EnGenius

SKYPOINT USER MANUAL

Contents

1. Introduction

Thank you for choosing the EOC65X Series. The EOC65X devices come equipped with SkyPoint software, offering a centralized and comprehensive web-based management solution for your network. With SkyPoint, you can leverage a highly scalable platform to manage your network seamlessly through a web browser. It features customizable dashboards and reports, providing deep monitoring and analysis capabilities to ensure your critical infrastructure is managed and monitored effectively. SkyPoint is designed to streamline network management, offering intuitive tools and insights to optimize your operations.

Table 1: SkyPoint Features

Feature	Description
Dashboard	One-page view of the status of all your radios in the network with events and a quick inventory of all radios active on the network.
Topology	Devices are listed hierarchically based on location with links showing on the map and logical structure showing as tree
Discovery & Provisioning	Quickly discover all radios by IP addresses & range. Automatic provisioning of radios by using pre-configured templates. Check firmware versions and upgrade easily; Replace hardware and restore configuration.
Maps	Google Maps with satellite view to position your devices and visualize their health and connectivity. Change the mode of the map to graphically display various wireless key performance indicators
User Management	Configuring and creating role-based users.
Automation and forecasting	A rich set of RESTful APIs allows integration with external CRM and reporting systems. For example, Integration with the Fusion/R12 CRM system allows for a management ticketing system (Opening / Closing) for different device issues at the customer sites.
Template-Based Configuration (Fixed Wireless)	Push configuration to the device of EnGenius devices across your network using templates

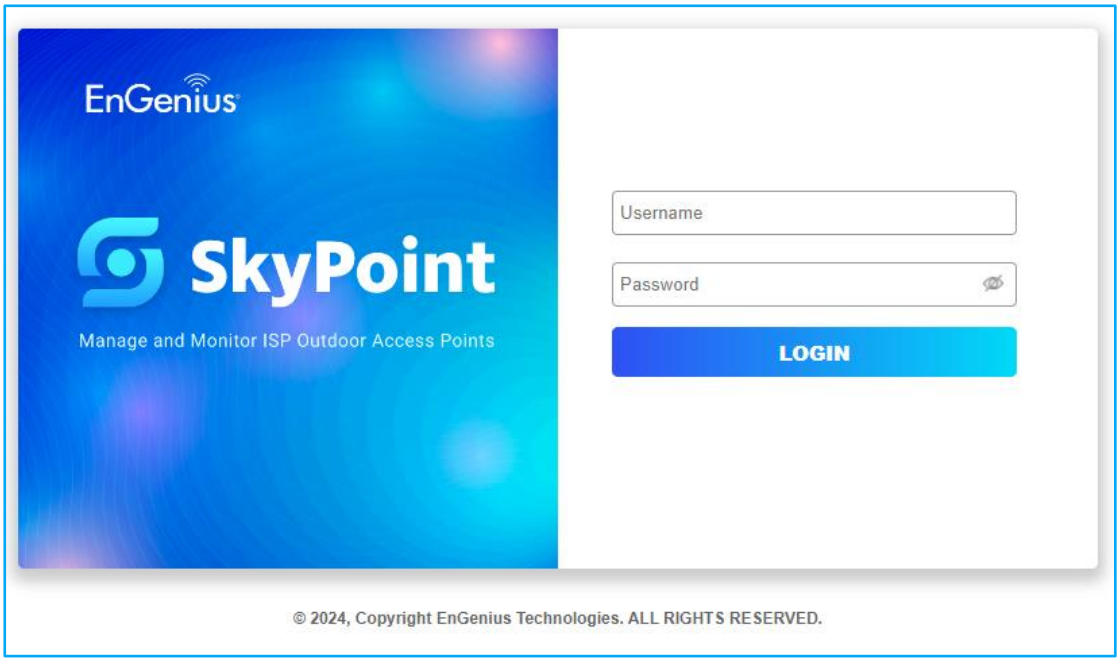
Table 2: Supported Devices and Firmware Version

Device	Version
EOC600/610	Firmware v1
EOC655	

2. Instructions for Login

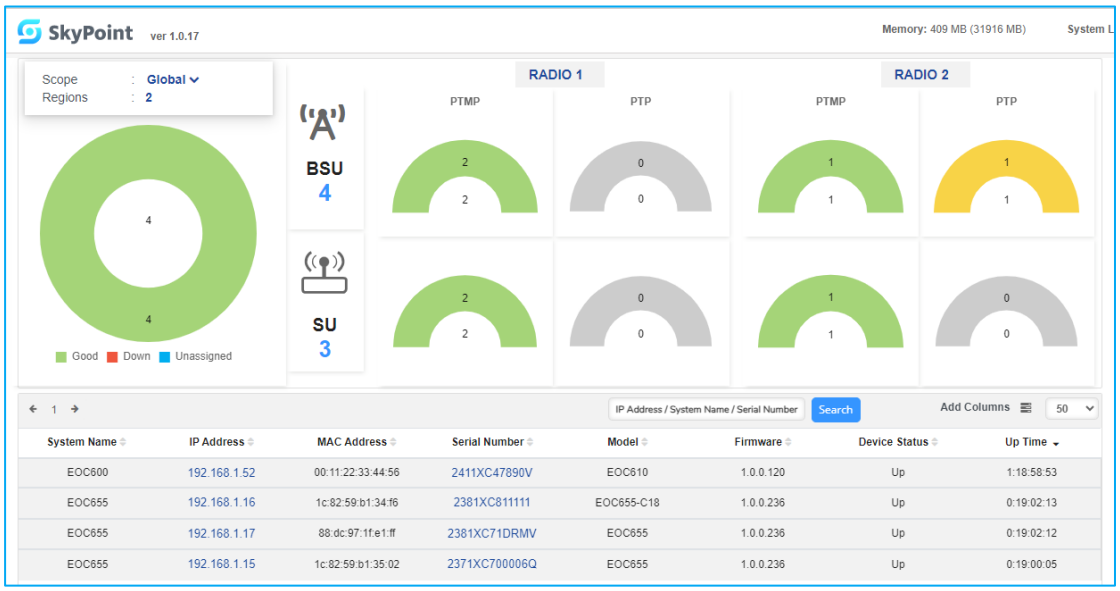
Launch the web browser. In the address field, type http://localhost:8980/skypoint/ in the address bar and press enter (PC) and you are redirected to the login screen.

- Login Screen
- Enter Username as “admin” and Password as “admin” and press Enter to continue.



3. Dashboard

The dashboard offers a comprehensive and visually intuitive overview of the entire network's current state, presenting crucial metrics derived from deployed radio units. With real-time performance graphs at their disposal, administrators can effortlessly monitor and assess the network's health, performance trends, and potential issues. This tool enables the identification and diagnosis of network problems quickly, facilitating prompt and informed decision-making. Additionally, the dashboard's user-friendly interface simplifies the complex data associated with network performance, making it accessible even to those with limited technical expertise. This allows for more efficient and effective management of the network, ensuring optimal performance and reliability.



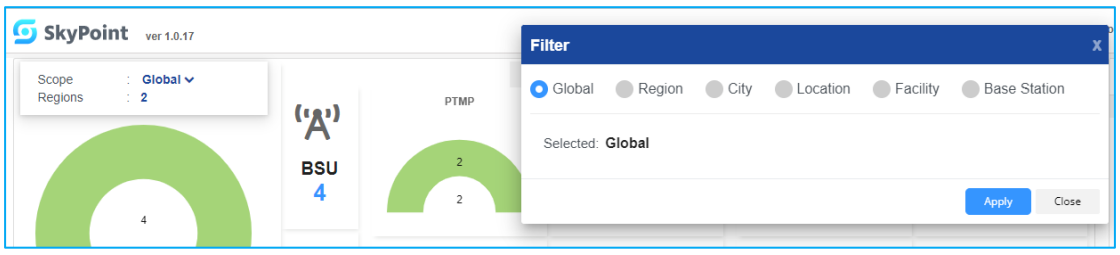
3.1 Menu

Icons	Description
	Dashboard The dashboard shows the overall status of the entire network in real time with the help of graphs and alerts and helps the administrator to analyze the status of the device.
	Discovery: Discovers all the available devices in the networks. There are three types of discovery: By IP address & By IP Range.

	Topology It shows the hierarchical view of devices in the tree structure. Devices are listed in the form of **Global**->**Default Region** -> **Default City -> Default Location** -> **Default Facility** -> **BSU** -> **SU**. Please refer to Topology for more details
	Configuration A user can create profiles and make basic configuration changes related to Radio1 / Radio2 and 2.4 GHz radios.
	Events Events and log messages are generated either by SkyPoint or the traps which are generated by devices when an event occurs in the device
	Inventory Reports It shows the list of devices added to the SkyPoint. Users can change the Scope/Region of the device from the Inventory, we can the details of the device like Device Name, IP Address, MAC Address, and Serial Number
	Settings Configurations related to the server are listed in “Settings”.

3.2 Scope Filter

SkyPoint offers a structured and hierarchical approach to organizing devices based on their installation locations, following a tiered framework: Global -> Region -> Location -> Facility. This organization allows for precise and efficient management of devices across various geographical and functional divisions. Each level of the hierarchy encompasses a broader scope, starting from individual facilities nested within locations, which in turn are grouped into regions, all under the overarching 'Global' category.



Upon the discovery of a new device, it is assigned to a specific facility, which is the most granular level in the SkyPoint hierarchy. A single location can host multiple facilities, reflecting the physical infrastructure and organizational needs of that area. Similarly, each region comprises several locations, allowing for regional oversight and management. The topmost 'Global' group acts as the umbrella under which all regions are unified, providing a comprehensive and global view of the network.

The platform's scope filter feature enhances network management capabilities by enabling users to filter and view device data based on selected criteria within the hierarchy—ranging

from a global perspective down to specific facilities. This filtering capability ensures that users can focus on the relevant subset of devices, improving operational efficiency and data visibility.

- Global Filter: When the 'Global' option is selected, the filter applies universally, offering a complete overview of the network's status and events across all devices, regardless of their specific locations or facilities.

- Region Filter: Selecting the 'Region' filter narrows down the view to include only the devices within one or multiple specified regions. This allows for regional analysis and management, providing insights tailored to the geographical segments of interest.

- Location Filter: By choosing the 'Location' filter, the data presented is limited to devices installed within a particular location or a set of locations. This level of filtering is useful for localized monitoring and management, offering detailed insights into specific areas.

- Facility Filter: The 'Facility' filter further refines the data visibility to devices associated with one or multiple facilities. This granular view is essential for facility-specific operations and troubleshooting, allowing for focused management of devices within those premises.

Additionally, the scope filter includes a "Base Station" option, extending the filtering capabilities to encompass base stations, thereby enhancing the platform's flexibility and applicability to various operational scenarios.

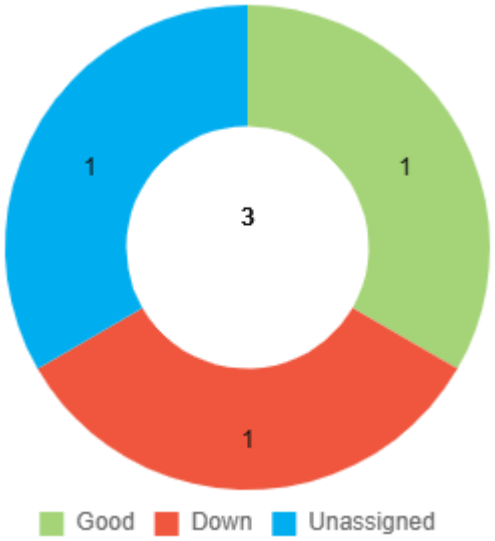
It's important to note that while the "Overall Status" remains unaffected by the scope filter, all other component data are dynamically filtered according to the selected scope. This design ensures that users have access to targeted and relevant data, facilitating effective decision-making and operational oversight.

3.3 Overall Status

The doughnut chart provides a visual overview of the network status across all devices within the SkyPoint system, categorized into four distinct statuses

represented by different colours: Good, No Link, Down, and Unassigned. Each color signifies a specific operational state of the devices, allowing for an at-a-glance understanding of the network's overall health and connectivity status.

- Good (Green): This category is marked in green and indicates the number of devices that are currently active and functioning as expected. Devices classified under "Good" are operational and successfully communicate within the network, showcasing optimal performance and reliability.



- Down (Red): The "Down" status is depicted in red and encompasses devices that are currently non-responsive. A device is considered "Down" if it fails to communicate or respond to network queries, which could be due to being powered off, disconnected, or experiencing other connectivity issues. This status is critical as it directly affects the network's integrity and availability.

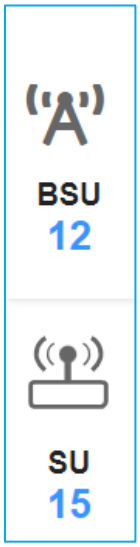
- Unassigned (Blue): Devices falling into the "Unassigned" category have been detected by SkyPoint but have not yet been configured or provisioned with a specific role or settings. Provisioning these devices involves assigning them a profile or utilizing the "Node View" section for default provisioning, which integrates them into the network for active use.

This doughnut chart serves as a crucial tool for network administrators and users, providing immediate insight into the distribution of device statuses within the SkyPoint network. By understanding the proportion of devices in each category, stakeholders can prioritize actions, such as provisioning unassigned devices or troubleshooting those marked as "No Link" or "Down," to maintain or enhance network performance and reliability.

3.4 Radio Type

The overall count status of radio types within the SkyPoint network is a crucial metric that provides insights into the distribution and operational state of Base Station Units (BSUs) and Subscriber Units (SUs) across the network. This count offers a snapshot of the network's composition, highlighting how many devices are functioning as BSUs versus SUs, which is essential for understanding the network's topology and operational dynamics.

- **Base Station Units (BSUs)**: BSUs serve as the backbone of the network, facilitating communication and data exchange among various nodes. The count of BSUs indicates the number of devices configured to provide coverage and connectivity to SUs. These units are critical for establishing and maintaining the network's infrastructure, ensuring that subscriber units can connect and communicate effectively within the network.
- **Subscriber Units (SUs)**: SUs are the devices that connect to the BSUs to gain access to the network. The count of SUs reflects the number of end-user devices or nodes that are connected to the network via BSUs. This count is indicative of the network's scale in terms of connected devices and the potential demand for the network's resources and bandwidth.



Understanding the overall count status of BSUs and SUs is vital for network management and planning. It enables network administrators to assess the network's capacity, identify potential bottlenecks or coverage issues, and plan for network expansions or optimizations accordingly. By analyzing the ratio of BSUs to SUs, administrators can also gauge the effectiveness of the current network design and make informed decisions regarding infrastructure investments and upgrades to meet future demands.

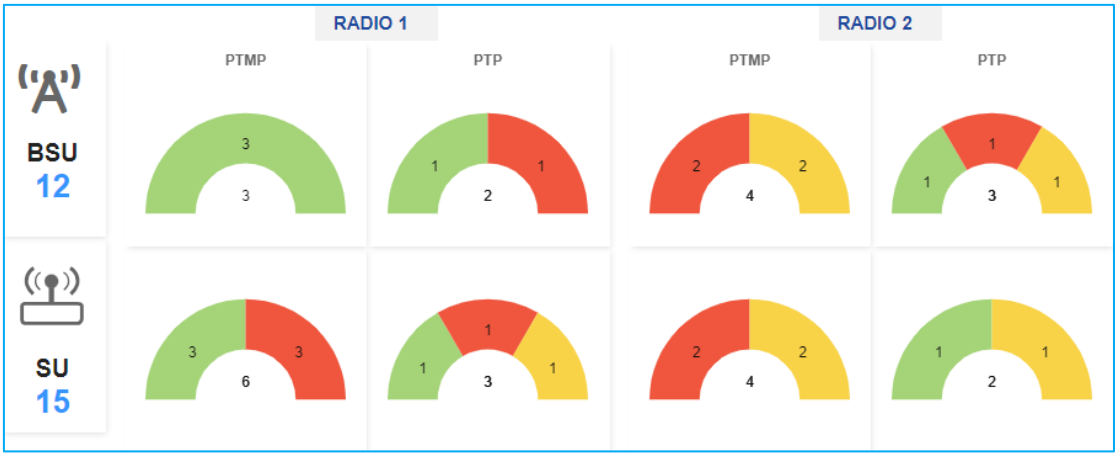
This count status is typically represented in a summary or dashboard within the SkyPoint system, providing a clear and concise overview of the network's current

state and facilitating quick assessments and decisions related to network management and expansion strategies.

3.5 Link/Radio Type

The dashboard provides a comprehensive view of the network's devices, showcasing the operational status across two radios, *Radio1* and *Radio2*. It distinguishes between devices functioning as Base Station Units (BSUs) and Subscriber Units (SUs), and further categorizes their operation into Point-to-Point (PTP) and Point-to-Multipoint (PTMP) modes. This layout allows for quick assessment of network performance, connectivity issues, and device distribution, facilitating efficient network management and troubleshooting.

BSUs: Displayed by operational radios (Radio1, Radio2) and mode (PTP, PTMP),



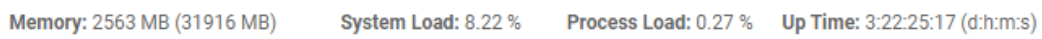
highlighting the network backbone's health and connectivity.

SUs: Also organized by radios and mode, offering insights into the end-user connectivity experience.

This dashboard serves as an essential tool for network administrators, providing a bird's-eye view of the network's infrastructure and enabling proactive management of network resources and devices.

3.6 Server Status

The top bar is designed to provide immediate, at-a-glance insights into the health and performance of the server. Here's a brief overview of how each element contributes to a comprehensive understanding of the system's current status:



- **Memory Usage**: This metric displays the total memory allocation versus current usage, giving administrators a quick snapshot of the system's memory health. High memory usage might indicate a need for optimization or upgrading system resources to prevent slowdowns or crashes.

- **System Load**: Representing the average load on the server over a specified period, this metric helps in understanding the system's current workload. It reflects the ongoing processes and tasks, indicating whether the system is under heavy load or operating smoothly within its capacity.

- **Process Load**: Specifically focusing on the number and state of active processes, this metric sheds light on the operational efficiency of the system. It helps in identifying any processes that are consuming excessive resources or if there are too many idle processes, allowing for better process management and optimization.

- **Server Uptime**: Displaying the duration for which the server has been continuously running, this metric is a key indicator of system stability and reliability. Longer uptime periods are generally positive, signifying stable and uninterrupted service, but they also necessitate careful monitoring to ensure that performance doesn't degrade over time due to memory leaks or resource depletion.

Together, these metrics provide a holistic view of the system's performance and health, enabling network administrators to make informed decisions regarding system maintenance, resource allocation, and potential upgrades. This top bar acts as a critical tool in the proactive management of the network infrastructure, ensuring optimal performance and minimizing downtime.

3.7 Events

The dashboard within SkyPoint provides a comprehensive interface for monitoring and managing events and log messages generated by both the SkyPoint system itself and the connected devices. This functionality is crucial for maintaining network health, troubleshooting issues, and ensuring optimal performance. Here’s a detailed breakdown of how this system operates:

Event Generation and Logging

- **SkyPoint Events**: SkyPoint autonomously generates event messages to indicate the status changes of devices (such as up/down states) or to log specific actions triggered within any of the SkyPoint interface pages. This includes activities like the initiation of a device discovery process, updates or changes in firmware, or the provisioning of a device.
- **Device-Generated Traps**: Apart from SkyPoint-generated events, the system also captures and logs "traps" or notifications from devices when specific events occur. These traps provide real-time alerts about device status changes or issues, enabling prompt response and resolution.

Event and Log Management

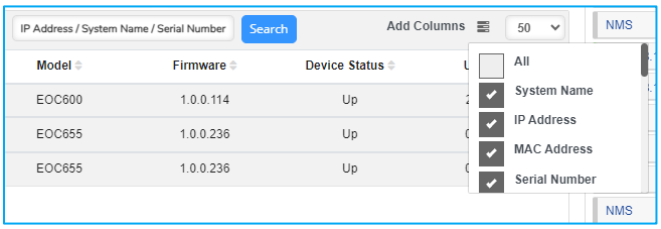
- **Events-Based Filter Selection**: The dashboard offers the capability to filter events based on various criteria, facilitating targeted analysis and management. Users can swiftly navigate through a vast amount of data to focus on the events that are most relevant to their current needs or investigations.
- **Time Duration Filtering**: By default, the dashboard displays events that occurred within the last 24 hours, offering a recent overview of network activities and status changes. However, users have the flexibility to extend this viewing window up to 48 hours, allowing for a broader analysis of events over time.
- **Severity-Based Filtering**: Events can also be filtered based on their severity, enabling users to prioritize their response efforts. This feature helps in distinguishing between critical issues that may require immediate attention and less urgent notifications.

Events	Definition
Critical	An event whose priority has been set as higher than the rest of the events and the user needs to consider resolving the issue immediately.
Major	Device Down
Minor	An event whose priority is set as minor and the user needs to consider the event like there has been configuration
Warning	An event whose priority is set as a warning and the user needs to consider the event like device CPU or memory going up
Normal	Events that have the priority set to normal and no action by the user is required like the device going up.
Cleared	The events whose severity level is high previously and is restored now. For e.g. A threshold alarm like CPU going high has a "Warning" severity and when the CPU comes back to normal has "Cleared" as the severity
Intermediate	This event denotes with no priority assigned

All	All the events are listed without filtering based on severity.

3.8 Add Column

The tabular data section of the dashboard is meticulously designed to present essential information for each device within the network, facilitating easy monitoring and management.



This section is fundamental for network administrators to quickly access and review the devices operational details at a glance. Here's a detailed overview of its features and capabilities:

Default Device Information

Upon accessing the tabular data section, users are presented with a set of default columns that provide critical information about each device. These default columns include:

- **System Name**: The designated name of the device within the network, facilitating easy identification.
- **Primary IP**: The main IP address assigned to the device, crucial for network communications.
- **MAC Address**: The unique media access control address of the device, serving as a hardware identifier.
- **Serial Number**: A unique identifier assigned by the manufacturer, useful for inventory and support.
- **Model Number**: The specific model identification, aiding in understanding the device's capabilities.
- **Firmware**: The current firmware version installed on the device, indicating its software level.
- **Status**: The operational status (e.g., up, down, unavailable) providing quick insight into the device's health.

- **Up Time**: Duration since the device was last rebooted, reflecting its current operational period.

Customization with “Add Columns” Option

To enhance the visibility and tailor the information to specific needs, an "Add Columns" feature allows users to include additional data points in the table. The selectable columns for deeper insights include:

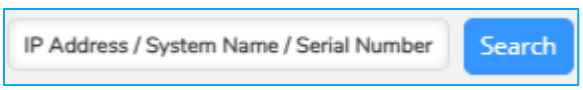
- **Radio Mode**: Indicates whether the device operates in single, dual, or multi-radio configurations.
- **Operational Mode**: Describes the operational setting of the device, such as PTP (Point-to-Point) or PTMP (Point-to-Multipoint).
- **Frequency**: The radio frequency or frequencies at which the device operates, essential for understanding spectrum use.
- **Bandwidth**: The data transmission capacity of the device, crucial for network performance analysis.
- **Channel**: The specific channel or channels the device uses for communication, impacting interference and connectivity and many more.

Viewing Options and Limitations

By default, the table is set to display information for 25 devices simultaneously, offering a balanced overview without overwhelming users. This default setting helps in maintaining clarity and focus on the displayed data, ensuring that administrators can efficiently navigate through device details. The design of this tabular data section, with its default visibility and customizable columns, underscores the dashboard’s versatility and user-centric approach, enabling effective network management through detailed and personalized device insights.

3.9 Search

The dashboard incorporates a highly flexible and efficient search functionality, enabling users to swiftly locate specific nodes within the network. This feature is designed to streamline network management tasks by allowing for precise queries based on key identifiers of the devices. Users can leverage the search capability using one of the following criteria:



- **IP Address**: By entering the IP address of a device, users can directly access its details. This is particularly useful for network troubleshooting and configuration tasks, where identifying a device by its network address is often the most straightforward approach.
- **System Name**: The search functionality also supports queries by the system name of the device. This option is ideal for administrators who are familiar with the naming conventions used within their network and wish to quickly access a particular device's information.
- **Serial Number**: For instances where hardware-specific identification is necessary, searching by the device's serial number provides an accurate method to pinpoint a device. This is especially useful for inventory management, warranty claims, or when dealing with support cases that require precise hardware identification.

This search mechanism enhances the dashboard's usability by enabling efficient navigation and management of network devices, thereby reducing the time and effort required to perform administrative tasks. It ensures that critical device information is readily accessible, facilitating effective decision-making and operational oversight.

4. Discovery

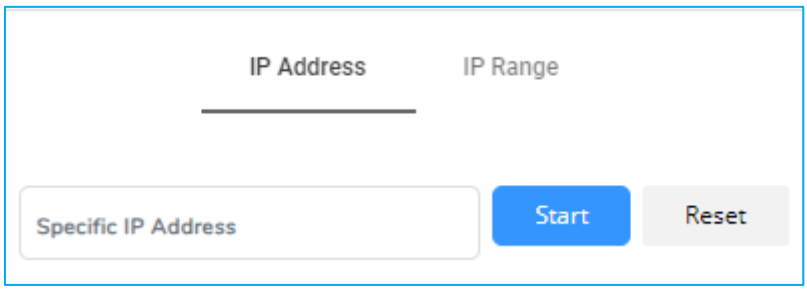
SkyPoint discovery feature is engineered to streamline the identification and integration of EnGenius radios within a network, employing a multi-step process that begins with the sending of ICMP packets to ascertain device availability at specific IP addresses. Following a successful ICMP response, SkyPoint initiates SNMP discovery packets to delve into the device's configuration details. This method ensures a thorough and efficient discovery process, catering to various network setups and requirements.

SkyPoint offers three distinct mechanisms for device discovery, accommodating a range of scenarios from individual device identification to bulk discovery across multiple networks:

4.1 IP Address Discovery

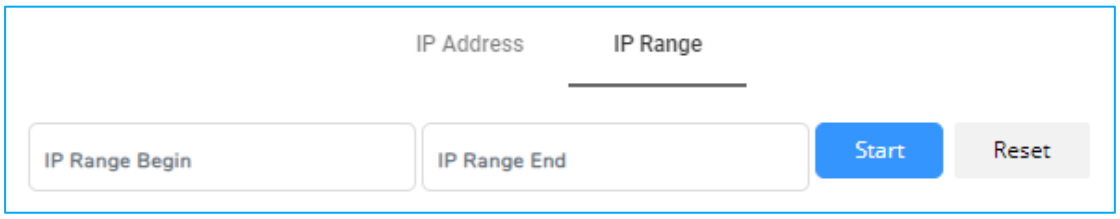
This method is designed for pinpointing a single device by its IP address. It's particularly useful for targeted discovery when the administrator knows the

exact IP address of the device they intend to integrate. For instance, entering an IP address like *"10.10.5.5"* directly leads to the discovery of that specific device.



4.2 IP Range Discovery

For broader discovery needs, SkyPoint enables the specification of an IP range. This approach is ideal for scanning a contiguous block of addresses within a network to identify all operational devices. By inputting a starting IP address (e.g., 10.10.5.1) and an ending address (e.g., 10.10.5.20), the system will discover all devices within this spectrum. Additionally, toggling the "By Range" option to "By Mask" allows for subnet-based discovery, where providing a subnet mask (e.g., 255.255.255.0) alongside a beginning IP address enables the system to scan all possible addresses within the subnet, up to the last usable address (e.g., from 192.168.1.1 to 192.168.1.254).



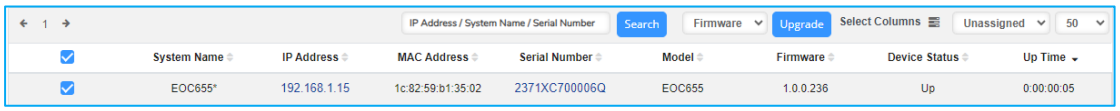
These diverse discovery options empower network administrators with flexible and powerful tools to efficiently identify and manage EnGenius radio devices, ensuring seamless network integration and optimization.

4.3 Data Table

After the discovery request is completed all the devices which are discovered will be listed under the discovery configuration. By default, all the unassigned devices will be listed in the table. Changing the option from "unassigned" to "All". Now you can see both unassigned and assigned devices in the list. There is an option to Provision (newly installed devices) or Profile / Firmware update (For existing devices) can be done: The picture below shows the **Firmware**, **Provision**.

4.4 Firmware Upgrade

The firmware upgrade feature allows you to push the latest or any of the available firmware into the SkyPoint. Select devices from the list select the firmware from the dropdown and click the "**Upgrade**" button.



Popup window will appear, select the latest are required firmware and click upgrade. (Check for Configuration section for uploading firmware's into SkyPoint server).

4.5 Provisioning

The process for provisioning devices within the network management system (NMS) is designed to be intuitive and efficient, allowing network administrators to quickly apply predefined configuration profiles to devices. This process ensures that devices are correctly configured to operate as intended within the network. Here's a step-by-step guide on how to provision devices using the system:

Step 1: Select Devices

- From the Device List: Navigate to the list of devices within the NMS dashboard. Here, you can view all detected devices, including those that are unprovisioned.
- Device Selection: Choose the devices you wish to provision by selecting them from the list. You can select individual devices manually or use the "All" option to select all listed devices, depending on your provisioning needs.

Step 2: Initiate Provisioning

- **Provision Option**: With the devices selected, locate the dropdown menu that provides various actions that can be applied to devices. Select the "Provision" option from this menu.
- **Upgrade Button**: After selecting the "Provision" option, click on the "Upgrade" button to proceed to the next step of the provisioning process.

Step 3: Configure Device Settings

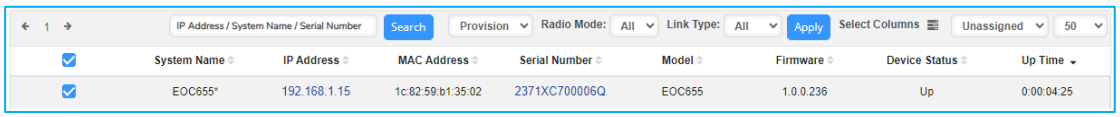
- **Select Radio Mode**: A prompt will appear requesting you to choose the radio mode for the selected devices. Options will include BSU (Base Station Unit) or

SU (Subscriber Unit), depending on the intended function of the device within the network.

- **Select Link Type**: Next, select the link type for the device, choosing between PTP (Point-to-Point) for direct connections between two points, or PTMP (Point-to-Multipoint) for connections between a single point and multiple endpoints.

Step 4: Apply Configuration Profile

- **Apply Button**: After setting the radio mode and link type, click the "apply" button to move to the configuration application stage.
- **Profile Selection**: At this stage, you'll have the option to apply a previously created configuration profile to the selected devices. These profiles are created in the Configuration section and contain predefined settings tailored to specific operational requirements.
- **Applying the Profile**: Choose the appropriate profile for your devices. You can apply this to newly assigned devices or to all selected devices, depending on your selection in the first step.



Completion

Once the profile is applied, the devices will be provisioned with the selected configurations, integrating them into the network with the designated roles and settings. This streamlined process facilitates the rapid deployment and integration of devices, ensuring they operate according to the network's specifications and standards.

This provisioning process underscores the NMS's capability to efficiently manage and configure network devices, significantly reducing manual configuration efforts and enhancing network reliability and performance.

4.6 Discovery Task

During the initiation of the discovery process within SkyPoint, the progress and outcomes of the discovery tasks are dynamically located on the bottom right side of the screen. This area, dedicated to "Discovery Task Details," is structured to provide immediate and clear insights into the ongoing discovery operations. The table includes several columns, each offering specific information regarding the discovery tasks:

Type	Time	Start	End	ICMP	SNMP	Status
ByRange	2021-05-17 13:19:37	192.168.1.66	192.168.1.68	2	2	Completed
ByRange	2021-05-17 13:19:22	192.168.1.11	192.168.1.12	2	2	Completed
Specfic	2021-05-17 12:56:26		192.168.1.12	1	1	Completed
Specfic	2021-05-13 18:53:03		192.168.1.12	1	1	Completed
Specfic	2021-05-13 17:23:43		192.168.1.12	1	1	Completed
ByRange	2021-05-10 12:33:51	192.168.1.1	192.168.1.1	3	3	Completed
Specfic	2021-05-06 17:46:20		192.168.2.21	0	1	Completed
ByRange	2021-05-06 17:37:36	192.168.1.66	192.168.1.68	3	3	Completed
Specfic	2021-05-06 17:36:39		192.168.1.11	0	1	Completed

Discovery Task Details Columns

- **Type**: This column identifies the method used for the discovery task. It distinguishes between three different types of discovery methods.
    - Specific: Indicates that a single, specific IP address was provided for the discovery of a single device.
    - By Range: Shows that a range of IP addresses was specified for the discovery task, aiming to identify multiple devices within that specified range.
    - By Mask: Reflects discovery tasks initiated using a subnet mask, targeting devices within a particular subnet.
- **Time**: Displays the exact time at which the discovery process was initiated. This timestamp is crucial for tracking when discovery activities were started and for correlating discovery tasks with network changes or configurations.
- **Start**: For discovery tasks classified under "By Range," this column shows the starting IP address of the range used for discovery. It marks the beginning of the IP address spectrum being scanned.
- **End**: Complementing the "Start" column, this field indicates the last IP address within the range for range-based discoveries. It defines the upper boundary of the IP address interval being examined.
- **ICMP**: Reveals the count of devices that responded to the ICMP ping. This metric is essential for understanding how many devices are actively responding on the network at the network layer level.
- **SNMP**: Shows the number of devices that responded to the SNMP discovery ping. This count provides insights into how many devices are not just active but also manageable and configured to communicate via SNMP, offering deeper network management capabilities.

- **Status**: Indicates the current status of the discovery task, detailing whether the discovery has been completed, is still in progress, or has encountered any issues. This column is key for real-time monitoring of discovery operations and for immediate identification of any potential problems that might require attention.

4.7 Summary

The Summary Graph feature in the discovery is designed to visually represent critical information about the network's devices, focusing specifically on the provisioning status. This graphical display aids in quickly assessing the current state of device deployment within the network, particularly highlighting the distinction between unprovisioned devices and their categorization as Base Station Units (BSUs) or Subscriber Units (SUs). Here's how the Summary Graph functions and what it offers:

Overview of Summary Graph

- **Total Unprovisioned Devices**: The graph starts by showcasing the total number of devices within the network that are yet to be provisioned. This gives an immediate sense of how many devices need attention to complete their network integration process.

- **Unprovisioned BSUs and SUs**: Further breaking down the total unprovisioned devices, the graph distinctly categorizes them into BSUs and SUs. This categorization is crucial for network administrators to understand the composition of unprovisioned devices, allowing for targeted action plans to provision BSUs and SUs according to network priorities and requirements.

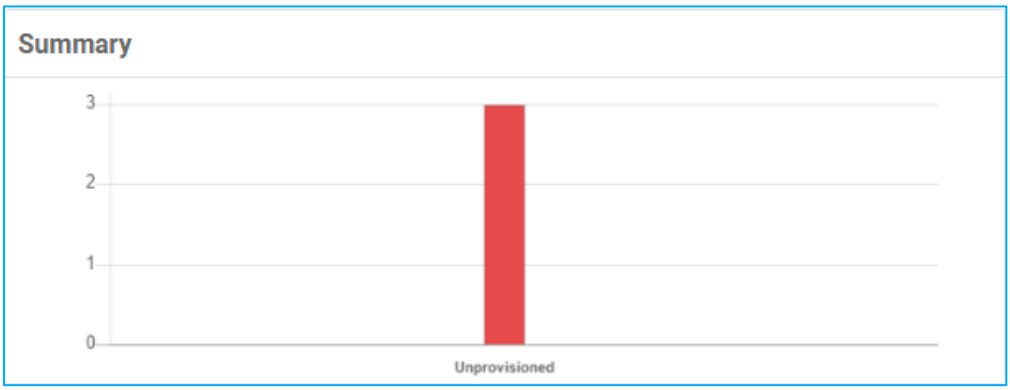
Benefits of the Summary Graph

- Quick Visual Insights: By presenting data graphically, the Summary Graph enables quick absorption of information about unprovisioned devices, saving time and simplifying the monitoring process.

- Prioritization of Provisioning Tasks: Understanding the split between unprovisioned BSUs and SUs helps in prioritizing provisioning tasks. For instance, provisioning BSUs might be prioritized to establish network backbones before focusing on SUs.

- Efficient Resource Allocation: Knowing the exact count of unprovisioned devices and their types allows for more efficient allocation of resources and personnel for the provisioning process.

- Strategic Planning: The graph aids in strategic planning by providing a clear picture of the network's expansion and integration status, guiding decisions on network growth and development.



The Summary Graph is an essential tool in the network management toolkit, offering a streamlined and effective way to monitor and plan the provisioning of network devices. Visually summarizing the status of unprovisioned devices and their classification into BSUs and SUs, supports more informed decision-making and enhances the efficiency of network administration tasks.

5. Topology

The topology view within the network management system offers a structured, hierarchical representation of network devices, facilitating a clear understanding of their interconnections and organizational relationships. This tree structure design provides a comprehensive overview of the network's architecture, from a global level down to individual devices, categorized as Base Station Units (BSUs) and Subscriber Units (SUs). Here's a detailed explanation of each level within the topology:

- **Global**
  The topmost level of the hierarchy represents the entirety of the network's infrastructure. Under the "Global" category, all regions within the network are aggregated, serving as the root section from which all other network segments derive.

- **Region**
  A subdivision under "Global," where each region encompasses one or more locations. This level allows for the organization and management of the network based on geographical or operational boundaries, facilitating region-specific configurations and oversight.

- **City**
  A subdivision under "Region," the "City" level details the specifies the city where network devices are deployed. Each City contains multiple Locations.

- **Location**
  Nested within a region, the "Location" level details the specific areas where network devices are deployed. Each location contains multiple facilities, offering a closer look at the network's deployment in distinct physical or logical areas.

- **Facility**
  The "Facility" level delves deeper into the network's structure, showcasing all BSUs and SUs installed within a particular facility. This granularity is crucial for managing devices based on their physical installation sites, enhancing targeted monitoring and maintenance activities.

Navigating the Tree Structure

- **Interactive Navigation**: By selecting a node within the tree (e.g., "Global," "Region," "Location"), the system dynamically loads and displays the subordinate elements associated with that node. For instance, clicking on the "Global" root element reveals all the regions, selecting a "Region" unveils the locations within it, and choosing a "Location" presents the facilities it comprises.
- **Device Connectivity Links**: Within this structure, the connectivity links between BSUs and SUs are visually represented, illustrating how subscriber units connect back to base stations. This visualization aids in understanding the network's operational flow and pinpointing areas of interest or concern for further action.

The topology view serves as an essential tool for network administrators, offering a macro-to-micro perspective on the network’s configuration and the physical or logical placement of devices. This hierarchical visualization supports efficient network planning, troubleshooting, and optimization efforts by providing a clear and accessible framework for navigating the complex web of network connections and devices.

5.1 Link View

The network management system's map view and hierarchical selection feature enhance the visualization and management of devices across different organizational levels—Region, Location, and Facility. This functionality allows network administrators to obtain a detailed and spatial understanding of device distribution within the network. Here's how it operates across different selections:

Region Selection

- **Device Listing by Region**: Upon selecting a Region, the system automatically lists all Locations within that Region below the selection. This hierarchical display facilitates an organized view of the network's structure, allowing for easy navigation and management at a regional level.
- **Map Visualization**: The map component provides a clustered view of the device count available in each Location under the selected Region. This visualization helps in identifying the density and distribution of devices across various locations, offering a geographical perspective on network deployment.

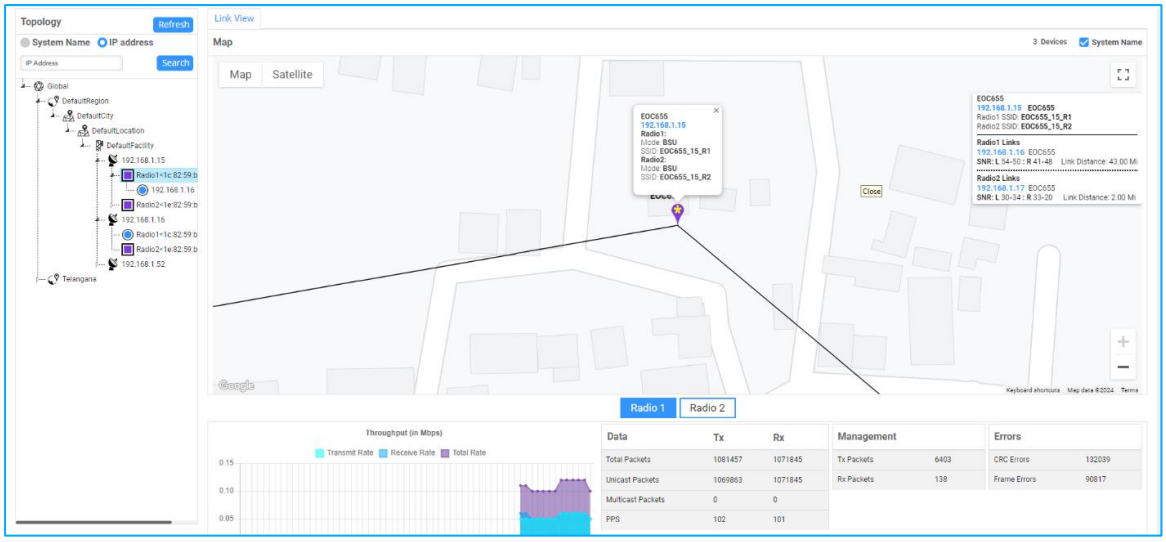
Location Selection

- **Facility Listing under Location**: Choosing a specific Location reveals all the Facilities situated within that Location. This detailed breakdown assists administrators in drilling down to specific areas of the network, enhancing the granularity of network oversight.
- **Clustered Map View of Facilities**: On the map, each Facility within the chosen location is represented in a clustered view, displaying the count of devices in each Facility. For accurate representation, facilities are plotted based on their approximate GPS coordinates, ensuring that the spatial distribution of devices is both meaningful and visually accessible.

Facility Selection

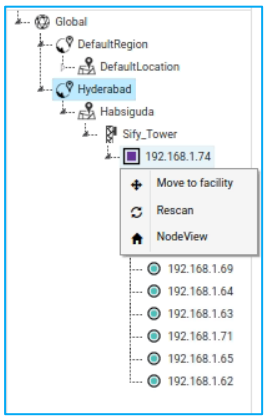
- **Device Listing under Facility**: Selecting a Facility provides a list of all devices installed at that location. Furthermore, these devices are also plotted on the map, granting a clear visual cue of their physical placement within the Facility.
- **Enhanced Device Visibility**: Through this selection, administrators can see the total number of devices at a glance, both in list form and as a spatial representation on the map. This dual view aids in comprehensive device management and planning, particularly useful for tasks such as troubleshooting, maintenance, and capacity planning.

This layered approach to device visualization and management—ranging from a broad regional overview down to specific facilities—empowers network administrators with the tools necessary for effective network oversight. The integration of map views with hierarchical device listings offers a potent combination of geographical and structural data, facilitating informed decision-making and strategic planning for network expansion and optimization.



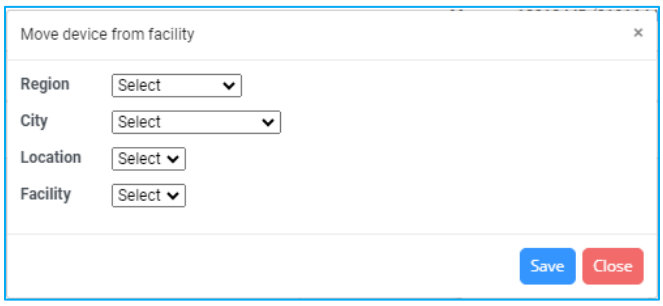
Upon Right-clicking on a facility, we can get an option to rescan the facility which will trigger a rescan on the selected facility

When we right-click on a node, it will give us with three options:



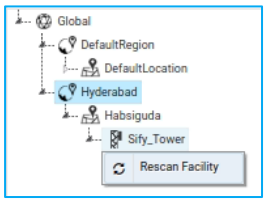
5.2 Move to Facility

We can move that particular node to a new facility.



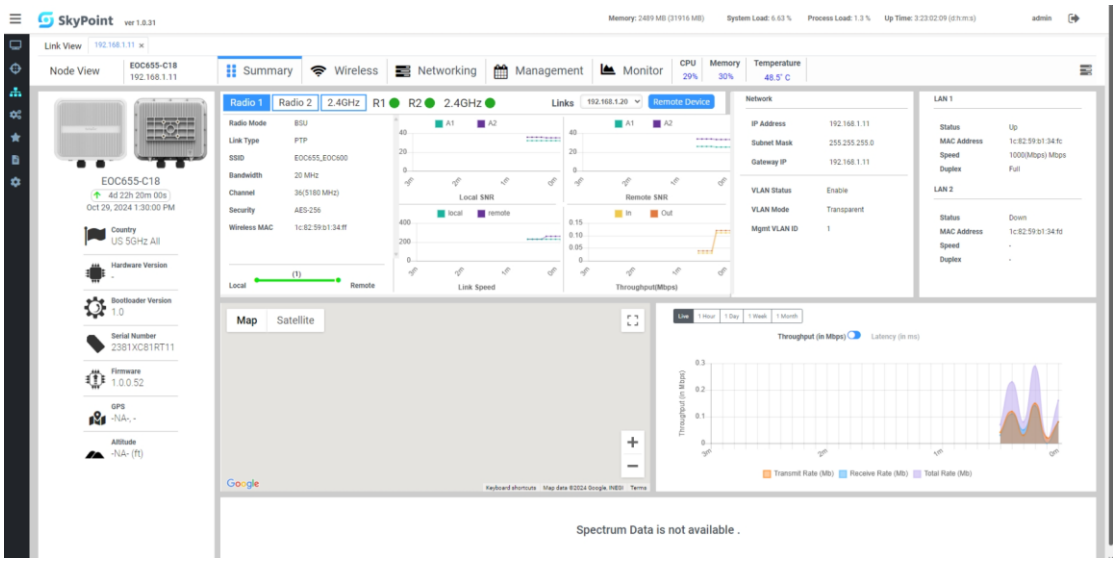
5.3 Rescan

It will initiate a re-scan for that particular node



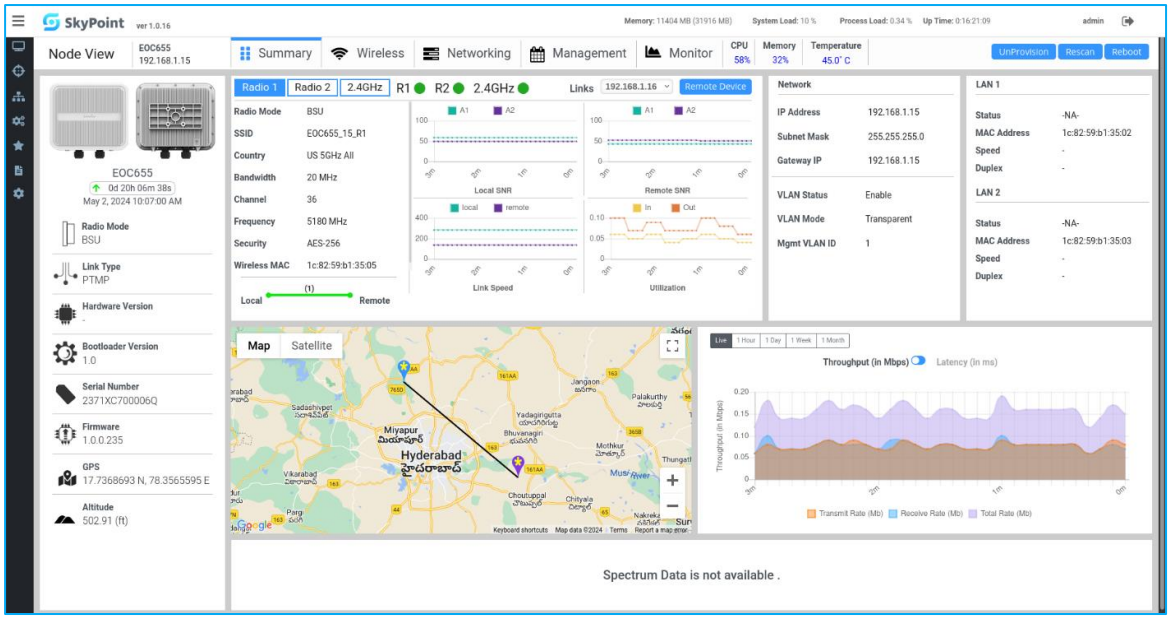
5.4 Node View

Clicking this function will open the node view of that particular node



6. Node View Dashboard

The Node View feature within the network management system is specifically designed to enhance device management by providing a dedicated interface for each selected device. This feature allows administrators to deep dive into the specifics of a device, offering both an overview of its current status on the dashboard and access to a suite of configuration options.



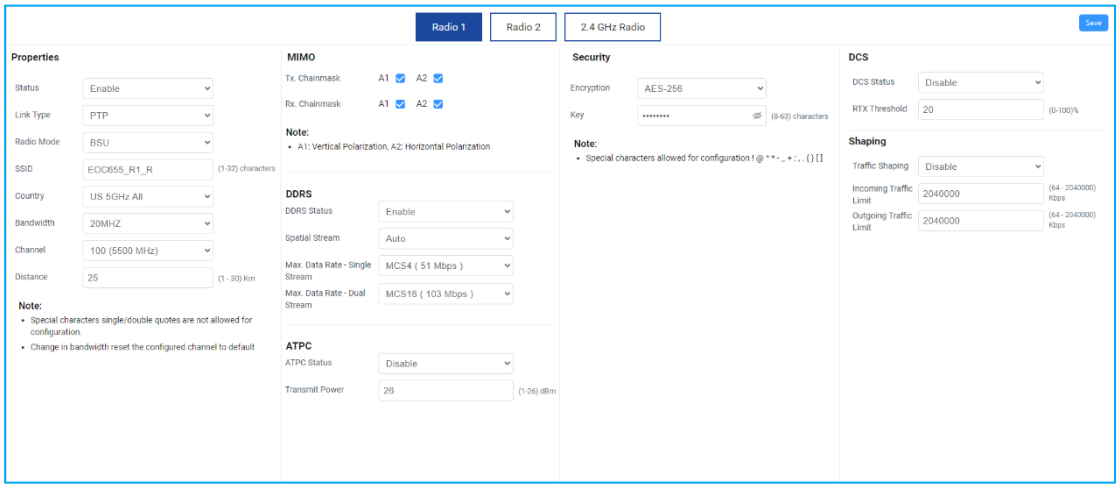
6.1 Summary

The overview details of the selected device showing **System** (Radio Model (with image), Hardware Version, Link Type, Bootloader Version, Firmware Version, Serial Number, Uptime, Temperature, CPU Usage, Memory Usage, GPS), **Network** (Ethernet MAC, IP address, Subnet Mask, Gateway IP, DNS IP, VLAN Status, Routing Model and, Link ID), **Wireless** (**Radio1 / Radio2 / 2.4GHz**: MAC, Link Type, SSID, Radio Mode, Bandwidth, Channel, Frequency, Remote Partners) along with throughput graph.

6.2 Wireless

Radio1 / Radio2

The below picture



6.3 Properties

- **Status:** User can **Enable/Disable** the status of Radio 1 / Radio 2
- **Link Type:** Select any desired Link type (**PTP**, **PTMP**) to apply to the device
- **Radio Mode:** The user has a choice to select any mode (BSU, SU) depending on his requirement
- **SSID:** Enter the **SSID**. (Service Set Identifier) The name is assigned to a Wi-Fi (wireless) network.

Note: All devices in the network must use the case-sensitive name (SSID) to communicate over Wi-Fi, which is a text string up to 32 characters long.

- **Country:** Select the appropriate frequency bands specific to the country
- **Bandwidth:**
- **Channel:**
- **Distance:**

Uplink Limit: To apply the specific bandwidth limit for **Uplink** (SU to BSU)

Downlink Limit: To apply the specific bandwidth limit for **Downlink** (BSU to SU)

Retries: The user can set the number of retries to resend the packet when it is dropped

6.4 MIMO/ DDRS/ ATPC

By default, the ports in the Tx and Rx are enabled. There are two ports in the radio one A1 port (Horizontal polarization) and another A2 port (Vertical polarization). If the user has packet loss are any error occurs in Tx (Transmitter) are Rx (Receiver) user can troubleshoot by disabling / Enabling one of the ports.

- **Tx Chainmask:** Select Port A1/ A2
- **Rx Chainmask:** Select Port A1/ A2

Note: By Default, both A1 and A2 ports of Tx and Rx are Enabled.

- **DDRS Status:** Select **Enable** / **Disable**

Note: DDRS will **Enable** the dynamic adjustment of the data rate for transmission of wireless traffic. This is especially crucial when different SUs can support various data rates because of different distances from the base station.

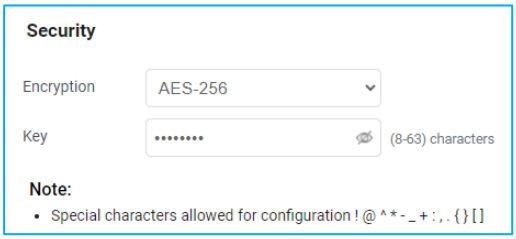
- **ATPC Status:** Select **Enable** / **Disable**

Note: ATPC **Enables** dynamic adjustment to transmit power for each SU to achieve the desired link Signal Noise Ratio without spilling additional power or interference into the environment. ATPC is also used to ensure that the radio accurately follows local Equivalent Isotropic Radiated Power (EIRP). e. If **disabled**, the user can manually adjust the transmit power. By default, ATPC is enabled on the device.

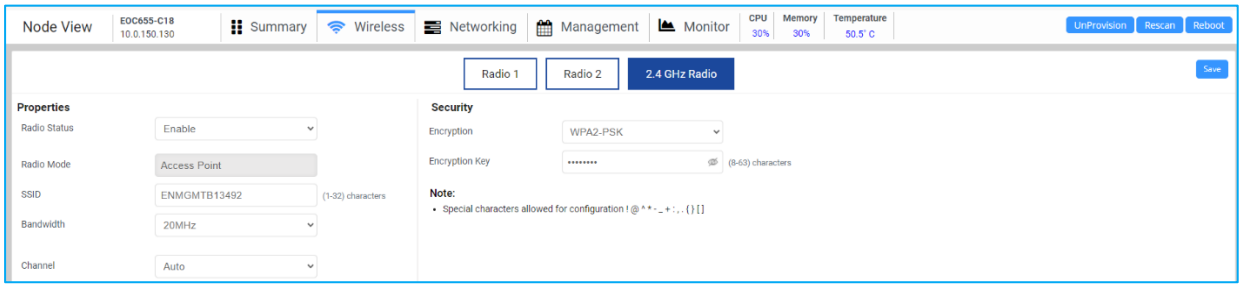
6.5 Security

The Advanced Encryption Standard (AES) is a universal standard for encrypting many types of electronic data. AES soon became the default encryption algorithm for protecting classified information, as well as the first publicly accessible and open cipher approved by the NSA for top-secret information.

Encryption: Select **AES-256** and enter the Encryption Key



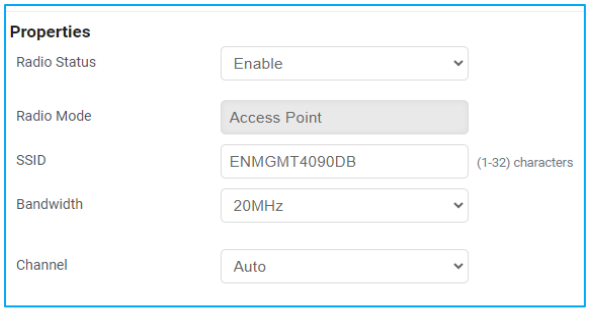
7. 2.4GHz



7.1 Properties

- **Radio Status:** Select **Enable/ Disable**
- **Radio Mode:** AP
- **SSID:** Enter the **SSID**. (Service Set Identifier) The name is assigned to a Wi-Fi (wireless) network.

Note: All devices in the network must use the case-sensitive name (SSID) to communicate over Wi-Fi, which is a text string up to 32 bytes long.



- **Bandwidth:** Select 20/40MHz
- **Channel:** Select a channel of frequency from 20/40MHz.

** Click the **Save** button to save changes**

7.2 Security

It is a method of securing your network using **AES-256** with the use of the optional Pre-Shared Key (**PSK**) authentication, which was designed for home users without an enterprise authentication server. Wi-Fi Protected Access 2 - Pre-Shared Key, also called WPA or WPA2.

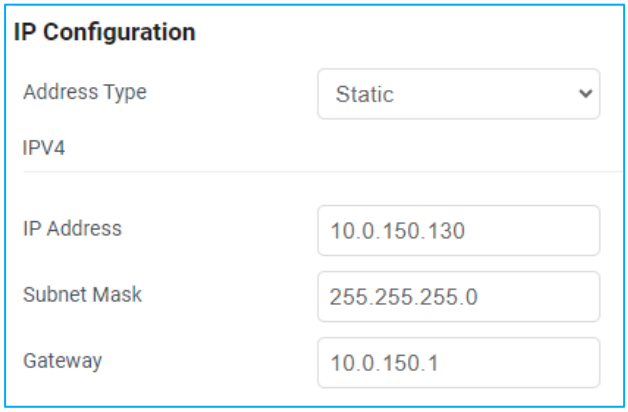
*Select **AES-256** and enter the Encryption Key*

** Click the **Save** button to save changes**

8. Network

8.1 IP Configuration

- **Address Type:** Select **Static** / **Dynamic**
- **IP Address:** Enter the **IP Address**
- **Subnet Mask**: Enter the **Subnet Mask**
- **Gateway**: Enter the **Gateway** IP Address
- **IP Address:** Enter the **IP Address**
- **Subnet Mask**: Enter the **Subnet Mask**



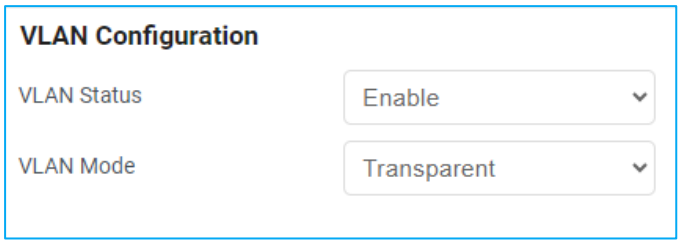
** Click the **Save** button to save changes**

8.2 VLAN

Note: A VLAN is a group of devices on one or more LANs that are configured to communicate as if they were attached to the same wire, when in fact they are located on a few different LAN segments. Because VLANs are based on logical instead of physical connections.

- **VLAN Status:** Select the status **Enable** / **Disable**
- **VLAN Mode:** Select the mode **Transparent**

** Click the **Save** button to save changes**



8.3 Ethernet

8.3.1 LAN1

- **Ethernet Speed:** Select **Auto Negotiation** / **100Mbps full** / **1000Mbps full**

Note: By default: Auto-Negotiation is selected

- **Ethernet MTU:** Default 1500 Bytes

** Click the **Save** button to save changes**

8.3.2 LAN2

- **Ethernet Speed:** Select **Auto Negotiation** / **100Mbps Full** / **1000Mbps Full / 2500 Full**

Note: By default: Auto-Negotiation is selected

- **Ethernet MTU:** Default 1500 Bytes)

- ** Click the **Save** button to save changes**

8.4 DHCP

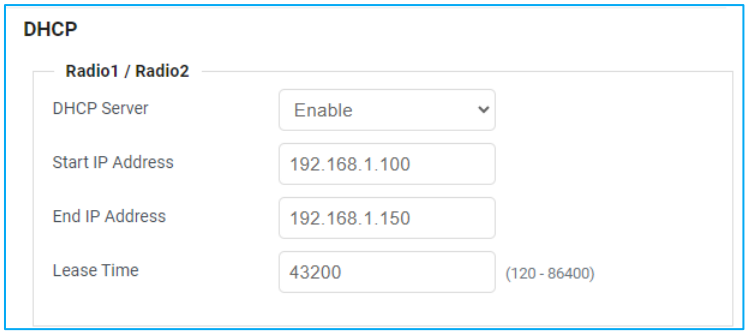
The Dynamic Host Configuration Protocol (DHCP) is a network management protocol used on UDP/IP networks whereby a DHCP server dynamically assigns an IP address and other network configuration parameters to each device on a network so they can communicate with other IP networks. DHCP settings will be available for both Radio1/Radio2 and 2.4GHz radios for BSU and for SU the option will be available only for 2.4GHz radios.

8.4.1 Radio1 / Radio2

- **DHCP Server:** Select **Enable** /**Disable** DHCP server in the devices.
- **Start IP Address:** The start IP Address is the range of free IP addresses that are assigned to connect to the client.
- **End IP Address:** The start IP Address is the range of free IP addresses that are assigned to connect to the client.

Note: The range free IP address start IP to end IP is given to create a DHCP server.

- **Lease Time:** The amount of time in seconds the network device can use the IP address in the network. The IP Address is reserved for that device until the reservation expires.



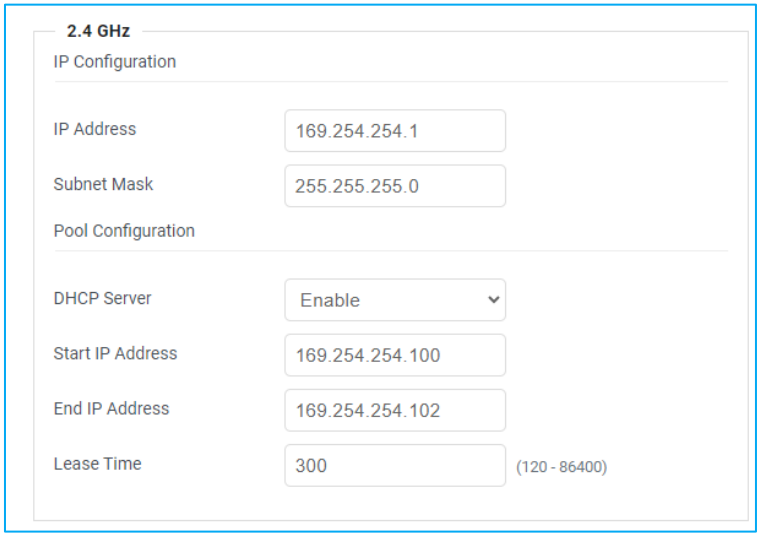
8.5 2.4 GHz

8.5.1 IP Configuration

- **IP Address:** Enter the IP address in the input box
  Subnet Mask: Enter the Subnet mask of the network

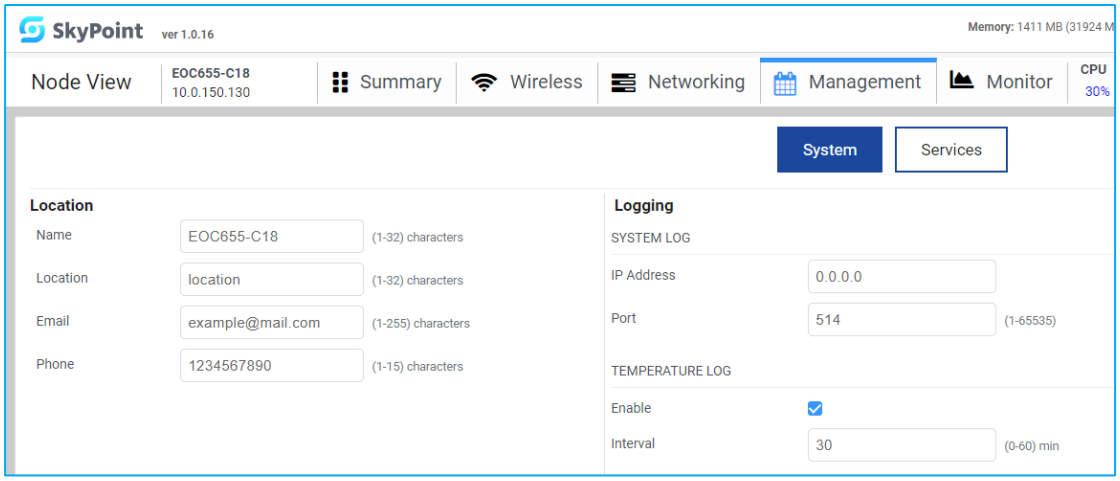
8.5.2 Pool Configuration

- **DHCP Server:** Select **Enable /Disable** DHCP server in the devices.
- **Start IP Address:** The start IP Address is the range of free IP addresses that are assigned to connect to the client.
- **End IP Address:** The start IP Address is the range of free IP addresses that are assigned to connect to the client.
- **Leased Time:** The amount of time in seconds the network device can use the IP address in the network. The IP Address is reserved for that device until the reservation expires.



9. Management

The management section contains the configuration for modifying the properties of the device which are required for managing the device.



The following are the sections in Node View Management:

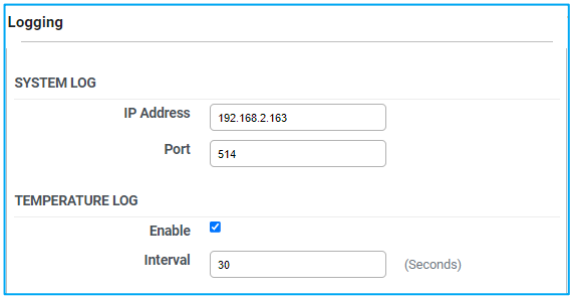
9.1 System

- **Location:** Contains the properties of the device which are required for identification of the device.
- **Name:** System Name/Customer name of the device
- **Location:** the location in which the device is installed.
- **Email:** Email address
- **Phone:** Phone number

9.2 Logging

The properties that need to be configured for logging the System log and the interval at which the temperature has to be logged.

- **System Log:** The IP address and the port of the syslog server to which the syslog events have to be logged. It has to be configured with the SkyPoint server address.



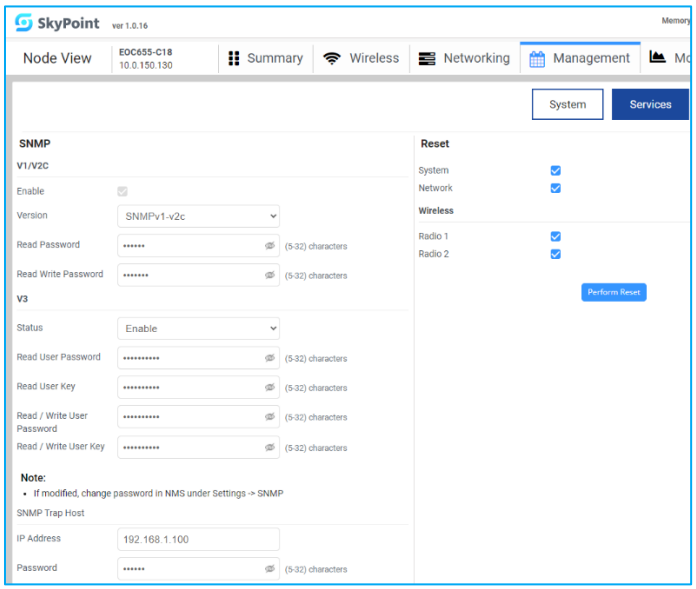
9.3 SERVICES

SNMP:

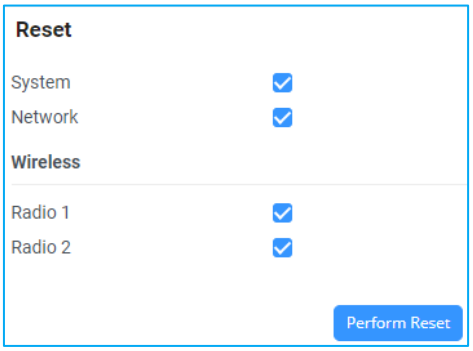
I. **Version:** SNMPv1 / SNMPV2, Read Password, Read/Write Password can be configured.

II. **V3**:
Status: Enable / Disable, Read User Password, Read User Key, Read/Write User Password, Read/Write User Key can be configured.

III. **SNMP Trap Host:** SNMP trap host server and community details are used for forwarding the traps to a management server. It has to be configured with the SkyPoint server address.

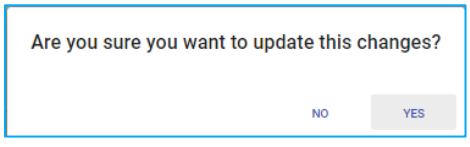


Reset: Reset the device to factory settings



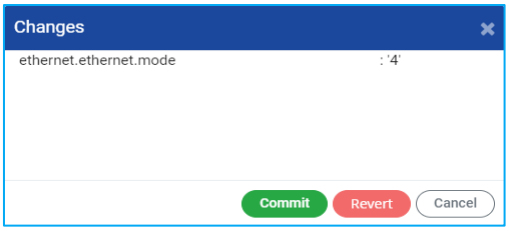
For Saving the configurations made in Node View

- Select Wireless, Network, or Management sections.
- Make the necessary changes and click on "Save" On clicking "Save" the changes are stored internally in the NMS server without being pushed to the device.
- Make any other changes if required and click on the "Save" button



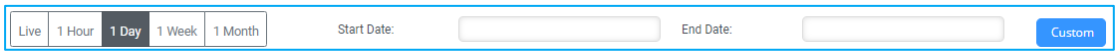
- Once all the changes are done click the "Apply" button.
- On clicking the "Apply" button, a popup is shown with the changes listed.

If all the changes or fine, the user can click on the "Commit" button or "Revert" button the clear the changes. click on "Cancel" to close the popup.

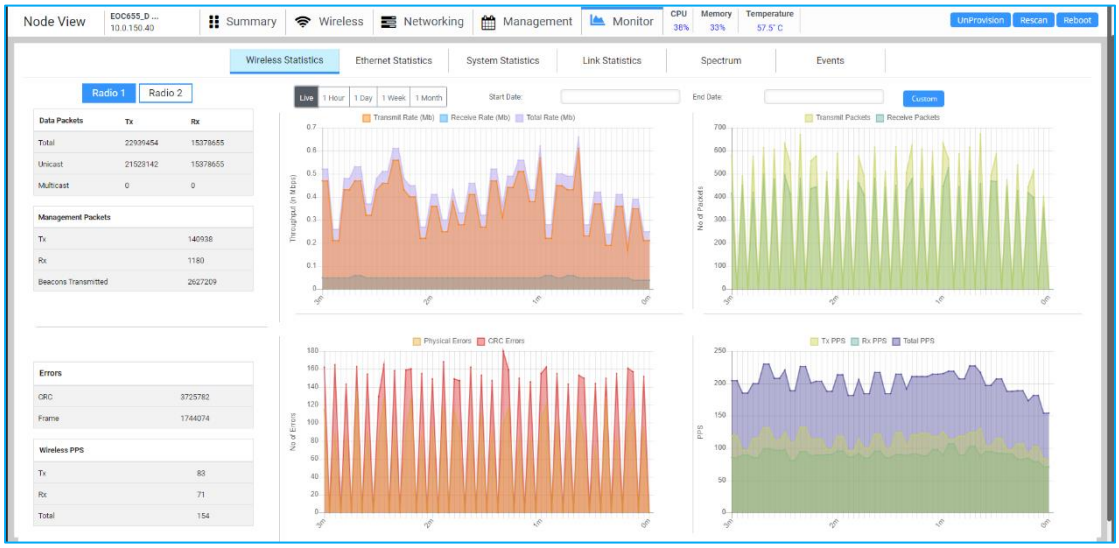


10.Monitor

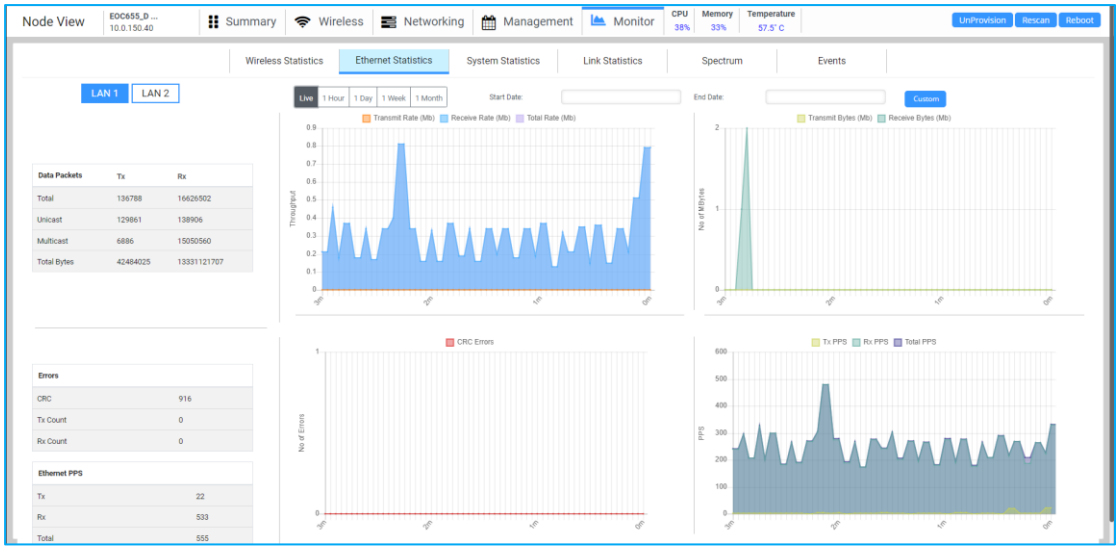
We can monitor the statistics of a particular node under this section. Here the monitoring can be done based on time. It can be Live, 1 Hour, 1 Day, 1 Week, 1 Month, or even a customized time frame (Start Date and End Date) as shown below:



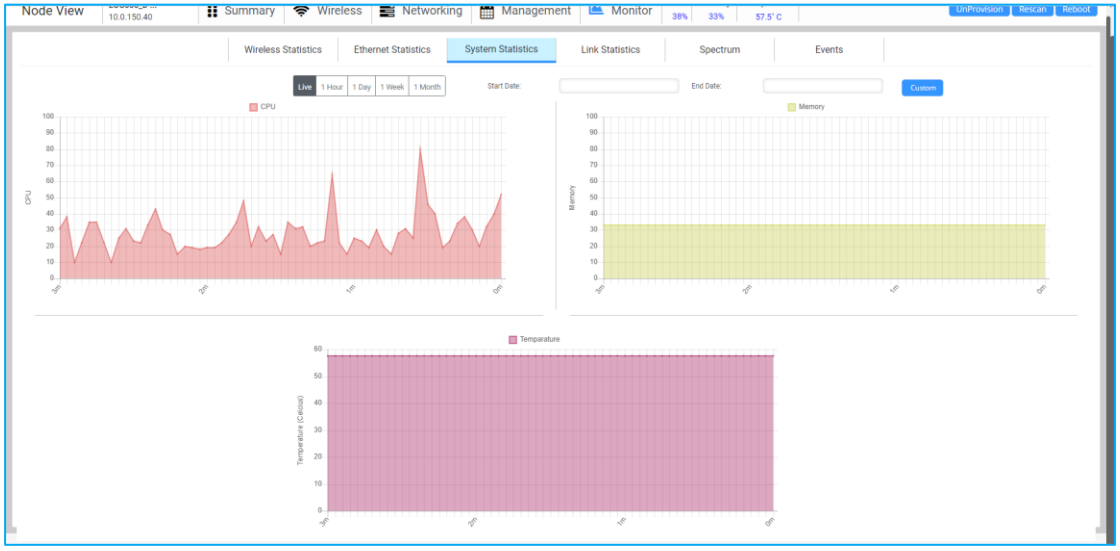
I. **Wireless Statistics** – These Stats will give an overview of the wireless stats like data packets, management packets, CRC errors, physical errors, and PPS Counts. The data will be shown as both numbers and live graphs.



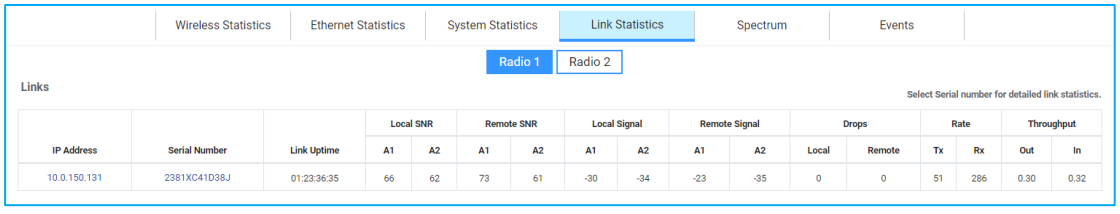
II. **Ethernet Statistics**– These Stats will give an overview of the ethernet stats like data packets (multicast, unicast, and total packets), CRC errors, and PPS Count. The data will be shown as both numbers and live graphs.



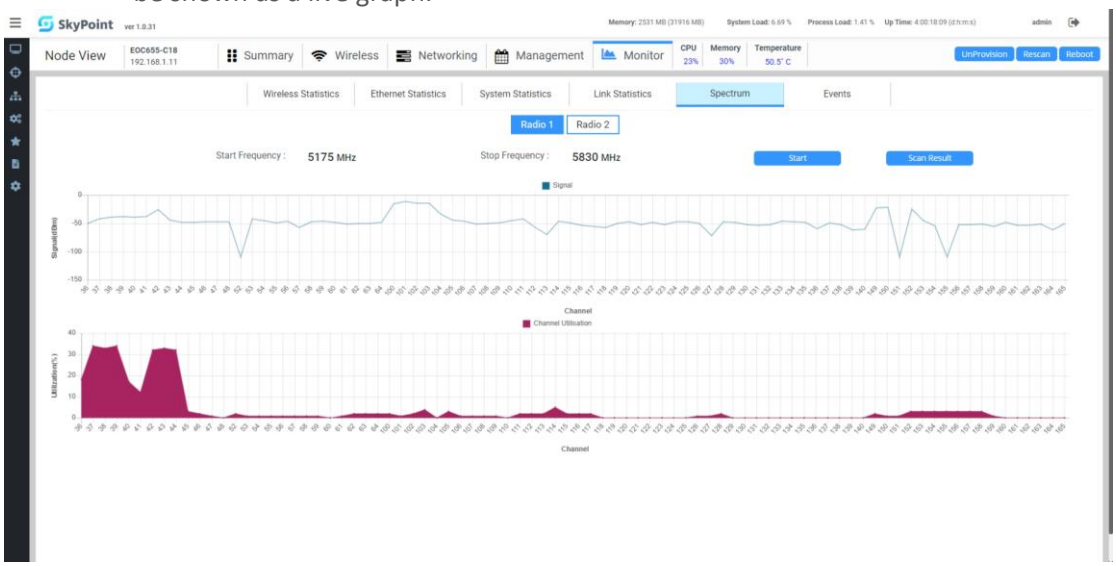
III. **System Statistics -** These Stats will give an overview of the system stats like CPU, memory, temperature, and distance. The data will be shown as a live graph.



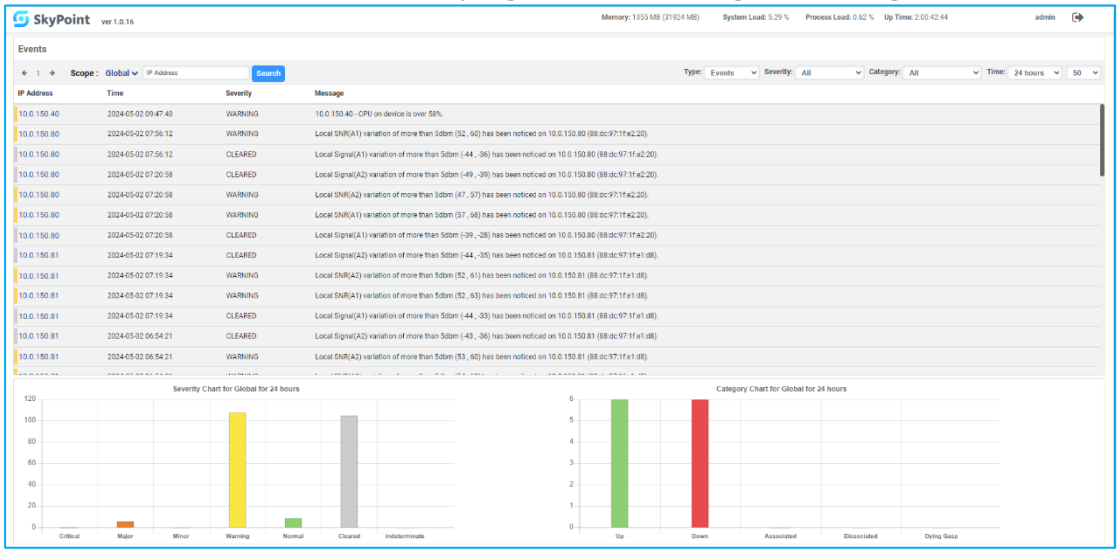
IV. **Link Statistics -** These Stats will give an overview of the link stats in a tabular format.



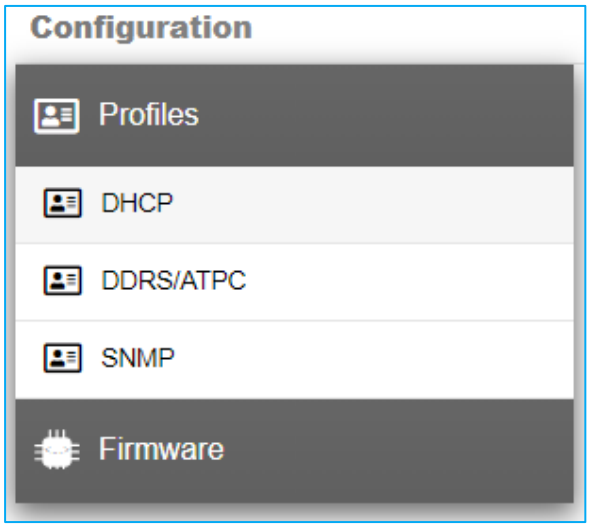
V. **Spectrum -** These Stats will give the results of the spectrum scan. The data will be shown as a live graph.



VI. **Events–** These stats will give all the events happening in the device. Event Type can be normal event and syslogs. The data is being shown in log format.



11.Configuration

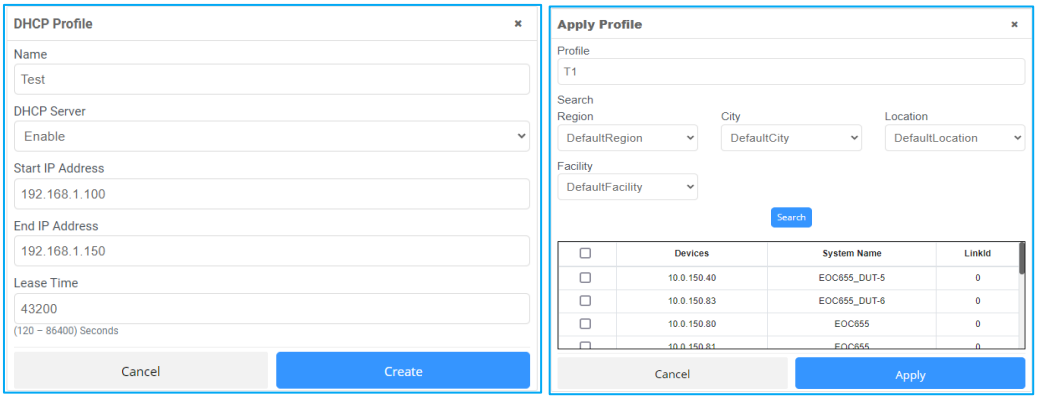


11.1 DHCP Profile

DHCP profile can be configured by clicking the DHCP tab from the dropdown menu of profiles as shown in the picture below

I. Create

DHCP profile is created by clicking the Create icon and entering the input fields like Name selecting the dropdown menu of Radio Mode, Link Type, and clicking the Create button to create a profile. For reference see the picture below



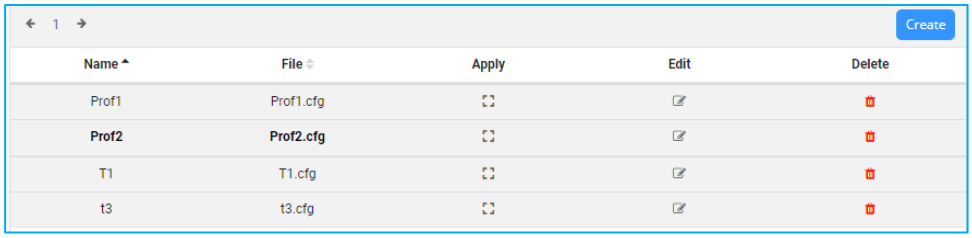
i.e. DHCP Create Profile and Apply Profile Images

II. Apply

Profiles can be applied by clicking the apply icon and existing profiles can be searched by entering their Region, Location, or Facility. Click the **Apply** button to apply changes as shown in the picture below

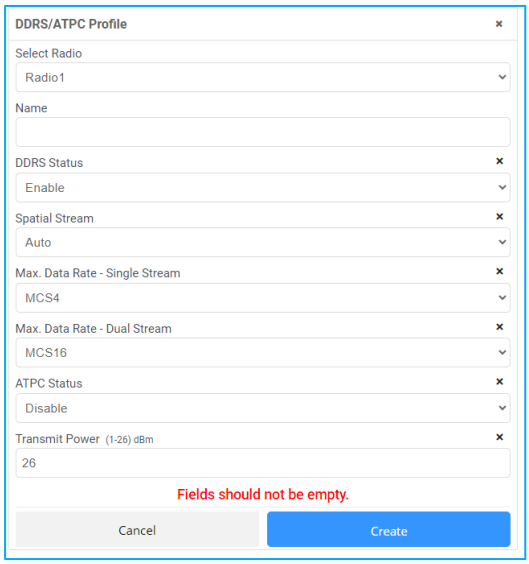
III. Edit

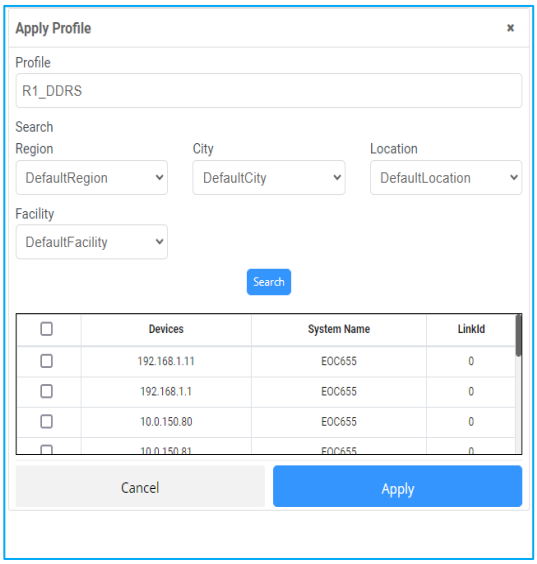
DHCP profiles can be edited by clicking the Edit icon changing the radio mode Link Type and other required parameters and then clicking **Update** button to apply changes



11.2 DDRS/ATPC

I. Create





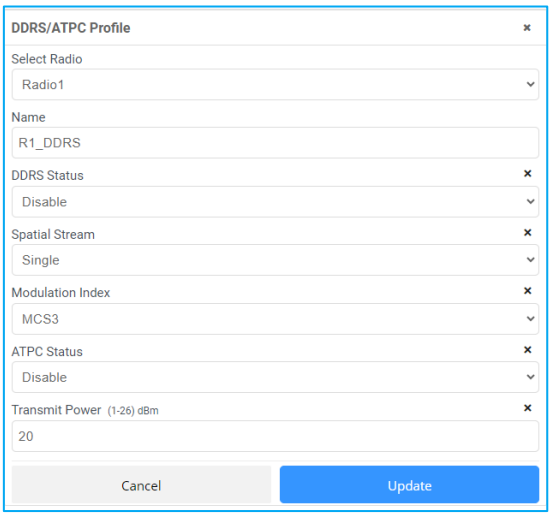
i.e. DDRS Create Profile and Apply Profile Images

II. Apply

Profiles can be applied by clicking the apply icon and existing profiles can be searched by entering their region, Location, or facility. Click the **Apply** button to apply as shown in the above picture.

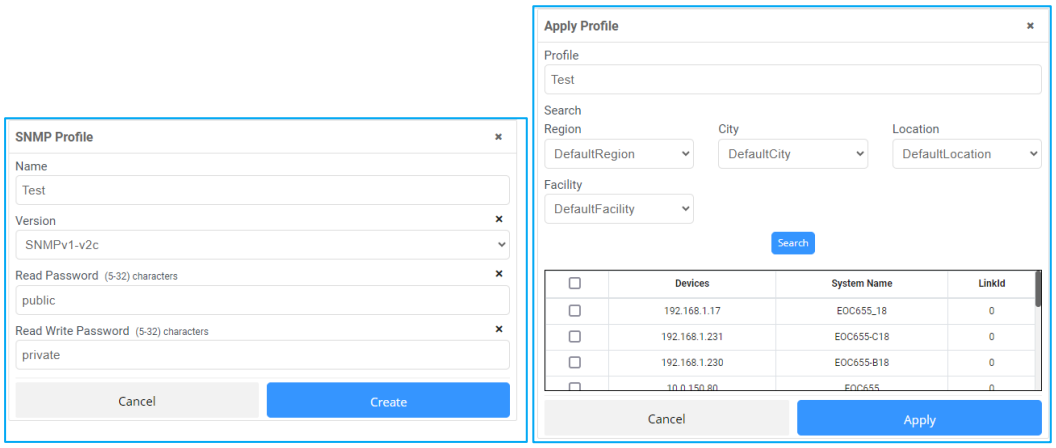
III. Edit

Transmit profiles can be edited by clicking the Edit icon and select the Radio Mode, Link Type, DDRS Status, Spatial Stream, modulation Transmit Power from the drop down and click **Update** button to incorporate changes



11.3 SNMP Profile

SNMP profile can be created by clicking the Create icon and entering the input fields like Name and selecting the dropdown of Radio Mode, Link Type click the Create button on the bottom of the input fields to create a profile for reference see the picture below



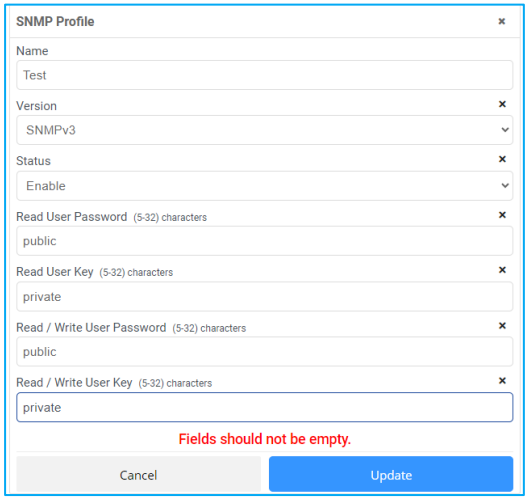
i.e. SNMP Create Profile and Apply Profile Images

I. Apply

SNMP profile can be applied by clicking the apply icon and existing profiles can be searched by entering their Region, Location, or Facility. Click the **Apply** button to apply as shown in the picture below

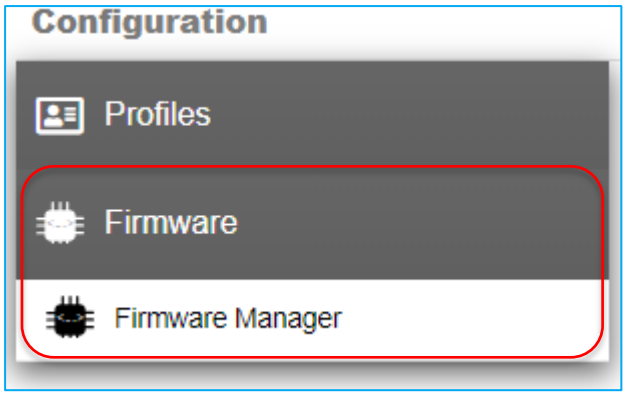
II. Edit

SNMP profiles can be edited by clicking the Edit icon and selecting the Radio Mode, Link Type Version, click the **Update** button to incorporate changes

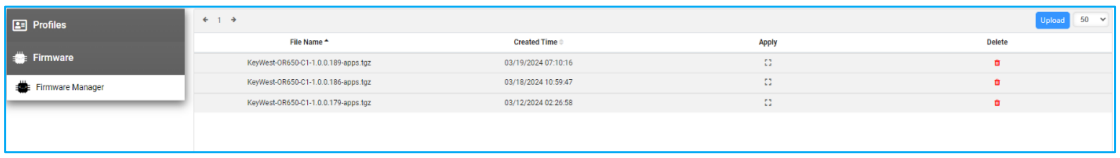


12. Firmware

Allows the users to upload new firmware into the NMS server. Users can also push the listed firmware to a list of devices or a single device. This section can be used for upgrading firmware on a single device for testing purposes. If the firmware is uploaded properly to the device without causing any breakdown, the user can use the Bulk firmware upgrade section to upload the firmware to the list of devices.

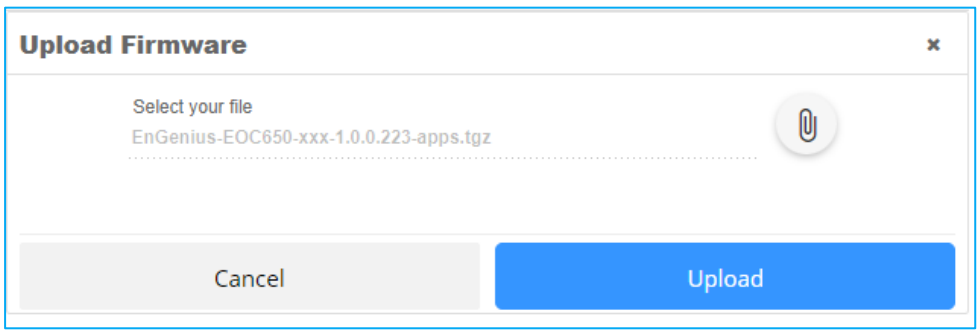


Before starting with the firmware upgrade, first, we'll upload the firmware onto the NMS. Click Upload Button, available on the right side of the Firmware Manager

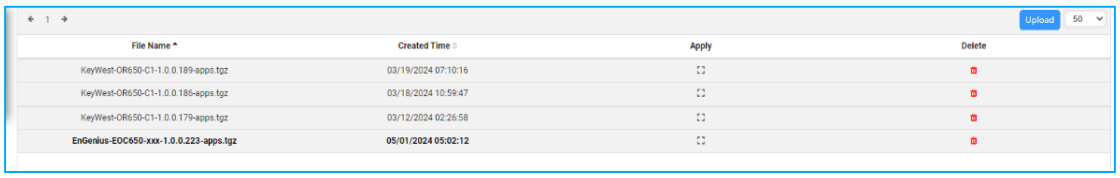


I. Firmware Upload

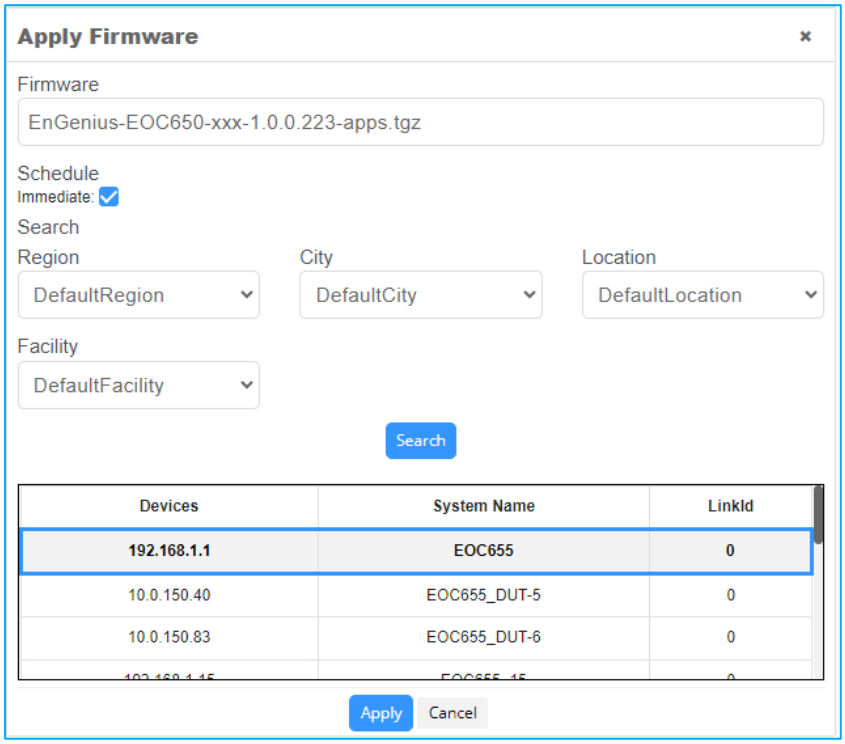
Click on the upload button and enter the version number of the firmware. A version of the firmware allows a fixed format with a major version and a minor version separated by an underscore (_).



After providing the version number select the file to be uploaded by clicking on the attachment icon. Once the upload is finished, the uploaded file will be listed in the available list of firmware. Select whichever firmware is needed and click on “Apply”



After checking the Apply Button checkbox (of required firmware), the Apply firmware window will appear, select the devices that need to be upgraded and click on “Apply” to start uploading the firmware with an option of doing it immediately or setting a later time by unchecking *Immediate*



12.1 Firmware upgrade

Allows to upgrade the firmware for the list of devices either by immediate action or by scheduling the task. Before initiating the task, the user has to upload the latest firmware which needs to be pushed to the devices.

Creating Firmware upgrade task:

1. Navigate to -> Configuration -> Firmware
2. Click on New Task -> on the right side the Bulk Firmware section will open.
3. Click on the drop-down -> "Firmware" to select the firmware that needs to be pushed.

4. Uncheck the checkbox for scheduling the task or keep it as it is for running the task immediately.
5. Select the devices by using the Region/Location/Facility filter for applying the configuration to the devices.
6. Click on the apply button to initiate the Firmware push task.

All the tasks which are executed are listed in the table available on their respective page. Each task is assigned with the following status:

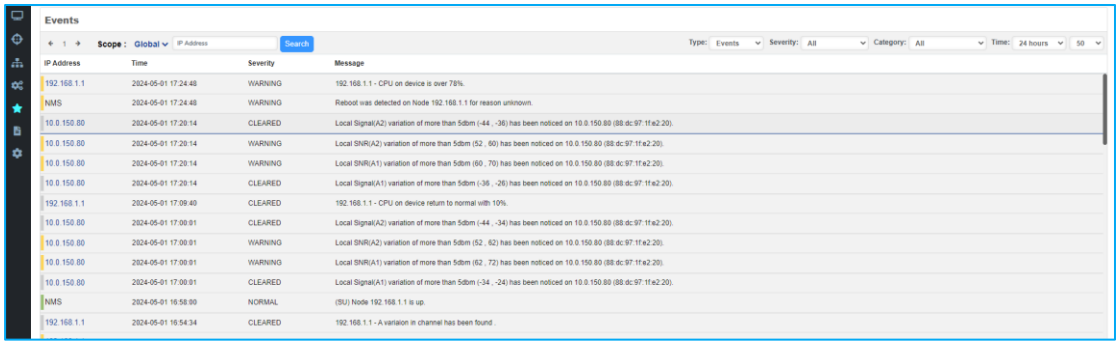
- Pending - which means the task is being scheduled and not yet executed
- Running - The task is in execution state.
- Successful - The task has finished the initiated and the operation is run properly without any issues
- Failed - The task has failed to execute. The reason for failure can be known by clicking on the task which opens up the individual status task which is executed on each of the devices.

Task Deletion - The user can delete a particular task that has completed execution or if a particular task is canceled. The tasks that are running cannot be deleted. The tasks that are pending can only be canceled first and later deleted. Select the task that needs to be deleted from the list of tasks and click on the delete button.

Task Cancellation - Tasks can be canceled if they are pending. Once the task is cancelled it will not execute. To cancel the task, select the task that is pending and click the cancel button in the particular row.

13. Events

Events section displays all the events generated by NMS internally like device status events (device up or device down) and traps received from the device. An option is provided for displaying syslog messages generated from the device. All the events are displayed in tabular form with details of the event related to IP Address, Time, Severity, Message.



I. IP Address

Denotes the address from where the trap is received as a message or the event that is generated by NMS on behalf of the device like threshold alarms. If the device is generated by NMS directly then the IP Address will be displayed as "NMS". On clicking the IP address or "NMS" the navigation takes place to the device node view page.

II. Time

Denotes the time on which the event is generated.

III. Severity

Severity denotes the intensity of the event which helps the user to act based on level. The following are the types of severity ordered based on priority from lower to higher

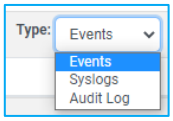
- Indeterminate - The events for which no priority has been assigned
- Cleared - The events whose severity level was high previously and is restored now. for e.g. A threshold alarm like CPU going high has a "Warning" severity and when the CPU comes back to normal has "Cleared" as the severity
- Normal - Events which has the priority set to normal and no action by the user is required like the device going up.
- Minor - An event whose priority is set as minor and the user needs to consider the event like there have been configuration changes to the device
- Warning - An event whose priority is set as a warning and the user needs to consider the event like the device CPU or memory going up
- Major - Event-triggered and treated as a higher priority like a device going down
- Critical - An event whose priority has been set as higher than the rest of the events. The user needs to resolve the issue immediately

IV. Message

The event message gives a brief description of the event

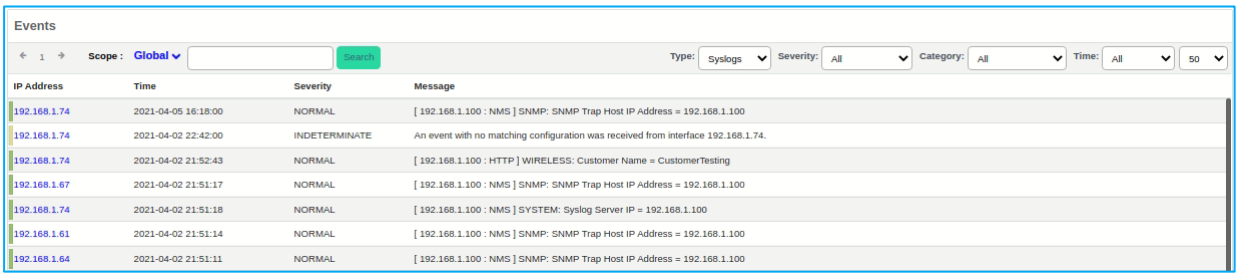
V. Type Filter

Provides the option of filtering the data to be displayed in the events table like switching the display of events from syslog's and events



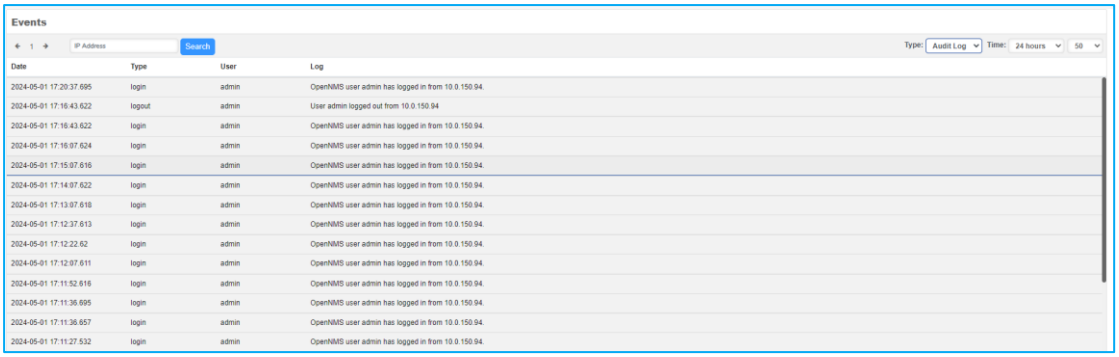
VI. Syslogs

Syslog is the log events that are forwarded by the device. It usually contains the changes to the configuration or any errors which are raised in the device. All the log events that are logged in the device can be accessed either in the events section or in the node view -> Monitor - Events section of the device.



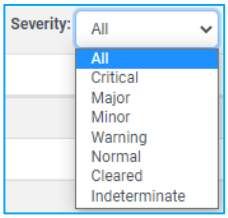
VII. Audit Logs

Audit logs are the logs that are generated whenever a particular change is made to the configuration of a particular device or any configuration changes are made in the SkyPoint server. It contains all activity related to the configuration changes Discovery initiation or Node modification done by the user right from log-in to log-out.



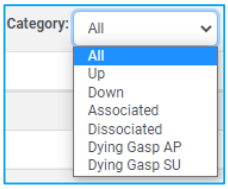
VIII. Severity Filter

Provides the option of filtering the data based on the filter



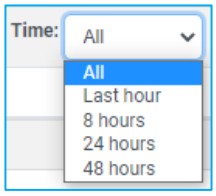
IX. Category

Filtering the events based on category like displaying all device **Down/Up** events

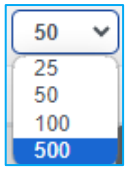


X. Time

Duration in which the events are generated. current filters provided are Last hour, 8 hours, 24 hours, 48 hours

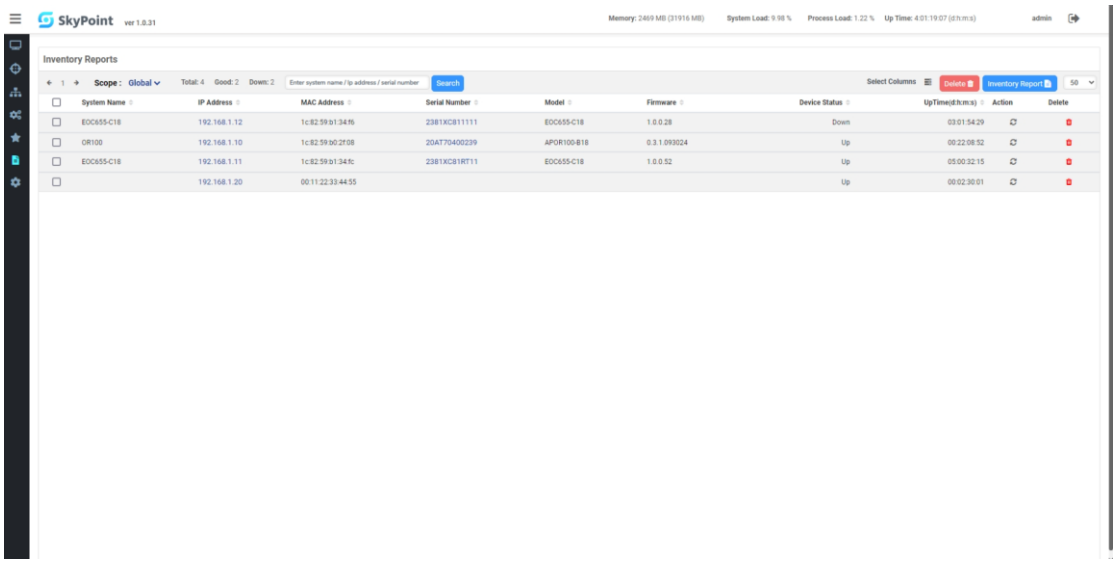


- All - By selecting the duration, a graph is shown based on severity and category. If "All" is selected as time filter no graphs will be displayed and all the events are displayed from recently received to last.
- Pagination
  Number of events to be displayed in the table.

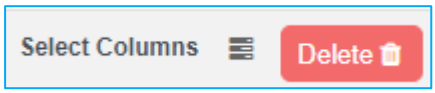


14. Inventory Reports

Lists all the devices which are currently discovered in SkyPoint. Devices can be filtered based on the Region/Location/Facility filter available and default number of devices listed are 25.



Users can change the devices to be listed from the filter available on the right-side top-corner drop-down. The following are the controls available in the inventory reports:



14.1 Select Columns:

Allows the user to show or hide the existing columns which are visible in the data table. The default columns listed are System Name, Primary IP, MAC address, Serial Number, Model number, Firmware and uptime. Additional to the device data columns two more columns are added in each row Action & Delete.

a. Action column - Rescan the particular device
b. Delete - Deletes a single device

14.2 Delete:

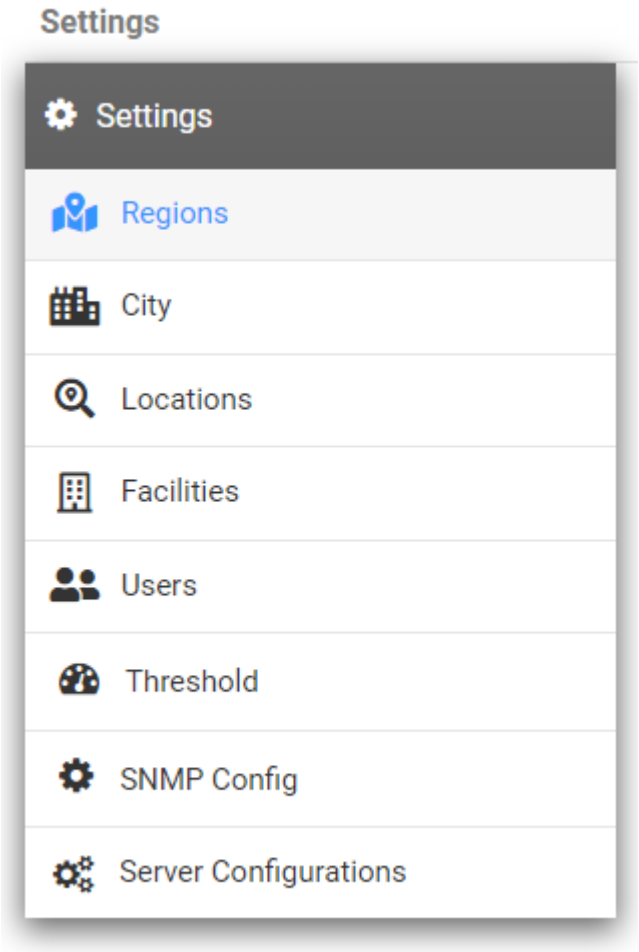
Deletes a single or a greater number of devices based on the selection. User can select which devices needs to be deleted by clicking on the checkbox available on the first column index. Once all the devices are selected clicking on "Delete" button opens a popup, if user wishes to delete the devices click "Yes" or "No" to cancel the operation.

14.3 Inventory Reports:

Returns the basic configuration of the device in CSV format. All the devices' data will be retrieved by clicking on the "Inventory Report" button.

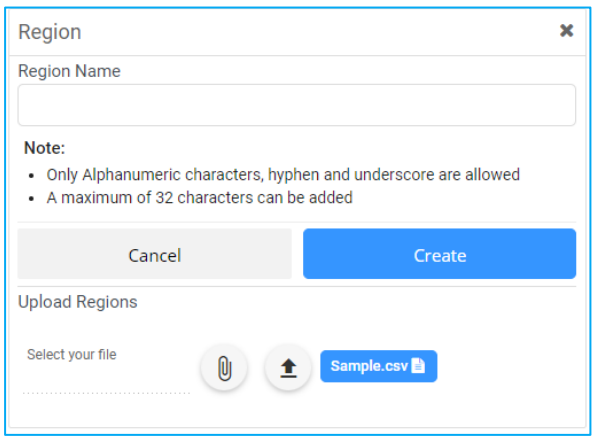
15. Settings

The settings section provides options for adding and configuring SkyPoint properties like creating and modifying Regions, Locations, Facilities, and users. Apart from creating new values user can also make SNMP-related configuration changes like when an SNMP configuration is changed in the device or when a new device has to be discovered that does not have the default SNMP read and write community, The user can configure for the IP address for which the values has to be modified. The settings section has the below components.

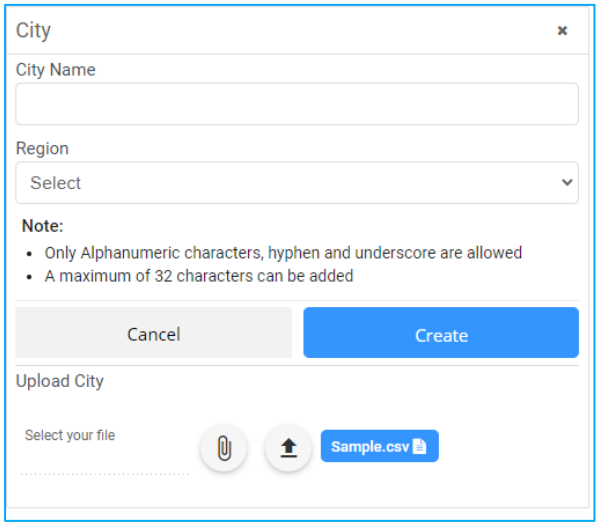


15.1 Regions

Regions are the root element in the topology tree structure and all the child elements like locations will be found under Regions. Users can create a new Region, Modify or Delete a region. While deleting user has to make sure that all the locations under the region have to be deleted first before deleting the region.

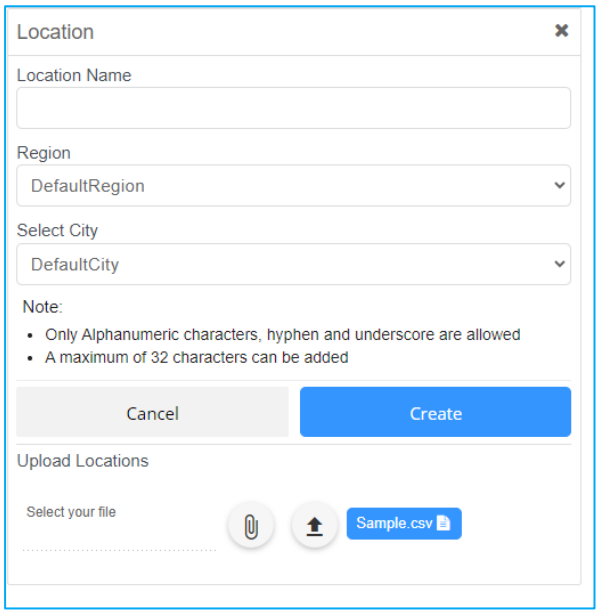


15.2 City



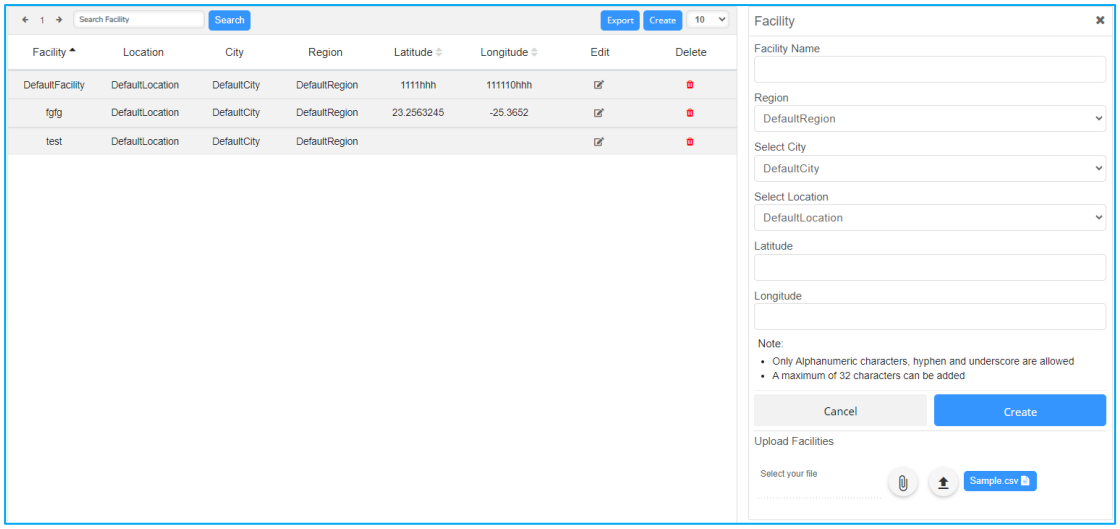
15.3 Locations

Locations are the logical grouping of the elements found under Regions. Multiple Locations can be created under a single Region.



15.4 Facilities

Facilities are the logical grouping of elements found under Locations. This group is the main group where all the discovered radios are listed.

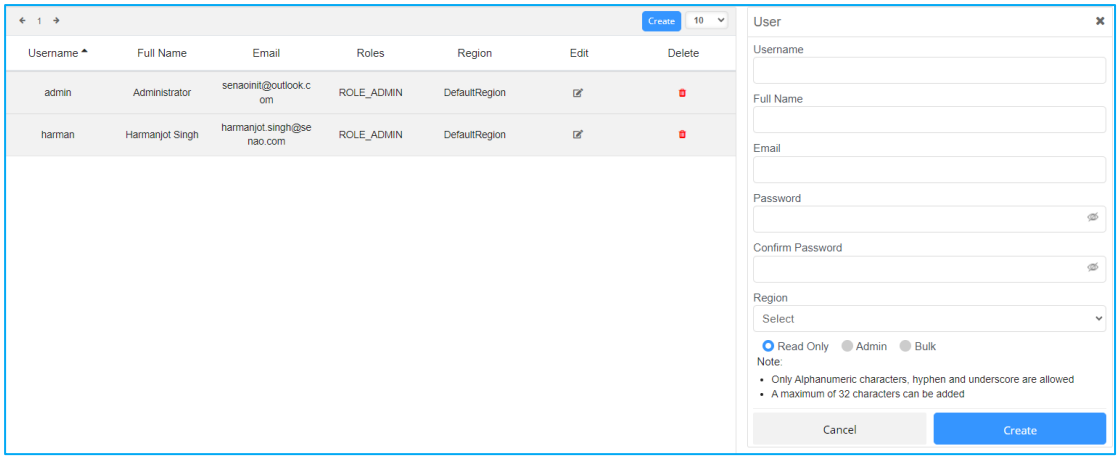


15.5 Users

The user's section allows in creation of new Users and assigning roles to the users while creating or updating. currently, SkyPoint supports 2 roles - Admin and read-only.

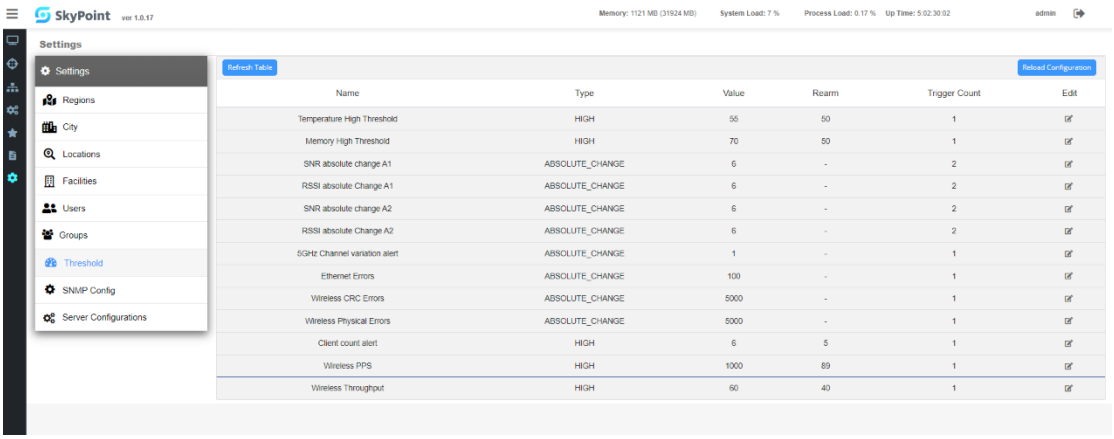
Admin role: All the users created, and the role of the admin assigned will act as admin and can make the configuration changes to the SkyPoint like creating or updating of the SkyPoint properties.

Read-Only role: *The read-only role restricts the users with the role to only view the* SkyPoint *content and cannot make any changes to the properties.*



15.6 Threshold

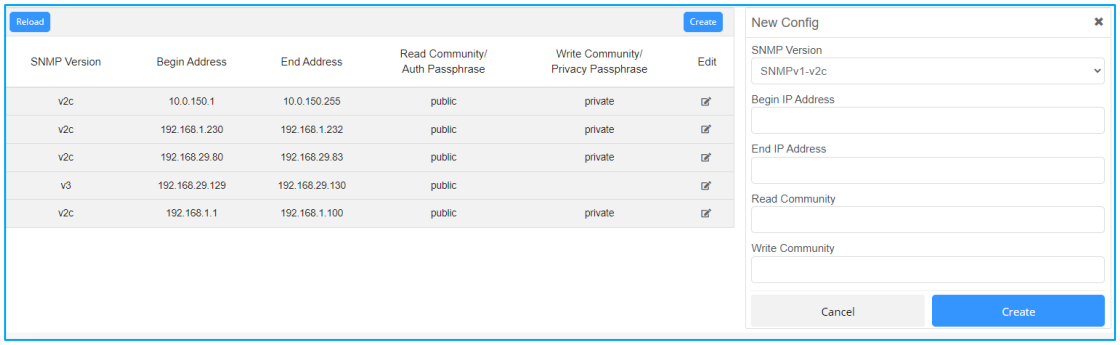
Threshold settings in network management are crucial for proactive monitoring. They define limits for performance metrics like Temperature, Memory, SNR, Ethernet/Wireless CRC Errors & etc. Effective threshold configuration enables early detection of issues, preventing downtime and optimizing resource utilization. Regular review and customization of thresholds ensure they remain aligned with network performance objectives. Utilize monitoring tools to track threshold violations and make data-driven decisions for network optimization.



15.7 SNMP Config

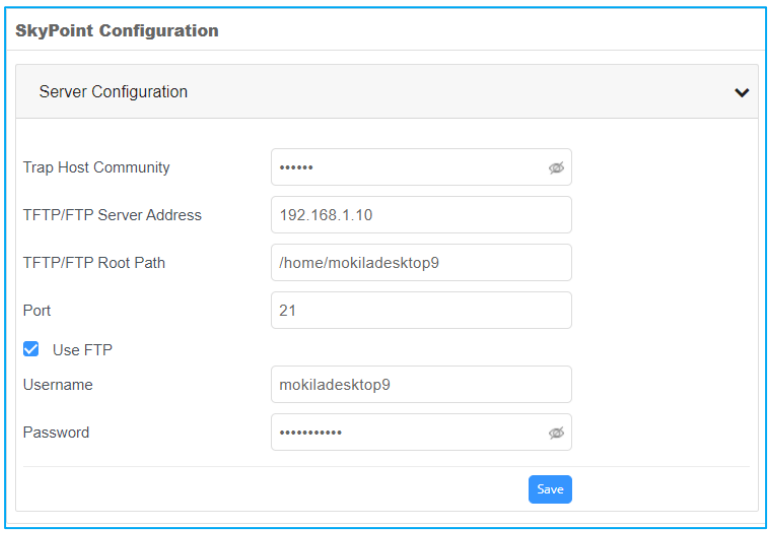
The SNMP Config section allows for modifying the SNMP Configuration of the SkyPoint. As SkyPoint collects and manages devices using SNMP protocol it is necessary to have the same configuration available in both the radio and SkyPoint. SkyPoint uses the default configuration of "public" as read community and "private" as write community for the devices to be discovered. If a particular radio with different community settings needs to be discovered, the user can provide either a separate SNMP configuration for a single device or a group of devices by providing a single IP address of the device or a range of IP addresses when a group of devices containing the same configuration.

If an SNMP configuration of a particular radio has been modified after the discovery user can provide the IP address and new SNMP configuration of the device and update the changes.



16. Server Configurations

Server Configuration provides basic properties used by SkyPoint like server Address, Trap Host Community, and TFTP root path.



16.1 Server Address

Server Address options allow SkyPoint to upload device firmware by using the address. As SkyPoint uses TFTP for uploading or downloading firmware and radio configuration it is important to provide the Server Address with the IP address on which the SkyPoint is using. The server address is also used by SkyPoint for receiving the traps forwarding by the devices.

16.2 Trap Host Community

The community used by SkyPoint for receiving the SNMP v2 traps.

16.3 TFTP Root Path

The path to the folder that is used by the TFTP Server. SkyPoint uses the path provided for uploading the firmware or configuration.

EnGenius Networks Inc.

1580 Scenic Ave. Costa Mesa, CA 92626
https://www.engeniustech.com/
Email: sales@engeniustech.com
Tel: +1 714 432 8668