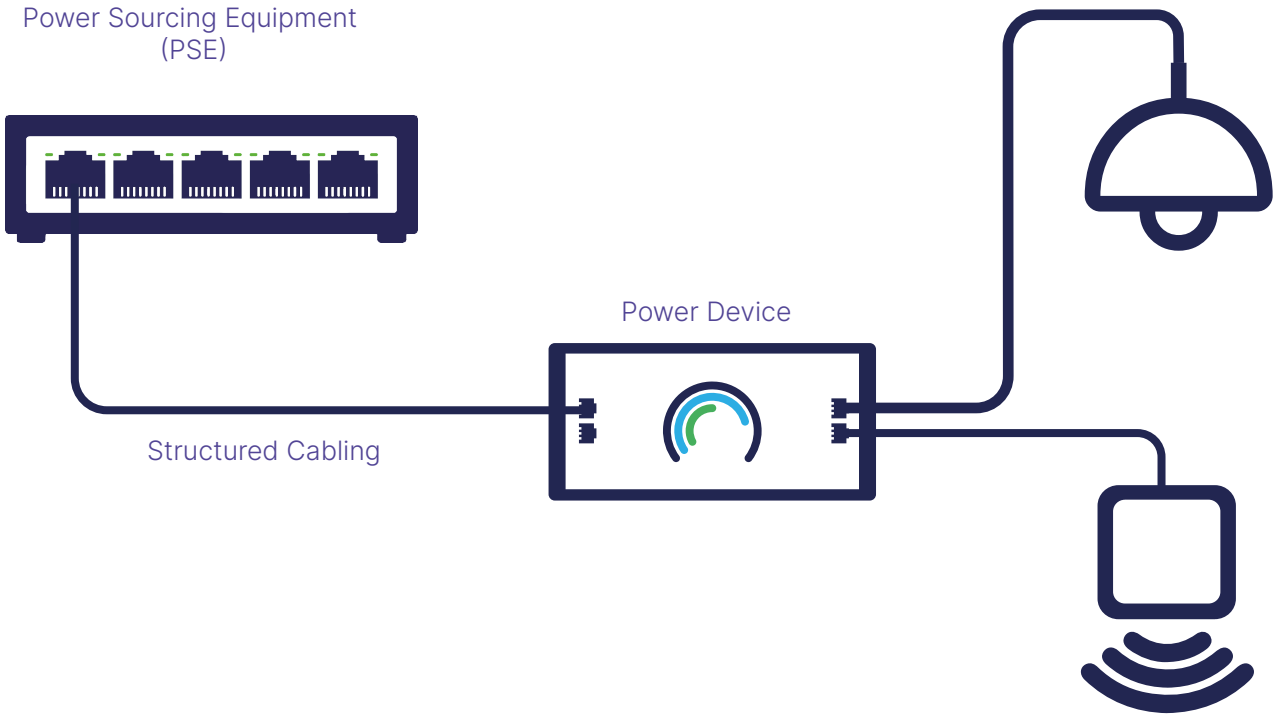
A power device is hardware device that receives the power allocated from the PSE. In the Inspextor system we directly communicate with our Node Driver Power Devices.

Structured Cabling or Home Run

These refer to the permanent or semi permanent (if in a tenant space) cabling that provide the data and/or power to a power device. In some cases it can be used connect PSE's to other PSE's or other networking equipment.

Node Driver

Node Driver is a specific kind of power device that MHT Technologies produces and you will commonly see it referred to as 'ND-######'. It is the Node Driver followed by the Serial Number of the device.



Inspextor Software Vocabulary

2Out

2Out is the modularized firmware that all MHT Technologies Manufactured devices are operating on in the software it is primarily referenced at the *Admin level* allowing users to understand what version of firmware they are operating.

Cluster

Is a logical representation for one or more PoE circuits. Clusters are what allows the Inspextor system to act on user input, analyze data and present information to applications.

Terminal

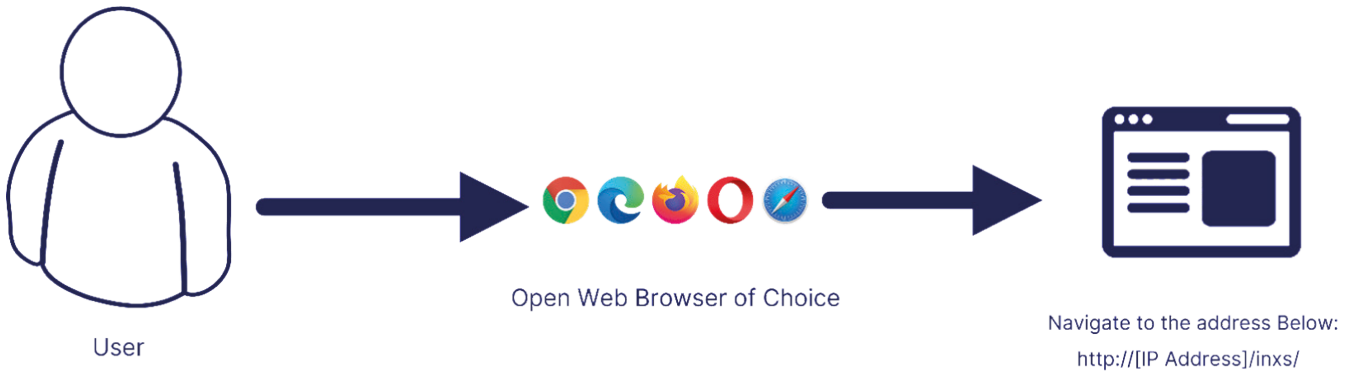
Advanced Users or admin users may hear about the Terminal which is a virtualized session that allows the user to send commands directly to Node Driver. It allows the team adjust light levels and set policies on the Node Driver itself.

Constrained Application Protocol (COAP)

Is a transfer protocol that is used industry wide for IoT devices. It is an Application Layer protocol that is used in simple network environments. MHT devices communicate between the Inspextor Software and the Inspextor PD or Node Driver.

Accessing Inspextor Web Interface

The Inspextor Appliance Operates on Linux based Architecture using a DHCP assigned address on startup granting the user/Installer a very intuitive start up procedure. When the network is up and operational, we can begin by accessing the appliance using our web browser.
The Inspextor software for initial installation is configured for best display on a windows or mac. It is advised that initially accessing the system is done by utilizing a PC or Mac Product. The server is first powered up it will begin all processes without the need for manual intervention on the device. However, you will need to source the IP Address from the Networking team for initial access. The figure below will help you with the source address you will enter in your web browsers address bar.



Default User and Initial Log in

When accessing the Inspextor software utilizing the provided user you will be greeted with the Main page as pictured below if this is a new setup up please utilize the credentials default credentials below

Default Credentials

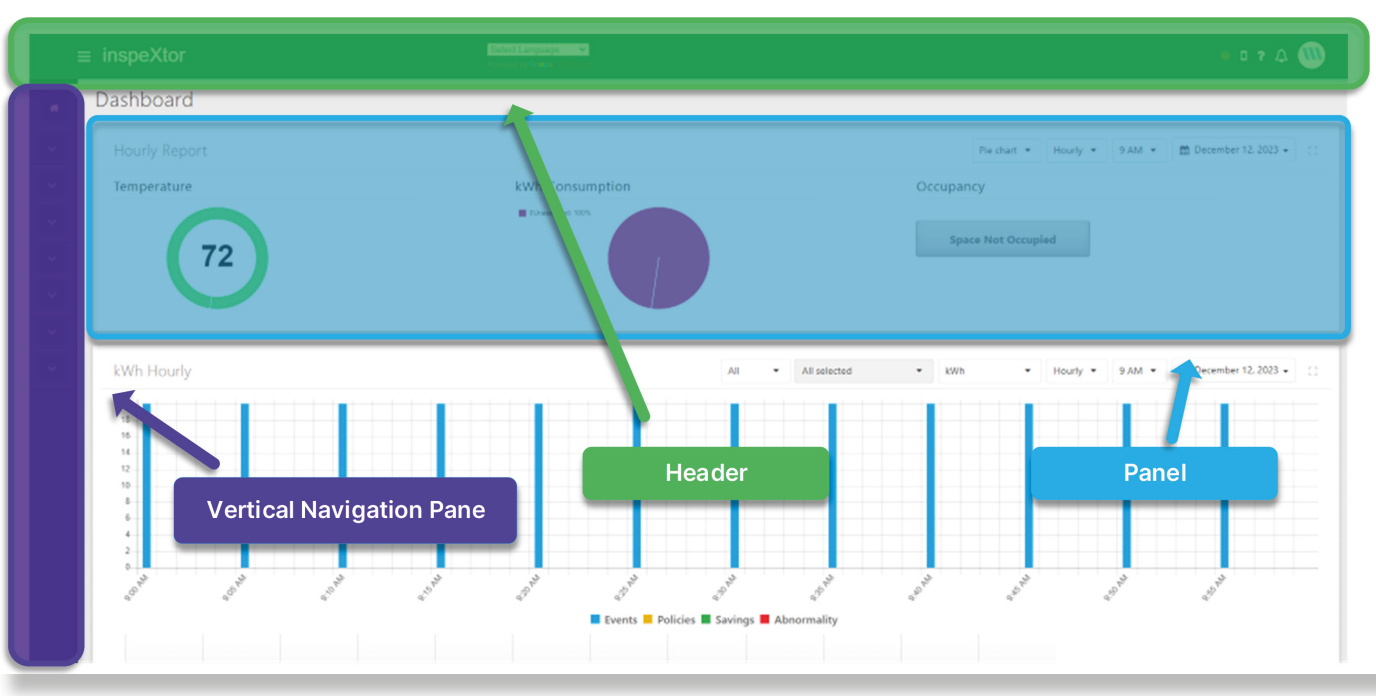
Username	admin
Password	mht-poe

Inspextor UI Structure Overview

To best read this guide this section establishes the structure of an Inspextor webpage as well as introduce the vocabulary associating the supported Inspextor PoE Devices to their representation in the Inspextor Software.

Inspextor Webpage Structure

The Inspextor software was designed with user experience in mind. It utilizes a prominent vertical navigation system to allow users to quickly navigate through the system. It also utilizes a modularized system of panels on each page to clearly define the structures of data and its use case. The subsection below will introduce those features. In future sections we will refer to these by there designators labeled below

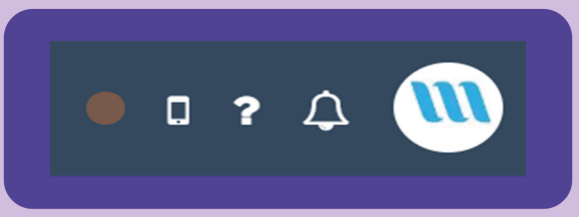


Page Header

The Page header as pictured above is present on each page as the user navigates through the software providing the user with important access to service impacting information in the Hot Buttons section while providing a means of translation into different languages.

The 3 Bars Adjacent to the Inspextor Logo are referred to as a hamburger menu and allow the user to access the Vertical Navigation bar

The Inspextor Software utilizes the Google Translate to provide an update selection of 133 different languages for the user to select from.



The Hot Buttons that are found in the Header Bar are utilized by the user to understand the state of the system and direct information each Icon is described in greater detail below

The **Status Light** allows the user the ability to see the status of the system and On-Hover a detail will appear describing the system state.

The **Mobile Dashboard** provides a quick means to change the system visibility to suit vertical orientated devices (Details can be found in the **UI Mobile Dashboard Section**).

The **Help** section is available on each page and provides direct information to allow the user direct access to page specific data for the Inspextor Software.

The **Alerts** are a quick view of the defined alerts page where system and user define alerts can be viewed in real time

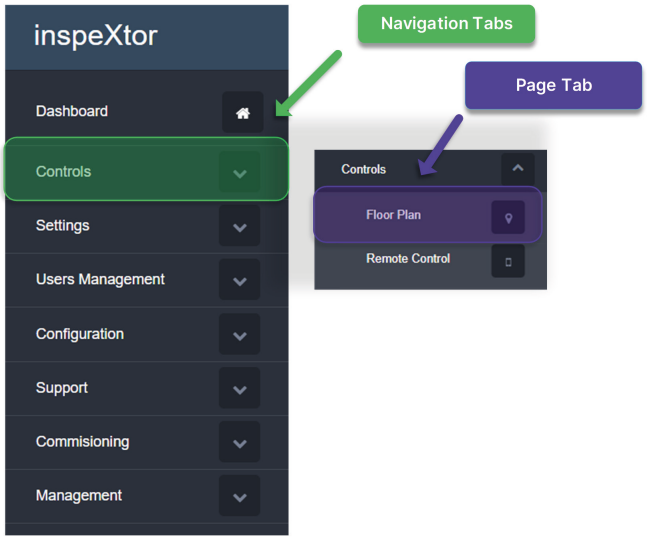
User Control allows a quick navigation to the User's profile as well as provide the means of logging out

Page Footer

The Page footer as pictured above is present on each page the data present while marginally less important provides much needed support content when reaching out to the MHT Support Team with question. The Contract ID is what the team utilizes to tie your installation to the license and the version is the Version Instance installed on your MHT Inspextor Appliance.

Vertical Navigation Pane

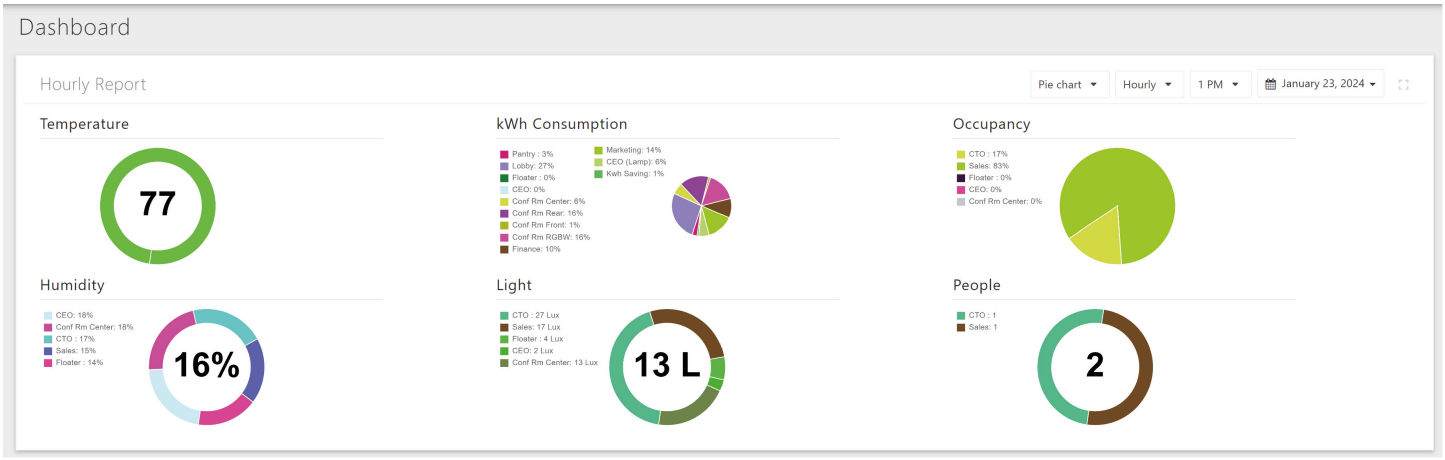
The Vertical navigation pane provides the main structure of the Inspextor software. Web pages are sorted into each Navigation Tab based on User-Centric perceived setting. In the displayed example the Remote Control Tab is located under the Controls tab providing a means of grouping these pages and functions for future development.



Navigation Tabs not shown here please see supplemental documentation for specific modules

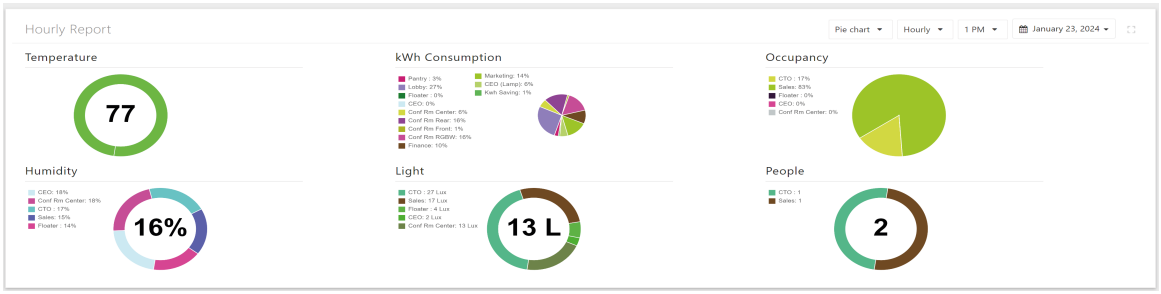
Dashboard

When signing in you will be presented with the Dashboard page. MHT Technologies has designed this page to present our clients with accurate and eye-catching data that can provide the user with the ability to access historical and near present data in panels. The Dashboard Page is currently populated with two panels each with a modifiable timelines in the upper right hand corner of each panel. In the following sections we will dive into more detail on the panels themselves and the data they represent



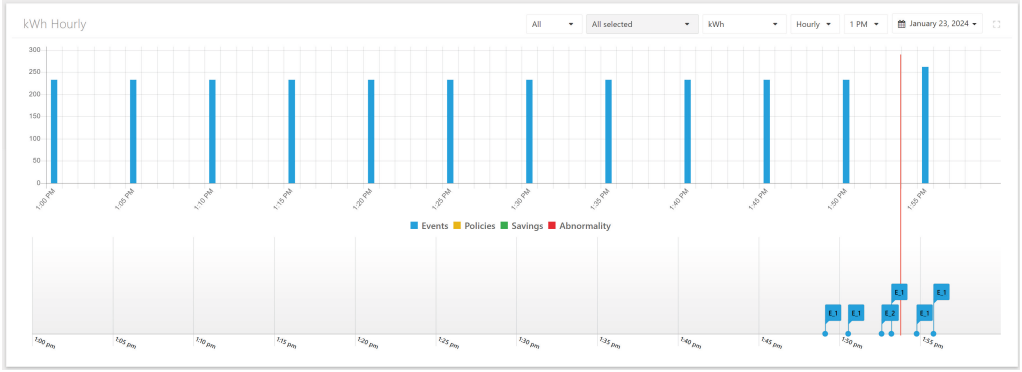
Panel 1: Hourly Report

The hourly report provides data on predetermined metrics that are averaged over the hour and presented at the top of the hour. In the example provided sensors from 3rd party vendors are providing data to the inspextor software to populate the Pie Charts listed below.

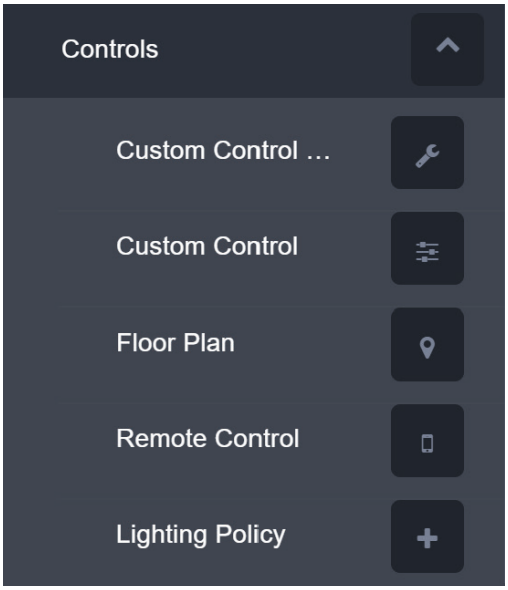


Panel 2: kWh Report

The kWh Hourly report utilizes metrics presented by the system to determine the hourly consumption of electricity and provide the user with accurate bar-charts that illustrate the changes in consumption over time.



Controls

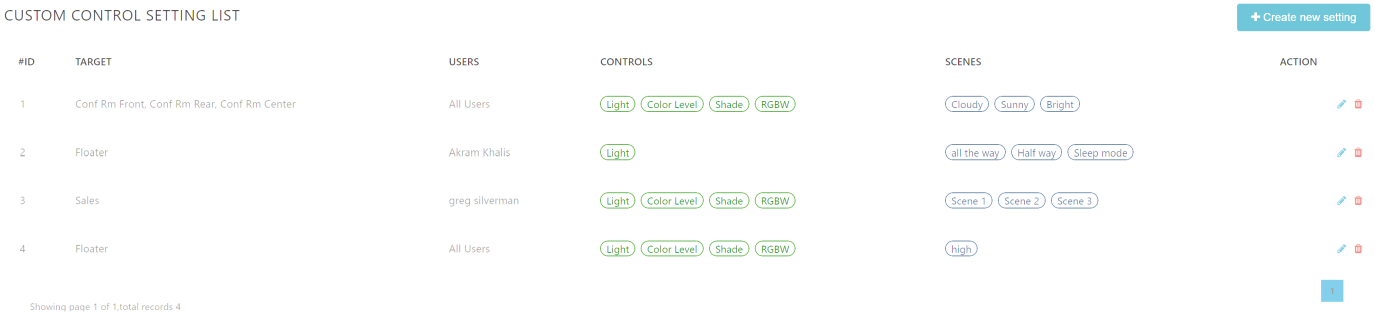


The Control group of devices are where controls and policies can be tested and programmed in this section we will dive into greater detail on the individual pages associated with the Controls Navigation tab.

Custom Control Setting List

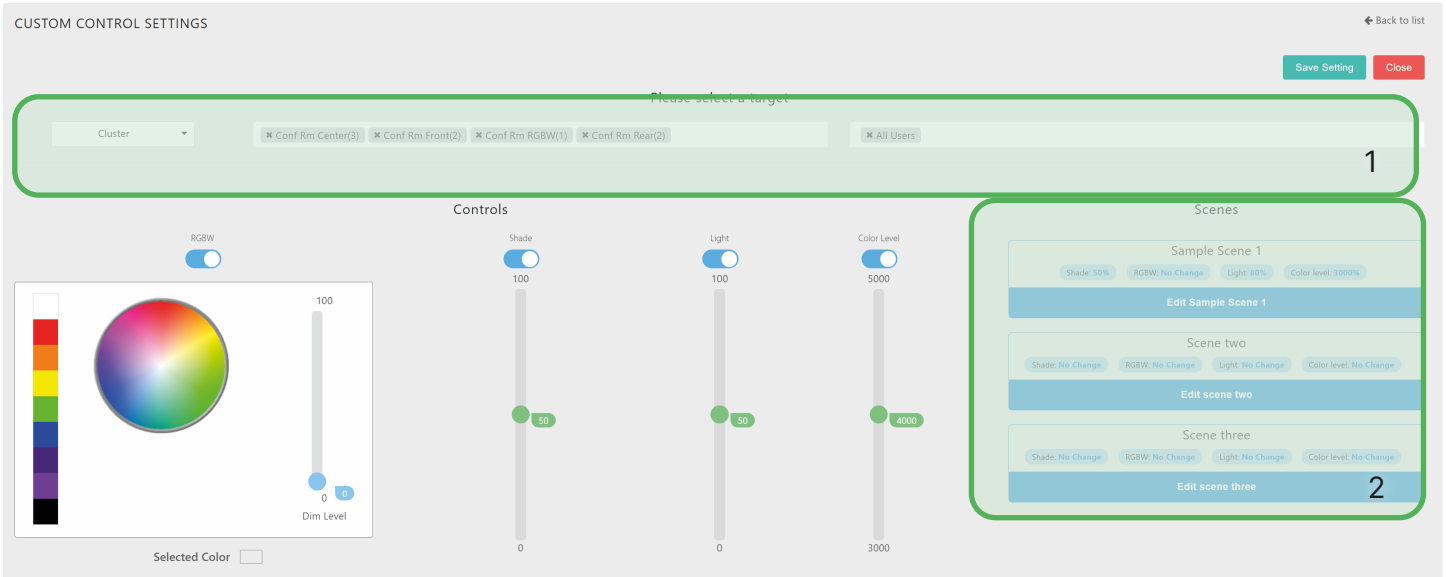
This Page is dedicated to assigning Cluster specific commands. It allows the administrator to configure a series of scenes that can be controlled from the custom control page. It is just another way that users can control the environment in their specific space.

When opening this page as an admin you are presented with a list of all configured settings it will list the targets, Users who can access them, the controls that are modifiable and the defined scene names.



New Custom Control Setting

Pictured below is the definition page presented when adding a new custom control setting. In this section we will review the parameters that can be adjusted when configuring custom controls for the user.

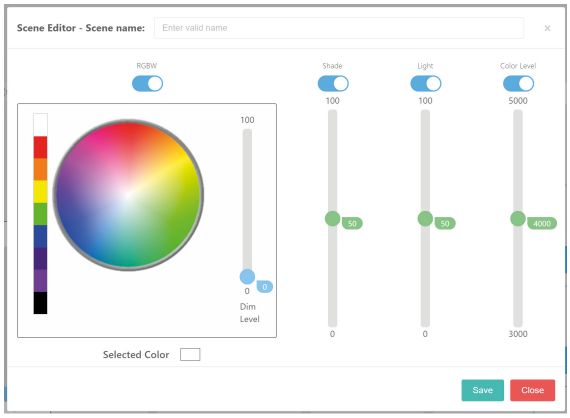


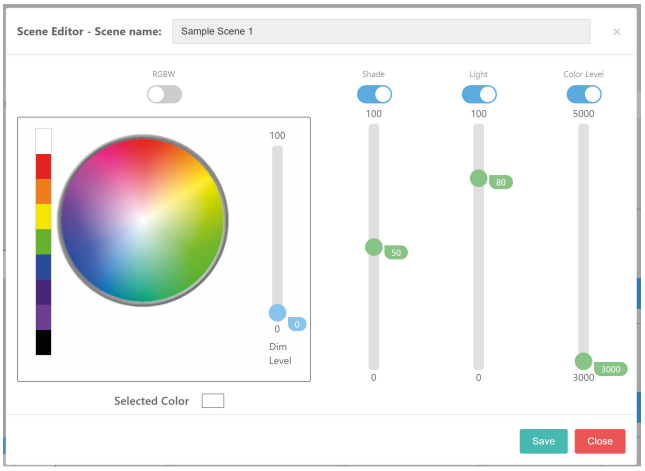
Panel 1: Selecting Target

When working with panel 1 it is important to select the cluster that you would like to configure the scenes for as well as the user that is allowed to access these scenes. This section can actually set the scenes in multiple clusters as well as provide the access to all or multiple specific users.

Panel 2: Scene Editor

In panel 2 the Edit Scene button allows you to declare edit the scene when selecting the edit scene option you will be presented with the pop out that is illustrated here. You will be required to provide a scene name and adjust the bars to setup the appropriate scene.

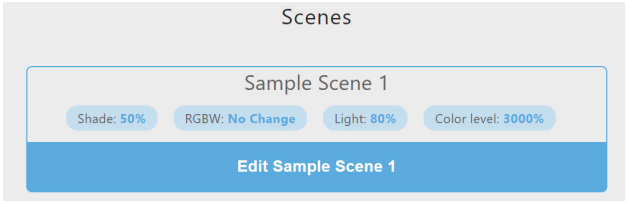


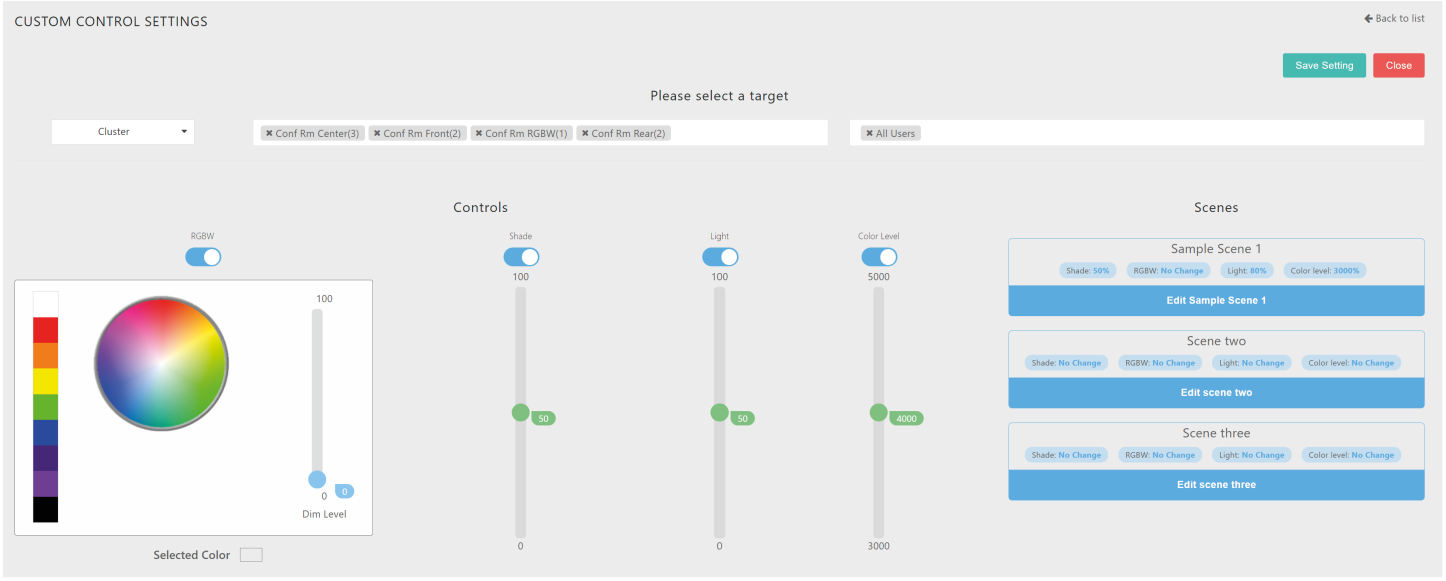


In the Example on the right you can see that “Sample Scene 1” is adjusting 3 Settings. It is adjusting the shades to 50%, The Lights to 80% and the Tunable White lights to 3000K.

Settings Apply to All Lights in the Declared Cluster in the Previous Page

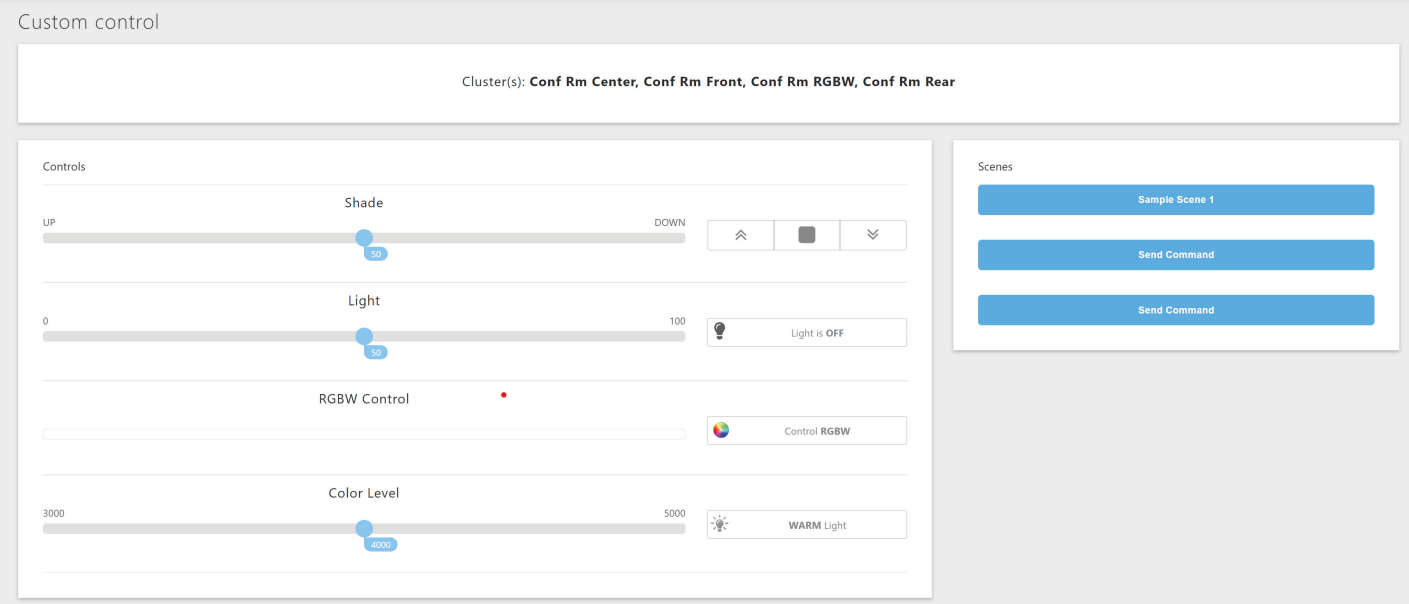
After Saving the settings we can confirm the settings were saved appropriately and that the new name has been accepted. If you save the Control Setting it will populate the List with your defined scenes accessible from the Custom Controls Page. That will be outlined in the next section.





Custom Control

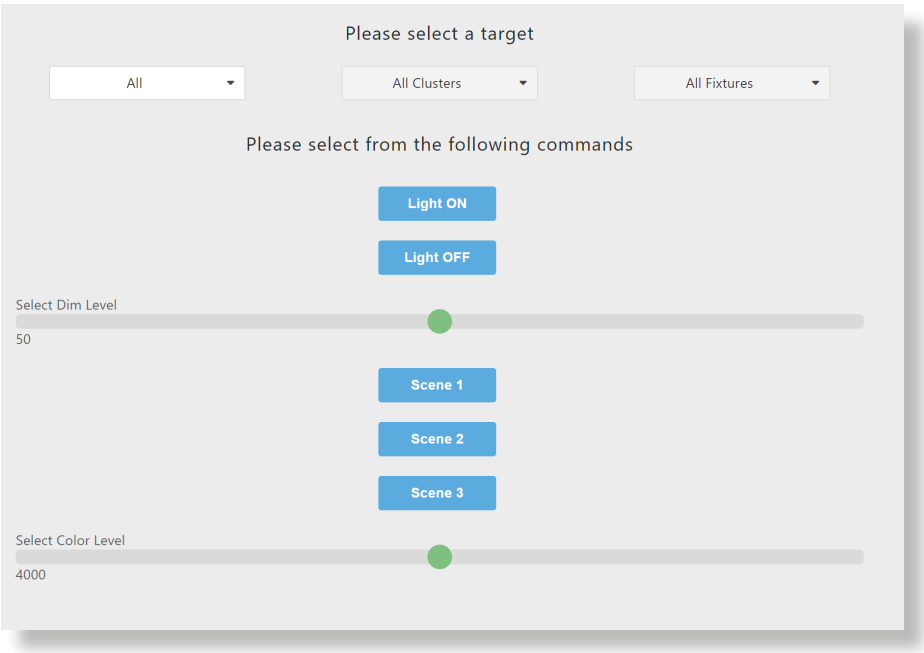
In the previous section we discussed what it looked like to configure Custom Control Settings. In this section we are going to talk about how to access those custom controls and utilize them. The Object of providing custom control is to allow the user to have more freedom over the control of the lights in there space without effecting any other aspect of the system.



In the previous section we created a custom control setting that granted access to the clusters in the conference room and allowed all users to access the clusters. It is now presented under the custom control tab and allows the user to access “Sample Scene 1” and the Lights and Shades in the associated clusters.

Remote Control

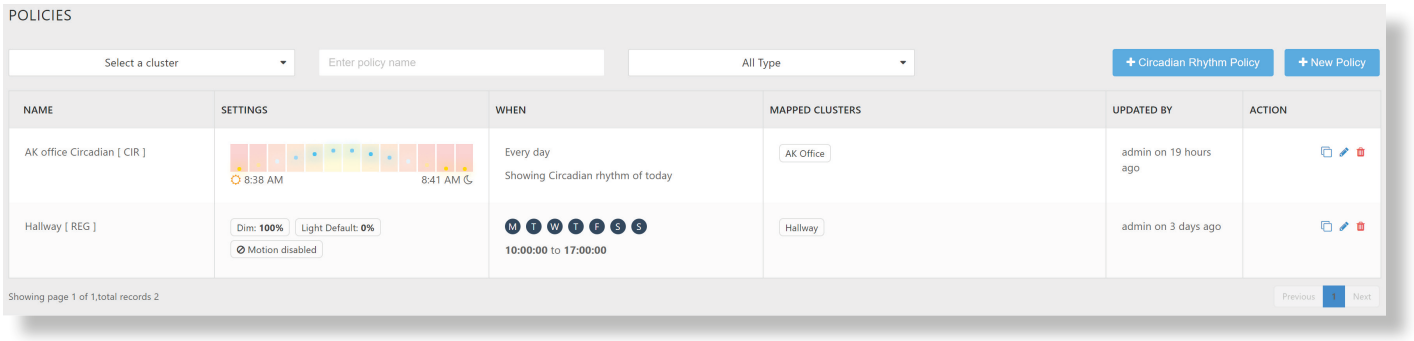
The Remote Control page is generally what we would refer to as the “Admin Controls Page” this page allows pointed controls of the individual fixtures and clusters of fixtures. These commands override the current cluster settings to validate light functionality. When utilizing this page if you select the target cluster from the system the “dim level” and “color level” will reflect the state of the cluster currently.



What sets the Remote Control section apart from the Custom Controls is the granularity of control. The Remote Control page can select individual driver channels to set dim level.

Lighting Policy

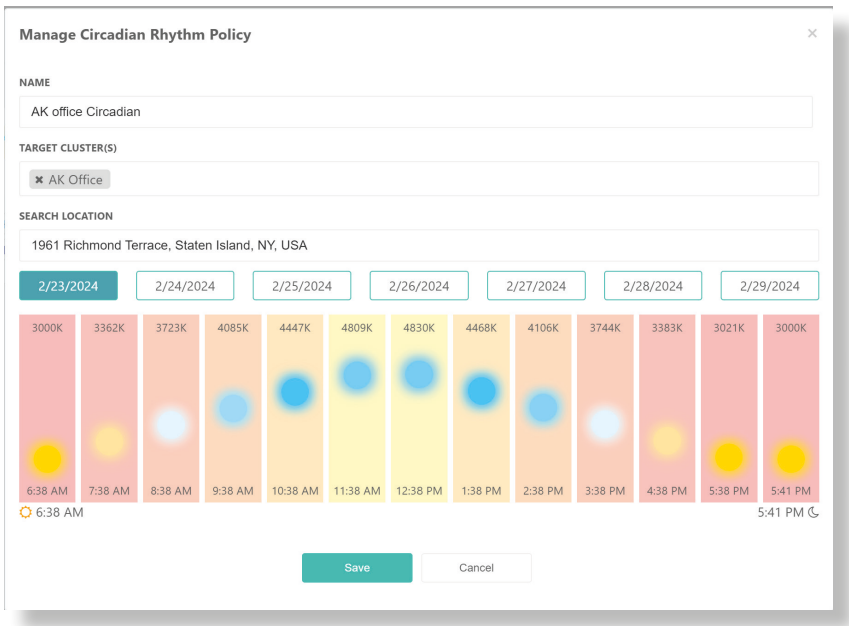
The lighting policy page is where the user can view, modify and create scheduled lighting control scenarios. In the screenshot below we have two different policy types. These policy's influence the clusters directly without the need for user input.



Circadian Rhythm [CIR] Policy:

The Circadian Rhythm policy as denoted in Policy 1 utilizes the cluster location in the settings and the frequency of policy repetition to simulate the human circadian rhythm for the environment associated. Displayed on the right is the policy being edited. This page is presented when selecting the edit key on the desired record which is the "pencil" icon.

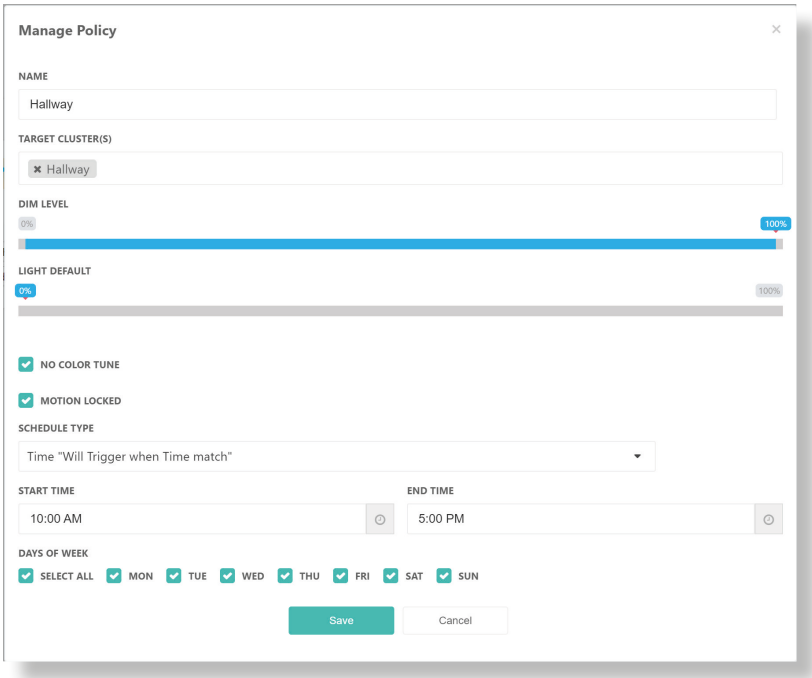
In the example provided the diagram shows hourly intervals and the clusters lighting will change to match the color of the sun as it moves throughout the sky. This provides support for the hypo-thalamus to help regulate the release of melatonin in our system.



Lighting Policy [REG] Policy:

A standard lighting policy as shown to the right, is utilized to conform to an SOO or sequence of operations.

In the scenario provided we have are forcing the lights to stay in the on state at 100% from the hours of 10:00am to 5:00pm every day. We have also chosen the Motion Locked which will ignore motion events and how they effect the space during the policy's effective.

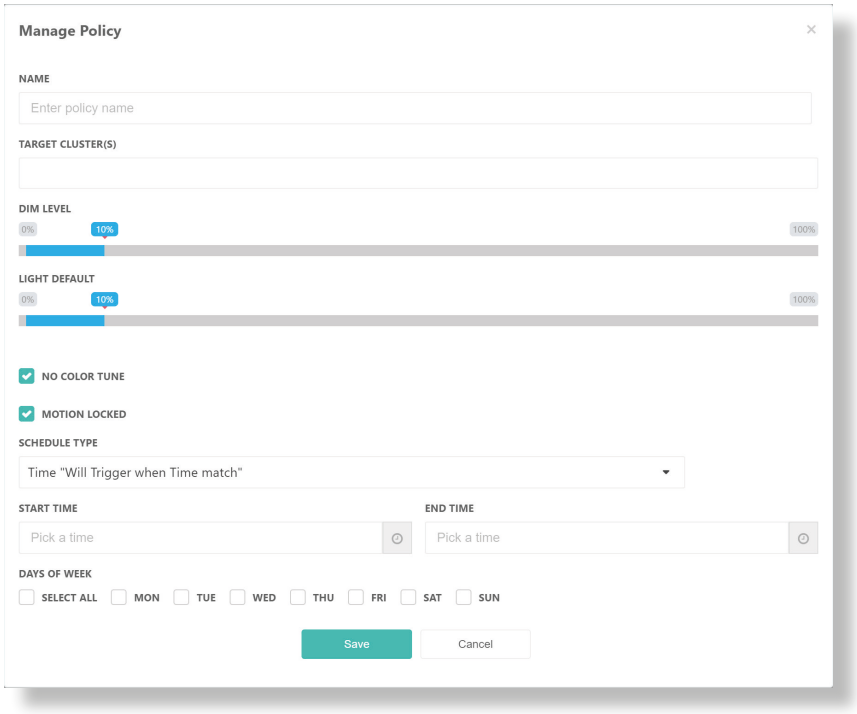


New Lighting Policy

In the previous section we introduced you to Lighting policies as well as provided context on there use cases. In this section we are going to review the procedure to creating the two different types of Lighting Policies.

Create New Lighting Policy:

When selecting the “new policy” from the Lighting Policies Main page you will be presented with the page shown to the right. Below we will provide context on the settings listed here.



Name:

It is important to provide the policy with an appropriate name as depending on the size of your installation it will be important when making future adjustments to the policy

Target Cluster(s):

Target Clusters allow you to provide the system with a series of clusters that this Policy will apply to. If you would like all hallways or room types to follow this policy then create one policy to affect all clusters the same by adding them all.

Dim Level:

This slider allows you to set the brightness of the lights during the policy’s implementation.

Lighting Default:

This slider returns the lights to the default state following the end of the policy

No Color Tune:

While this setting is checked it will apply the Lighting policy without effecting the color tuning fixtures. If the clusters in the list have a Circadian Rhythm Policy leave this box checked.

Motion Locked:

This is not currently used in this release please leave this checked during deployment

Schedule Type:

Time and Date “Will Trigger when specific date match”

This setting allows you to select a specific date and a Time to execute this policy this is helpful when a business is closed as lighting will stay off based on preset dates and times

Time” Will Trigger when Time Match”

This setting is utilized for daily re-occurring policies that are utilized at minimum weekly if not daily it uses day of the week and time of day to trigger the policy.

Circadian Rhythm [CIR] Policy:

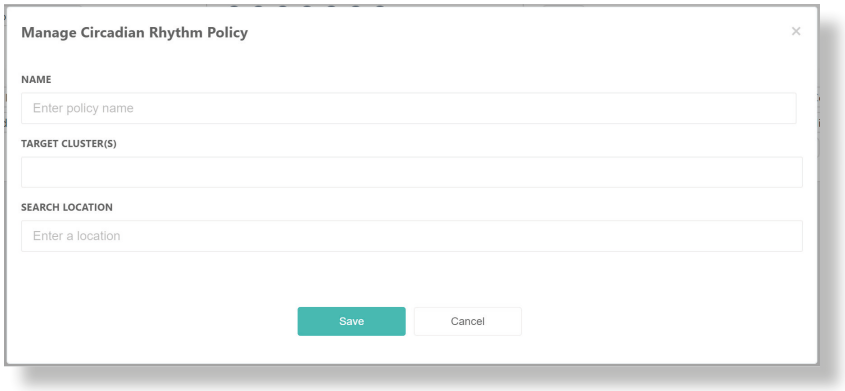
When selecting the “Circadian Rhythm Policy” from the Lighting Policies Main page you will be presented with the page shown to the right. Below we will provide context on the settings listed here.

Name:

It is important to provide the policy with an appropriate name as depending on the size of your installation it will be important when making future adjustments to the policy

Target Cluster(s):

Target Clusters allow you to provide the system with a series of clusters that this Policy will apply to. If you would like all hallways or room types to follow this policy then create one policy to affect all clusters the same by adding them all.

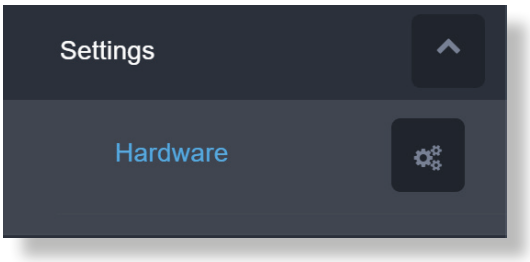


Search Location:

The search location utilizes the google maps API to auto-fill the text entered after accepting the text entry from the auto-fill list generated it will automatically generate the locational data needed to create the Circadian Rhythm Policy.

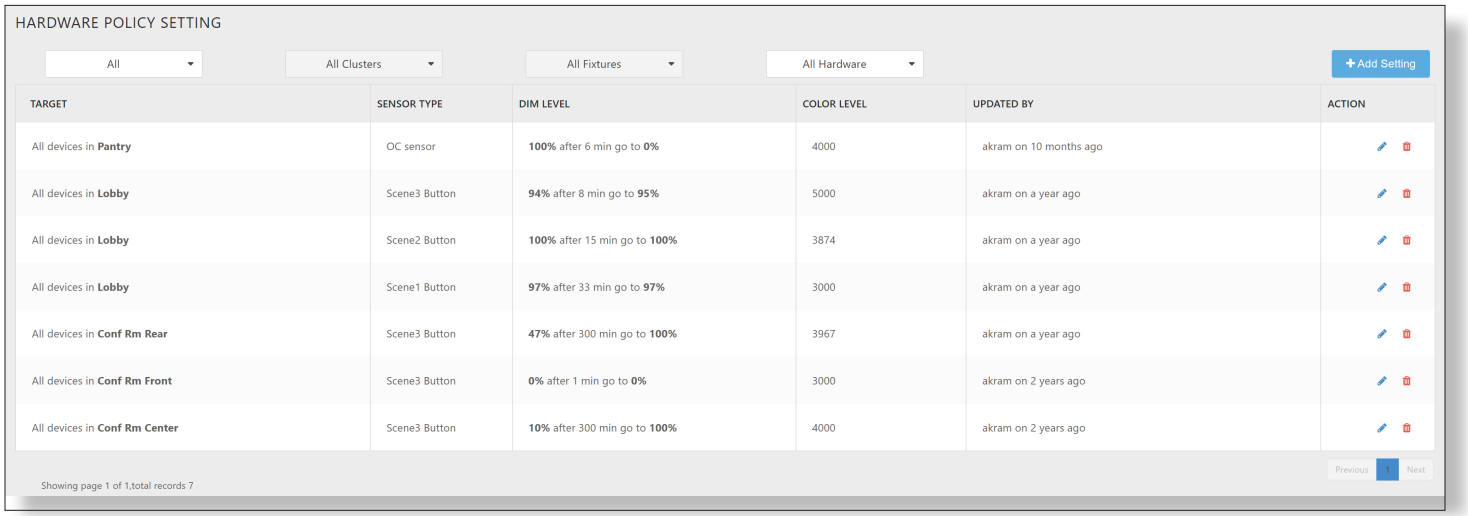
Settings

The Settings currently features a single page. This page is where hardware events can be programmed to trigger events within the cluster.



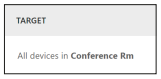
Hardware Policy Settings

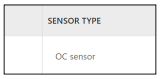
In this section we are going to look at navigating the The Hardware Policy page as pictured below. The page below provides a group of hardware policy settings listed in a single panel. This panel has a nested table with a series of fields that represent the policies nested within.



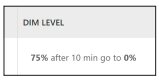
Hardware Policy Table

Target: provides a description the devices affected by the hardware policy.





Sensor Type: Is the device type that the Hardware Policy is applied to. For a list of Sensor Types see (New Hardware Policy Setting Page)



Dim Level: provides a description the hardware policies initial dim level, duration and post dim level.

Color Level: is the integer Kelvin Value for the color of the lighting in the space during the Hardware Policy Execution.

Updated By: creates a meta data trail that allows the user to see the party that was responsible for the hardware policy creation and the last time it was updated

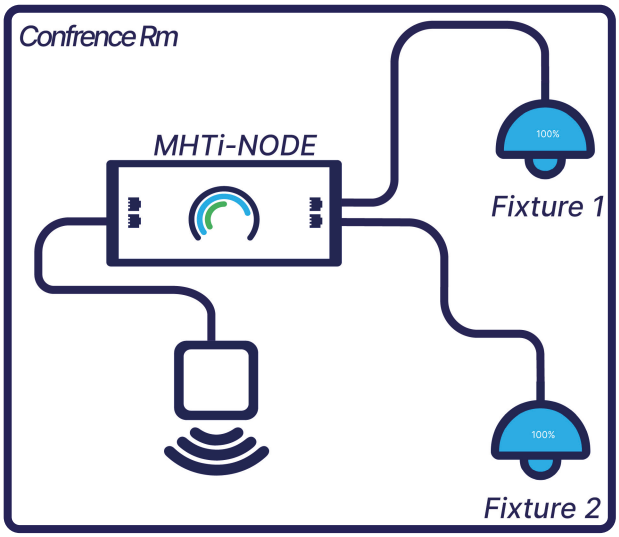
Action Buttons: are used to modify existing hardware policies. The buttons displayed are the "pencil" which will be discussed in further detail in the (Modify Existing Policy Setting) section and the "trash can" which will prompt the user for disposal of the Hardware Policy Setting.

Trash Can

Pencil

New Hardware Policy Setting

In the diagram to the right there are 2 fixtures and a sensor attached to a single circuit. In this example we are going to assume that the cluster is just the items listed in this figure. In this section we are going to create a policy that will utilize the occupancy sensor to trigger the lights to turn on based initial detection of the user entering the space.
We will set the policy timer to shut off the lights off following the expiration of the policy timer. In order to better explain this we are going to list the settings below.



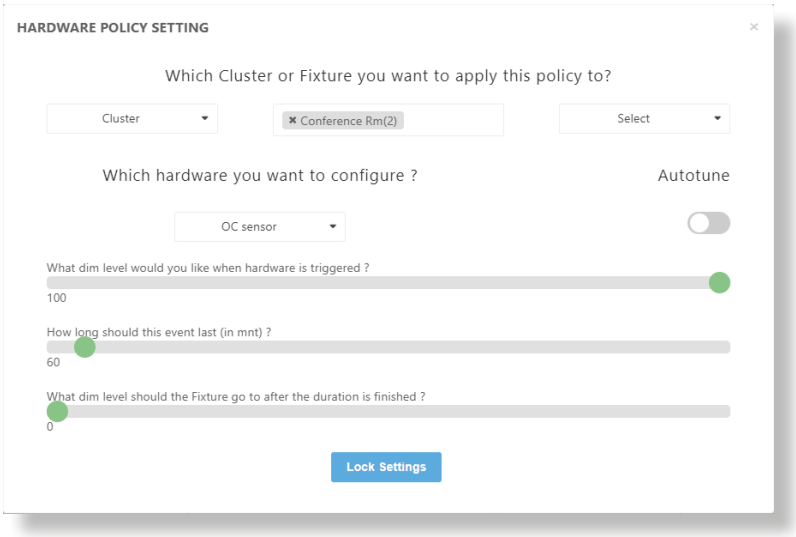
Conference Room Policy:

- Auto On / Auto Off
- Vacancy Time Out: 60 mins
- Occupancy Light Level : 100%
- Vacancy Light Level: 0%

Now that we have these settings written in a way that we can easily communicate lets create this setting.

New Hardware Policy Setting Page

After selecting the Add Setting button you will be presented a screen shown below. We have adding the listed settings above while selecting the “OC Sensor” option which will inform the inspextor system what event it will be listening for in order to begin execute this policy. If you review the image provided you can see that we have declared the 100% light level the length of time that it should last and the light level after the event has concluded. There are many other hardware types that can be programmed to allow the user to have more methods of input into the system. Listed below are a few more hardware types that can be programmed.



Hardware Types

- On Button
- Cancel Button
- Scene1 Button
- Scene2 Button
- Scene3 Button

Modify Existing Policy Setting

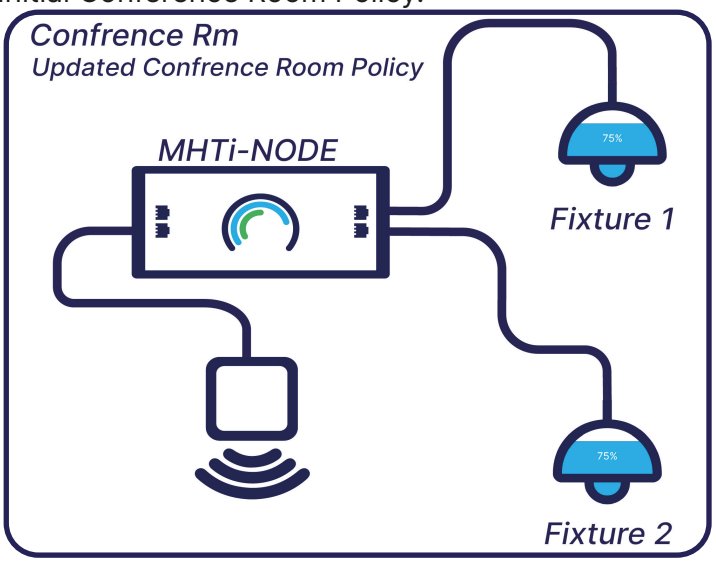
In the add new example we created the policy listed below in order to modify that policy we will need to locate the policy in the list provided. If you look below you will see the record pulled from the *Hardware Settings Table*. Review that against the Initial Conference Room Policy.

Initial Conference Room Policy:

- Auto On / Auto Off
- Vacancy Time Out: 60 mins
- Occupancy Light Level : 100%
- Vacancy Light Level: 0%

Updated Conference Room Policy:

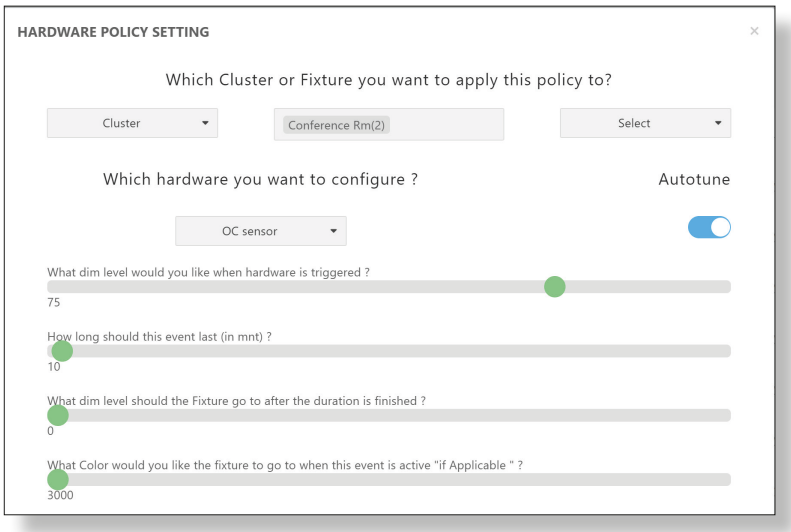
- Auto On / Auto Off
- Vacancy Time Out: 10 mins
- Occupancy Light Level : 75%
- Vacancy Light Level: 0%



Above is a list of the new settings that the client would like to implement in-order to do so we can just simply update the settings by utilizing the modify icon in the same row as the “Initial Conference Room Policy”.

TARGET	SENSOR TYPE	DIM LEVEL	COLOR LEVEL	UPDATED BY	ACTION
All devices in **Conference Rm**	OC sensor	**100%** after 60 min go to **0%**	3000	Broc on an hour ago	

Modify Hardware Policy Setting Page



After selecting the Modify settings Icon under the Action field you will be presented with the *Hardware Policy Setting* Page. Pictured to the left you can see that the sliders have been adjusted to reflect the requested hardware changes that are reflected in the *Hardware Settings Table* as shown below

TARGET	SENSOR TYPE	DIM LEVEL	COLOR LEVEL	UPDATED BY	ACTION
All devices in **Conference Rm**	OC sensor	**75%** after 10 min go to **0%**	3000	Broc on 4 minutes ago	

Hardware Policy Settings cannot be duplicated

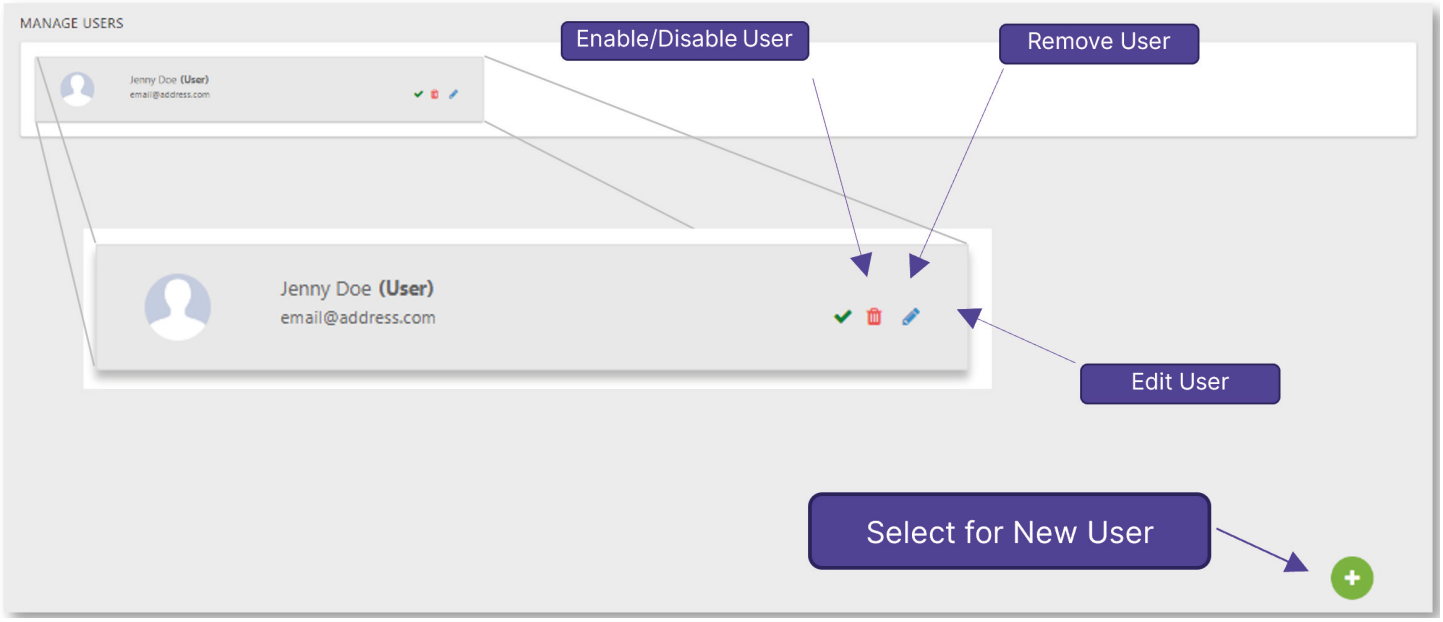
User Management

User Controls

The Inspextor Create User page is where you can modify user access permissions and edit your user list. This section will walk you through the process of adding a new administrator so that your installer/commissioning agent can securely access the Inspextor Software. In the subsection below we will introduce user management and creating a new user.

User Management

In the example provided we have the user, Jenny Doe. From the user page we have 3 options to manage the user, Disable, Remove and Edit. Disabling the User will remove the Users access to the system and editing the user will allow us to update the permissions and contact users' information. The permissions and contact information can be seen in the User Details example where we have made Jenny's Account.



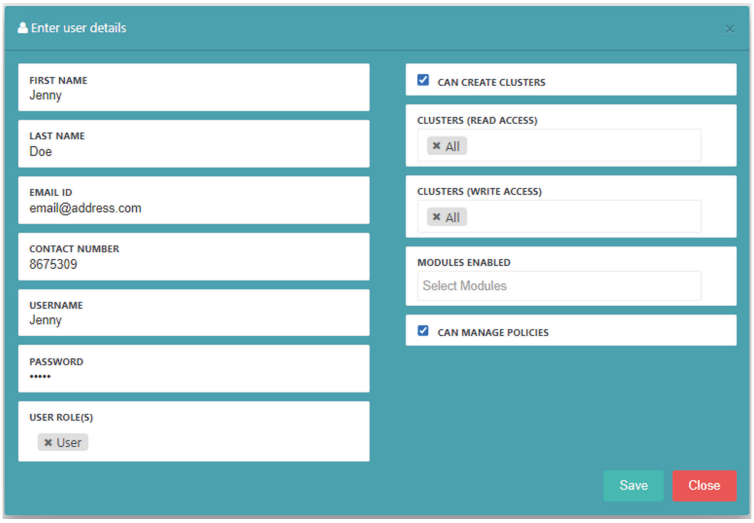
New User Details Page

In this subsection we are going to introduce the User Details Section. When creating a user, the system requires all fields as default except for modules enabled. In this Scenario Jenny is going to utilize the User Role “User” this will allow here access to the system with viewing privileges. The associated fields will be outlined below.

Clusters

Clusters are the defined groups of devices that make up the physical space Inspextor devices are in examples would include Private Office, Room 123. This is how the Inspextor Software groups devices to generate usage data and scenes.

In the Example provided we have granted Jenny the ability to create, view and modify All clusters.



Policies

Policies are defined hardware events that can be used to modify the clusters state. Policy triggers can be wall button presses and Motion Sensor Events.

In the Example Provided we have granted Jenny the ability to create, view and modify policies.

Configuration

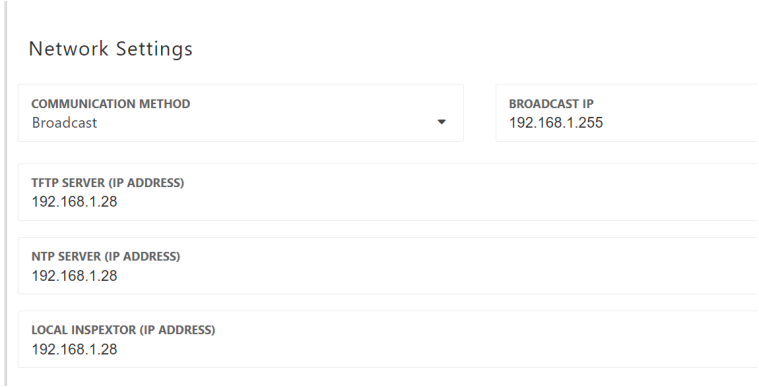
Inspextor Setting

The Inspextor settings page is split into 5 panels as shown below. It is important to have a through understanding of the system before users attempt to access this page as settings in this page can have an adverse effect on the system if mis-configured

Panel 1: Network Settings

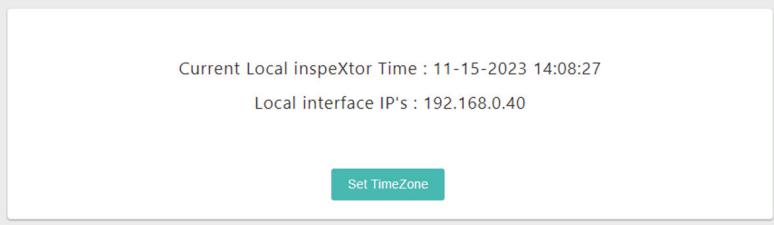
This is where you can locate and provide reference information for the server to communicate to the nodes and where network information can be acquired. This is also the location where you can modify the advertised address of the TFTP Server so that the nodes can find their firmware updates. These Settings should be verified but should not be adjusted unless the Commissioning Agent is Informed.

Communication Method: Server broadcast method.
Broadcast IP Address: This is the broadcast address for the network.
TFTP Server: This is an advertised address for the location of the TFTP server that has Firmware Updates
NTP Server: This is for the Network Time Protocol Server and is helpful with providing the appropriate relative time with the existing network infrastructure.
Local Inspextor: This is the address of the Inspextor Instance.



Panel 2: Time Zone Settings

This is to provide reference for the cloud platform and alerting aspects of the Inspextor software allowing accurate data for the systems databases. This section is basic just validate and update your settings based on the location of the installation.



Panel 3: Software Communication Settings

This group of settings is where we can control cloud communications, settings broadcasting, node and Inspextor event redirection, and node status update frequency. These setting should be left in there current state unless otherwise directed an authorized representative.

Event Redirection

This is a simple toggle and allows us to activate events to be redirected to a different location.

Settings Broadcast

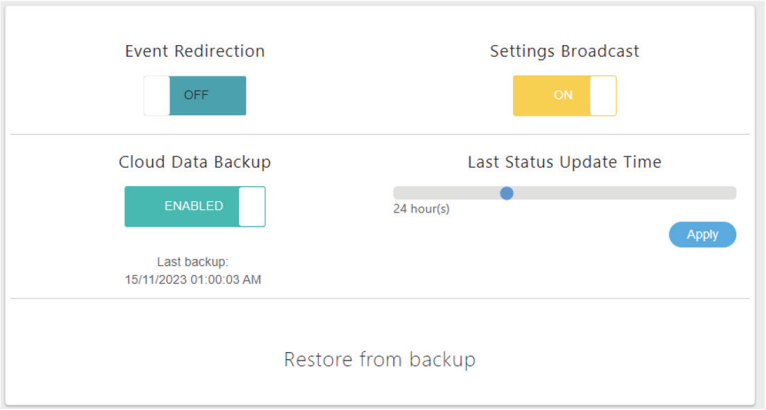
Settings Broadcast is enabled by default and is utilized to broadcast the data that we have declared in Panel 1.

Cloud Data Backup

Cloud Data Backup is a simple enable and disable that allows the Inspextor software to send a database backup to our cloud servers to provide warm backup capabilities in the event of an

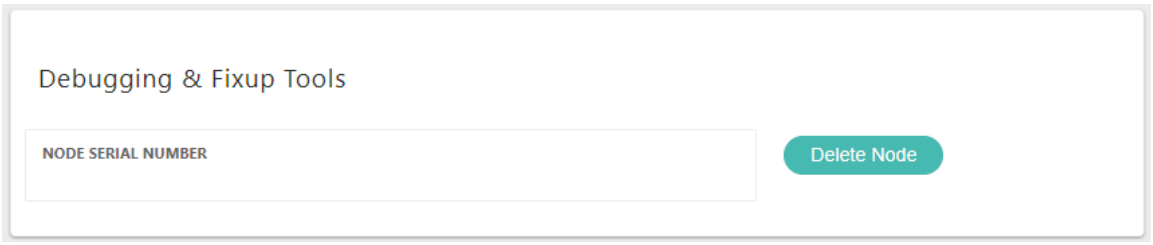
Last Status Update Time

The last Status Update time is a slider that allows us to adjust the frequency of the status updates from the Node devices. The default time is set as 24 hours, and it is recommended that for the purposes of start-up that it is left at



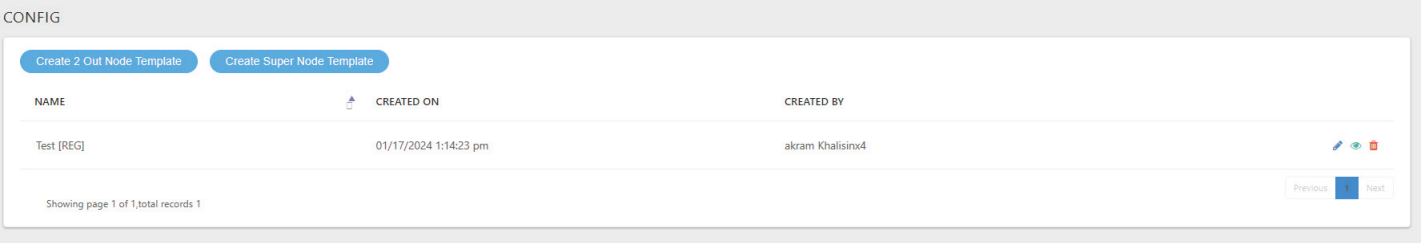
Panel 4: Debugging & Fix-up

This panel allows installers to remove stubborn to discover or modify devices to be removed from the system buy simply typing the serial number and selecting delete node.

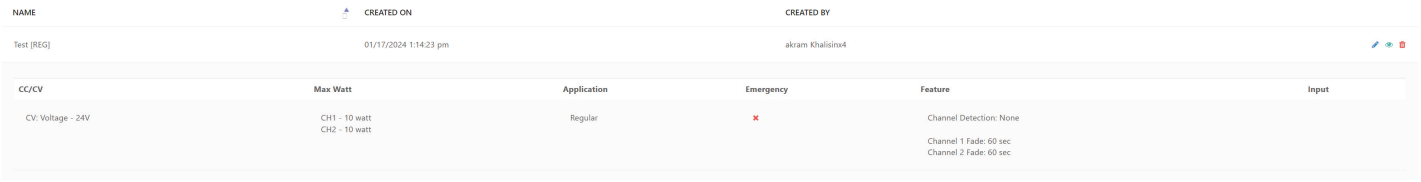


Node Templates

Node configuration templates allow the admin user to define default properties for different types of nodes in the system. There are two types of nodes: “2 Out Node (Regular Node)” and “Supernode”. This templated approach allows the user to create templates that can be applied to specific node circuits that are repeated. As shown below page is in a tabled format that allows the user to see all defined Templates.

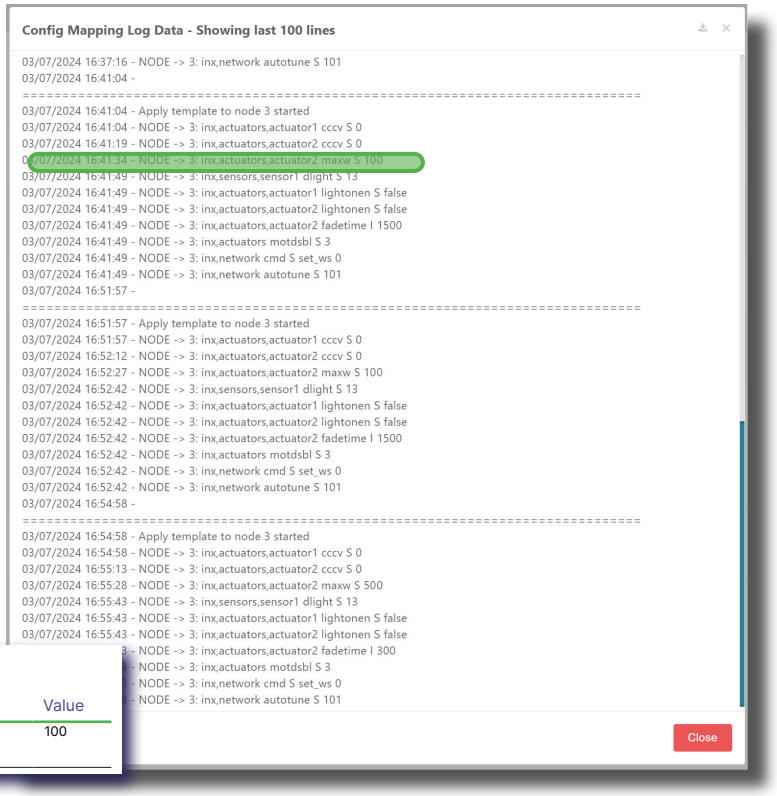


The picture below shows the result of selecting the “View” Action Button. It allows a high-level view of what the template defines. In this situation it will configure the device for CV 24V and 2 10 Watt fixtures.



Analyzing the Node Map Log

In the previous section we introduced the Node Mapping Log and how it is influenced by the Auto Mapping feature on the Node Mapping Templates. In this section we are going to look at the details provided by this log. On the Node Mapping Log page the user will find the “eye” icon at the end of each individual record if this is selected the user will be presented with the pop out pictured here. The Data present in this pop out presents us with a clear picture of the commands being sent to the Node to achieve the desired templated configuration. The records are populated with the Date, Time, and commands being sent. This pop out also allows the user to download the log as a whole in order to view on your local machines. In the upper right hand corner of the pop out you will find the download button. The file will download with a “.log” file type this file type can be opened in the notepad on windows machines.

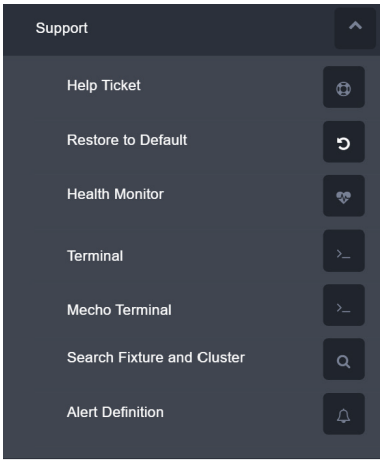


Data Log Record Explained

Time	Target	Path	Context	Data Type	Value
03/07/2024 16:41:34	NODE	inx,actuators,actuator2	maxw	S(String)	100

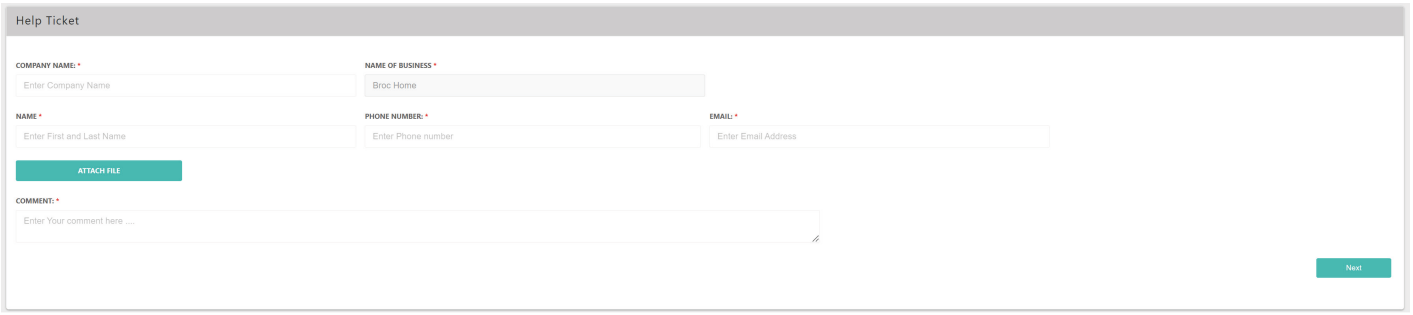
Support

This Section is where the user will find the support tools that can help trouble-shoot the errors that they are encountering in there environment. In the next few sections we will address the use case for each of the pages and dive into the details about what each page means.



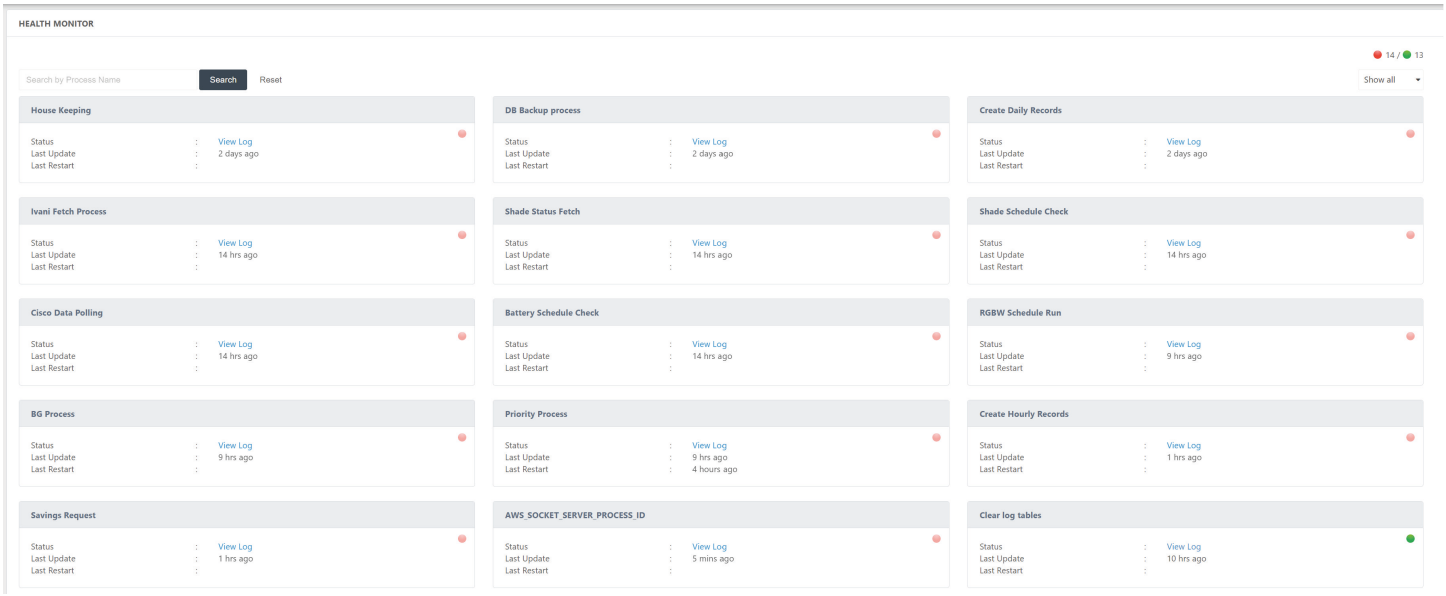
Help Ticket

The Section is where the user will find the support tools that can help troubleshoot the errors that they are encountering in there environment. In the next few sections we will address the use case for each of the pages and dive into the details about what each page means.



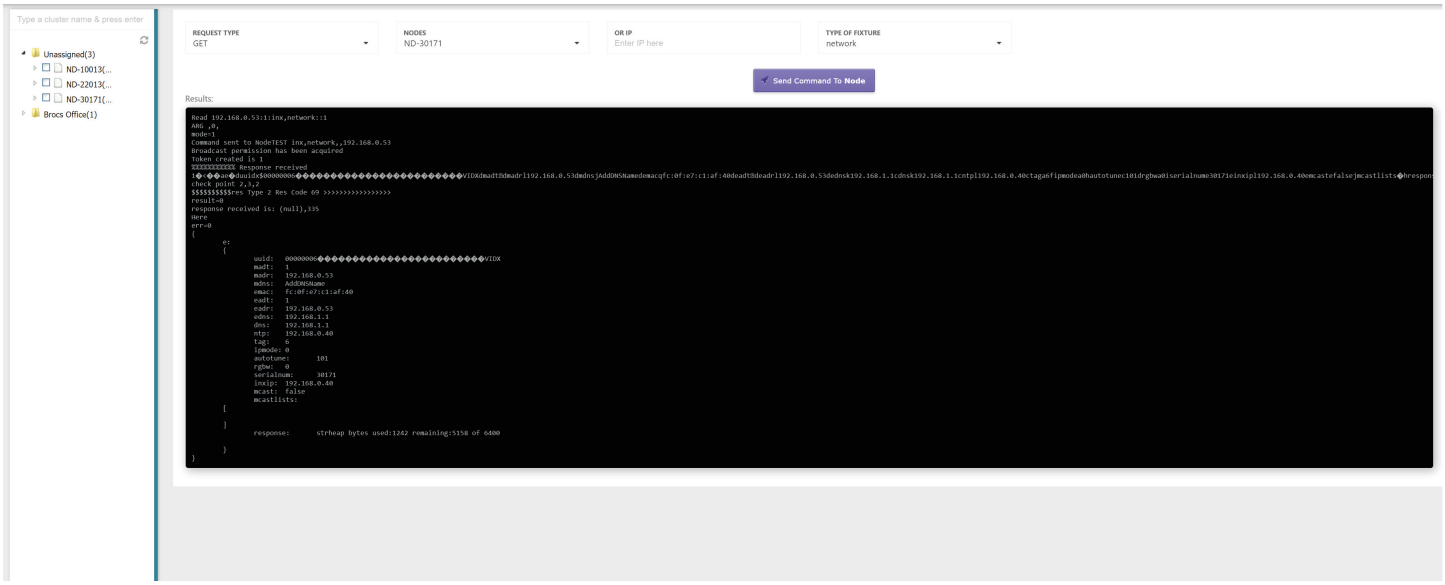
Health Monitor

The Health Monitor is a list of running process and there operating status'. Each process has a log that outputs status changes and errors. The View log allows the user to view "process" output data and can be copied to a text file for further support.



Terminal

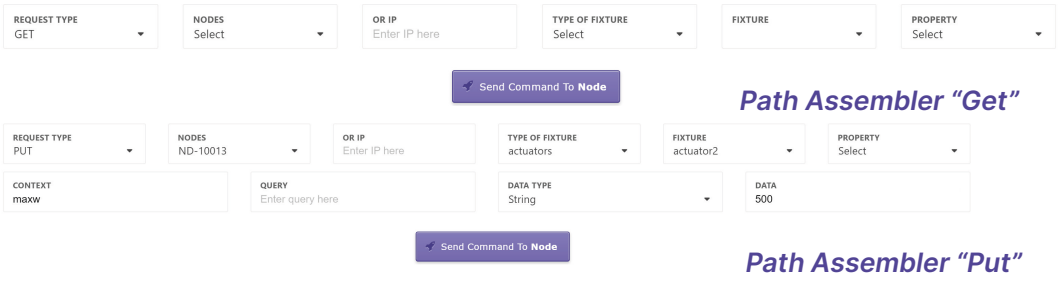
The Terminal is the most powerful page in the system with direct access to devices in the system it allows the user direct access to send Requests directly to the devices in the system. It is advised that only intermediate users access this page. Changing settings in this page can effect system stability and have unintended consequences.



Terminal Vocabulary

Path/Path Assembler

In the terminal the path/path assembler is the Inspextors tool to help the user assemble a path to ask the node for information or to set settings in the node.

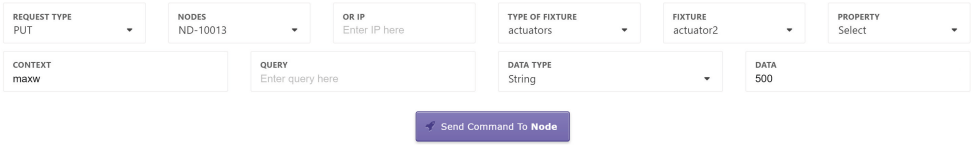


Get

The term "Get" in this context is a defined request type that is utilized to ask the MHTi Node for an explicit response. In the photo below the user has used the path assembler with the "Get" request to ask device "ND-30171" to return its network page.

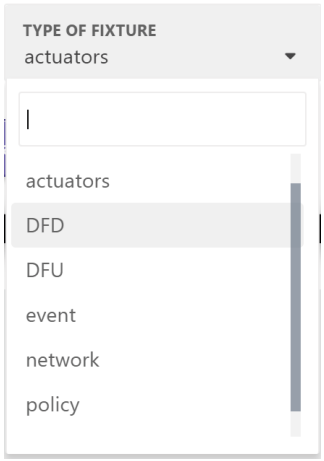
Put

The term "Put" in this context is a request. The Put request is utilized to set settings on the MHTi Node the "Results" section will reflect whether the command got a response. In the photo below the user has used the Path Assembler with the "Put" request to tell the device "ND-10013" to modify the "actuators/ actuators2" (Channel 2) to set its "maxw"(Max Wattage) value as a "string" to "500" (50 watts) .



Working with Get Responses

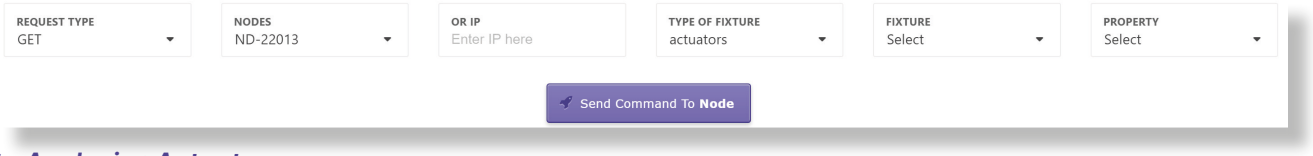
In the Previous section we introduced the use cases for the “Get’s” and “Put’s” in this section we are going to review the high level responses when utilizing the “Get” Request. This section will review the responses to Get Requests with the high level node pages that are shown on the right.



In the following sections we will utilize an example MHTi-NODE-90 device and query the list of pages shown and provide a high level overview of the “Results” section

Actuators

The Actuators page contains the explicit information about the LED Driver channels associated with the Node Device. In the picture below we can see that the User is querying the “ND-22013” for the actuators configuration.



Results Analysis : Actuators

Shown Below are the result of the command from the previous command that have been trimmed to the data specific to the actuators all data before the first “{“ is system data confirming the sent and the status of the response. The curly bracket separate the defined Actuators on the Node Driver. In the table below we will breakout the items in the actuators in settings and descriptions.

Actuator 1

```
uuid:   00000008000000000000000000000000VIDX
n:      13
maxw:   100
dims:   100
motdsbl:        3
prphtag:        20
cccv:   0
colconf:
els:    false
dimels: 25
lightonen:      true
pwmfreq:        25000
shortdetect:    false
fadetime:       0
pp:     100
lighton:        none

voltage:        55446
current:        73
power:  3878
vout:   0
iout:   0
```

Actuator 2

```
uuid:   0000000a000000000000000000000000VIDX
n:      13
maxw:   100
dims:   100
motdsbl:        3
prphtag:        0
cccv:   0
colconf:
els:    false
dimels: 25
lightonen:      true
pwmfreq:        25000
shortdetect:    false
fadetime:       0
pp:     100
lighton:        none
```

Setting	Description
uuid	Unique Identifier
n	Input control
maxw	max wattage output
dims	is the dimmed level of the channel
motdsbl	Enables and Disables Motion Events
prphtag	Not Used
cccv	Defines the Driver Mode
colconf	Not Used
els	Emergency Lighting Service
dimels	The dim level in emergency mode
lightonen	
pwmfreq	Frequency in Hz of the driver
shortdetect	is the channel shorted
fadetime	
pp	percentage power of the channel
lighton	
Voltage	measured voltage mV
current	measured current mA
power	measured power in mW
vout	
iout	

The device results above are from an MHT-NODE-90 device which has only 2 actuators present when querying “actuators” it will present all actuators. If you looking for a specific actuator utilize the “fixture menu” in the “path assembler” and select the actuator you are referencing.

Note: When querying the Super Node for an actuator summary it will not return the packet size is too large

Network

This section will provide an in-depth look at the network page. The network page does not have any sub pages like the actuators section previous. All settings can be viewed from this level with out the need for further modifications to the path.

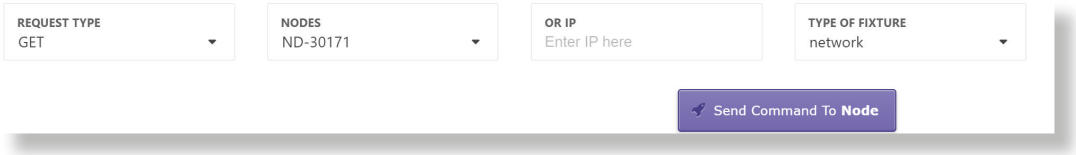
Results Analysis : Network

In the section below we will provide some detail on the individual settings that are present in the network page of the node. The purpose of this page is to provide the user with a view of the settings that effect how the nodes communicate with the network, the inspextor server and between nodes themselves.

Setting	Description
Uuid	Universal unique identifier
madt	
madr	
mdns	
emac	mac address
eadt	
eadr	
edns	
dns	
ntp	Address of network time protocol
tag	
ipmode	
autotune	Auto tune feature
rgbw	rgbw feature
serialnum	Serial number of the device
inxip	Ip address of the inspextor server
mcast	Status of multicast usage
macastlists	
response	
em_mode	Determines if the device is in EM Mode
em_time	Is the time before the device move to “EM status”
des_power	declared power consumption for static power allocation PSE’s

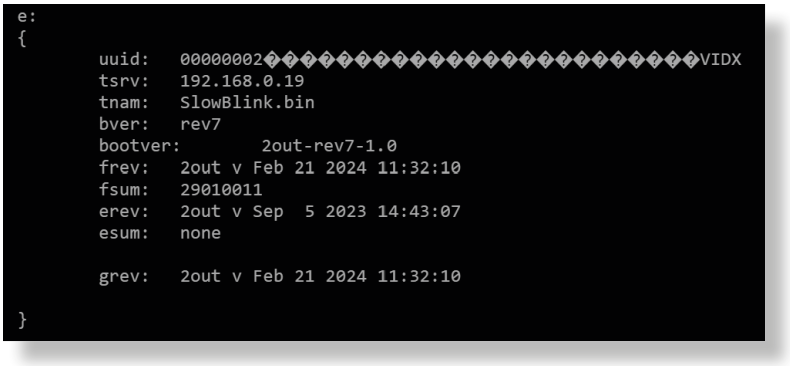
DFD/DFU

This section will provide an in-depth look at the network page. The network page does not have any sub pages like the actuators section previous. All settings can be viewed from this level with out the need for further modifications to the path.



Results Analysis : DFD/DFU

In the section below we will provide some detail on the individual settings that are present in the network page of the node. The purpose of this page is to provide the user with a view of the settings that effect how the nodes communicate with the network, the inspextor server and between nodes themselves.

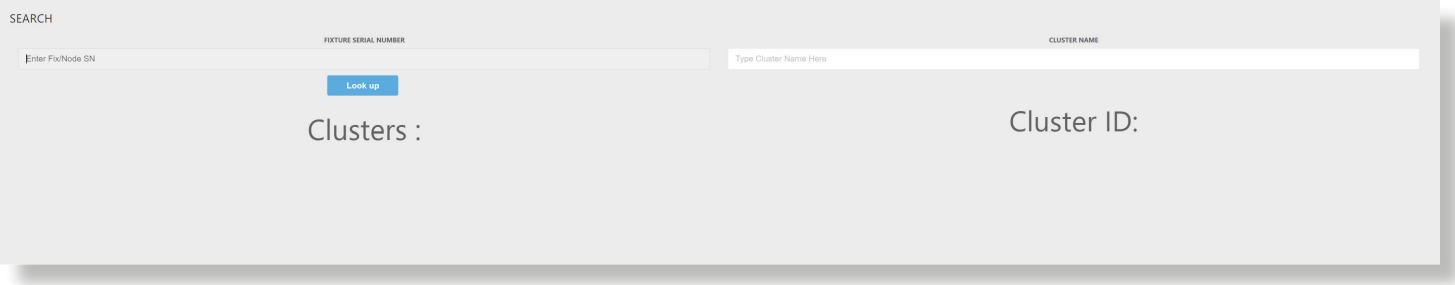


Setting	Description
Uuid	Universal unique identifier
tsrv	tftp server ip address
tnam	binary file name
bver	Board Revision Number
bootver	Firmware Boot Version
frev	
fsum	
erev	
esum	
grev	Golden Revision

Setting	Description
uuid	universal unique identifier
updt	update Trigger Value
bver	Board Revision Number
bootver	Firmware Boot Version
frev	
appdbver	app database version
nvmdbver	non-volatile memory version

Search Fixture

The Section is where the user will find the support tools that can help troubleshoot the errors that they are encountering in there environment. In the next few sections we will address the use case for each of the pages and dive into the details about what each page means.



Commissioning

Pull Schedules

Pull Schedule Introduction

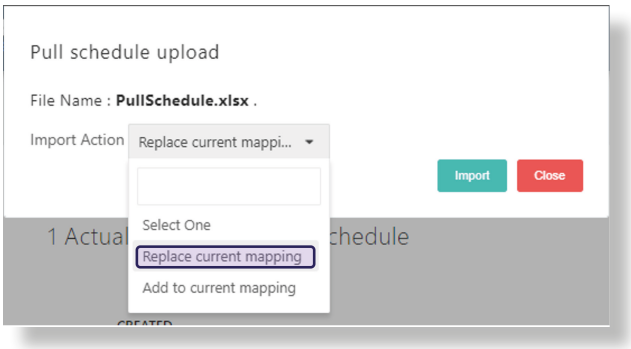
The Pull Schedule page is a play on the content that is normally present in Engineering drawings that define the physical beginning and end of a conductor in an installed system. In this instance the user will upload very similar data into the Inspextor system.

In the Auto Discovery process the Inspextor system locates and provides the MHT PoE devices an “ID Tag” to allow the internal database to recognize them and store the serial numbers of each device.

Initial Pull Schedule Configuration

It is important before you begin Pull Schedule configuration that the device you are working from can open an .xlsx (MS-XLSX) Microsoft Excel. If your machine can open the specified file type continue with the steps below.

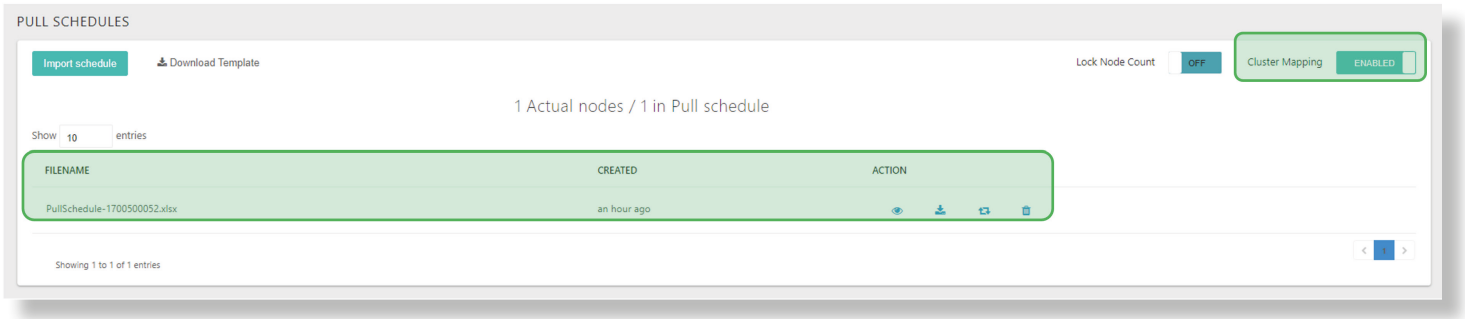
- Access the Commissioning > Pull Schedule Page
- Note: in the photo above under the section FILENAME no file name is present
- Select Download Template
- Locate the file “clusterMap-v3.xlsx” in your default save location.
- Rename the Default File “PullSchedule”.
- Upload the “PullSchedule” file utilizing the “Import schedule” button.



Modifying Uploaded Pull Schedule

When Modifying the Pull Schedule, it is important to understand the state of the installation as well as the Pull Schedule page.

The page below is a sample that has a single instance of the ***Pull Schedule*** uploaded and ***Cluster Mapping*** is enabled. If the page is without a file in the ***Pull Schedule Table***, the user will need to repeat the (Initial Pull Schedule Configuration Section). There are 2 methods for editing the Pull Schedule while in production.
The document can be downloaded and edited in Excel, or it can be edited in line using a pop out form.



Seeing the table above has a file listed shows that this instance of the Inspextor system has an uploaded Pull Schedule. It is important to understand the Action and how that section applies to the system.

View Device Table

This Action allows you to view the Devices listed in the pull schedule as well as allow you to modify the individual records of them utilizing the pencil icon on each record.

Download Pull Schedule

This Action allows you to download the associated pull schedule as a .xlsx file to modify multiple records and re upload the document.

Re-Populate Pull Schedule

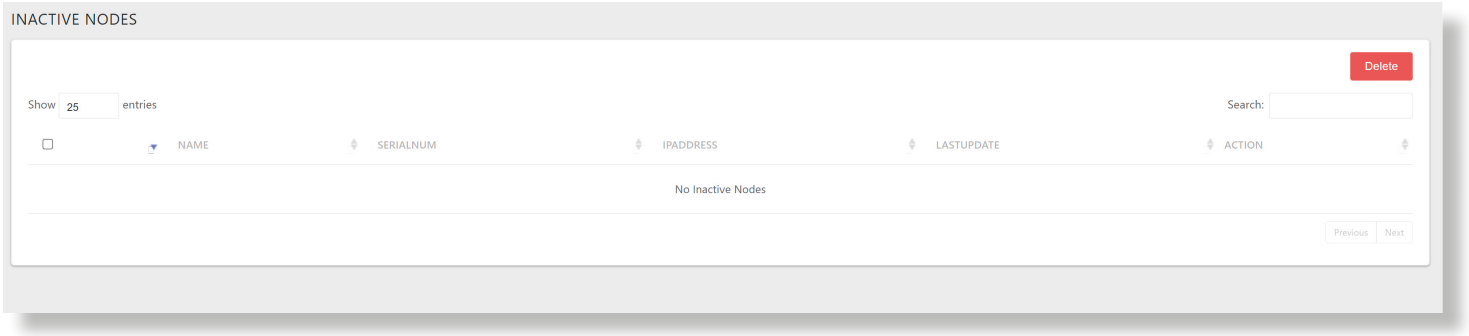
This Action pulls the data out of the Inspextor system and appends it to the pull schedule allowing the Auto Discovery page to auto populate the pull schedule.

Delete Pull Schedule

This Action Deletes the Pull Schedule from the system.

Inactive Nodes

The Inactive Nodes page is where records for stored for nodes that were present in the system at a one point and have since been removed or are non operational. In the image below the single panel on this page presents the device name, serial number, Last Known IP Address and the last time that the device was present in the system.

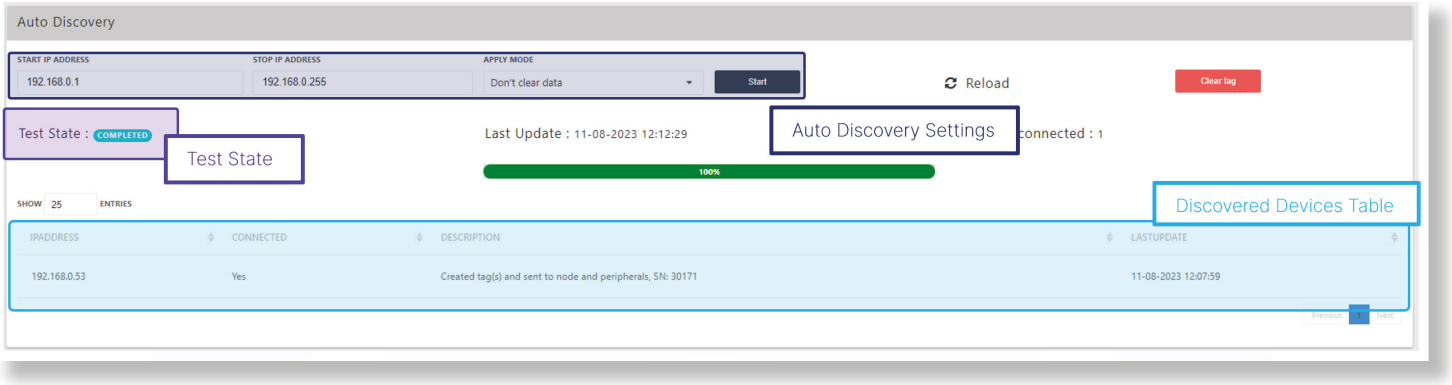


Management

The Management Navigation Tab is where the installation specific details are housed. It provides access to advanced troubleshooting settings, Licensing information, Firmware Updating and Device Discovery. It is not advised that a standard user access this area without express guidance from the installing agent or an MHT Support Agent.

Node Auto Discovery

The Auto Discovery is section is utilized to provide the Inspextor system a method of Initial device discovery. Inspextor Devices when powering up do not acknowledge the inspextor system and operate in a autonomous state until the Inspextor server discovers them and takes control of the devices. This autonomous operation state allows devices to operate without the inspextor software if an outage would occur. The discovery procedure is outlined below in the next section.



Auto Discovery Settings:

- Start Ip Address:
  - Format: x.x.x.x
  - This is the starting address for the auto discovery process for the Inspextor server.
- Stop Address:
  - IP Format: x.x.x.x
  - This is the last address for the auto discovery process for the Inspextor server.
- Apply Mode:
  - Don't Clear data
    - Selecting this option will retain all data in the ***Discovered Devices Table.***
  - Clear data
    - Selecting this option will retain all data in the ***Discovered Devices Table.***

Test State:

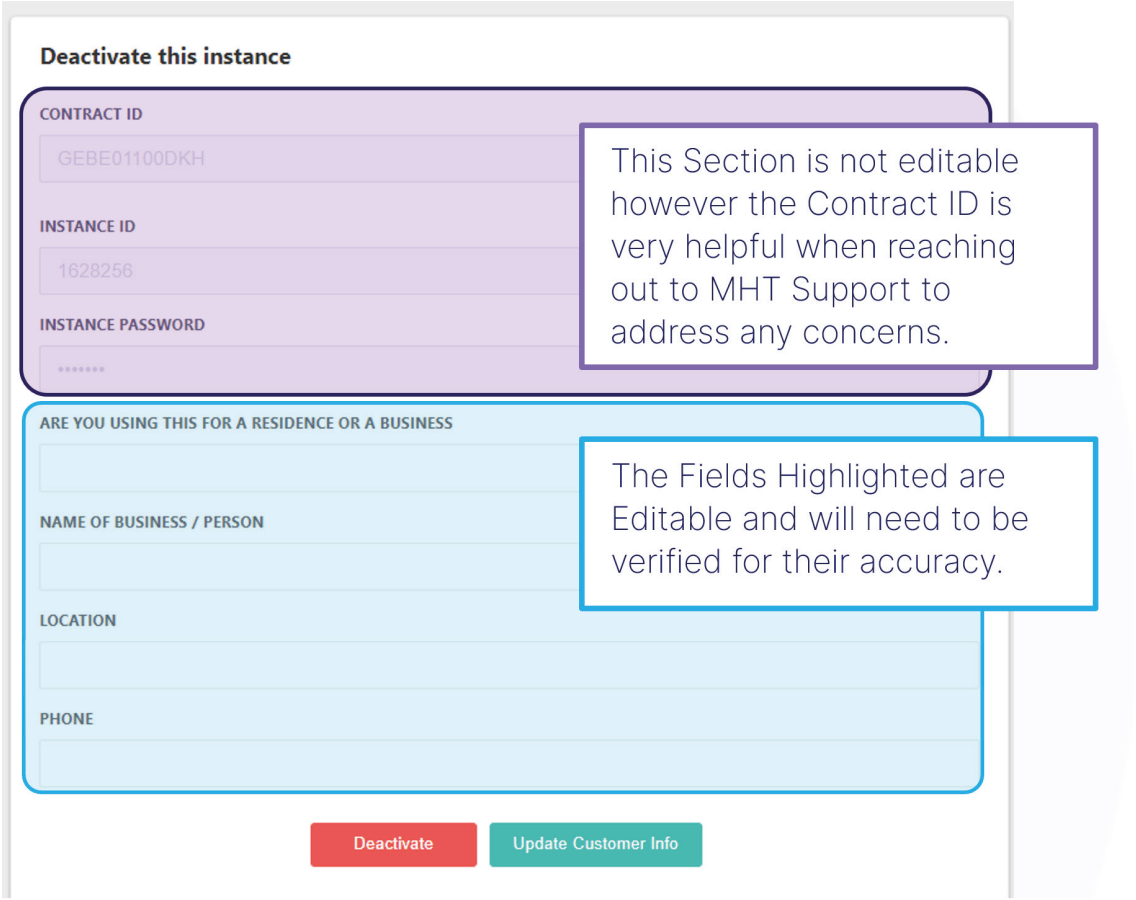
- Scheduled:
  - This is displays to inform the user that the setting s listed above have been accepted and it is ready to execute.
- In Progress:
  - This will display along with the status bar to the right. (Below Last Update) when the search is being executed. The user can navigate away from the page during the search.
- Completed:
  - This status will be displayed with the associated status bar displaying 100% and all devices listed in the ***Discovered Devices Table***. When the Discovery is complete.

Discovered Devices Table:

- IP Address:
  - The reported IP Address of the MHT PoE device.
- Connected:
  - Confirms a stable connection to the MHT PoE device.
- Description:
  - This column defines the action taken by the Inspextor system after discovery.
- Last Update:
  - This will stamp the date and time of the devices last status update to the Inspextor Software.

Activate/Deactivate

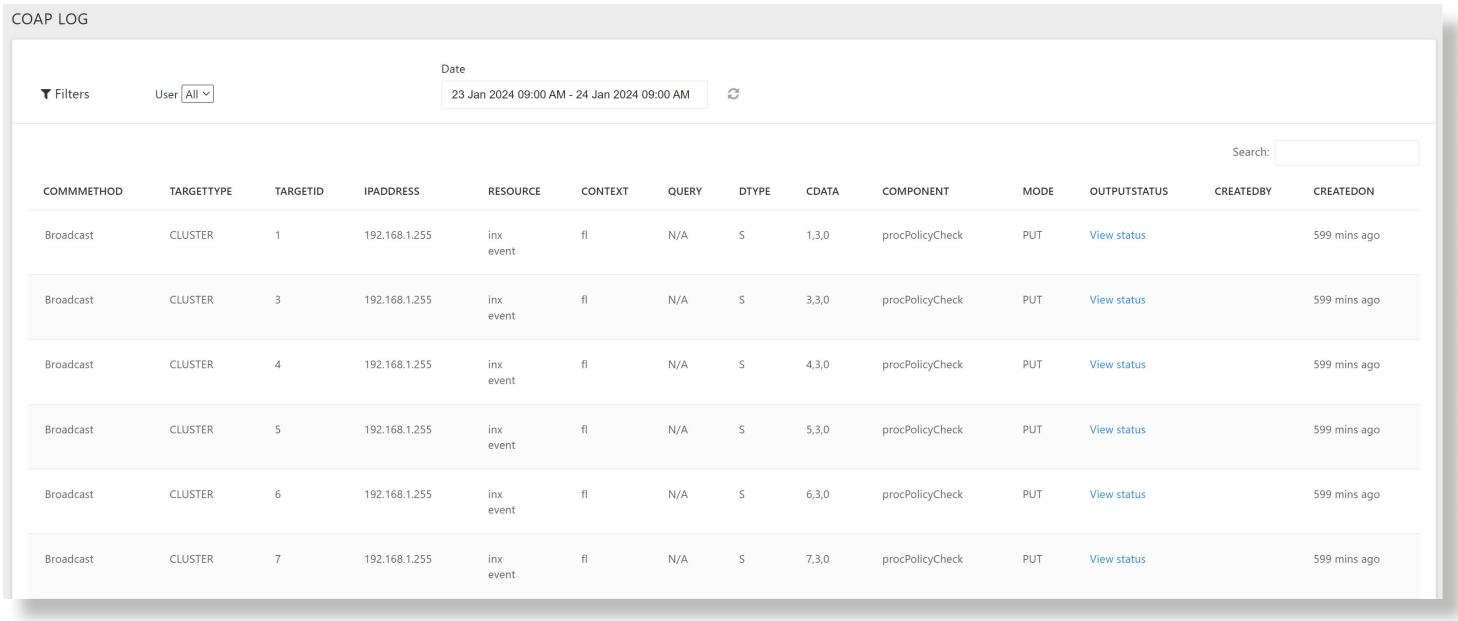
Activate and Deactivate page is colloquially known as instance controls. It is where the server itself can control it's software licensing and device location. In the photo below you can see a few of the settings are available for monitoring purposes.



COAP Log

The COAP Log is an advanced troubleshooting section that allows an advanced user to troubleshoot communication errors between the software and the devices in the example below the table is populated with a series of COAP Events that allow the user to view traffic disseminated from the Inspextor Software to the Inspextor PoE Devices.

Selecting the View status allows the User to View the structure of the COAP message. The user can also sear the records by utilizing the search bar.



Further Reading

The MHTi-Appliance is now operational in its application and is now ready for the Installers/Commissioning Agents to document and commission this instance of MHT's PoE Solution. If the reader is looking for further understanding, please see the links below for further information of about the Inspextor system.

Technical Articles:

https://mhttechnologieshelp.zendesk.com/hc/en-us

MHT Technologies:

https://mht-technologies.com/

Contact Support/Sales

+1-718-524-4370

sales@mht-technologies.com

HQ/MANUFACTURING:

1961 Richmond Terrace Staten Island, NY 10302

SHOWROOM/INNOVATION LAB:

241 W 37th Street New York, NY 10018