FortiWLM MEA - Administration-Guide

Version 8.6.3

FORTINET DOCUMENT LIBRARY
https://docs.fortinet.com

FORTINET VIDEO GUIDE
https://video.fortinet.com

FORTINET BLOG
https://blog.fortinet.com

CUSTOMER SERVICE & SUPPORT
https://support.fortinet.com

FORTINET TRAINING & CERTIFICATION PROGRAM
https://www.fortinet.com/support-and-training/training.html

NSE INSTITUTE
https://training.fortinet.com

FORTIGUARD CENTER
https://fortiguard.com/

END USER LICENSE AGREEMENT
https://www.fortinet.com/doc/legal/EULA.pdf

FEEDBACK
Email: techdoc@fortinet.com

February 09, 2022
FortiWLM MEA 8.6.3 Administration-Guide
02-863-609781-20220209

TABLE OF CONTENTS

Change Log

Date	Change Description
2022-02-09	FortiWLM MEA 8.6.3 release version.

Key Concepts

The *Wireless Manager Management Extension Application* (FortiWLM MEA) web based application suite is an intelligent management system that helps you to easily manage your wireless network. You can manage controllers and access points mapped to the network to provide real-time data that enables centralized and remote monitoring of the network.

The FortiWLM MEA container is hosted on the FortiManager integrated platform that provides centralized management of Fortinet products and other devices. You can access FortiWLM MEA to monitor FortiGate controllers from the FortiManager application. You can monitor networks with FortiGate deployments, and stations and access points' usage and diagnostic information (individually and groups) using the FortiWLM MEA.

The FortiWLM MEA application is a management extension application that can only be used to monitor the wireless network. Wireless configuration must be done directly on FortiGates.

This section contains information about the following key concepts and features of FortiWLM MEA:

- Administrative Domain on page 6
- Controllers on page 6
- Controller Groups on page 7
- Access Points on page 7
- Access Point Groups on page 7
- Stations on page 7
- Station Groups on page 7
- Device Inventory on page 8
- Maps on page 8

Administrative Domain

Administrative domains (ADOMs) enable administrators to manage only those controllers that they are specifically assigned, based on the ADOMs which they access. You can manage FortiWLM MEA using the root ADOM or create a new ADOM.

For more information on creating and managing ADOMs, see the *FortiManager Administration Guide*.

Controllers

Controllers are the FortiGate devices in the wireless network managed by FortiWLM MEA.

You may add FortiGate devices to FortiManager and FortiWLM MEA in the following order:

1. The ADOM of FortiManager
2. FortiWLM MEA

For more information about adding FortiGates to FortiManager and FortiWLM MEA:

- See Adding FortiGate devices to FortiManager on page 11.
- See Adding FortiGate devices to FortiWLM MEA on page 11.

Controller Groups

A Controller Group may be defined as a coherent group of FortiGates placed in distinctive geographic locations or logically managed by the same configuration. Controllers in a controller group may be of different hardware models running different firmware versions. Each controller in a controller group can belong to only one controller group.

Access Points

Access Points (APs) are devices connected to and managed by FortiGates. APs allow other wi-fi based endpoint devices to connect to the wireless network.

Access Point Groups

An AP Group is a coherent group of APs belonging to the same FortiGate or different FortiGates placed in distinctive geographic locations. An AP group may consist of APs with different hardware models or APs from controllers having different firmware versions.

Stations

Stations are wi-fi based endpoint devices such as phones, laptops, computers, and so on that are connected to APs in the wireless network.

Station Groups

A Station Group may be defined as a coherent group of endpoint devices connected to a distinct AP, or endpoint devices connected to different APs in a distinctive geographic location. Stations in a station group may be of various kinds, having different hardware models, or running different OS versions.

Device Inventory

An inventory of FortiGates and APs in the wireless network maintained by FortiWLM MEA is called as the device inventory for that wireless network.

Maps

Maps are image files that accurately represent the physical layout of a site and are as close to scale as possible. Maps are created to visually track the APs in a wireless network.

Getting Started with FortiWLM MEA

FortiWLM MEA allows you to monitor, operate, and administer FortiGates in a wireless network.

This section provides a summary of how to get started with FortiWLM MEA:

1. Enable FortiWLM MEA. See Enabling FortiWLM MEA on FortiManager on page 10.
2. Add FortiGate devices to FortiManager. See Adding FortiGate devices to FortiManager on page 11.
3. Add FortiGate devices to FortiWLM MEA. See Adding FortiGate devices to FortiWLM MEA on page 11.
4. Monitor wireless networks. See Monitoring Devices and Network Traffic on page 12.
5. Operate wireless networks. See Operating Devices in a Wireless Network on page 58.
6. Administer wireless networks. See Administering FortiWLM MEA on page 86.

ADOM and Non-ADOM Modes

You can manage FortiWLM MEA in the ADOM or non-ADOM mode. For more information on creating and managing ADOMs, see the *FortiManager Administration Guide*.

While creating an ADOM, select FortiGate version 6.4 to enable access to FortiWLM.

In the ADOM mode, all data displayed in FortiWLM is based on the devices managed by the particular ADOM. However, the following administrative data is displayed for all devices irrespective of the ADOM they belong to.

- Licensing
- System Settings
- Upgrade (WLM Upgrade and Patch Management)

- In the ADOM mode FortiGates must be added in the FortiManager, see section Adding FortiGate devices to FortiManager on page 11.
- In the non-ADOM mode, FortiGates must be added in FortiWLM MEA, see section Adding FortiGate devices to FortiWLM MEA on page 11.

After you add FortiGates to FortiWLM MEA, FortiWLM MEA communicates with FortiManager to obtain data. You can view the *Access Points* chapter in the *FortiManager Administration Guide* for more information on configuring APs.

By default, ADOMs are disabled. Enabling and configuring ADOMs can only be done by super user administrators.

Enabling the ADOM Mode

To enable the ADOM mode, log in to the FortiManager as a super user administrator.

1. Go to *System Settings > Dashboard*.
2. In the *System Information* widget, toggle the *Administrative Domain* switch to *ON*.
   You will be automatically logged out of the FortiManager and returned to the log in screen.

Disabling the ADOM Mode

To disable the ADOM Mode, you are required to remove all the devices from non-root ADOMs. That is, add all devices to the root ADOM.

1. Delete all non-root ADOMs.
   Only after removing all the non-root ADOMs can ADOMs be disabled.
2. Go to *System Settings* > *Dashboard*.
3. In the *System Information* widget, toggle the *Administrative Domain* switch to *OFF*.
   You will be automatically logged out of the FortiManager and returned to the log in screen

The ADOMs feature cannot be disabled if ADOMs are still configured and have managed devices in them.

Enabling FortiWLM MEA on FortiManager

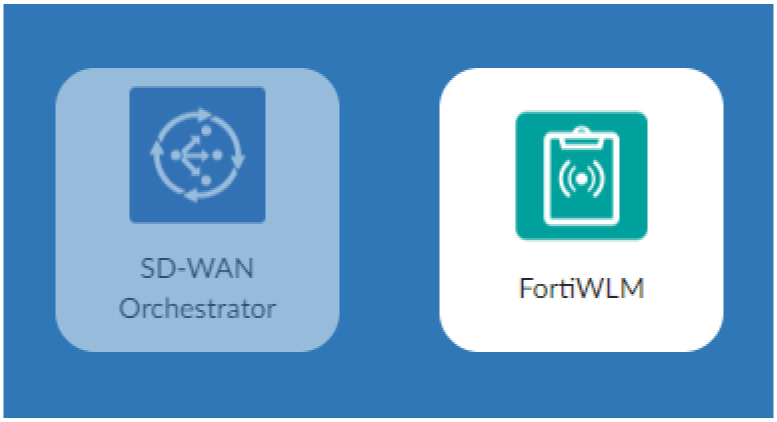
You can access the FortiWLM MEA management extension application from the *Management Extensions* tile on the FortiManager ADOM.

Only administrators with a *Super_User* profile can enable management extensions.

A CA certificate is required to install management extensions on FortiManager. See *CA certificates* in the *FortiManager Administration Guide*.

To enable FortiWLM MEA on FortiManager:

1. Go to the ADOM.
2. Click the *Management Extensions* tile.
3. Click the grayed out tile for FortiWLM MEA to enable the application.
   Grayed out tiles represent management extensions that have not been enabled. In the following example, *SD-WAN Orchestrator* is enabled, and FortiWLM MEA is disabled.



4. Click *OK* in the dialog that appears. It may take some time to install the application.

Adding FortiGate devices to FortiManager

Before you can add FortiGate devices to FortiWLM MEA, you may add them to FortiManager. Because FortiWLM MEA supports the ADOM, add the devices to the ADOM.

It is recommended to add FortiGate as model devices to control the order of configuration installation. You want to install the FortiWLM MEA configuration before the firewall configuration.

For details about adding model devices to FortiManager, see the *FortiManager Administration Guide*.

Adding FortiGate devices to FortiWLM MEA

To add devices to FortiWLM MEA, see Adding controllers to the device inventory on page 59.

Monitoring Devices and Network Traffic

After you have configured a wireless network, you can monitor the network as well as individual devices in the network from the *Monitor* tree menu in the navigation menu on the left side of the screen.

If you expand the *Monitor* menu item, you can access the following branches:

- Overview on page 12
- Detailed Dashboard on page 45
- Trends on page 51
- Topology on page 54

Overview

The *Overview* branch provides a way to access the various dashboards available to a user to monitor the wireless network.

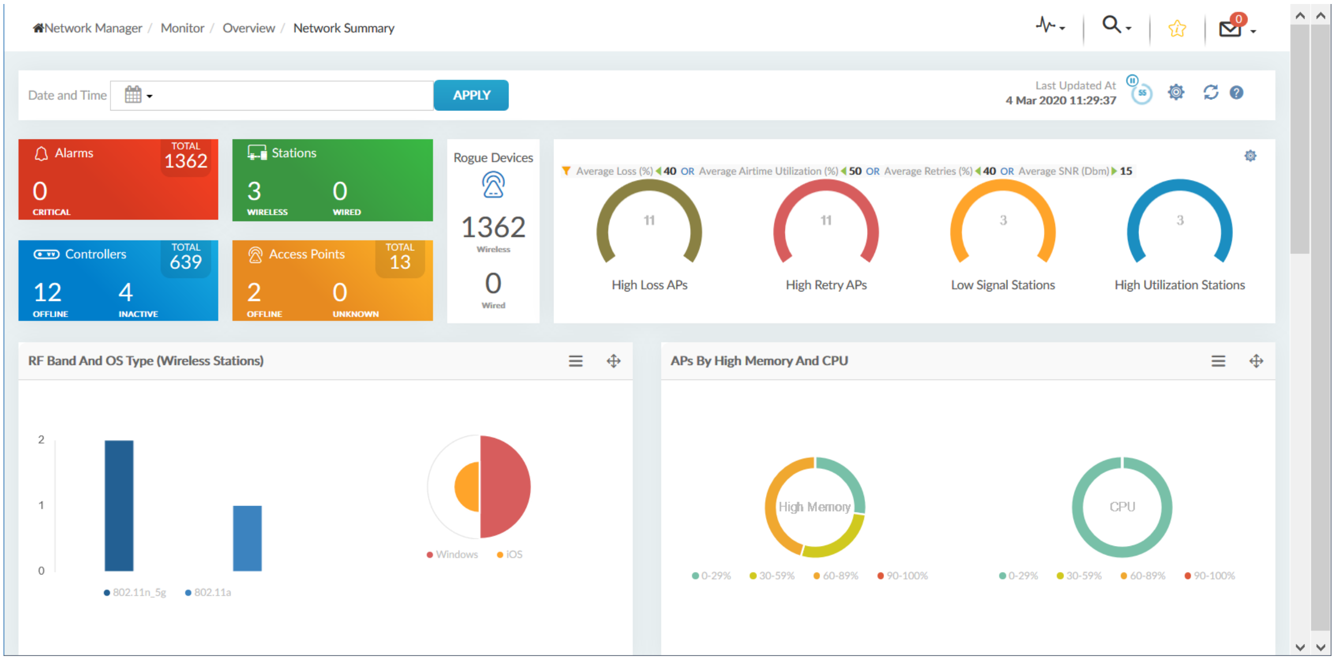
You can access the following dashboards from the *Overview* branch:

- Network Summary on page 12
- AP Group Summary on page 16
- Access Point on page 20
- Station Group on page 28
- Stations on page 31
- Application Monitoring on page 33
- Channel Summary on page 35
- Fault Management on page 36
- Network Heat Maps on page 42
- Location Services on page 43

Network Summary

The *Network Summary* dashboard provides statistics of the types of devices connected to the wireless network and their performance. It provides a summary view of the wireless network statistics, including network wide performance distribution of wireless controllers and access points. It gathers the data from all managed controllers and access points at specific intervals. The graphical representation of Controllers, Access Points, Stations, and so on, provides a glimpse of the wireless network, based on the fetched data for the configured period of time, and within the administrative scope of the logged in user.

By default, a user lands on the *Network Summary* dashboard, after logging in to FortiWLM MEA.



The *Network Summary* dashboard is organized into:

- Dashboard Settings on page 13
- Overall Network Statistics on page 14
- Network Health and Trends on page 15

Dashboard Settings

The dashboard settings allow you to control the display of widgets or panels on the dashboard. To access the dashboard settings, click the ⚙ button on the upper-right of the *Network Summary* dashboard.

The dashboard generates and displays data at configured time intervals. To change that behavior, you can select the time interval from the *Date and Time* drop-down list or define a custom time range, and click *Apply*.

To control which widgets are displayed on the dashboard, you can select the required options to filter them from the following available network health parameters:

Parameters	Options to filter by
Network Health	• RF Band and OS Type (Wireless Stations) • APs by High Memory and CPU • Controllers by High Memory and CPU • Top Applications and OS Type (Wired Stations)
Trend	• Stations and Throughput • Low Signal And High Loss Stations
Default	• Recent Activities • Client Density

Overall Network Statistics

The network statistics section of the dashboard provides the overall statistical details of Controllers, Access Points, Stations, and Alarms within the wireless network. The details are displayed in the form of colorful widgets. The available widgets are as follows:

Widgets	Description
Alarms	Provides the total count of alarms raised. Click on the number of critical alarms to view the detailed summary of alarms raised, displayed in a pop-up modal window. Information like *Date/Time*, *Alarm Name*, *Category*, *Fdn*, *Controller ID*, *Message*, and so on is displayed.
Stations	Provides the total count of stations connected to an AP. Click on the number of wireless/wired stations to view the detailed summary of stations, displayed in a pop-up modal window. Information like *Station MAC Address*, *Station IP Address*, *Station IPv6 Address*, *Essid*, *Channel*, *SNR*, *RF band*, *OS type*, *RX rate*, *TX rate*, *Controller ID*, *AP ID*, *Interface Index*, and so on is displayed.
Controllers	Provides the total count of offline/inactive controllers. Click on the number of offline/inactive controllers to view the detailed summary of controllers, displayed in a pop-up modal window. Information like *Controller*, *Description*, *Model*, *Software Version*, *Management State*, *Last Time*, and so on is displayed.
Access Points	Provides the total count of offline/unknown APs in the network. Click on the number of offline/unknown APs to view the detailed summary of APs, displayed in a pop-up modal window. Information like *AP Name*, *IP Address*, *MAC Address*, *Model*, *Connectivity Mode*, *Software Version*, *Location*, *Last Time*, *Controller Name*, and so on is displayed.
Rogue Devices	Provides the total count of wired and wireless rogue devices (APs and stations) in the network. Click on the number of wireless/wired rogue devices to view the detailed summary of the rogue devices, displayed in a pop-up modal window. Information like *Controller Name*, *Rogue MAC Address*, *Rogue Type*, *BSSID*, *Channel*, *SSID*, *AP Reported*, *Location*, *Date*, *Time*, and so on is displayed.

The dashboard provides threshold configuration and filtering capability for APs and Stations within the network to display statistical charts. The configurable threshold settings are *Average Airtime Utilization (%)*, *Average Loss (%)*, *Average Retries (%)*, and *Average SNR (Dbm)*. Depending upon the threshold settings configurations, the information about APs and Stations is graphically charted as follows:

APs/Stations	Description
High Loss APs	Provides the total count of APs in the network that have an average loss percentage greater than the *Average Loss (%)* setting as configured. Click on the graphical representation to navigate to the *AP Groups* dashboard with the same filter applied.
High Retry APs	Provides the total count of APs in the network that have an average retry percentage greater than the *Average Retries (%)* setting as configured. Click on the graphical representation to navigate to the *AP Groups* dashboard with the same filter applied.
Low Signal Stations	Provides the total count of stations in the network that have an average SNR lesser than the *Average SNR (Dbm)* setting as configured. Click on the graphical representation to navigate to the *Station Groups* dashboard with the same filter applied.

APs/Stations	Description
High Utilization Stations	Provides the total count of stations in the network that have an averageairtime utilization greater than the *Average Airtime Utilization (%)* setting as configured. Click on the graphical representation to navigate to the *Station Groups* dashboard with the same filter applied.

Network Health and Trends

The dashboard panels display network health and trends of devices in the wireless network. The trend graphs display data for the last 10 minutes. Depending upon which panels are selected in the dashboard settings to be displayed on the dashboard, some or all of the panels may be displayed. The following panels are available to be displayed on the dashboard:

- RF Band and OS Type (Wireless Stations) on page 15
- Stations and Throughput on page 15
- Low Signal and High Loss Stations on page 16
- APs by High Memory and CPU on page 16
- Controllers by High Memory and CPU on page 16
- Top Applications and OS Type (Wired Stations) on page 16
- Recent Activities on page 16
- Client Density on page 16

RF Band and OS Type (Wireless Stations)

This panel provides the statistics for stations associated with each:

- **RF band** - The bar chart provides a graphical representation of stations for each RF band. Each vertical bar represents the total number of stations connected to a particular RF band, for example, 802.11a, 802.11b, 802.11bg, bgn, and so on. Each station type is represented by a unique color. Hover over a vertical bar in the graph to view the total number of stations connected to that particular RF band. Click on the graph legend to view the associated station details like *Station MAC Address*, *Station IP Address*, *Station IPv6 Address*, *Essid*, *Channel*, *SNR*, *RF Band*, *OS Type*, *RX Rate*, *TX Rate*, *Controller ID*, *AP ID*, *Interface Index*, and so on.
- **OS type** - The pie chart provides a graphical representation of stations for each OS type. Each slice of the pie represents the total number of stations running a particular OS type. A maximum of six different OS types are plotted on the pie chart. The remaining OS types are displayed under the *Others* category. Hover over a pie slice in the pie chart to view the total number of stations running that particular OS type. Click on each of the OS types to view a detailed summary of the stations running that particular OS type. Click on the chart legend to view the associated station details like *Station MAC Address*, *Station IP Address*, *Station IPv6 Address*, *Essid*, *Channel*, *SNR*, *RF Band*, *OS Type*, *RX Rate*, *TX Rate*, *Controller ID*, *AP ID*, *Interface Index*, and so on.

Stations and Throughput

This panel displays a plotting of the total number of stations and the throughput against time. The graph displays the aggregate *Number of Stations* connected to the wireless network and the average *Throughput (Mbps)* at 10-minute intervals.

Each bar represents the maximum number of stations connected to the wireless network and the average throughput during that interval. Hover over each of the bars to view the station count and throughput during that interval.

Low Signal and High Loss Stations

This panel is a trend graph that displays the total number of stations in the network facing low signal and high loss at any given point. High Loss is defined as the percentage of the number 802.11 unicast packets transmitted for which no 802.11 acknowledgment is received, which is greater than 40%.

Hover over each of the intervals on the graph to see a summary of the high loss and low signal stations, as per the average loss percentage and SNR, as configured. You can configure the threshold for High Loss and Low Signal from the available settings. The graph is plotted based on your configurations.

APs by High Memory and CPU

This panel categorizes all the APs by CPU usage and Memory utilization. Various ranges that fall under each of these two categories are 0 to 29%, 30 to 59%, 60 to 89%, and 90 to 100%. Hover over each of these ranges in the chart to view the number of APs in that particular range.

Controllers by High Memory and CPU

This panel categorizes all the controllers by CPU usage and Memory utilization. Various ranges that fall under each of these two categories are 0 to 29%, 30 to 59%, 60 to 89%, and 90 to 100%. Hover over each of these ranges in the chart to view the number of APs in that particular range.

Top Applications and OS Type (Wired Stations)

This panel provides the summary of the top five applications used in the network and also the frequently used OS types, for wired stations.

Recent Activities

This panel displays the last forty user activities in the last 24 hours.

Client Density

This panel displays the client density heat map from the visualization dashboard. By default, the first floor on the map is displayed. You can select the floor you want to view.

You can also enable the overlay options, AP (displays the AP name and AP ID) and Heat Canvas (the regions around APs corresponding to the AP throughput), on the map. Additionally, you can zoom in and zoom out within the maps.

Only APs that have clients associated with them will be displayed.

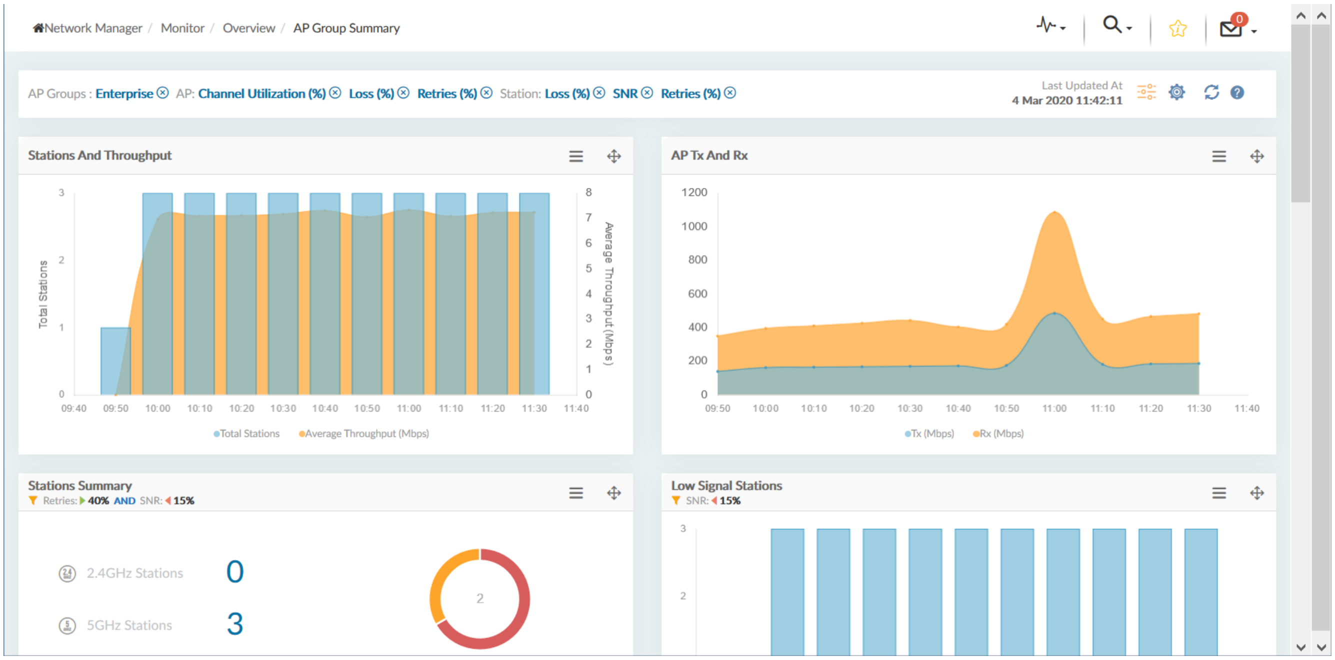
Click on an AP to view the associated details like *AP ID*, *AP Name*, *AP MAC*, *Controller*, *Total Stations*, and so on.

AP Group Summary

An AP Group is a coherent group of APs belonging to the same controller or different controllers placed in distinctive geographic locations. An AP group may consist of APs with different hardware models or APs from controllers having different FortiWLC versions. When an AP is added to a group, all the radios of the AP are also part of that group.

The data of APs within any selected AP group is used to present information on the *AP Group Summary* dashboard. The data is generated at configured time intervals on the server. By default, the time intervals are: two hours for trend graphs, and ten minutes for other widgets. All the links or pop-up modal screens from the *AP Group Summary* dashboard and status bar display current data from trends, statistics, and top five APs.

You can access the *AP Group Summary* dashboard through *Monitor* > *Overview* > *AP Group Summary*.



The *AP Group Summary* dashboard is organized into:

- Dashboard Settings on page 17
- Dashboard Filtering on page 18
- Trends, Statistics, and Top 5 APs on page 18

Dashboard Settings

The dashboard settings allow you to control the display of widgets or panels on the dashboard. To access the dashboard settings, click the ⚙ button on the upper-right of the *AP Group Summary* dashboard.

To control which panels are displayed on the dashboard, you can select the required options to filter them from the following available AP Group parameters:

Parameters	Options to filter by
Top 5 APs	• High Channel Utilization APs • High Retry APs • High Loss APs • Top Applications and APs by Usage
Trend	• Stations and Throughput • Low Signal Stations

Parameters	Options to filter by
	• High Loss Stations • High Loss APs Trend • AP Tx and Rx
Statistics	• Access Points • Stations

Dashboard Filtering

The dashboard provides threshold configuration and filtering capability for APs and Stations within AP Groups to graphically represent the information and display statistical charts. To access the threshold configuration and filtering settings, click the ☰ button on the upper-right of the *AP Group Summary* dashboard.

For any selected AP Group from the tree menu, the configurable threshold settings for:

- APs are *Average Channel Utilization (%)*, *Average Loss (%)*, and *Average Retries (%)*
- Stations are *Average Loss (%)*, *Average SNR*, and *Average Retries (%)*.

You can choose whether all selected threshold settings pass or just one passes, by toggling the slider below the settings for APs and Stations. Depending upon the threshold settings configurations, information about APs and Stations is graphically charted into panels on the dashboard.

The dashboard generates data at configured time intervals. You can select a duration from the *Date and Time* drop-down list or define a custom time range, and click *Apply* to set that duration.

You can also choose to save the filter settings to access the saved filer later. Click the *Save* button, type a name for the filter, and click *Save*. To make that filter as the default filter, select the *Set as Default Filter* option before you save it.

Trends, Statistics, and Top 5 APs

This section of the *AP Group Summary* dashboard graphically represents the APs/Stations statistics and trends that belong to a selected AP group. By default, the trend graphs display data for the last two hours. Depending upon the threshold settings configurations and filters, and the panels selected to be displayed, the APs/Stations are graphically charted as follows:

- High Channel Utilization APs on page 19
- High Retry APs on page 19
- High Loss APs on page 19
- Top Applications and APs By Usage on page 19
- Stations and Throughput on page 19
- Low Signal Stations on page 19
- High Loss Stations on page 19
- High Loss APs Trend on page 20
- AP Tx and Rx on page 20
- Access Points on page 20
- Stations on page 20

High Channel Utilization APs

Provides the top five APs in the network that have an average channel utilization greater than the *Average Channel Utilization (%)* setting as configured. The chart displays the name and the corresponding average channel utilization in percentages of APs in the groups of 2.4 GHz and 5 GHz bands.

Click on the AP name to navigate to the *Access Point* dashboard.

High Retry APs

Provides the top five APs in the network that have an average retry percentage greater than the *Average Retries (%)* setting as configured. The chart displays the name and the corresponding average retries in percentages of APs in the groups of 2.4 GHz and 5 GHz bands.

Click on the AP name to navigate to the *Access Point* dashboard.

High Loss APs

Provides the top five APs in the network that have an average loss percentage greater than the *Average Loss (%)* setting as configured. The chart displays the name and the corresponding average loss in percentages of APs in the groups of 2.4 GHz and 5 GHz bands.

Click on the AP name to navigate to the *Access Point* dashboard.

Top Applications and APs By Usage

This panel provides the summary of highly used applications within the selected AP Group and also the top five APs with the highest average throughput within the AP Group.

Stations and Throughput

This panel displays a plotting of the total number of stations and the throughput against time. The graph displays the aggregate *Number of Stations* connected to the APs within the selected AP Group and the average *Throughput (Mbps)* at a given time.

Each bar represents the maximum number of stations connected to the APs within the selected AP Group and the average throughput during that interval. Hover over each of the bars to view the station count and throughput during that time interval.

Low Signal Stations

This panel is a trend graph that displays the total number of stations in the network having low SNR. SNR is defined as the signal strength relative to the background noise.

Hover over each of the intervals on the bar graph to see a summary of the maximum number of stations connected and the total number of low signal stations as per the average SNR as configured. You can configure the threshold for *Average SNR* from the available filter options. The graph is plotted based on the configurations.

High Loss Stations

This panel is a trend graph that displays the total number of stations in the network having a High Loss. High Loss is defined as the percentage of the number 802.11 unicast packets transmitted for which no 802.11 acknowledgment is received, which is greater than 40%.

Hover over each of the intervals on the bar graph to see a summary of the maximum number of stations connected and the total number of high loss stations as per the average loss percentage as configured. You can configure the threshold for *Average Loss (%)* from the available filter options. The graph is plotted based on the configurations.

High Loss APs Trend

This panel provides the total count of APs in the network that have an average loss percentage greater than the *Average Loss (%)* setting as configured in the AP group threshold settings. Hover over each of the sections to see the maximum number of connected APs and the total number of high loss APs.

AP Tx and Rx

This panel is a trend graph that displays the average *Tx* and *Rx* utilization (Mbps) of all the access points in the AP group.

Access Points

This panel displays the details of all APs in the AP group that satisfy the threshold configuration settings and the applied filters.

Click on the AP name to navigate to the *Access Points* dashboard.

Stations

This panel displays the details of all stations connected to each of the APs in the AP group that satisfy the threshold configuration settings, and the applied filters.

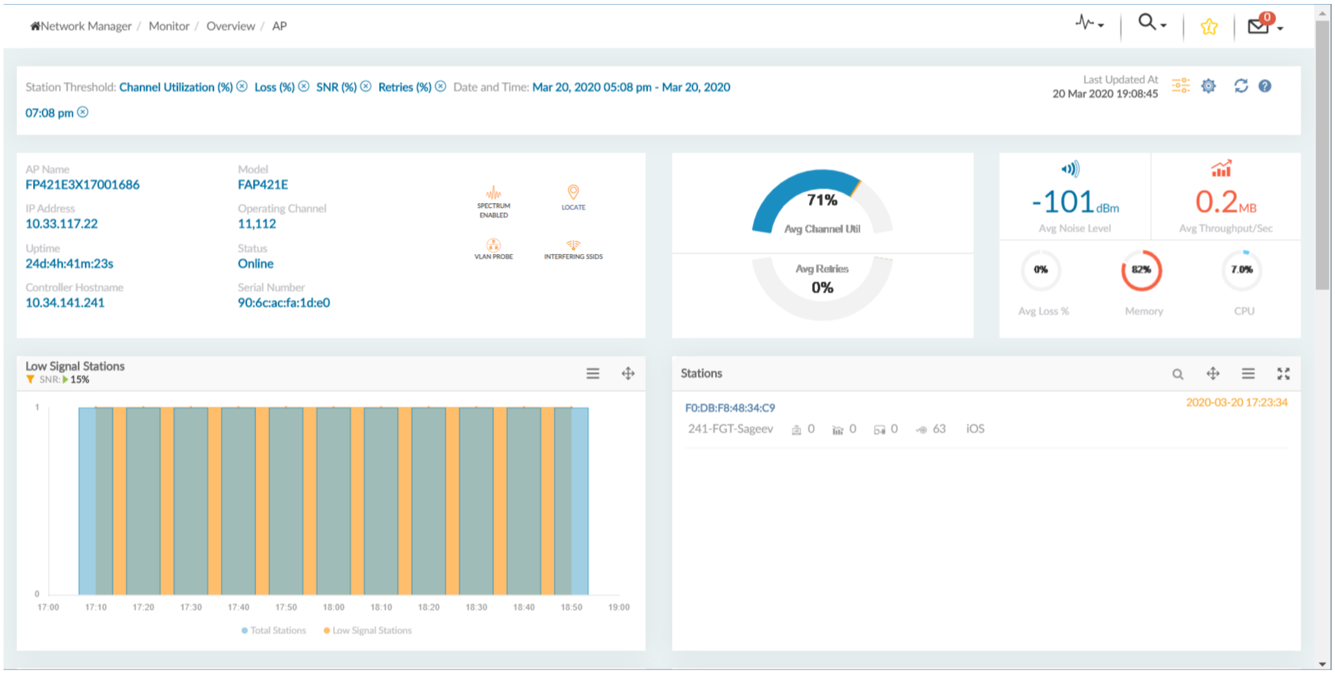
Click on the Station name to navigate to the *Stations* dashboard.

Access Point

The *Access Point* dashboard provides in-depth information about AP activity. It provides a graphical representation of the throughput, station count, noise level, loss percentage, channel utilization percentage, and the health of stations connected to the selected AP that is connected to a controller managed by FortiWLM MEA.

The representational data is generated at configured time intervals on the server. By default, the time intervals are: two hours for trend graphs, and ten minutes for other widgets. All the links or pop-up modal screens from the *Access Point* dashboard and status bar display current data. Offline APs are also displayed on the dashboard.

You can access the *Access Point* dashboard through *Monitor* > *Overview* > *AP* .



Network Manager / Monitor / Overview / AP

Station Threshold: Channel Utilization (%) Loss (%) SNR (%) Retries (%) Date and Time: Mar 20, 2020 05:08 pm - Mar 20, 2020 07:08 pm

Last Updated At 20 Mar 2020 19:08:45

AP Name: FP421E3X17001686
Model: FAP421E
IP Address: 10.33.117.22
Operating Channel: 11,112
Uptime: 24d:4h:41m:23s
Status: Online
Controller Hostname: 10.34.141.241
Serial Number: 90:6c:ac:fa:1d:e0

F0:DB:F8:48:34:C9 2020-03-20 17:23:34
241-FGT-Sageev 0 0 0 63 iOS

The *Access Point* dashboard is organized into:

- Dashboard Settings on page 21
- Dashboard Filtering on page 22
- Dashboard Icons on page 22
- Access Point Summary on page 26
- Trends, Statistics, and Top 5 APs on page 26

Dashboard Settings

The dashboard settings allow you to control the display of widgets or panels on the dashboard. To access the dashboard settings, click the ⚙ button on the upper-right of the *Access Point* dashboard.

To control which widgets or panels are displayed on the dashboard, you can select the required options to filter them from the following available AP parameters:

Parameters	Options to filter by
Top 5 APs	• Applications and Stations by Usage
Trend	• Stations and Throughput • Low Signal Stations • High Loss Stations • AP Tx and Rx
Statistics	• Stations • Alarms • Stations Summary

Dashboard Filtering

The dashboard provides threshold configuration and filtering capability for stations connected to any AP to graphically represent the information and display statistical charts. To access the threshold configuration filtering settings, click the ☰ button on the upper-right of the *Access Point* dashboard.

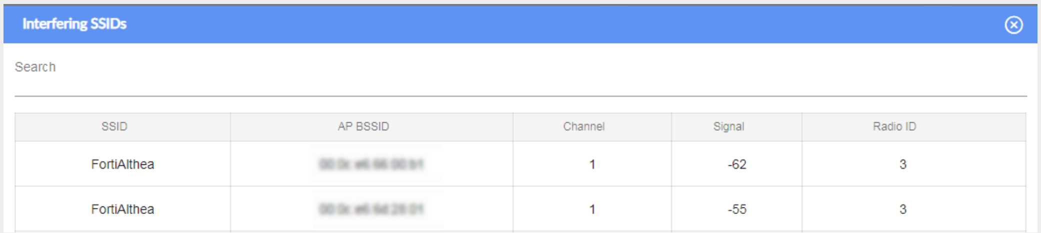
For any selected AP that belongs to a selected controller from the drop-down menus, the configurable threshold settings for Stations are *Average Channel Utilization (%)*,*Average Loss (%)*, *Average SNR*, and *Average Retries (%)*. Depending upon the threshold settings configurations, the information about Stations and the selected AP is graphically charted into panels on the dashboard.

The dashboard generates data at configured time intervals. You can select a duration from the *Date and Time* drop-down list or define a custom time range, and click *Apply* to set that duration.

You can also choose to save the filter settings to access the saved filer later. Click the *Save* button, type a name for the filter, and click *Save*. To make that filter as the default filter, select the *Set as Default Filter* option before you save it.

Dashboard Icons

The dashboard icons allow you to monitor the status and health of the access points. The following icons are available on the dashboard.

<table>
<tr><th>Icons</th><th>Features</th></tr>
<tr><td><b>Locate</b></td><td>Click this icon to view the location of an access point in the heat map. This option is disabled if the access point is not placed on the floor map.</td></tr>
<tr><td><b>Interfering SSIDs</b></td><td>You can view the details of interfering SSIDs associated with an AP; the SSID name, related AP BSSID, channel, signal strength and the Radio ID are displayed in the AP dashboard. To view the interfering SSID details, ensure that the AP radio is configured in the access point mode in FortiGate <i>(Managed FortiAP Profile</i>).

Interfering SSIDs
Search
<table>
<tr><th>SSID</th><th>AP BSSID</th><th>Channel</th><th>Signal</th><th>Radio ID</th></tr>
<tr><td>FortiAlthea</td><td>[redacted]</td><td>1</td><td>-62</td><td>3</td></tr>
<tr><td>FortiAlthea</td><td>[redacted]</td><td>1</td><td>-55</td><td>3</td></tr>
</table>
</td></tr>
<tr><td><b>Spectrum Enabled</b></td><td>Click this icon to view the Spectrum Analyzer, see Spectrum Analyzer on page 22.</td></tr>
<tr><td><b>VLAN Probe</b></td><td>Click this icon to configure VLAN probe on FortiGate controllers only, see VLAN Probe on page 25.</td></tr>
</table>

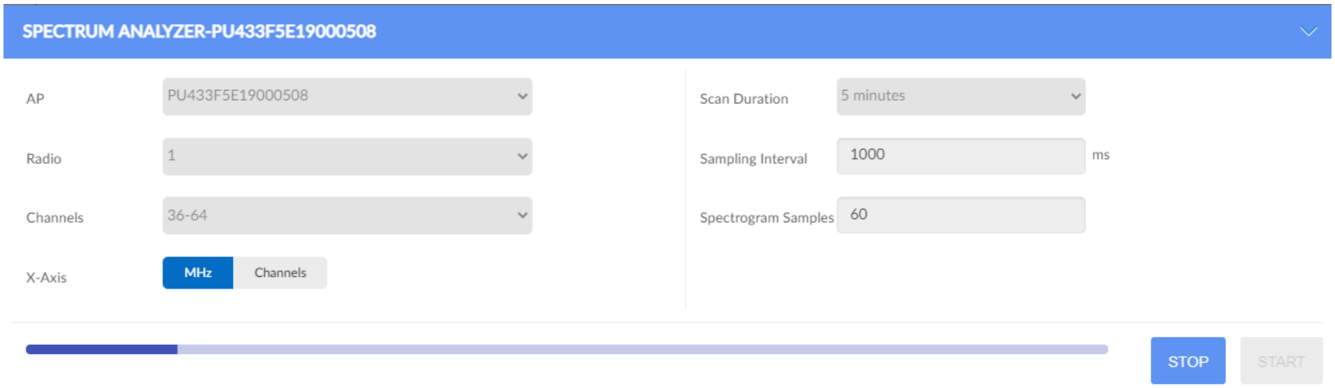
Spectrum Analyzer

The Spectrum Analyzer Dashboard screen presents the interference information gathered from various radios. It provides a graphical representation of the interference devices activity in the 2.4Ghz and 5Ghz spectrum.

Select the channels to be scanned and configure. The spectrum analyzer result displays widgets with the type of interference, signal strength, impacted channels, and spectrum current utilization, start and end time and duration of the interference. It classifies non-WiFi interferences to easy identification of the source.

- You can select the **AP, Radio**, and **Channels** to be scanned for interferences.
- The **Scan Duration** can be set to 1, 5, 30, 60 minutes or Infinite. When Infinite is selected the scan is performed till it is manually stopped.
- The **Sampling Interval** and the number of **Spectrogram Samples** cannot be modified.

Select **Start** and the GUI periodically polls the spectrum analysis data based on the fixed sampling interval of 1000 milliseconds.



SPECTRUM ANALYZER-PU433F5E19000508

AP: PU433F5E19000508

Radio: 1

Channels: 36-64

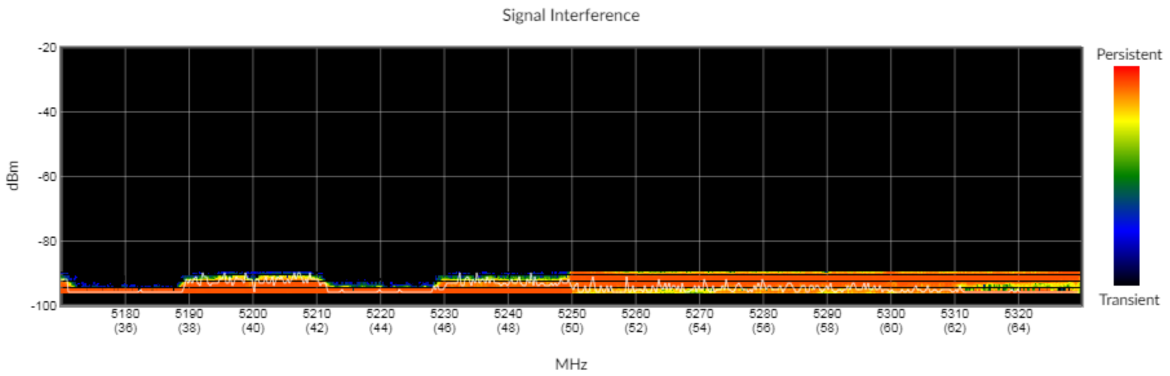
X-Axis: MHz Channels

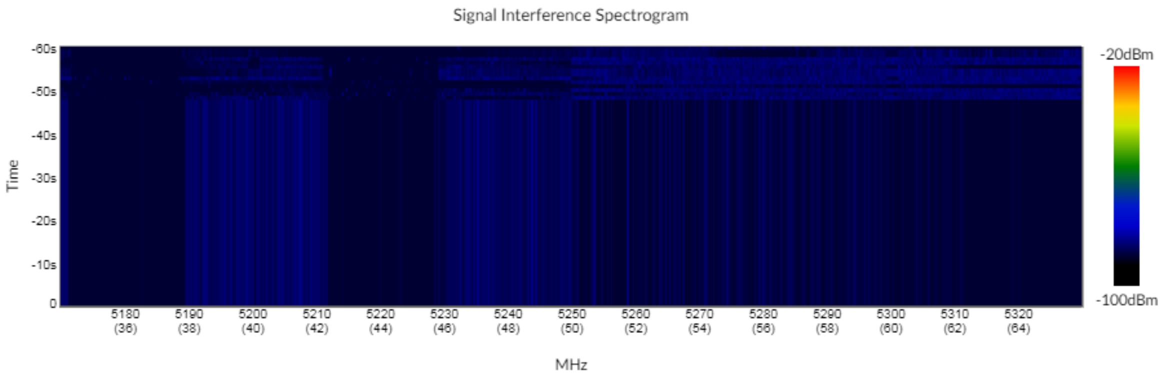
Scan Duration: 5 minutes

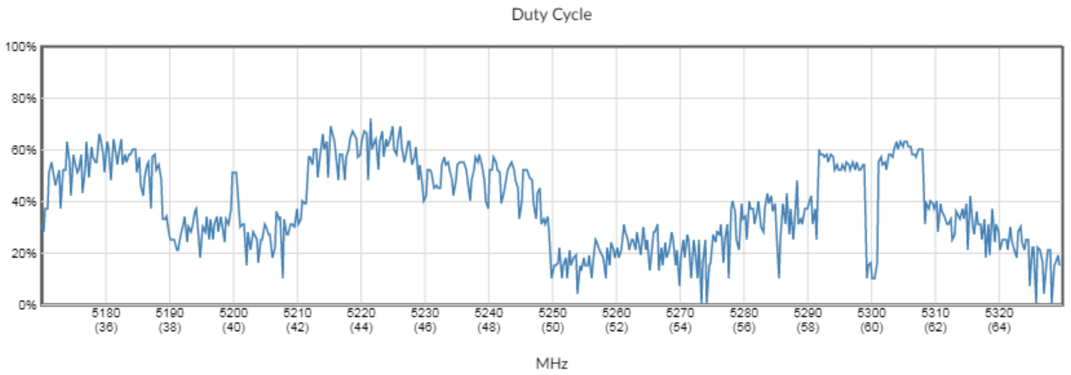
Sampling Interval: 1000 ms

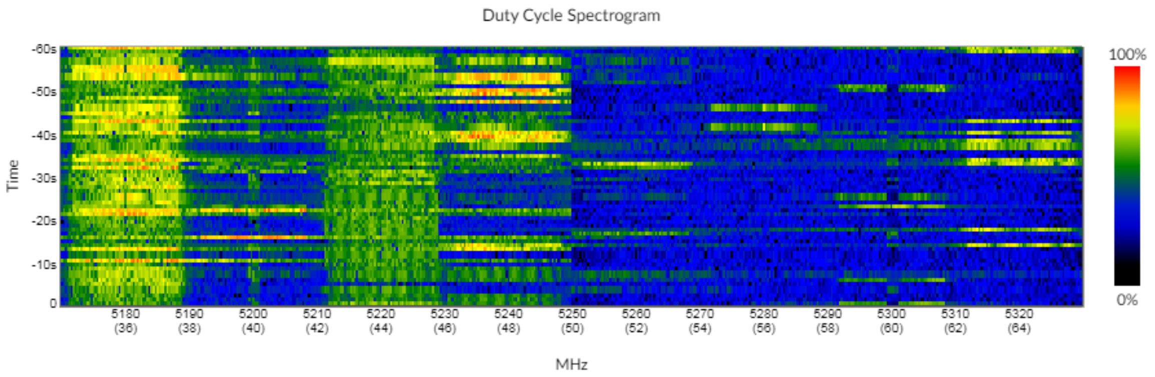
Spectrogram Samples: 60

Data is visualized as 4 charts representing signal interference marking the noise levels for each channel, signal interference spectrogram representing 60 samples for different channels at specific time intervals, the duty cycle charts marking the extent to which a non-WiFi device/neighbouring AP is interfering, and the duty cycle spectrogram representing 60 such duty samples for each channel over a period of time.


Signal Interference
dBm
-20
-40
-60
-80
-100
5180 (36)
5190 (38)
5200 (40)
5210 (42)
5220 (44)
5230 (46)
5240 (48)
5250 (50)
5260 (52)
5270 (54)
5280 (56)
5290 (58)
5300 (60)
5310 (62)
5320 (64)
MHz
Persistent
Transient

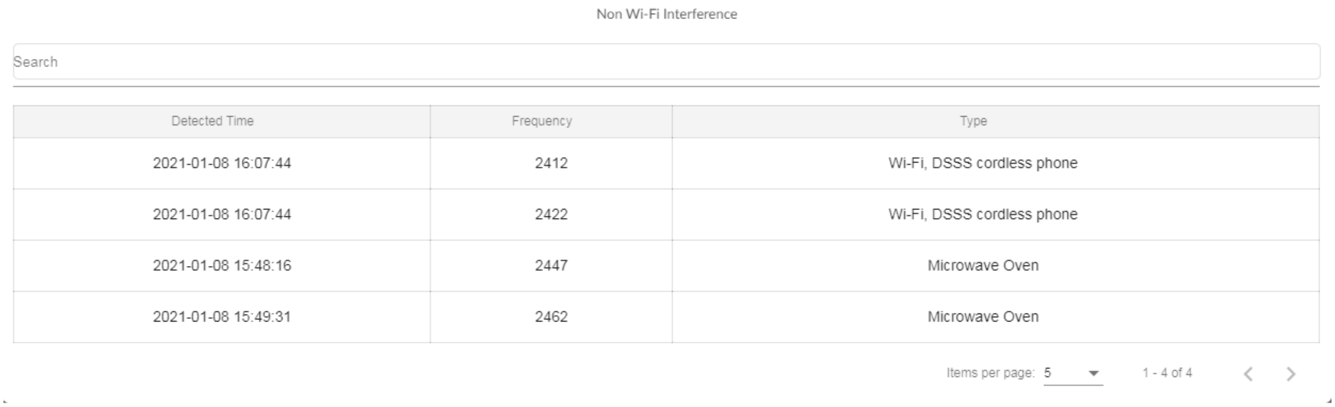

Signal Interference Spectrogram
Time
-60s
-50s
-40s
-30s
-20s
-10s
0
5180 (36)
5190 (38)
5200 (40)
5210 (42)
5220 (44)
5230 (46)
5240 (48)
5250 (50)
5260 (52)
5270 (54)
5280 (56)
5290 (58)
5300 (60)
5310 (62)
5320 (64)
MHz
-20dBm
-100dBm


Duty Cycle
100%
80%
60%
40%
20%
0%
5180 (36)
5190 (38)
5200 (40)
5210 (42)
5220 (44)
5230 (46)
5240 (48)
5250 (50)
5260 (52)
5270 (54)
5280 (56)
5290 (58)
5300 (60)
5310 (62)
5320 (64)
MHz


Duty Cycle Spectrogram
Time
-60s
-50s
-40s
-30s
-20s
-10s
0
5180 (36)
5190 (38)
5200 (40)
5210 (42)
5220 (44)
5230 (46)
5240 (48)
5250 (50)
5260 (52)
5270 (54)
5280 (56)
5290 (58)
5300 (60)
5310 (62)
5320 (64)
MHz
100%
0%

The tabular data for non-WiFi interference displays the time and frequency of last detection and any of the following type interference.

- Microwave Oven
- Video Bridge
- Wi-Fi, DSSS cordless phone
- Bluetooth, FHSS cordless phone



Non Wi-Fi Interference

Detected Time	Frequency	Type
2021-01-08 16:07:44	2412	Wi-Fi, DSSS cordless phone
2021-01-08 16:07:44	2422	Wi-Fi, DSSS cordless phone
2021-01-08 15:48:16	2447	Microwave Oven
2021-01-08 15:49:31	2462	Microwave Oven

Notes:

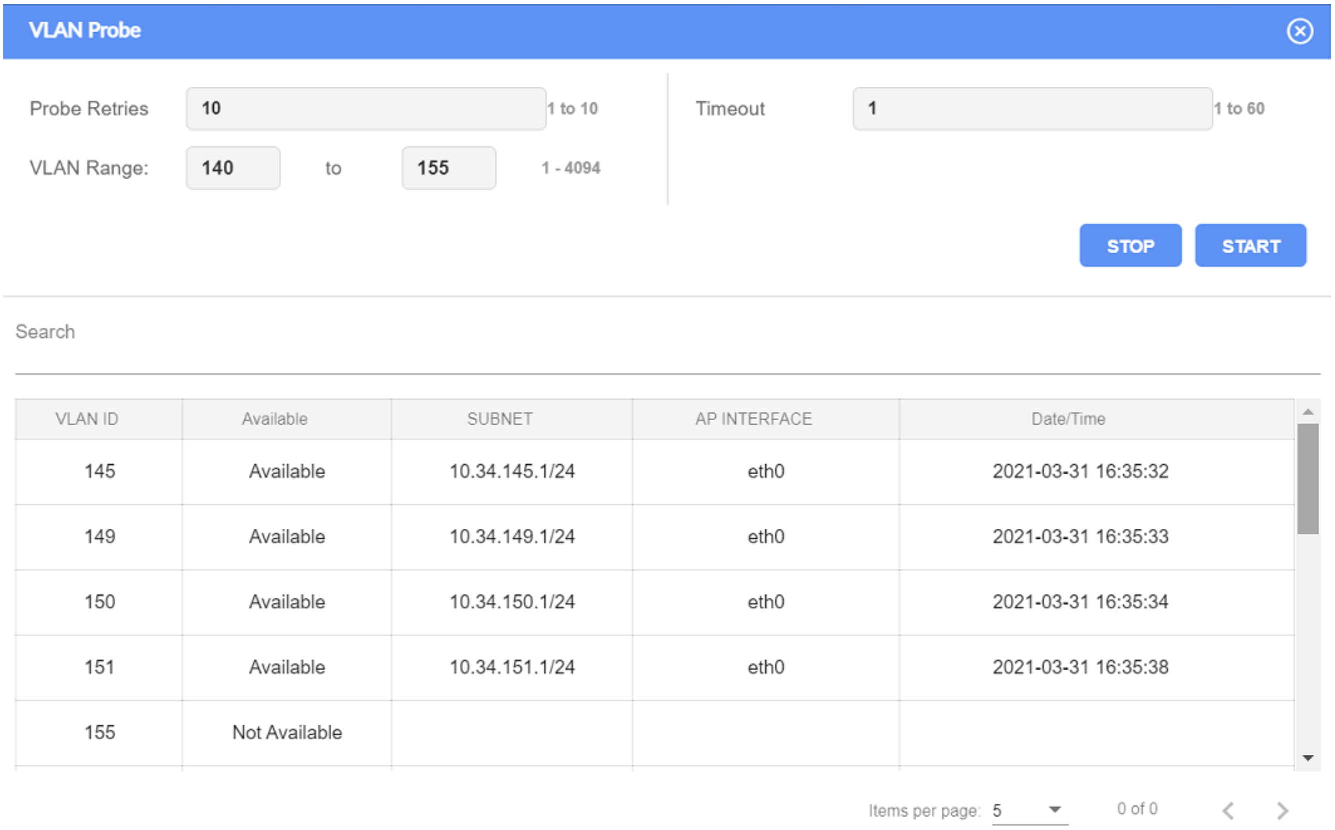
- FAP-U models support Spectrum Analyzer only if the radio is configured in *Dedicated Monitor* mode.
- FAP models support Spectrum Analyzer in AP mode and *Dedicated Monitor* mode; in the AP mode, the radio scans only operating channels.
- FAP-U43xEV supports Spectrum Analyzer only on radio 3 configured in the *Dedicated Monitor* mode.

VLAN Probe

VLAN probe feature enables FortiAPs to probe connected VLANs and subnets. It sends DHCP probes from the FortiAP’s Ethernet interface to specific VLANs on the wired interface and returns information on their availability and subnet details. This helps diagnose and troubleshoot WiFi deployment issues.

- **Probe Retries**: Configure the number of retries before timeout. The valid range is 1 to 10 with a default value of 10.
- **Timeout**: Configure the timeout for the VLAN probe. The valid range is 1 – 60 seconds with a default value of 5 seconds.
- **VLAN Range**: Select the range of VLANs to probe. The valid range is 1 -4094.

Select **Start** and VLAN probe is initiated as per configurations.



VLAN Probe

Probe Retries: 10 (1 to 10)

Timeout: 1 (1 to 60)

VLAN Range: 140 to 155 (1 - 4094)

VLAN ID	Available	SUBNET	AP INTERFACE	Date/Time
145	Available	10.34.145.1/24	eth0	2021-03-31 16:35:32
149	Available	10.34.149.1/24	eth0	2021-03-31 16:35:33
150	Available	10.34.150.1/24	eth0	2021-03-31 16:35:34
151	Available	10.34.151.1/24	eth0	2021-03-31 16:35:38
155	Not Available			

Items per page: 5

0 of 0

Access Point Summary

The information of a selected AP is summarized in the form of on-screen widgets. The first widget displays information like *AP Name*, *Model*, *IP Address*, *Operating Channel*, *Uptime*, *Status*, *Controller Hostname*, *Serial Number*, and so on, and interactive icons to monitor AP health. The second widget displays a graphical representation of the *Average Channel Utilization (%)* and *Average Retries (%)* of the selected AP in the groups of 2.4 GHz and 5 GHz bands. The third widget displays the *Average Noise Level (dBm)*, *Average Throughput (Kbps)*, *Average Loss (%)*, *Memory (%)* and *CPU (%)* utilization, and so on.

This widget data is displayed at configured time intervals. By default, it is ten minutes.

Trends, Statistics, and Top 5 APs

This section of the *Access Point* dashboard graphically represents the statistics of a selected AP. By default, the trend graphs display data for the last two hours. Depending upon the threshold settings configurations and filters, and the panels selected to be displayed, the AP and the corresponding Stations information is graphically charted as follows:

- Stations and Throughput on page 27
- Low Signal Stations on page 27
- High Loss Stations on page 27
- AP Tx and Rx on page 27
- Applications and Stations by Usage on page 27

- Stations Summary on page 27
- Stations and Alarms on page 27

Stations and Throughput

This panel displays a plotting of the total number of stations and the throughput against time. The graph displays the aggregate *Number of Stations* connected to the selected AP and the average *Throughput (Mbps)* at a given time.

Each bar represents the maximum number of stations connected to the selected AP and the average throughput during that interval. Hover over each of the bars to view the station count and throughput during that time interval.

Low Signal Stations

This panel is a trend graph that displays the total number of stations having low SNR and connected to the selected AP. SNR is defined as the signal strength relative to the background noise.

Hover over each of the intervals on the bar graph to see a summary of the maximum number of stations connected and the total number of low signal stations as per the average SNR as configured. You can configure the threshold for *Average SNR* from the available filter options. The graph is plotted based on the configurations.

High Loss Stations

This panel is a trend graph that displays the total number of stations having a High Loss and connected to the selected AP. High Loss is defined as the percentage of the number 802.11 unicast packets transmitted for which no 802.11 acknowledgment is received, which is greater than 40%.

Hover over each of the intervals on the bar graph to see a summary of the maximum number of stations connected and the total number of high loss stations as per the average loss percentage as configured. You can configure the threshold for *Average Loss (%)* from the available filter options. The graph is plotted based on the configurations.

AP Tx and Rx

This panel is a trend graph that displays the average *Tx* and *Rx* utilization (Mbps) of the selected AP.

Applications and Stations by Usage

This panel displays the summary of the applications used the most by the selected AP and also the top five stations with the highest average bandwidth utilization.

Stations Summary

This panel displays the summary of all the stations connected to the selected AP with the classification of stations by OS type. The total count of each of the 5 GHz stations, 2.4 GHz stations, high retries stations, and low SNR stations is displayed.

Stations and Alarms

The *Stations* panel displays the total number of stations connected to the selected AP, and the *Alarms* panel displays the alarms reported for that AP.

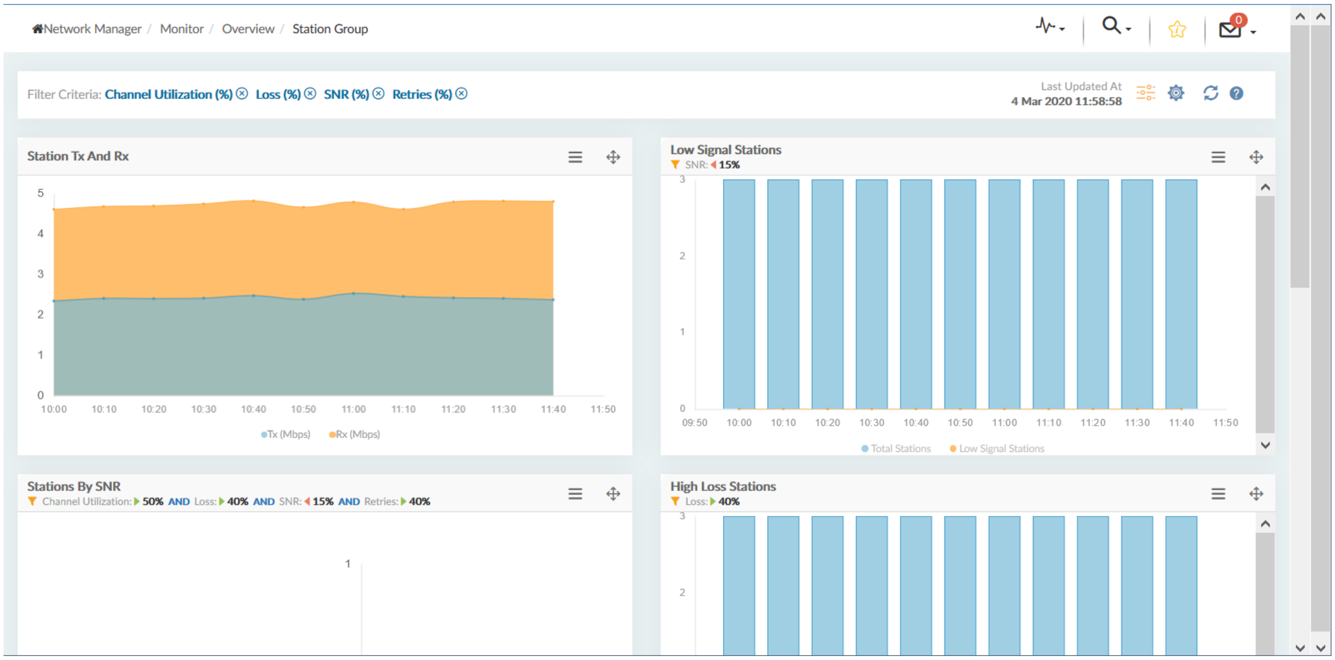
Station Group

The *Station Group* dashboard displays the summary of all the stations within a selected station group. The summary includes the status, activity, and health details of all the stations in a station group.

The data is generated at configured time intervals on the server. By default, the time intervals are: two hours for trend graphs, and ten minutes for other widgets. You can click on each of the stations on the dashboard to navigate to the *Stations* dashboard for that particular station.

The *Station Group* dashboard displays current data from trends, statistics, and top five stations within a stations group.

You can access the *Station Group* dashboard through *Monitor* > *Overview* > *Station Group* .


Network Manager / Monitor / Overview / Station Group

Filter Criteria: Channel Utilization (%) ⊗ Loss (%) ⊗ SNR (%) ⊗ Retries (%) ⊗

Last Updated At 4 Mar 2020 11:58:58

The *Stations Group* dashboard is organized into:

- Dashboard Settings on page 28
- Dashboard Filtering on page 29
- Trends, Statistics, and Top 5 Stations on page 29

Dashboard Settings

The dashboard settings allow you to control the display of widgets or panels on the dashboard. To access the dashboard settings, click the ⚙ button on the upper-right of the *Stations Group* dashboard.

To control which panels are displayed on the dashboard, you can select the required options to filter them from the following available Station Group parameters:

Parameters	Options to filter by
Top 5 Stations	• Applications and Stations • Channel Utilization • Stations by SNR

Parameters	Options to filter by
	• Stations by Retries
Trend	• Low Signal Stations • High Loss Stations • Station Tx and Rx
Statistics	• Stations

Dashboard Filtering

The dashboard provides threshold configuration and filtering capability for stations within the selected Stations Group to graphically represent the information and display statistical charts. To access the threshold configuration and filtering settings, click the ☰ button on the upper-right of the *Stations Group* dashboard.

For any Stations Group selected from the drop-down menu, the configurable threshold settings for Stations are *Average Channel Utilization (%)*,*Average Loss (%)*, *Average SNR*, and *Average Retries (%)*.

You can choose whether all selected threshold settings pass or just one passes, by toggling the slider below the settings for Stations. Depending upon the threshold settings configurations, information about Stations is graphically charted into panels on the dashboard.

The dashboard generates data at configured time intervals. You can select a duration from the *Date and Time* drop-down list or define a custom time range, and click *Apply* to set that duration.

You can also choose to save the filter settings to access the saved filer later. Click the *Save* button, type a name for the filter, and click *Save*. To make that filter as the default filter, select the *Set as Default Filter* option before you save it.

Trends, Statistics, and Top 5 Stations

This section of the *Stations Group* dashboard graphically represents the Stations statistics and trends that belong to a selected Stations Group. By default, the trend graphs display data for the last two hours. Depending upon the threshold settings configurations and filters, and the panels selected to be displayed, the Stations are graphically charted as follows:

- Channel Utilization on page 29
- Applications and Stations on page 30
- Stations by SNR on page 30
- Stations by Retries on page 30
- Low Signal Stations on page 30
- High Loss Stations on page 30
- Stations Tx and Rx on page 30
- Stations on page 30

Channel Utilization

Provides the top five stations in the network that have an average channel utilization greater than the *Average Channel Utilization (%)* setting as configured. The chart displays the name and the corresponding average channel utilization in percentages of stations in the groups of 2.4 GHz and 5 GHz bands.

Click on a station name to navigate to the *Stations* dashboard with the same filter applied.

Applications and Stations

This panel provides the summary of highly used applications and the associated stations within the selected Stations Group, and also the top five stations with the highest average throughput within the Stations Group.

Stations by SNR

This panel groups stations based on the *Average SNR* setting as configured in the filter criteria and lists the top five stations within the group with the lowest average SNR. The stations are classified into *Excellent*, *Good*, *Fair*, and *Bad* categories based on their SNR.

Hover over the bars to view the number of stations in each of the categories. Click on a station name to navigate to the *Stations* dashboard.

Stations by Retries

This panel groups the stations based on the *Average Retries (%)* setting as configured in the filter criteria and lists the top five stations within the group with the highest average retries. The chart displays the name and the corresponding maximum average retries in percentages of stations in the groups of 2.4 GHz and 5 GHz bands.

Low Signal Stations

This panel is a trend graph that displays the total number of stations in the selected Stations Group having low SNR. SNR is defined as the signal strength relative to the background noise.

Hover over each of the intervals on the bar graph to see a summary of the maximum number of stations connected and the total number of low signal stations as per the average SNR as configured. You can configure the threshold for *Average SNR* from the available filter options. The graph is plotted based on the configurations.

High Loss Stations

This panel is a trend graph that displays the total number of stations in the selected Stations Group having a High Loss. High Loss is defined as the percentage of the number 802.11 unicast packets transmitted for which no 802.11 acknowledgment is received, which is greater than 40%.

Hover over each of the intervals on the bar graph to see a summary of the maximum number of stations connected and the total number of high loss stations as per the average loss percentage as configured. You can configure the threshold for *Average Loss (%)* from the available filter options. The graph is plotted based on the configurations.

Stations Tx and Rx

This panel is a trend graph that displays the average *Tx* and *Rx* utilization (Mbps) of all the stations in the selected Stations Group.

Stations

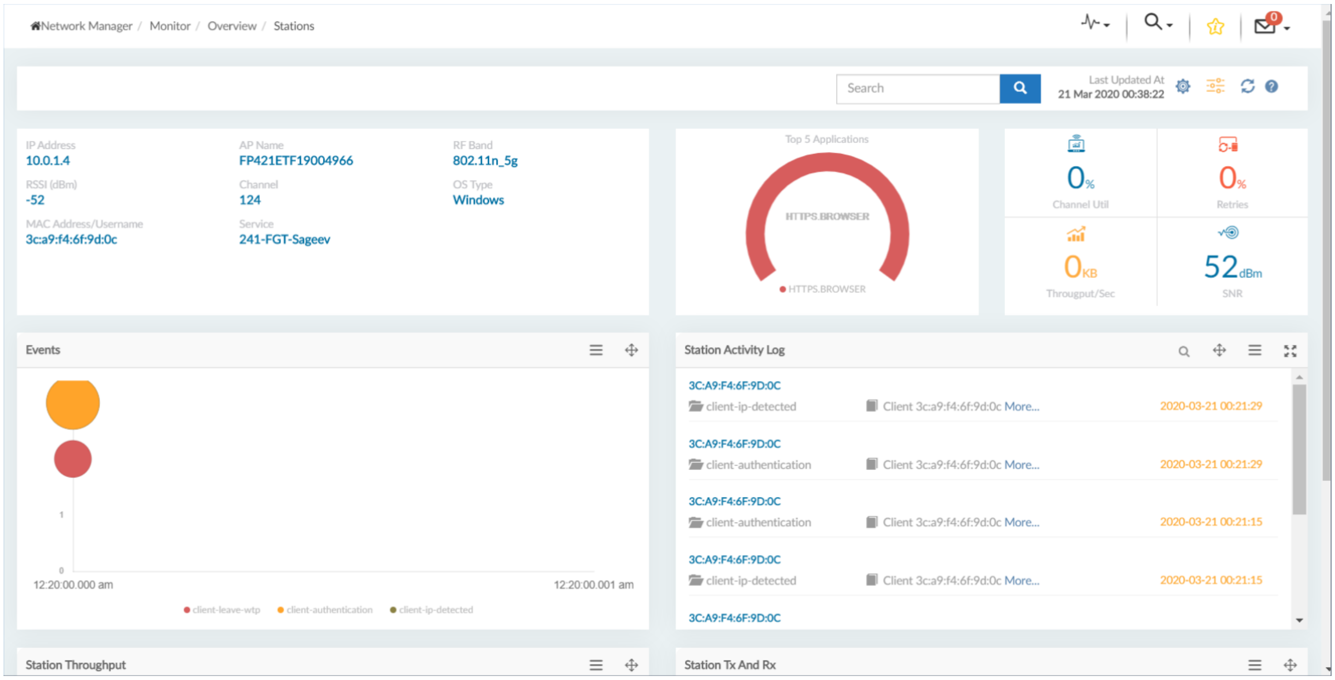
This panel displays the details of all the stations in the selected Stations Group that satisfy the threshold configuration settings and the applied filters. Click on the station name to navigate to the *Stations* dashboard.

Stations

The *Stations* dashboard provides in-depth information about station activity. It provides a graphical representation of the events and the health of stations connected to an AP that is connected to a controller managed by FortiWLM MEA.

The representational data is generated at configured time intervals on the server. By default, the time intervals are: two hours for trend graphs, and ten minutes for other widgets. All the links or pop-up modal screens from the *Stations* dashboard display current data.

You can access the *Stations* dashboard through *Monitor* > *Overview* > *Stations* .



Network Manager / Monitor / Overview / Stations

Last Updated At 21 Mar 2020 00:38:22

IP Address	AP Name	RF Band
10.0.1.4	FP421ETF19004966	802.11n_5g
RSSI (dBm)	Channel	OS Type
-52	124	Windows
MAC Address/Username	Service	
3c:a9:f4:6f:9d:0c	241-FGT-Sageev	

Station Activity Log

```
3C:A9:F4:6F:9D:0C
client-ip-detected          Client 3c:a9:f4:6f:9d:0c More...       2020-03-21 00:21:29
3C:A9:F4:6F:9D:0C
client-authentication       Client 3c:a9:f4:6f:9d:0c More...       2020-03-21 00:21:29
3C:A9:F4:6F:9D:0C
client-authentication       Client 3c:a9:f4:6f:9d:0c More...       2020-03-21 00:21:15
3C:A9:F4:6F:9D:0C
client-ip-detected          Client 3c:a9:f4:6f:9d:0c More...       2020-03-21 00:21:15
3C:A9:F4:6F:9D:0C
```

The *Stations* dashboard is organized into:

- Dashboard Settings on page 31
- Dashboard Filtering on page 32
- Stations Summary on page 32
- Statistics on page 32

Dashboard Settings

The dashboard settings allow you to control the display of widgets and panels on the dashboard. To access the dashboard settings, click the ⚙ button on the upper-right of the *Stations* dashboard.

To control which widgets or panels are displayed on the dashboard, you can select the required options to filter them from the following available Stations parameters:

Parameters	Options to filter by
Statistics	• Events • Station Activity Log

Parameters	Options to filter by
Trend	• Station Throughput • Station Tx and Rx

Dashboard Filtering

The dashboard provides station selection and filtering capability for stations in the wireless network to graphically represent the information and display statistical charts. To access the station selection and filtering settings, click the ☰ button on the upper-right of the *Stations* dashboard.

Station Selection options change based on the *Selection Type* option you choose from the available options like *Controller*, *AP Group*, and *Station Group*. Depending upon which option you choose from the *Selection Type* options, you can narrow down the selection of the required station to monitor.

The dashboard generates data at configured time intervals. You can select a duration from the *Date and Time* drop-down list or define a custom time range, and click *Apply* to set that duration.

Stations Summary

The information of a selected Station is summarized in the form of on-screen widgets. The first widget displays information like *IP Address*, *AP Name*, *RF Band*, *RSSI (dBm)*, *Channel*, *OS Type*, *MAC Address/Username*, *Service*, and so on. The second widget displays a graphical representation of the *Top 5 Applications* of the selected Station. The third widget displays the *Channel Utilization (%)*, *Retries (%)*, *Throughput (Kbps)*, and *SNR (dBm)*.

This widget data is displayed at configured time intervals. By default, it is ten minutes.

Statistics

This section of the *Stations* dashboard graphically represents the statistics of a selected station. By default, the trend graphs display data for the last two hours. Depending upon the threshold settings configurations and filters, and the panels selected to be displayed, the stations information is graphically charted as follows:

- Events on page 32
- Station Throughput on page 32
- Station Tx and Rx on page 33
- Station Activity Log on page 33
- Station Location on page 33

Events

Events are significant occurrences that take place on the managed network. This panel represents the event instances generated based on certain condition. Events such as *Band Steering*, *SIP*, *Diagnostics*, *DHCP*, and so on are displayed.

Station Throughput

This panel displays the combined transmitted and received bytes (Mbps) of a station during the last two hours.

Station Tx and Rx

This panel is a trend graph that displays the average *Tx* and *Rx* utilization (Mbps) of the selected station.

Station Activity Log

This panel displays the station logs or activities of the selected station. It represents station events of all the stations. Most station events are updated almost immediately after the event occurs. The last forty events of the last one hour are available on the server.

Station Location

This panel provides a graphical representation of the number of stations per floor. The floor map allows you to view the movement of stations on a floor in the last twenty four hours using the time-line view, with *play* and *pause* options. By default, the latest location of a station is displayed on the floor map.

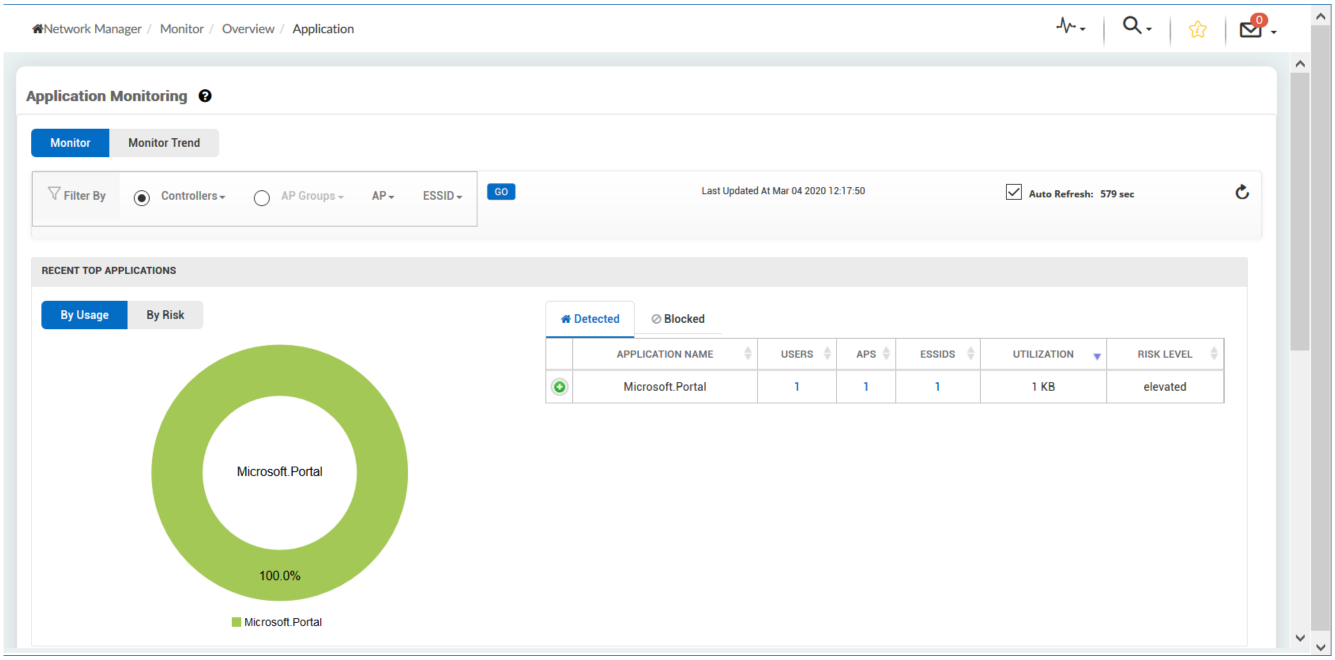
This panel is only available on the dashboard when the location services option is enabled on the system.

Application Monitoring

The *Application Monitoring* dashboard allows you to monitor and/or block traffic for applications in your network. This is made possible by creating policies that can either block and/or monitor application traffic at various access levels for one or more controllers.

The *Application Monitoring* dashboard can only be used to monitor application traffic. Policy configuration must either be done directly on FortiGates or on *AP Manager* in FortiManager.

You can access the *Application Monitoring* dashboard through *Monitor > Overview > Application*.



Network Manager / Monitor / Overview / Application

Application Monitoring

Filter By ● Controllers ○ AP Groups AP ESSID GO

Last Updated At Mar 04 2020 12:17:50

☑ Auto Refresh: 579 sec

RECENT TOP APPLICATIONS

	APPLICATION NAME	USERS	APS	ESSIDS	UTILIZATION	RISK LEVEL
⊕	Microsoft.Portal	1	1	1	1 KB	elevated

The *Application Monitoring* dashboard is organized into the following two tabs:

- Monitor on page 34
- Monitor Trend on page 35

Monitor

The *Monitor* tab allows you to monitor network traffic by applications and users (clients). You can filter to view the applications and users either by *Controllers* or *AP Groups*, and then selecting the desired *APs* and/or *ESSIDs*. The most recent top applications and users are displayed in separate panels below the filtering options on the *Monitor* tab. Applications and users can be monitored either by usage or by risk.

Monitoring by usage

You can monitor network traffic by usage for applications or users by clicking on the *By Usage* tab within the *RECENT TOP APPLICATIONS* or *RECENT TOP USERS* panels. Each of these panels display a pie chart and a table with data from the top ten applications or users.

Hover over the pie slices to see traffic usage in percentage of an application or a user.

The table in the *RECENT TOP APPLICATIONS* panel enlists the top ten applications, *Detected* and *Blocked*, for each of which you can view the following:

- Application Name
- Number of users using the application
- Number of APs serving the users using the application
- Number of ESSIDs of users using the application
- Total traffic utilization in MB
- The associated risk level of the application

The table in the *RECENT TOP USERS* panel enlists the top ten users, for each of which you can view the following:

- Serial Number
- Number of applications used
- Number of APs serving the users using the application
- Number of ESSIDs of users using the application
- Total traffic utilization in MB

Monitoring by risk

Click the *By Risk* tab within each of the panels to group applications and users based on their risk values and usage information. Applications and users are assigned with *low*, *elevated*, *medium*, *high*, or *critical* risk values.

The pie charts group the applications and users based on their risk values. Click on each of these risk values on the pie chart to view the top ten applications/users in that category along with their usage.

Each of the tables in both the panels display the total traffic utilization along with either the application name or the serial number, depending upon which panel you are monitoring by risk.

Monitor Trend

The *Monitor Trend* tab displays network traffic by applications and users trends. Click on the *Monitor Trend* tab on the *Application Monitoring* dashboard to view the trends. The filtering options remain the same as on the *Monitor* tab.

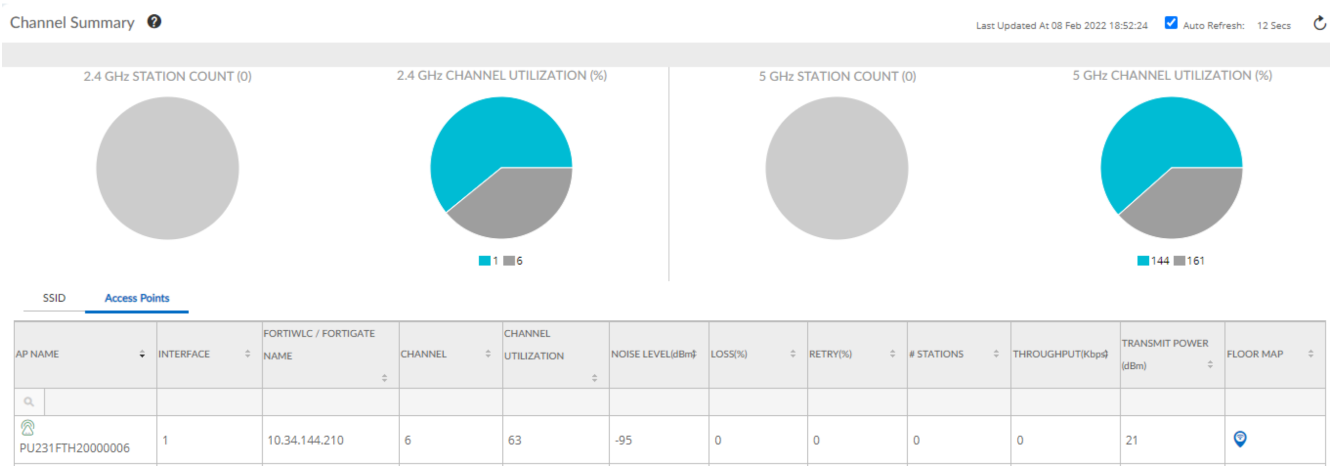
The applications and users trends are represented graphically in the form of bar graphs. The total *Throughput (MB)* is plotted against the reporting period. The reporting period may be selected to be: two hours (*2h*), one day (*1d*), one week (*1w*), one month (*1m*), or a custom date range, from the upper-right section of the panels.

The trend graph data is maintained only for the last thirty days.

Channel Summary

This dashboard displays detailed summary of channel utilization. The pie charts provide a breakup of channel usage on 2.4 Ghz and 5 Ghz radios. For each of the radios two pie charts are displayed..

- **Station Count** - The number of stations connected to a specific channel in the radio.
- **Channel Utilization** - The total channel utilization (in percentage) of a channel in the radio.


Channel Summary
Last Updated At 08 Feb 2022 18:52:24
☑ Auto Refresh: 12 Secs
2.4 GHz STATION COUNT (0)
2.4 GHz CHANNEL UTILIZATION (%)
1
6
5 GHz STATION COUNT (0)
5 GHz CHANNEL UTILIZATION (%)
144
161
SSID
Access Points

AP NAME	INTERFACE	FORTIWLC / FORTIGATE NAME	CHANNEL	CHANNEL UTILIZATION	NOISE LEVEL(dBm)	LOSS(%)	RETRY(%)	# STATIONS	THROUGHPUT(Kbps)	TRANSMIT POWER (dBm)	FLOOR MAP
PU231FTH20000006	1	10.34.144.210	6	63	-95	0	0	0	0	21	

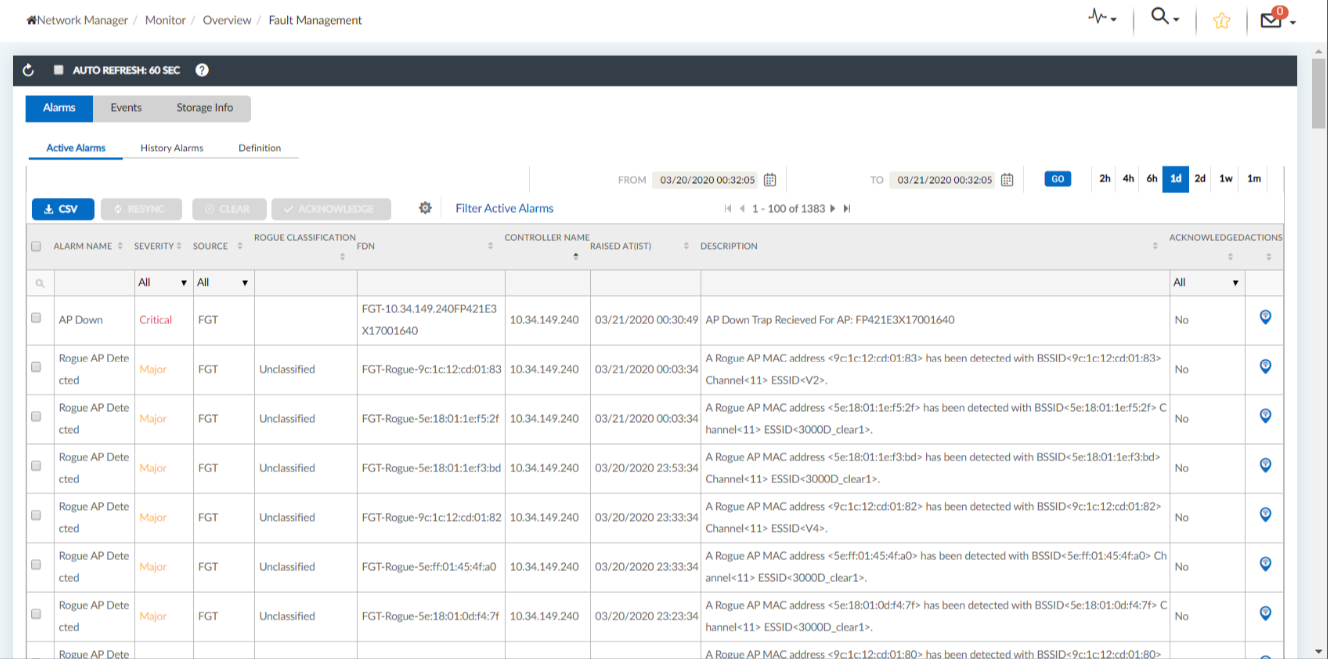
The *SSID* and *Access Points* tabs provide details on various channel utilization parameters. The *SSID* tab sorts and filters data based on the SSID and the *Access Points* tab sorts and list data based on APs.

- **SSID** - The name of the SSID in your network.
- **FortiGate Name** - The IP address of the controller that terminates the AP with this SSID.
- **AP Count** - The number of AP's broadcasting this SSID.
- **Channel** - The channel numbers that are in use of this SSID.
- **Stations** - The number of stations that are connected to this SSID.
- **Throughput** - The total throughput of traffic passing through this SSID.
- **AP Name** - The name of AP's connected to the SSID.
- **Interface** - The Ethernet interface terminating at the controller.
- **Channel** - The channel number in use for this AP.
- **Channel Utilization** - Total channel utilization (in percentage) by the AP.
- **Noise Level (dBM)** - Noise level as detected by the AP.
- **Loss (%)** - The transmit loss percentage.
- **Retry (%**) - The retry percentage.
- **Stations** - Number of stations connected to this AP
- **Throughput (Kbps)** - Total throughput of traffic passing through this AP
- **Transmit Power** - The AP's transmission power.
- **Floor Map** - Click the icon to get the physical location of the AP.

Fault Management

The *Fault Management* dashboard is used to detect the faults encountered in the network. The detected faults may be notified as *Alarms*.

You can access the *Fault Management* dashboard through *Monitor* > *Overview* > *Fault Management*.



□	ALARM NAME	SEVERITY	SOURCE	ROGUE CLASSIFICATION	FDN	CONTROLLER NAME	RAISED AT(IST)	DESCRIPTION	ACKNOWLEDGED	ACTIONS
		All	All						All	
□	AP Down	Critical	FGT		FGT-10.34.149.240FP421E3X17001640	10.34.149.240	03/21/2020 00:30:49	AP Down Trap Recieved For AP: FP421E3X17001640	No	
□	Rogue AP Detected	Major	FGT	Unclassified	FGT-Rogue-9c:1c:12:cd:01:83	10.34.149.240	03/21/2020 00:03:34	A Rogue AP MAC address <9c:1c:12:cd:01:83> has been detected with BSSID<9c:1c:12:cd:01:83> Channel<11> ESSID<V2>.	No	
□	Rogue AP Detected	Major	FGT	Unclassified	FGT-Rogue-5e:18:01:1e:f5:2f	10.34.149.240	03/21/2020 00:03:34	A Rogue AP MAC address <5e:18:01:1e:f5:2f> has been detected with BSSID<5e:18:01:1e:f5:2f> Channel<11> ESSID<3000D_clear1>.	No	
□	Rogue AP Detected	Major	FGT	Unclassified	FGT-Rogue-5e:18:01:1e:f3:bd	10.34.149.240	03/20/2020 23:53:34	A Rogue AP MAC address <5e:18:01:1e:f3:bd> has been detected with BSSID<5e:18:01:1e:f3:bd> Channel<11> ESSID<3000D_clear1>.	No	
□	Rogue AP Detected	Major	FGT	Unclassified	FGT-Rogue-9c:1c:12:cd:01:82	10.34.149.240	03/20/2020 23:33:34	A Rogue AP MAC address <9c:1c:12:cd:01:82> has been detected with BSSID<9c:1c:12:cd:01:82> Channel<11> ESSID<V4>.	No	
□	Rogue AP Detected	Major	FGT	Unclassified	FGT-Rogue-5e:ff:01:45:4f:a0	10.34.149.240	03/20/2020 23:33:34	A Rogue AP MAC address <5e:ff:01:45:4f:a0> has been detected with BSSID<5e:ff:01:45:4f:a0> Channel<11> ESSID<3000D_clear1>.	No	
□	Rogue AP Detected	Major	FGT	Unclassified	FGT-Rogue-5e:18:01:0d:f4:7f	10.34.149.240	03/20/2020 23:23:34	A Rogue AP MAC address <5e:18:01:0d:f4:7f> has been detected with BSSID<5e:18:01:0d:f4:7f> Channel<11> ESSID<3000D_clear1>.	No	
	Rogue AP Dete							A Rogue AP MAC address <9c:1c:12:cd:01:80> has been detected with BSSID<9c:1c:12:cd:01:80>		

The *Fault Management* dashboard is composed of the following three tabs:

- Alarms on page 37
- Events on page 40
- Storage Info on page 41

Alarms

An *Alarm* is defined as a persistent fault in the network. Each alarm can be raised multiple times on different objects. No new alarms can be raised on the same object until the old alarm is cleared. The same alarm on the same object can be raised with different severity levels. During such scenarios, the new alarm will clear the old alarm.

Each alarm consists of two states:

- Active state: A raised alarm is always in the active state
- Cleared state: Raised alarms can be cleared by the module through which they were raised or you can manually clear them.

The Alarms tab is composed of the following sub-tabs:

- Active Alarms on page 37
- History Alarms on page 39
- Definition on page 40

Active Alarms

The *Active Alarms* sub-tab displays all the *Critical*, *Major*, *Minor*, and *Information* alarms. The Active Alarms table summarizes the following:

Field	Description
Alarm Name	Displays the name of the alarm.
Severity	Displays the severity level of an alarm. The various severity levels are as follows: - Critical Alarms: Critical alarms are represented by a red color indicator, like `Critical`, and need immediate action. Typical critical alarms are raised either when a controller or an AP is down, or when a rogue AP is detected. The rogue alarm is raised when a wired rogue is detected. - Major Alarms: Major alarms are represented by an orange color indicator, like `Major`, and need action whenever required. Typical major alarms are raised due to authentication failure. - Minor Alarms: Minor alarms are represented by a yellow color indicator, like `Minor`, and do not require any action. Typical minor alarms are raised due to MIC errors. - Information Alarms: Information alarms are represented by a blue color indicator, like `Information`, and are for information only. They do not require any action.
Source	The source where an alarm is raised: *AP*, *Controller*, or *NM*.
FDN (Full Distinguished Name)	FDN identifies the name of the device that triggered the alarm.
Controller	Provides the controller IP address or host name.
Raised At	Displays the date and time at which the alarm was raised, in MM/DD/YYYY HH:MM:SS format. The displayed date and time will be in the system default time zone. To change the time zone, click ⚙ > *Change Timezone*, and select the required option.
Description	Provides detailed information regarding the alarm, including identifying device details.
Acknowledged	Displays *Yes* if you have acknowledged a raised alarm. By default, it is set to *No*.
Actions	All AP related alarms display an AP location icon in the *Actions* column. Click on the icon to see the AP locator screen displaying the selected AP located on the floor.

You can select one or more active alarms and either *Clear* or *Acknowledge* them.

Clearing active alarms

To clear active alarms:

1. Select one or more active alarms.
2. Click on the *Clear* button. The *Clear Alarm* dialog is displayed with the following options:

Field	Description
User Name	Displays the username of the logged-in user.
Date	Displays the current date and time, in MM/DD/YYYY HH:MM:SS format.

Field	Description
Comment	You must add comments while clearing an alarm. It is mandatory to add a comment.

3. Add a comment and click on the *Clear* button.

After you clear an active alarm, FortiWLM MEA sends the *clear alarm* notification to *System Director* for those alarms which are cleared manually.

Acknowledging active alarms

To acknowledge active alarms:

1. Select one or more active alarms.
2. Click on the *Acknowledge* button. The *Acknowledge Alarm* dialog is displayed with the following options:

Field	Description
User Name	Displays the username of the logged-in user.
Date	Displays the current date and time, in MM/DD/YYYY HH:MM:SS format.
Comment	You must add comments while clearing an alarm. It is mandatory to add a comment. A comment added while alarm acknowledgment may be modified.

3. Add a comment and click on the *Acknowledge* button.

After you acknowledge an active alarm, FortiWLM MEA sends the *acknowledge alarm* notification to *System Director* for those alarms which are acknowledged manually.

To see the active alarms in a CSV format, select one or more active alarms and click on the *CSV* button. The *Active Alarms: CSV* dialog is displayed. You may also download the list of active alarms in CSV format by clicking on the *Download* button.

The *Filter Active Alarms* button allows you to filter alarms based on specified values for the available alarms attributes. You can filter using one or more attributes simultaneously; for example, you can filter alarms by specifying the *Alarm Name*, and then selecting the *Source*. You may save or reset the current filter settings by clicking the appropriate buttons. You may also filter alarms raised in a specific time range by selecting the appropriate time range or by clicking the predefined time periods.

History Alarms

The *History Alarms* sub-tab displays all the cleared alarms from the *Active Alarms* sub-tab. The *History Alarms* sub-tab is similar to the *Active Alarms* sub-tab in all aspects except for the tables on these sub-tabs, which are almost similar as well. The only differences being the addition of the *Cleared At* column and the deletion of the *Actions* column.

The *Cleared At* column displays the date and time at which the alarm was cleared, in MM/DD/YYYY HH:MM:SS format.

The displayed date and time will be in the system default time zone. To change the time zone, click ⚙ > *Change Timezone*, and select the required option.

All other options on the *History Alarms* sub-tab remain the same as the *Active Alarms* sub-tab.

Definition

The *Definition* sub-tab displays a table with various alarm definitions along with a summary of additional alarm attributes. The alarms definition table shows various alarms attributes like *Alarm Name*, *Description*, *Severity*, *Source*, *Triggering Condition*, and *Triggering Threshold*.

If you select an alarm from the table and click on the *Edit* button, or if you click on an alarm name from the table, the *Configure Alarm* dialog appears. The *Configure Alarm* dialog summarizes *Alarm info*, *Alarm Options*, and *Trigger Condition*. The *Trigger Condition* field is only available for alarms that belong to FortiWLM MEA, and you can specify a value for the *Threshold* field for those alarms.

Events

Events are significant occurrences that take place on the wireless network. Event instances are generated based on triggering conditions. Each event can be generated multiple times.

The *Events* tab is composed of the following two sub-tabs:

- Events on page 40
- Definition on page 41

Events View

The *Events View* sub-tab displays all the *Critical*, *Major*, *Minor*, and *Information* events. The Events View table summarizes the following:

Field	Description
Event Name	Displays the name of the event and what it is about.
Severity	Displays the severity level of an event. The various severity levels are as follows: • Critical Events: Critical events are represented by a red color indicator, like `Critical`, and need immediate action. Typical critical events are generated either when a controller or an AP is down. • Major Events: Major events are represented by an orange color indicator, like `Major`, and need action whenever required. Typical major events are generated due to authentication failure. • Minor Events: Minor events are represented by a yellow color indicator, like `Minor`, and do not require any action. Typical minor events are generated due to MIC errors. • Information Evenst: Information alarms are represented by a blue color indicator, like `Information`, and are for information only. They do not require any action.
Source	The source where an event is generated: *AP*, *Controller*, or *NM*.
FDN (Full Distinguished Name)	FDN identifies the name of the device that triggered the event.
Controller	Provides the controller IP address or host name.
Generated At	Displays the date and time at which the event was generated, in MM/DD/YYYY HH:MM:SS format.

Field	Description
	The displayed date and time will be in the system default time zone. To change the time zone, click ⚙ > *Change Timezone*, and select the required option.
Description	Provides detailed information regarding the generated event.

To see the events in a CSV format, select one or more events and click on the *CSV* button. The *Events: CSV* dialog is displayed. You may also download the list of events in CSV format by clicking on the *Download* button.

The *Filter Events* button allows you to filter events based on specified values for the available events attributes. You can filter using one or more attributes simultaneously; for example, you can filter events by specifying the *Event Name*, and then selecting the *Source*. You may save or reset the current filter settings by clicking the appropriate buttons. You may also filter events raised in a specific time range by selecting the appropriate time range or by clicking the predefined time periods.

Definition

The *Definition* sub-tab displays a table with various events definitions along with a summary of additional events attributes. The events definition table shows various events attributes like *Event Name*, *Description*, *Severity*, *Source*, *Triggering Condition*, and *Triggering Threshold*.

If you select an event from the table and click on the *Edit* button, or if you click on an event name from the table, the *Configure Event* dialog appears. The *Configure Event* dialog summarizes *Event info*, *Event Options*, and *Trigger Condition*. The *Trigger Condition* field is only available for events that belong to FortiWLM MEA, and you can specify a value for the *Threshold* field for those events.

Storage Info

The *Storage Info* tab displays the storage configuration details for *Events* and *History Alarms*.

In both the *Events* and the *History Alarms* sections, the following fields are displayed:

Field	Description
Storage Capacity	Displays the maximum number of events or alarms that can be stored in the database. The maximum storage capacity is 2000000 rows for alarms and 4000000 rows for events.
Current Usage	Displays the current usage of events or alarms storage in percentage.

Additionally, there are *Purge Options* available in both the *Events* and *History Alarms* sections, which are as follows:

Field	Description
Number of events/alarms to keep after every purge	Displays the percentage of events/alarms to be retained after purge.
Schedule Purge	Displays the scheduled time of purge for events/alarms. Select the desired time from the

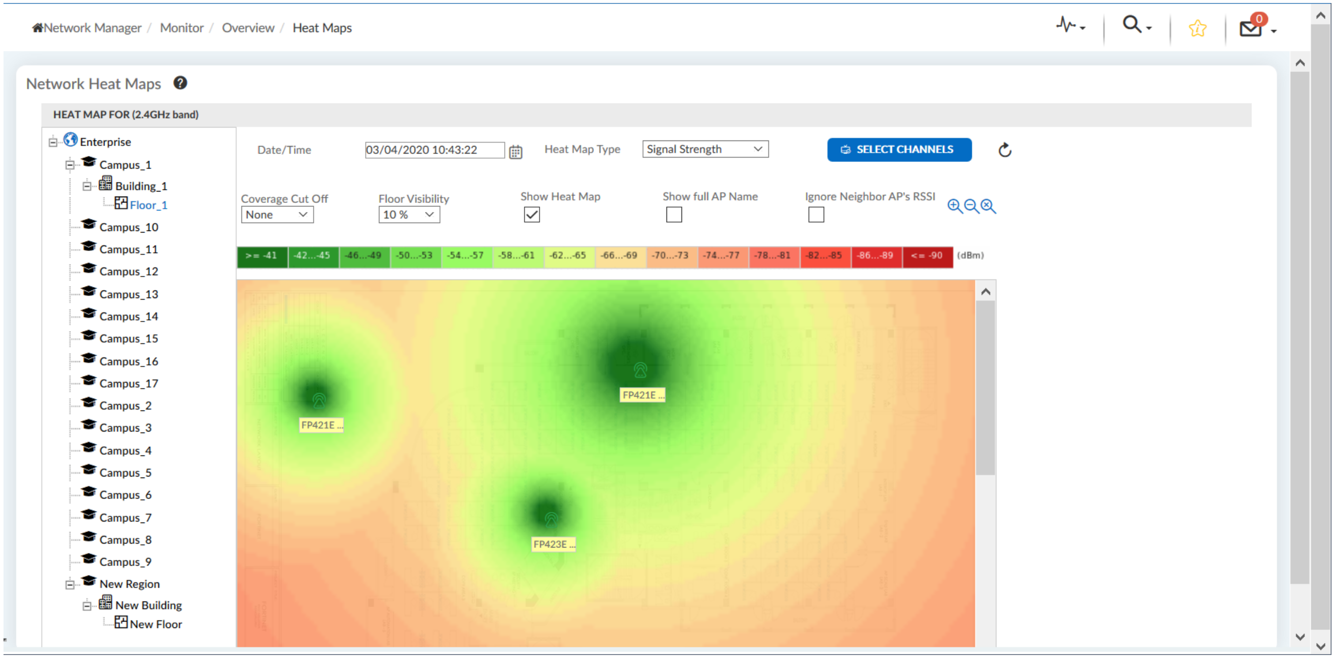
Field	Description
	drop-down menu to purge events/alarms daily at the specified time.
Enable Auto System Purge	Select this option to enable automatic purging of events/alarms once usage reaches 99%.

You may also click on the *Purge Now* button to purge the events/alarms with the options as selected. To save or reset the configurations, click *Save* or *Reset* respectively.

Network Heat Maps

The *Network Heat Maps* dashboard provides a visualization feature allowing you to check the coverage and performance of APs in the wireless network. The dashboard displays actual AP statistics retrieved from the controller, extrapolated into graphic files known as *Heat Maps*. Heat maps can be generated for historical data.

You can access the *Network Heat Maps* dashboard through *Monitor* > *Overview* > *Heat Maps*.



Network Manager / Monitor / Overview / Heat Maps

Network Heat Maps

HEAT MAP FOR (2.4GHz band)

Date/Time 03/04/2020 10:43:22

Heat Map Type Signal Strength

Coverage Cut Off None

Floor Visibility 10 %

Show Heat Map ☑

Show full AP Name □

Ignore Neighbor AP's RSSI □

By default, heat maps are displayed for the current time. The *Date/Time* field allows you to choose a custom date/time.

Select a floor from the left tree menu on the dashboard to view the heat map associated to that floor. The *Heat Map Type* selection allows you to view the following five types of heat maps:

- Throughput: The *Throughput* heat map uses different colors for regions around APs corresponding to the AP Throughput value.
- Loss: The *Loss* heat map uses different colors for regions around APs corresponding to the AP Loss value.
- Channel Utilization: The *Channel Utilization* heat map uses different colors for regions around APs corresponding to the AP channel utilization value.
- Number of Stations: The *Number of Stations* heat map uses different colors for regions around APs corresponding to the number of stations per AP.
- Signal Strength: The *Signal Strength* heat map shows the availability of signal over any area represented by the floor map. Select different *Coverage Cut Off* values to view the corresponding signal coverage.

> To represent accurate signal values for all the APs located on the floor, FortiWLM MEA displays a *Signal Strength* heat map for all the APs, irrespective of whether the logged in user has access rights for those APs or not.

You can control the visibility of a heat map by selecting an option from the *Floor Visibility* drop-down list. Select or deselect the *Show Heat Map* checkbox to toggle the display of the selected heat map.

By default, data from all the channels is used to generate heat maps. To view heat maps from specific channels:

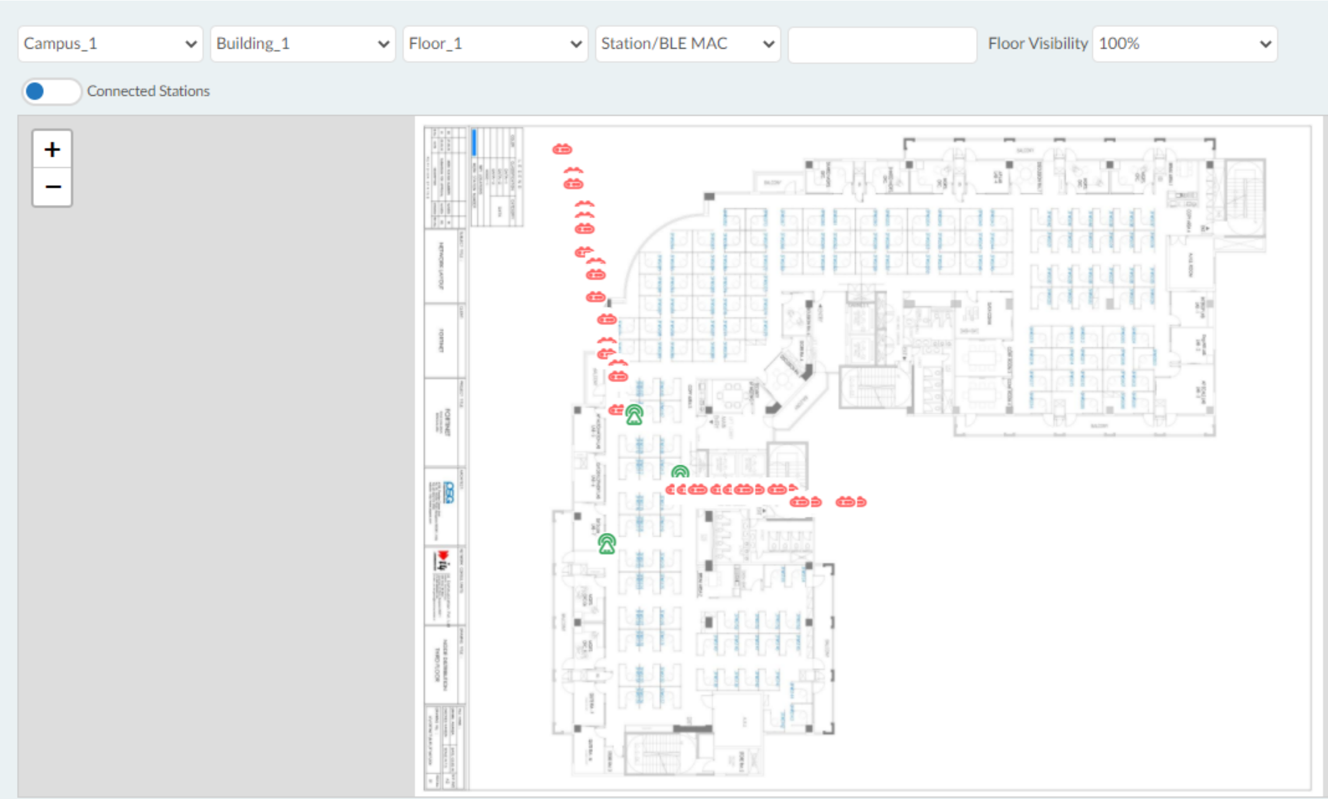
1. Click on the *Select Channels* button in the upper-right section of the panel. The *Select Channels* dialog appears.
2. Select an option from the available options:
   a. *All*. This option is selected by default.
   b. *2.4 GHz (Channels <= 11)*
   c. *5 GHz (Channels >= 36)*
   d. *Selected*. If you choose this option, select the required checkboxes for the available channels below it.
3. Click *Save*. The *Select Channels* dialog disappears.
4. Click on the ↻ button next to the *Select Channels* button to refresh the heat map view.

Location Services

The locationing feature plots the current location of all stations/rogue APs on the floor map imported into FortiWLM MEA. FortiWLM MEA plots the current location based on the location feed received from APs and does not display the movement of the devices. You can filter and view device locations based on the site, building, and floor. You can access the *Location Services* screen through *Monitor* > *Overview* > *Location Services*. The following filter can also be applied.

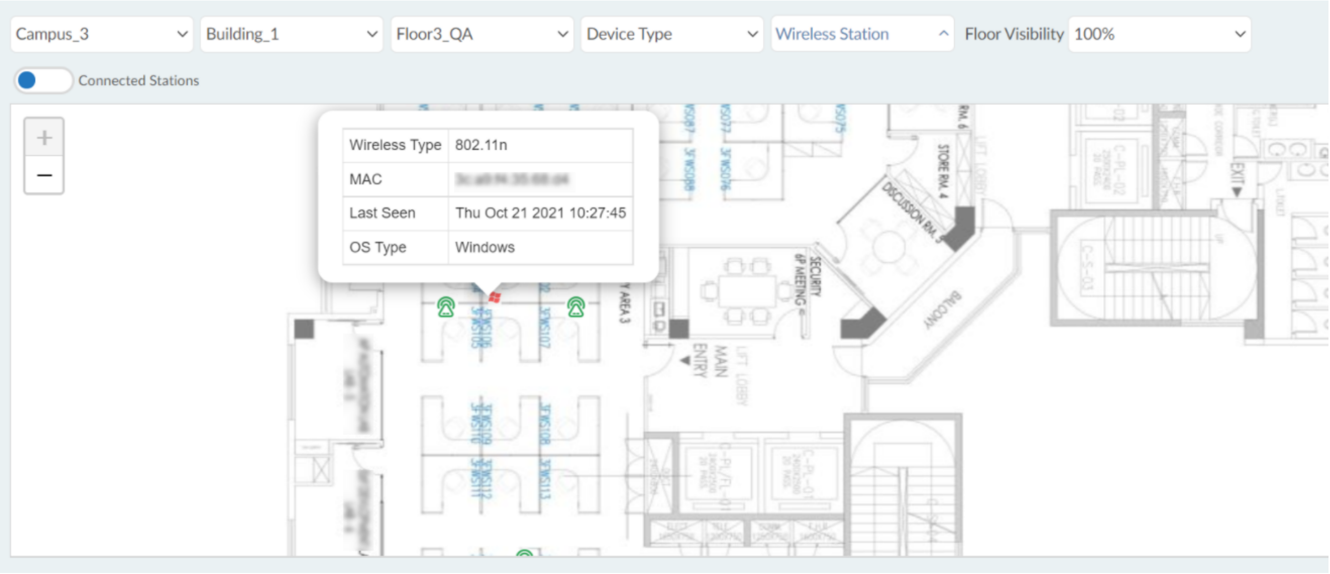
- Device Type
- Wireless Type
- OS Type
- Station MAC
- Station/BLE MAC
- Accuracy
- Rogue MAC

You can set the **Floor Visibility** and magnify the floor view.



Campus_1 | Building_1 | Floor_1 | Station/BLE MAC | Floor Visibility 100%

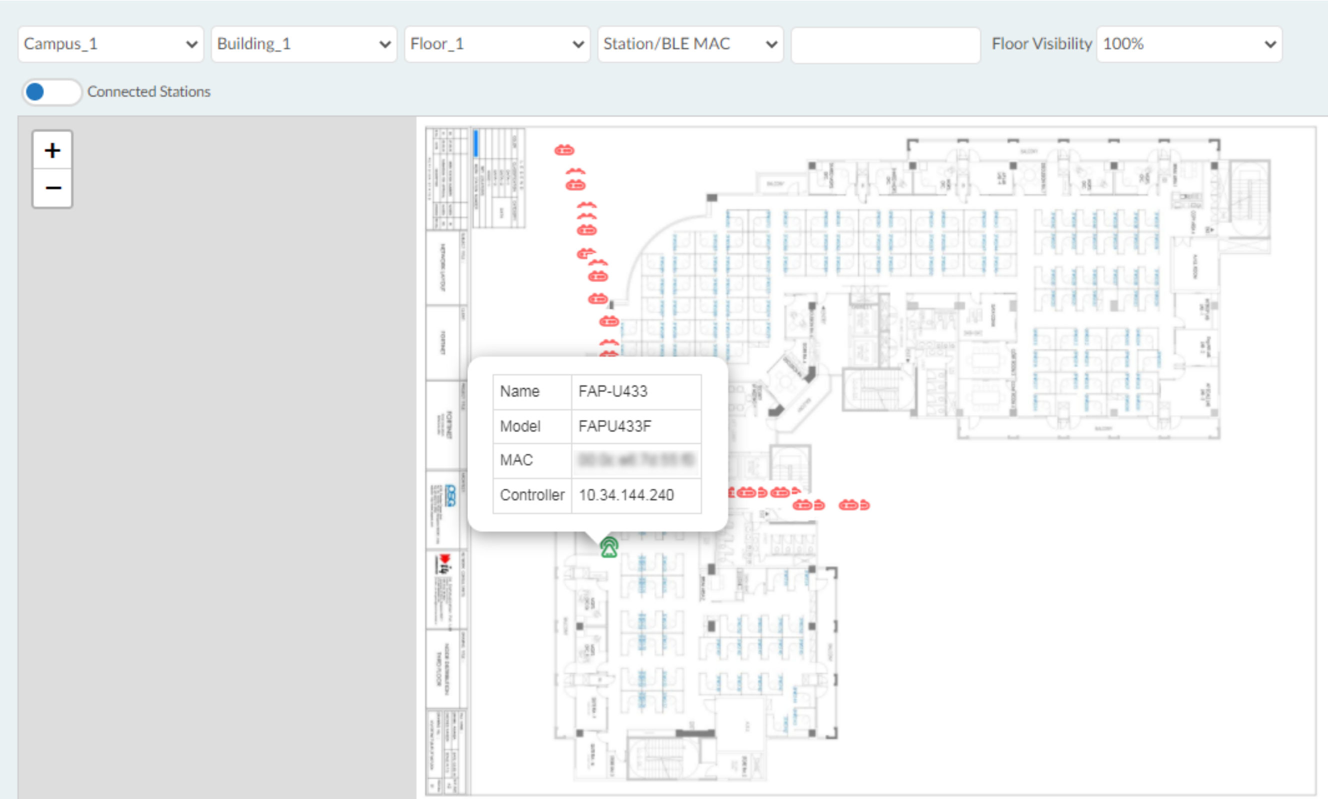
Connected Stations



Campus_3 | Building_1 | Floor3_QA | Device Type | Wireless Station | Floor Visibility 100%

Connected Stations

Wireless Type	802.11n
MAC	[redacted]
Last Seen	Thu Oct 21 2021 10:27:45
OS Type	Windows



Campus_1

Building_1

Floor_1

Station/BLE MAC

Floor Visibility: 100%

Connected Stations

Name	FAP-U433
Model	FAPU433F
MAC	[redacted]
Controller	10.34.144.240

Detailed Dashboard

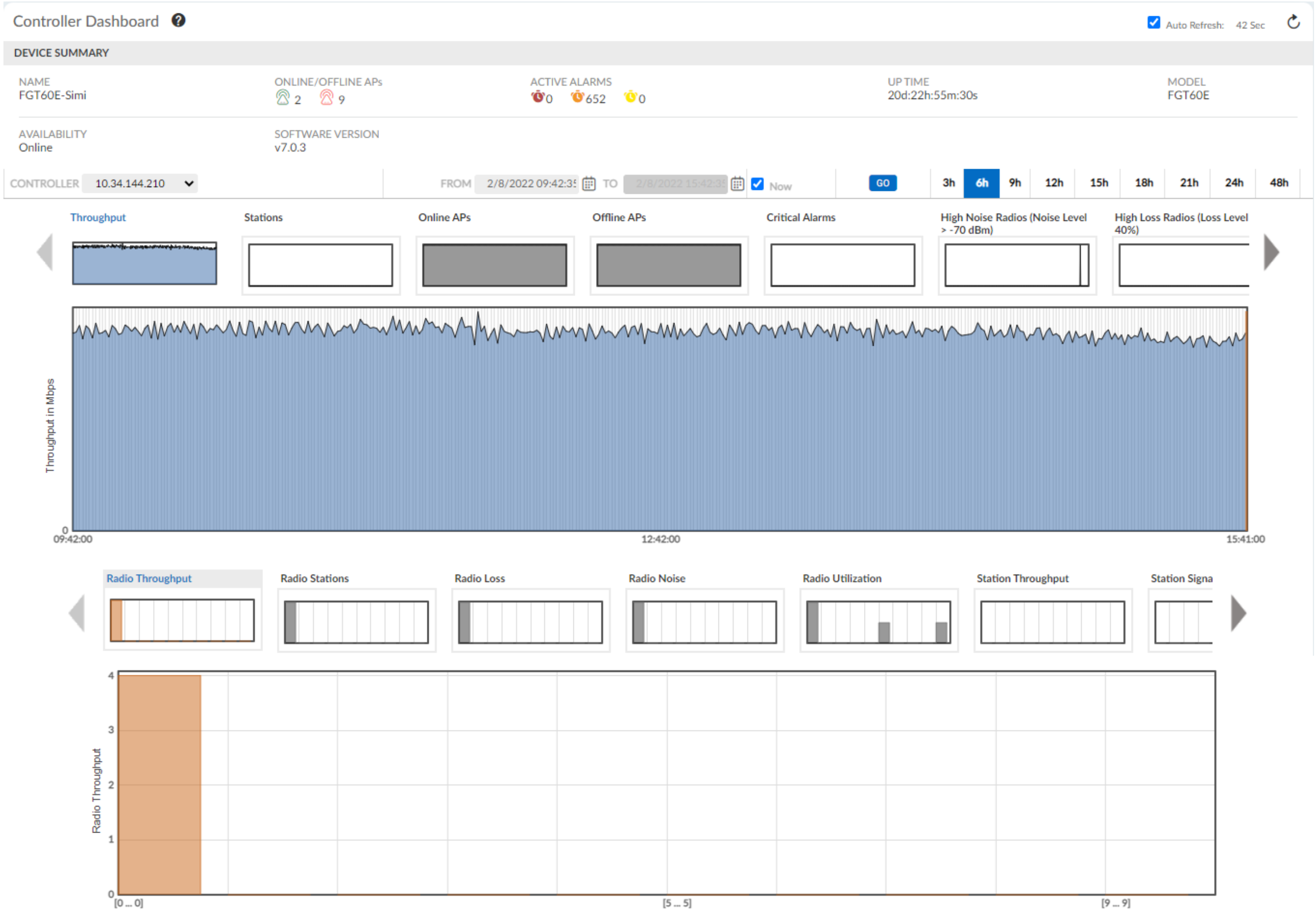
The detailed dashboards provide at-a-glance system information related to the controllers, APs, and stations managed by FortiWLM MEA. Navigate to *Monitor* > *Detailed Dashboard*.

- Controllers on page 45
- AP on page 47
- Stations on page 49

Controllers

This dashboard displays detailed controller activity. It provides the graphical representation of the *Throughput* , *Stations, Online APs, Offline APs, Critical Alarms, High-Noise Radios, High- Loss Radios, High-Loss Stations, Low-Signal Stations*, and *Rogue AP*s of the selected controller that are managed by FortiWLM MEA. The results for the controller are displayed in the upper graphs and results per radio is displayed in the lower set of graphs.

Select a controller IP address and details such as name, location, the number of online or offline APs connected, availability status, active alarms, up time, software version, and model is displayed. The upper graphs display the results for the **controller** or trend graphs for the selected controller and the lower graphs are **distribution** state graphs for a respective parameter at a given time. Click a smaller upper graph to view a larger version displayed in the middle of the dashboard.



Controller Dashboard

☑ Auto Refresh: 42 Sec

DEVICE SUMMARY

NAME FGT60E-Simi

ONLINE/OFFLINE APs 2 9

ACTIVE ALARMS 0 652 0

UP TIME 20d:22h:55m:30s

MODEL FGT60E

AVAILABILITY Online

SOFTWARE VERSION v7.0.3

CONTROLLER 10.34.144.210

FROM 2/8/2022 09:42:3 TO 2/8/2022 15:42:3 ☑ Now

The trends based on controller selection is monitored by selecting the trend duration. The time period can be modified from 1 to 48 hours by selecting the Interval or by selecting the *From* and *To* duration of time.

The following **controller** trend information is displayed.

Chart	Description
Throughput	Displays the controller's throughput. This value is the sum (in Mbps) of all Rx and Tx transmissions.
Stations	Displays the stations associated with a controller. All stations connected to the controller are included.
Online APs/Offline APs	Displays the total number of online and offline APs associated with the controller.
Critical Alarms	Displays the number of critical alarms on this controller. An alarm is defined as *critical* when the *Notification Filter* is created (Alarm Severity).
High-Noise Radios	Displays the number of radios on this controller experiencing noise greater than threshold (-70 dBm). The threshold cannot be changed at this time.
High-Loss Radios	Displays the number of radios on this controller experiencing loss greater than the threshold (40%). The threshold cannot be changed at this time.
High-Loss Stations	Displays the number of stations on this controller experiencing loss greater than

Chart	Description
	the threshold (40%). The threshold cannot be changed at this time.
Low-Signal Stations	Displays the number of stations on this controller that are connected at signal strength <= -80Dbm.
Rogue APs	Displays the number of rogue APs detected on this controller.

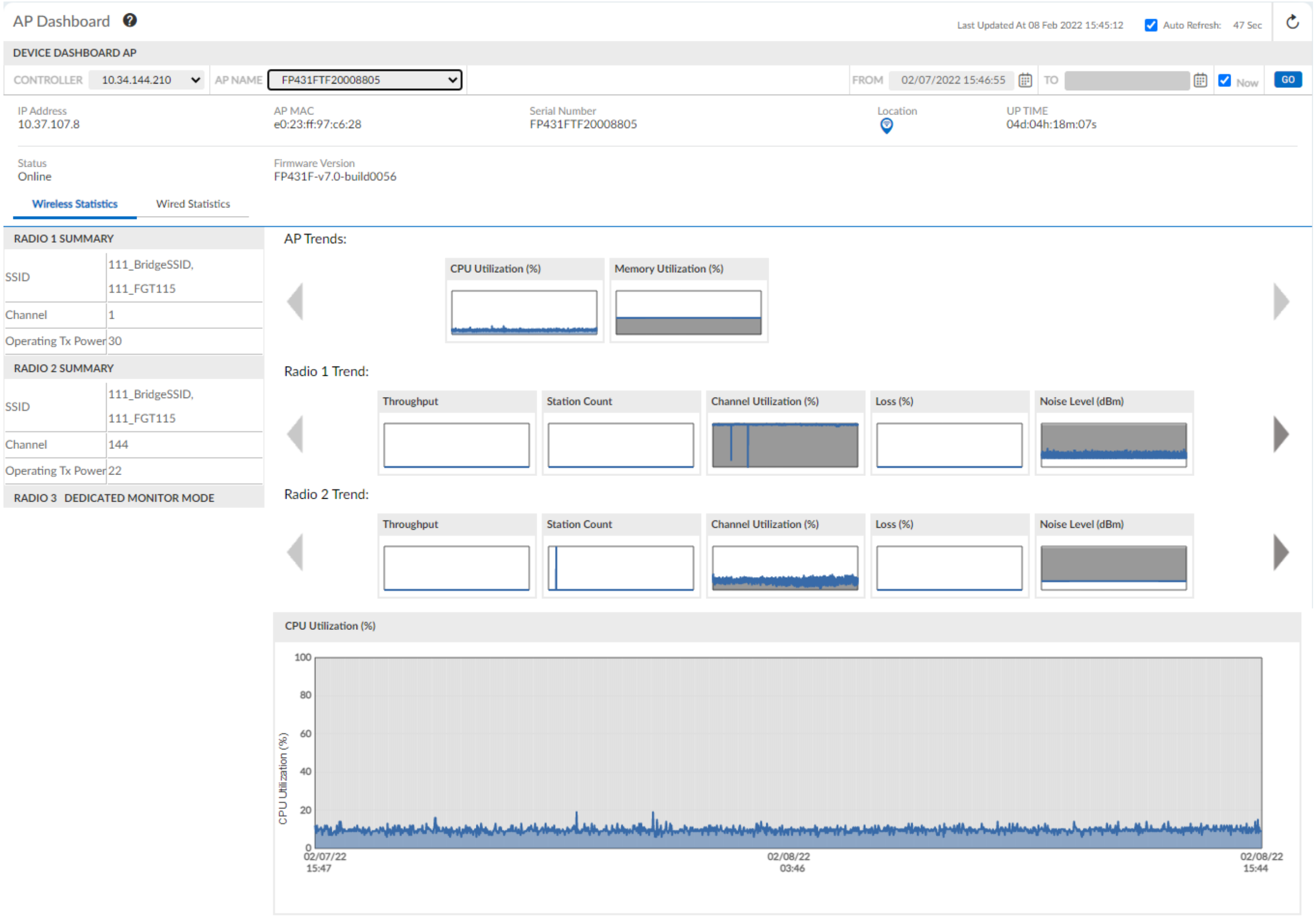
The graphs in the lower half of the dashboard are **distribution** state graphs for the respective parameter at a given time. Click on any top graphs and the expanded graph is displayed.

Chart	Description
Radio Throughput	Classification of radios into ten groups based on throughput.
Radio Stations	Classification of radios into ten groups based on the number of stations.
Radio Loss	Classification of radios into ten groups based on loss greater than the threshold (40%).
Radio Noise	Classification of radios into ten groups based on noise greater than the threshold (-70 dBm).
Radio Utilization	Classification of radios into ten groups based on channel utilization.
Station Throughput	Classification of stations into ten groups based on throughput.
Station Signal	Classification of stations into ten groups based on signal strength lower than the threshold (-80 dBm).
Station Loss	Classification of stations into ten groups based on loss greater than the threshold (40%).
Station Airtime	Classification of stations into ten groups based on airtime utilization.

AP

This dashboard displays detailed AP activity and provides the graphical representation of the *Throughput, Station Count, Noise Level, Loss%*, and *Channel Utilization%* of each radio on AP connected to the controller which is managed by FortiWLM MEA. The trend result for each of the radios of the selected AP is displayed on the top portion of the window and trends per radio in the lower portion of the dashboard.

Select a controller IP address and the list of APs located on the selected controller is displayed. Select the AP and a time period. The time interval cannot be more than 1 day.



AP Dashboard

Last Updated At 08 Feb 2022 15:45:12 ☑ Auto Refresh: 47 Sec

DEVICE DASHBOARD AP

CONTROLLER 10.34.144.210 AP NAME FP431FTF20008805 FROM 02/07/2022 15:46:55 TO ☑ Now GO

IP Address
10.37.107.8

AP MAC
e0:23:ff:97:c6:28

Serial Number
FP431FTF20008805

Location

UP TIME
04d:04h:18m:07s

Status
Online

Firmware Version
FP431F-v7.0-build0056

Wireless Statistics Wired Statistics

RADIO 1 SUMMARY	
SSID	111_BridgeSSID, 111_FGT115
Channel	1
Operating Tx Power	30
RADIO 2 SUMMARY	
SSID	111_BridgeSSID, 111_FGT115
Channel	144
Operating Tx Power	22
RADIO 3 DEDICATED MONITOR MODE	

Wireless Statistics

The trend result for each of the radios of the selected AP is displayed in the graphs on the top portion of the dashboard and trends per radio in the lower portion of the dashboard. The number of radios displayed varies from one AP to another and the set of graphs displayed depends on the number of interfaces in AP. The following graphs are displayed for each radio on the AP:

- Throughput (Kbps)
- Station Count
- Noise Level
- Loss %
- Channel Utilization %

Summary - The details of the selected AP are displayed, these include, the IP address, AP MAC address, serial number. Click on the location icon to view the AP location map, the AP uptime, operational status, and the associated firmware version.

Radio Summary- The wireless radio summary displaying the associated SSID, operating channel, and the operating Tx power. The summary is displayed for all radios of the selected AP.

AP Trends - The trend result are displayed for CPU utilization and memory utilization percentages of the selected AP.

Wired Statistics

The trend result for LAN1 and LAN2 interfaces of the selected AP is displayed in the graphs on the top portion of the dashboard and trends per interface in the lower portion of the dashboard. The quantity of inbound/outbound octets and input/output errors are displayed for LAN1 and LAN2 interfaces.

Stations

This dashboard displays a variety of performance trends for a selected station. On the *Stations* dashboard obtain a **Station Key**. Select a controller and enter the time manually or click the *Calendar* icon, the *End Time* is automatically selected to the current date. To modify the time, de-select the *Now* option. Select one of the stations and click **Save**; the selected station is displayed in the **Station Key** field.

The following charts display the station trends. Hover over the chart to view the date, time and value for that point and right-click and select **Show Details** to view more information.

Chart	Description
Station Throughput	Displays a station's combined transmitted and received bytes during a 10 minutes or 1 minute based on the configured polling interval. This chart is updated every 10 minutes or 1 minute based on the configured polling interval.
Signal Strength	Displays the signal strength (dBm) for this station in the time period indicated. This chart is updated every 10 minutes.
Loss %	Displays the station's transmit loss percentage for all unicast data frames.
Airtime Utilization	Displays station airtime utilization percentage.

The following **station information** is displayed.

Parameters	Description
MAC Address	Displays the MAC address of the Station.
IPv4 Address	Displays the IPv4 address of the Station.
IPv6Address	Displays the IPv6 address of the Station.
User Name	Displays the user name.
Station Type	Displays the type of station; *Wireless Station* or *Wired Station*.
OUI Name	Displays the OUI Name of the station.
Device Type	Displays whether the type of device to which the station is connected to. For example, Google Nexus 4 Phone, Blackberry and so on.
OS Type	Displays the Station distribution based on the OS Type. For example, Apple iOS, Microsoft Windows XP and so on.
Radio Type	Displays the radio type to which the station is connected.
Data Rate	Displays the data rate in Mbps for the selected point on the graph.
Service Name	Displays the service name to which the station is connected to.
AP ID	Displays the AP to which the station was associated at the time of the event.

Parameters	Description
AP Name	Displays the name of the AP to which the station was associated at the time of the event. Select the link of the AP Name. The *AP Dashboard* is displayed.
Controller	Displays the IP address of the controller connected to the station.

The history of events accomplished through FortiWLM MEA for this station is displayed. View this list in CSV format by clicking *CSV*. The following information is included for each event in the **Station History**.

Category	Description
Go to Visualization	The *Visualization* feature allows to monitor the coverage and performance of the WLAN APs using maps (graphics files) that is imported to represent the site. Heat maps display the actual AP statistics that are retrieved from the controller and extrapolated into heat maps.
Show AP Location	The *AP Locator* screen displays the selected AP located on the floor.
Date/Time	Displays the *Date/Time* of the station event occurred.
Duration	Displays the *Duration* of the station associated with the AP.
Controller	Displays the *Controller ID* to which the station was associated at the time of the event. The service appliance ID is always number 1 and controllers are assigned numbers from 2 through (2^32 - 1).
AP ID	Displays the ID of the AP to which the station was associated at the time of the event.
AP Name	Displays the name of the AP to which the station was associated at the time of the event. Select the link of the AP Name. The *AP Dashboard* is displayed.
Radio	Displays the number of radios.
Station IP4	Displays the station IPv4 address.
Station IPv6	Displays the station IPv6 address.
User Name	Displays the authorized user name (If any) used to log in.
SSID	Displays the SSID that the station associated with in the last session.
Start Time	Displays the time the station connected during the last association.
Stop Time	Displays the time the station disconnected during the last association.
CSV	Select the *CSV* link. A summary of the station history of all the above mentioned fields are displayed.

The **Station Activity Log** displays the most recent 1000 station events in the selected interval. Most station events are updated almost immediately after the event occurs. All events are available on the server; to view other events, refine the time interval. The events are divided into the six *Station Details* categories. Hover over an event to see the date and time with a short description of the event. Right-click and select **Show Details** to view event details. Up to 1000 events are displayed; once the number reaches 1000, additional events are not listed. If additional events are important for troubleshooting, refine the time interval. The **Station Events** table displays the following information for each of the event.

Parameter	Description
Date/Time	Displays the *Date/Time* of the event occurred.
Event Type	Displays the event type.
Description	Displays the description provided for each of the Event.

You can limit the number of events displayed by indicating a specific station MAC address. You can also limit the time frame or filter the event type. To filter the event type, click *Filter* and select the event categories that you want displayed. You can filter events for viewing based on any or all of these criteria:

- IP Address Discovered
- 802.11 State
- 802.1x Authorization
- MAC Filtering
- SIP
- DHCP
- CP User Authorization
- Encryption
- Band Steering
- Diagnostics

Trends

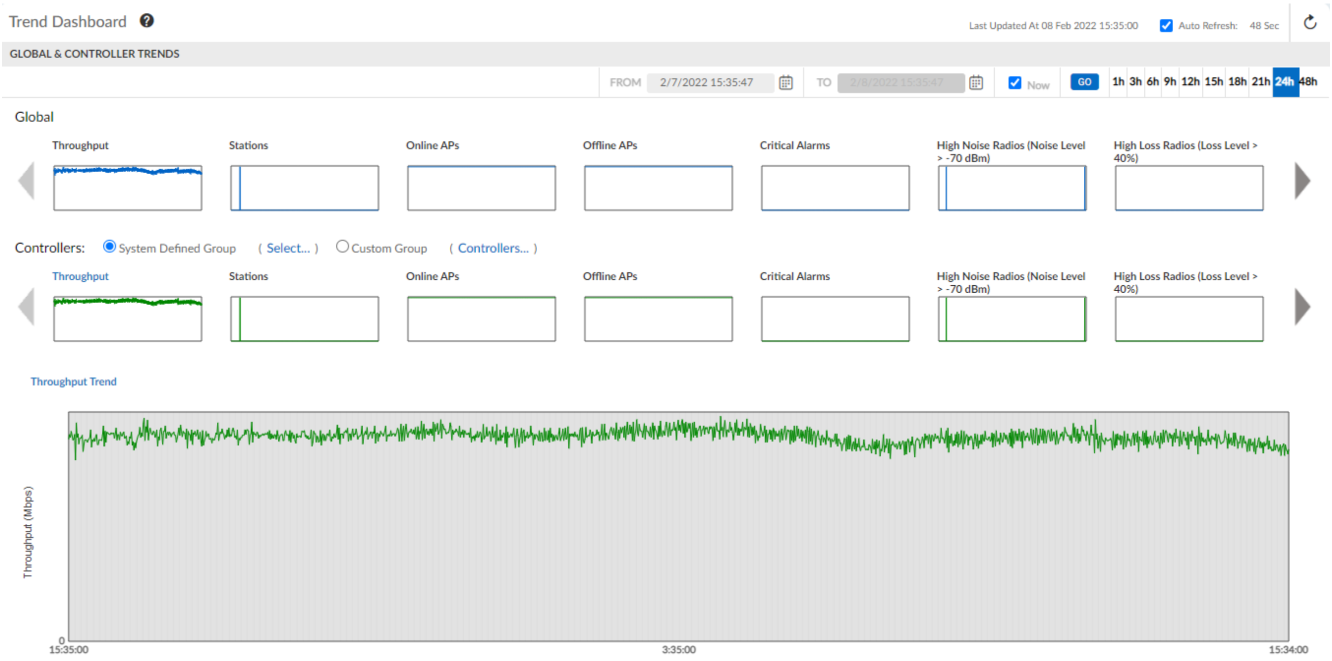
The Trend dashboards provide the aggregate global trend performance and controller error rates over a period of time. Navigate to *Monitor* > *Trends*.

- Trend on page 51
- Long Term Trend on page 53

Trend

This dashboard displays the aggregate global trend performance and error rates for controllers over time for trends. FortiWLM MEA collects statistics from a controller and stores it in the database. The *Trend* dashboard provides the data collected for a single controller or up to five controllers. The trends per controller can be edited by selecting the controllers from the *Custom Group* option on the trend dashboard.

The *Trend* Dashboard displays the *Global Trends* (All controllers) in the graphs on the top portion of the window and *Trends* per controller on the lower portion of the window. Multiple lines are sometimes displayed in the lower set of charts due to multiple controller selection. The trends are plotted for the last 1 to 48 hours by representing up to five controllers at a time. The time period can be modified from 1 to 48 hours by selecting the *Trend Interval* or by selecting the *From* and *To* duration of time.


Trend Dashboard
Last Updated At 08 Feb 2022 15:35:00
☑ Auto Refresh: 48 Sec
GLOBAL & CONTROLLER TRENDS
FROM 2/7/2022 15:35:47
TO 2/8/2022 15:35:47
☑ Now
GO
1h 3h 6h 9h 12h 15h 18h 21h 24h 48h
Global
Throughput
Stations
Online APs
Offline APs
Critical Alarms
High Noise Radios (Noise Level > -70 dBm)
High Loss Radios (Loss Level > 40%)
Controllers: ● System Defined Group (Select...) ○ Custom Group (Controllers...)
Throughput
Stations
Online APs
Offline APs
Critical Alarms
High Noise Radios (Noise Level > -70 dBm)
High Loss Radios (Loss Level > 40%)
Throughput Trend
Throughput (Mbps)
0
15:35:00
3:35:00
15:34:00

Click on one of small graphs in the dashboard to view a larger version displayed in the center of the dashboard. Hover the mouse pointer on a graph to view the time and value of that data point.

The following **Global Trends and Controller Trends** charts are displayed.

Chart	Description
Throughput	Throughput represents all controllers' throughput aggregated. This value is determined with the formula *TX_unicast_data_bytes* + *RX_unicast_data_bytes) / time_duration* * 8. Fractional values are included in the previous bar. For example, if throughput is 10.5, it is counted in bar 9-10 (assuming bars are 9-10,11-12 and so on).
Stations	Total number of stations associated to Network Manager controllers during the time period selected.
Online APs	Online APs displays the sum of all online APs on up to 5 controllers.
Offline APs	Offline APs displays the sum of all offline APs on up to 5 controllers.
Critical Alarms	Critical Alarms represents the aggregate number of all critical alarms on up to 5 controllers.
High Noise Radios	The High Noise Radio chart is the aggregate number of radios experiencing noise greater than threshold (-70 dBm). You cannot change thresholds at this time.
High Loss Radios	The High Loss Radio chart is the aggregate number of radios experiencing loss greater than the threshold (40%). You cannot change thresholds at this time.
High Loss Stations	Aggregate number of high-loss stations for each ten minute period. High loss is defined as 40%.

Chart	Description
Low RSSI Stations	The Low RSSI Stations chart is the aggregate number of stations on all controllers that are experiencing loss greater than the threshold (-80dBm). You cannot change thresholds at this time.
Rogue APs	Rogue APs represents the classification of controllers into ten groups based on number of rogue APs detected on each controller.

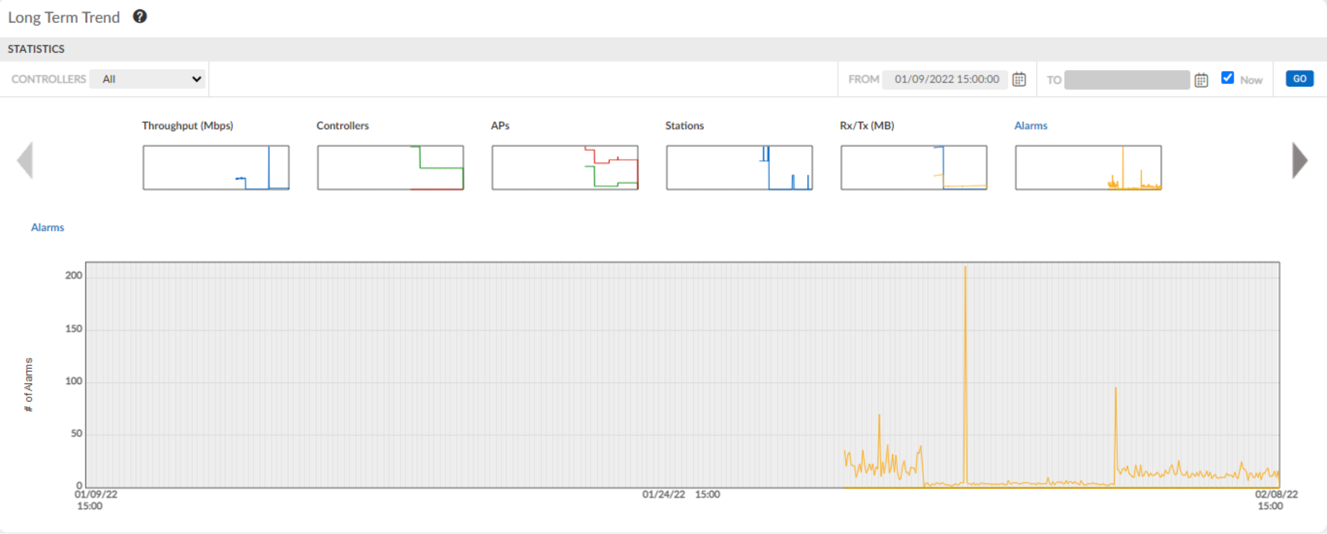
Click **Enable Auto Refresh** to keep updating this window every minute. Otherwise, the data is updated only when you open the window.

Long Term Trend

The FortiWLM MEA collects the statistical data from the controller and provides an option to view the *Long Term Trend* for predefined parameters. The long term trend data is a graphical representation for the statistics gathered over the period of time.

The *Long Term Trend* dashboard displays the per controller view or the aggregate-controller view (default view). The trend data for a maximum of one year and a minimum period of two hours is displayed. The long term trend data stored in the database cannot be modified. The FortiWLM MEA summarizes the data in three pre-defined sample periods.

- **Hourly** - If the time range to be graphed is 1 month or less than one month, the trend graph is displayed with hourly sample points. This is the default view.
- **8 Hours** - If the time range to be graphed is more than one month and less than 8 months, the trend graph is displayed with 8 hours sample points. The sampling time can also be configured on the **Maintenance** screen (*Administration* > *Maintenance* > *Statistics section* > *Long Term: 8 Hourly Data Aggregation Period Begins At (AM)*).
- **24 Hours** - If the time range to be graphed is more than 8 months and up to 1 year, the trend graph is displayed with 24 hours sample points.



By default, all controllers are included but you can select a specific controller from the controllers list. In this case, data is automatically refreshed. Enter the period manually or select the calendar icon to set the date and time.

Chart	Description
Throughput	Displays the total number of controllers' throughput aggregated. Right-click and select *Show Details* on the graph to view the details of throughput.
Controllers	Displays the total number of polled controllers. Both online (green) and offline (red) controllers can be viewed. The number of managed controllers in the graph can be viewed by hovering over the graph. Right-click and select *Show Details* to view the details of online and offline controllers.
APs	Displays the total number of APs present on the polled controllers. Both online (green) and offline (red) APs can be viewed. The number of APs associated with the managed controllers can be viewed by hovering tover the graph. Right-click and select *Show Details* to view the details of the online and offline APs.
Stations	Displays the total number of stations associated to the controllers for the selected time period. The number of stations in the graph can be viewed by hovering over the graph. Right-click and select *Show Details* to view the details of the stations associated.
Rx/Tx	The *Receive* data and *Transmit* data graph displays the data transferred in bytes. The number of *Receive* data and *Transmit* data (in bytes) can be viewed by hovering over the graph. Right-click and select *Show Details* to view the details of the data transferred in bytes.
Alarms	Displays the aggregate number of all alarms on all polled controllers. The following are the types of color-coded alarms. • Red - Critical • Orange - Major • Yellow - Minor The number of the *Critical*, *Major*, and *Minor* alarms in the graph can be viewed by hovering over the graph. Right-click and select *Show Details* to view the details.

Topology

Topology is a tree view that illustrates the physical or logical placement of hardware devices in the network. The *Topology* branch provides a way to access the various topologies available to a user to monitor the wireless network.

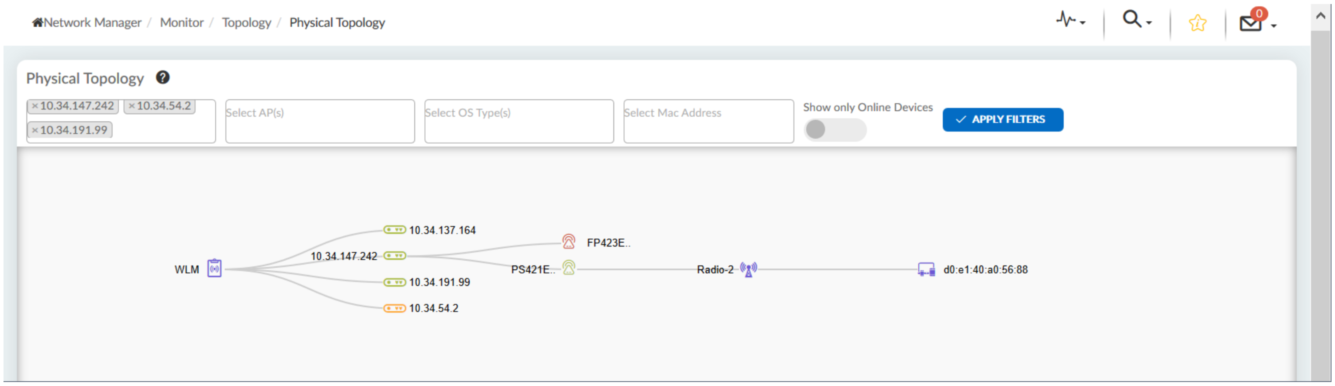
You can access the following topology views from the *Topology* branch:

- Physical Topology on page 54
- Logical Topology on page 55

Physical Topology

The *Physical Topology* dashboard provides a visualization/illustration of the physical placement of devices, such as, controllers, APs, and stations connected within your network in a hierarchical pattern. The physical topology is representational; you cannot modify the placement of devices on this page.

You can access the *Physical Topology* dashboard through *Monitor* > *Topology* > *Physical Topology*.



The hierarchy of devices in the physical topology view is **FortiWLM MEA > Controller > Access Point > Radio > Station**. Each of the devices in the hierarchical view is represented by a clickable node. Click on a node to display the next available devices in the hierarchy. Hover over the device name for additional information about the device.

The status of controllers or APs is indicated by different colors. Icons for controllers and APS may be of the following colors:

- Green: Indicates an online and active device
- Orange: Indicates an online and unknown (unmanaged) device
- Red: Indicates an offline device

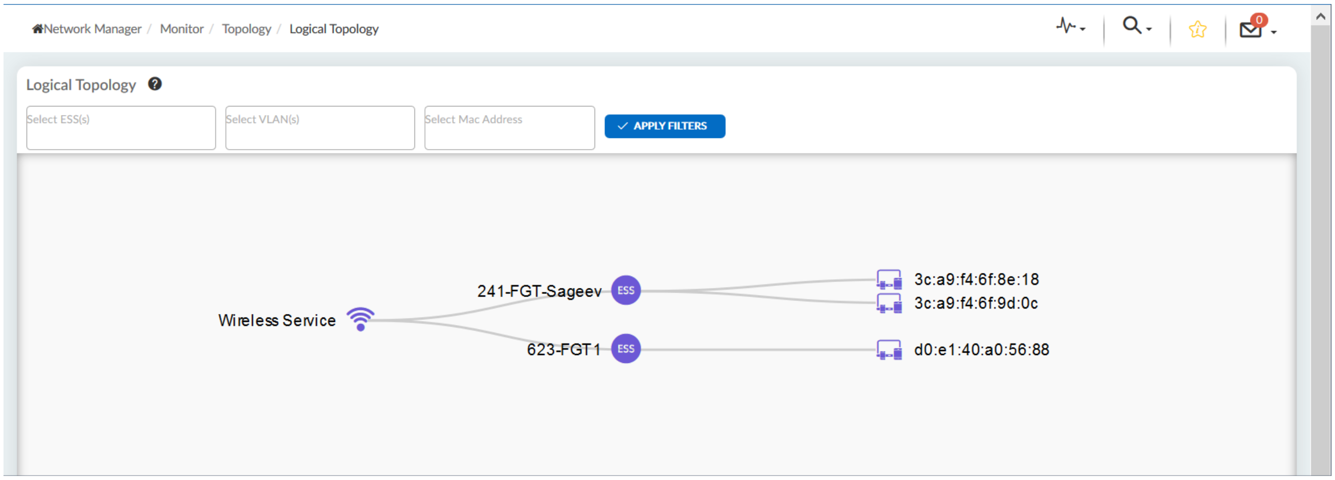
If a controller or AP name is on the right of its icon, it implies that the device has no child associated with it in the hierarchy.

You can filter and view the devices selectively. The available filter options are: *Controllers*, *APs*, *OS Types*, and device *MAC Address*.

Logical Topology

The *Logical Topology* dashboard provides a visualization/illustration of the configured wireless service, the associated ESS pushed through the wireless service, VLAN (if applicable), and the stations connected to each ESS in a hierarchical pattern. The physical topology is representational; you cannot modify the placement of devices on this page.

You can access the *Logical Topology* dashboard through *Monitor* > *Topology* > *Logical Topology*.



The hierarchy of devices in the logical topology view is **FortiWLM MEA > ESS > VLAN > Station**. Each of the devices in the hierarchical view is represented by a clickable node. Click on a node to display the next available devices in the hierarchy. Hover over the device name for additional information about the device.

If a controller or AP name is on the right of its icon, it implies that the device has no child associated with it in the hierarchy.

You can filter and view the devices selectively. The available filter options are: *ESS*, *VLANs*, and device *MAC Address*.

Configuring Devices

You can configure the location services to locate a client / station / rogue AP in your network.

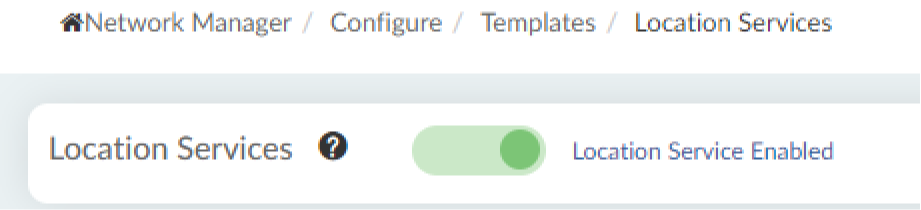
Locationing Services on page 57

Locationing Services

The location service captures parameters at pre-defined intervals and sends them as UDP packets to your location engine to locate the position of a client / station / rogue AP in your network.

You can access the *Location Services* screen through *Configure* > *Templates* > *Location Services*.

Enable location service on this page and configure the following **FortiAP** Profile in your FortiGate.



1. Configure the WIDS profile for the AP radio.
2. Configure the following parameters in **Location Based Services > FortiPresence**.
   - Project Name: **FWLM**
   - Password: The secret key displayed in **Administration > System Settings > Maintenance**.
   - FortiPresence server IP: FortiWLM IP address.
   - FortiPresence server Port: **14013**
   - Report Rogue APs: **Enable**
   - Configure Report transmit frequency (seconds)

Note: A minimum of 3 APs must be placed in the map for locationing service to detect them.

Operating Devices in a Wireless Network

Operation of devices within the wireless network managed by FortiWLM MEA involves the management of various devices, the various device groups, the various available system log and diagnostic tools, maps management, and so on.

The *Operate* branch from the tree menu in the left navigation pane provides a way to access the various network operation tools through the following branches:

- Inventory on page 58
- Groupings on page 62
- Tools on page 65
- Maps on page 69

Inventory

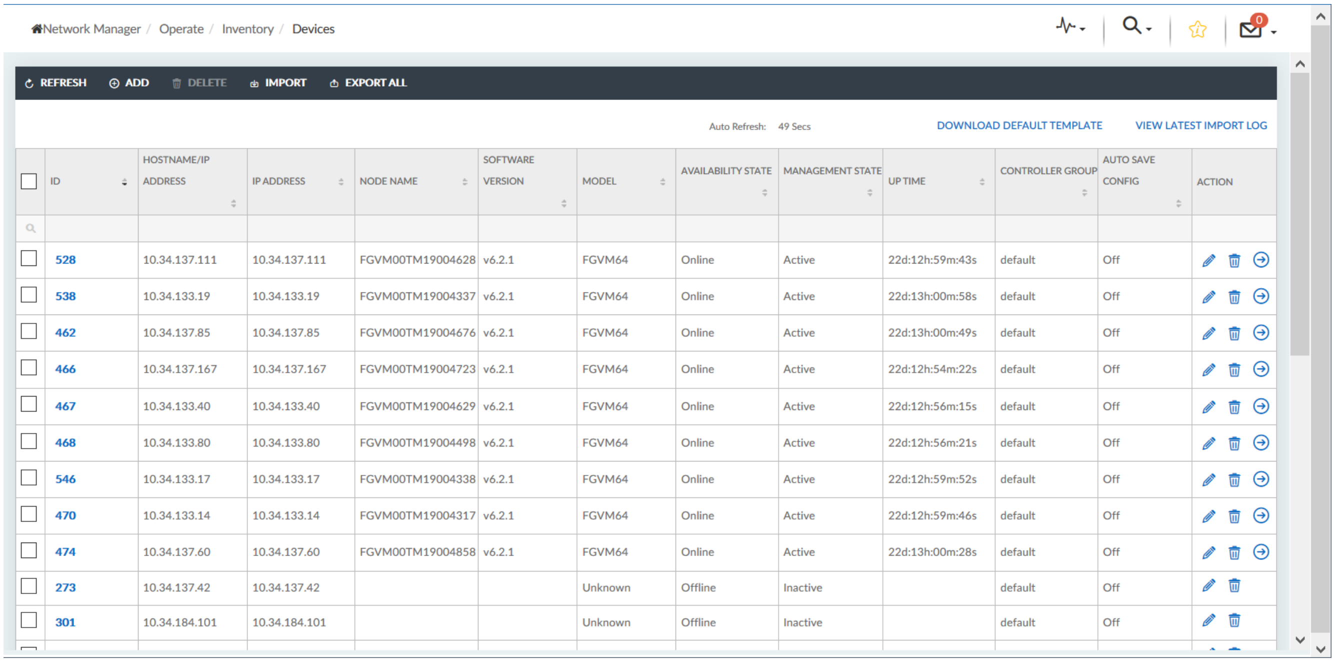
FortiWLM MEA keeps track of the various devices in the wireless network by maintaining an inventory. It allows you to discover and manage controllers and APs. The *Inventory* branch of the tree menu in the left navigation pane is further branched into:

- Devices on page 58
- Access Points on page 60

Devices

The *Devices* inventory lists all the devices in the wireless network inventory managed by FortiWLM MEA. Each of the devices are listed in table rows with their details summarized. You can *Add* devices, and *Delete* or *Export* devices from the Inventory on the *Devices* dashboard. You can also *Edit* an existing device or navigate to the device GUI to manage it directly.

You can access the *Devices* inventory through *Operate* > *Inventory* > *Devices* .



Network Manager / Operate / Inventory / Devices

Auto Refresh: 49 Secs

□	ID	HOSTNAME/IP ADDRESS	IP ADDRESS	NODE NAME	SOFTWARE VERSION	MODEL	AVAILABILITY STATE	MANAGEMENT STATE	UP TIME	CONTROLLER GROUP	AUTO SAVE CONFIG	ACTION
□	528	10.34.137.111	10.34.137.111	FGVM00TM19004628	v6.2.1	FGVM64	Online	Active	22d:12h:59m:43s	default	Off	
□	538	10.34.133.19	10.34.133.19	FGVM00TM19004337	v6.2.1	FGVM64	Online	Active	22d:13h:00m:58s	default	Off	
□	462	10.34.137.85	10.34.137.85	FGVM00TM19004676	v6.2.1	FGVM64	Online	Active	22d:13h:00m:49s	default	Off	
□	466	10.34.137.167	10.34.137.167	FGVM00TM19004723	v6.2.1	FGVM64	Online	Active	22d:12h:54m:22s	default	Off	
□	467	10.34.133.40	10.34.133.40	FGVM00TM19004629	v6.2.1	FGVM64	Online	Active	22d:12h:56m:15s	default	Off	
□	468	10.34.133.80	10.34.133.80	FGVM00TM19004498	v6.2.1	FGVM64	Online	Active	22d:12h:56m:21s	default	Off	
□	546	10.34.133.17	10.34.133.17	FGVM00TM19004338	v6.2.1	FGVM64	Online	Active	22d:12h:59m:52s	default	Off	
□	470	10.34.133.14	10.34.133.14	FGVM00TM19004317	v6.2.1	FGVM64	Online	Active	22d:12h:59m:46s	default	Off	
□	474	10.34.137.60	10.34.137.60	FGVM00TM19004858	v6.2.1	FGVM64	Online	Active	22d:13h:00m:28s	default	Off	
□	273	10.34.137.42	10.34.137.42			Unknown	Offline	Inactive		default	Off	
□	301	10.34.184.101	10.34.184.101			Unknown	Offline	Inactive		default	Off	

To add, delete, edit, or export devices:

- See Adding controllers to the device inventory on page 59.
- See Editing existing controllers in the device inventory on page 59.
- See Deleting controllers from the device inventory on page 60.
- See Exporting from the device inventory on page 60.

Adding controllers to the device inventory

In the ADOM mode, you can add controllers managed by the particular ADOM of the FortiManager. In the non-ADOM mode, you can add any controller managed by FortiManager.

To add a controller to the device inventory:

1. Click *Add* on the upper-left of the devices inventory. The *Add Device* dialog appears. You can *Discover Device* using *Add Model Device* option where the FortiGate controller is discovered manually using the serial number. The added controller is in the offline state. See the *FortiManager Administration Guide* for procedural steps to add devices to FortiManager.
   The *Add Device(s) from FortiManager* option lists the controllers managed by the particular ADOM in FortiManager. Select the required controller.
2. Click *Save*. The controller is added to the device inventory table.

Editing existing controllers in the device inventory

To edit/modify an existing controller in the device inventory:

1. Select a device by clicking on the device check box from the devices table.
2. Click on the ✎ button from the *Actions* column. The *Edit Device* dialog appears.

3. Modify/edit the fields as required. The fields are the same as the *Add Device* fields with the exception of a few additional fields that are grayed.
4. Click *Save*. The device is edited and updated with the changes in the device inventory table.

Deleting controllers from the device inventory

To delete an existing controller from the device inventory:

1. Select a device by clicking on the device check box from the devices table.
2. Click *Delete* on the upper-left of the devices inventory table or click on the 🗑 button from the *Actions* column. The *Delete Device* confirmation dialog appears.
3. Click *OK*. The device is deleted from the device inventory table.

When you delete a device with an *Active* value for its *Management State* parameter, the device is not permanently deleted but its *Management State* is set to *Deleted*, and the device is no longer monitored by the system. This is done to preserve the references to the device statistics collected by the system. To permanently deleted a device, repeat the above steps on a device with a *Management State* set to *Deleted*.

Exporting from the device inventory

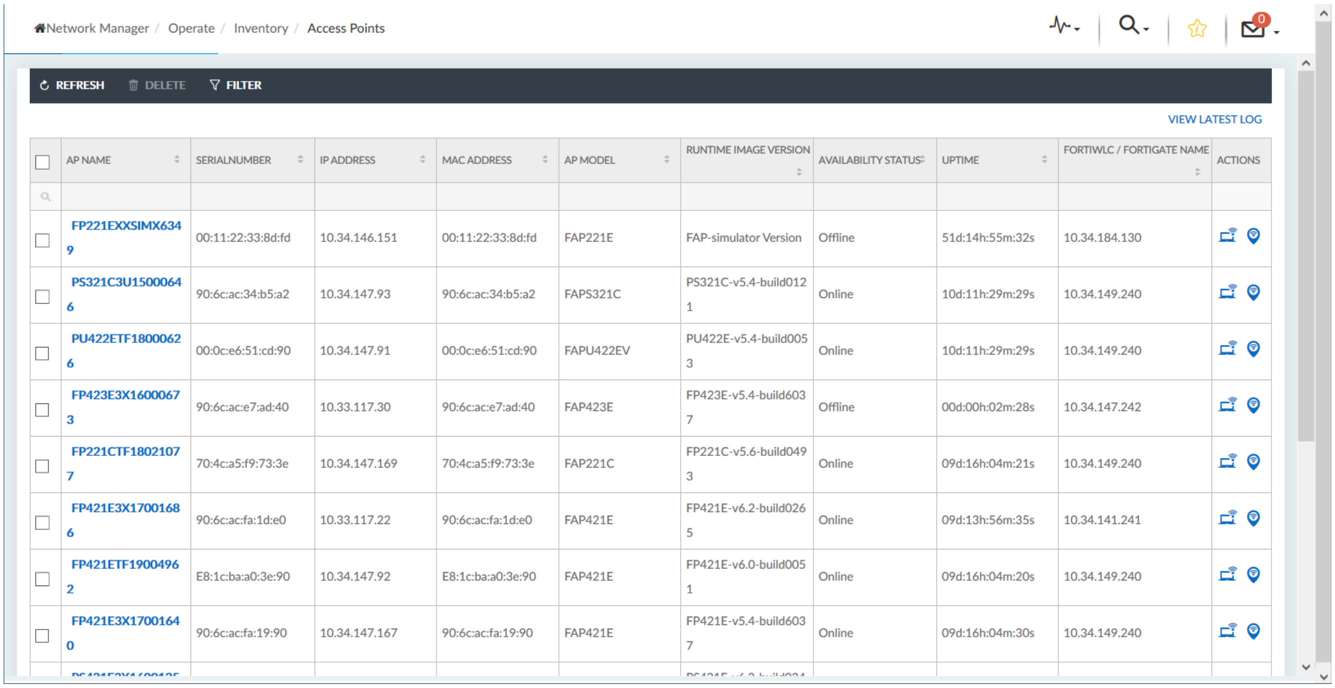
To export all controller information from the device inventory:

1. Click *Export All* on the upper-left of the devices inventory table.
2. Save the *Devices.csv* file exported by the system to your device drive.

Access Points

The *Access Points* inventory lists all the APs in the wireless network inventory managed by FortiWLM MEA. Each of the APs are listed in table rows with their details summarized. You can *Delete* or *Filter* APs from the *Access Points* inventory. You can also view the *AP* dashboard or view AP location by navigating away from the AP inventory table.

You can access the *Access Points* inventory through *Operate* > *Inventory* > *Access Points*.



□	AP NAME	SERIALNUMBER	IP ADDRESS	MAC ADDRESS	AP MODEL	RUNTIME IMAGE VERSION	AVAILABILITY STATUS	UPTIME	FORTIWLC / FORTIGATE NAME	ACTIONS
□	FP221EXXSIMX6349	00:11:22:33:8d:fd	10.34.146.151	00:11:22:33:8d:fd	FAP221E	FAP-simulator Version	Offline	51d:14h:55m:32s	10.34.184.130	
□	PS321C3U15000646	90:6c:ac:34:b5:a2	10.34.147.93	90:6c:ac:34:b5:a2	FAPS321C	PS321C-v5.4-build0121	Online	10d:11h:29m:29s	10.34.149.240	
□	PU422ETF18000626	00:0c:e6:51:cd:90	10.34.147.91	00:0c:e6:51:cd:90	FAPU422EV	PU422E-v5.4-build0053	Online	10d:11h:29m:29s	10.34.149.240	
□	FP423E3X16000673	90:6c:ac:e7:ad:40	10.33.117.30	90:6c:ac:e7:ad:40	FAP423E	FP423E-v5.4-build6037	Offline	00d:00h:02m:28s	10.34.147.242	
□	FP221CTF18021077	70:4c:a5:f9:73:3e	10.34.147.169	70:4c:a5:f9:73:3e	FAP221C	FP221C-v5.6-build0493	Online	09d:16h:04m:21s	10.34.149.240	
□	FP421E3X17001686	90:6c:ac:fa:1d:e0	10.33.117.22	90:6c:ac:fa:1d:e0	FAP421E	FP421E-v6.2-build0265	Online	09d:13h:56m:35s	10.34.141.241	
□	FP421ETF19004962	E8:1c:ba:a0:3e:90	10.34.147.92	E8:1c:ba:a0:3e:90	FAP421E	FP421E-v6.0-build0051	Online	09d:16h:04m:20s	10.34.149.240	
□	FP421E3X17001640	90:6c:ac:fa:19:90	10.34.147.167	90:6c:ac:fa:19:90	FAP421E	FP421E-v5.4-build6037	Online	09d:16h:04m:30s	10.34.149.240	

To filter APs in or delete APs from the inventory table:

- See Filtering APs in the inventory table on page 61.
- See Deleting APs from the inventory table on page 61.

Filtering APs in the inventory table

To filter the APs in the inventory table:

1. Click *Filter* on the upper-left of the AP inventory table. The *Location Filter* dialog appears.
2. Select the desired *Campus*, *Building*, and/or *Floor Fields*.
3. Click *Save*. The filter is applied to the AP inventory table.

Deleting APs from the inventory table

To delete APs from the inventory table:

1. Select an AP by clicking on the AP check box from the AP inventory table.
2. Click *Delete* on the upper-left of the AP inventory table.
3. Click *OK*. The AP is deleted from the AP inventory table.

You can only delete disabled or offline APs.

Groupings

FortiWLM MEA facilitates grouping of access points and stations operating in the wireless network for group monitoring and administration. The *Groupings* branch of the tree menu in the left navigation pane is further branched into:

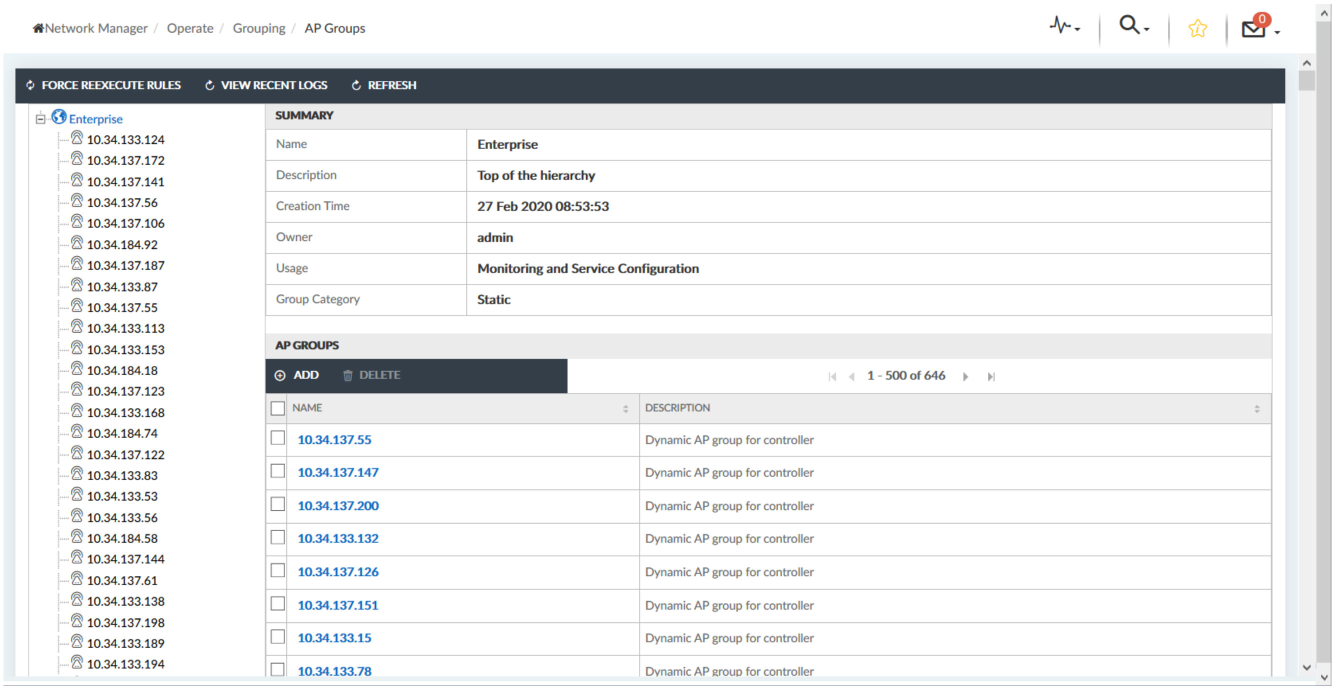
- AP Groups on page 62
- Station Groups on page 64

AP Groups

APs can be grouped together and assigned to an AP group. The *AP Groups* screen allows you to create AP groups and assign APs to it. An AP may belong to multiple AP groups. An AP group may be created with APs on the same controller or on multiple controllers. An AP group may consist of APs of different hardware models, or APs from controllers running different system director versions. AP group usage types are classified as: *Monitoring and Service Configuration*, and *Device Administration*.

AP groups of the *Device Administration* usage type have a restriction that an AP can belong to only one *Device Administration* AP group. This prevents multiple device configurations being applied to an AP.

You can access the *AP Groups* screen through *Operate* > *Grouping* > *AP Groups*.



SUMMARY

Name	Enterprise
Description	Top of the hierarchy
Creation Time	27 Feb 2020 08:53:53
Owner	admin
Usage	Monitoring and Service Configuration
Group Category	Static

AP GROUPS

□	NAME	DESCRIPTION
□	10.34.137.55	Dynamic AP group for controller
□	10.34.137.147	Dynamic AP group for controller
□	10.34.137.200	Dynamic AP group for controller
□	10.34.133.132	Dynamic AP group for controller
□	10.34.137.126	Dynamic AP group for controller
□	10.34.137.151	Dynamic AP group for controller
□	10.34.133.15	Dynamic AP group for controller
□	10.34.133.78	Dynamic AP group for controller

The *AP Groups* screen displays a tree menu in the left with the *Enterprise* group being the top level node in the hierarchy. By default, the *Enterprise* node is selected and summarized on the screen. Following the *Enterprise* summary, all AP groups belonging to the *Enterprise* group are tabulated in the *AP Groups* table. You can click on any node in the tree or an AP name in the *AP Groups* table to see a summary of that AP group.

If you click on an AP group, apart from the summary of that AP group, you can also view any *Member Sub-groups* and the *Member APs* of that AP group.

To add, delete, or edit AP groups:

- See Adding AP groups to FortiWLM MEA and APs to AP groups on page 63.
- See Deleting AP groups from FortiWLM MEA on page 63.
- See Editing existing AP groups in FortiWLM MEA on page 64.

Adding AP groups to FortiWLM MEA and APs to AP groups

Adding AP groups

To add an AP group:

1. Click *Add* on the upper-left of the *AP Groups* table. The *Add AP Groups* dialog appears.
2. Type a name for your AP group in the *Name* field.
3. Type a description for your AP group in the *Description* field. This step is optional.
4. Select the *Group* type to be either *Static* or *Dynamic*. If you choose the *Dynamic* option, you will also have to match the *Rule Conditions* as required.
5. Select the *Usage* type to be *Device Administration* if required. By default, the *Monitoring and Service Configuration* option is selected.
6. Click *Save*. The AP group is created successfully.

You can also add a *Sub-group* to which you can add APs within an AP group. Select an AP group to add a sub-group to it. The procedure to add a sub-group is similar to that of adding an AP group.

Adding APs to AP groups

To add APs to an AP group:

1. Select an AP group to which you want to add APs.
2. Click *Add* on the upper-left of the *Member APs* table. The *AP Selection* dialog appears.
3. Filter the APs displayed based on the *Campus*, *Building*, and *Floor* fields if required. The filtered results are displayed in the table.
4. Select the APs you want to be included in the AP group.
5. Click *Save*. The selected APs are added to the AP group successfully.

Deleting AP groups from FortiWLM MEA

To delete an AP group:

1. Click *Enterprise* in the left tree menu of the *AP Groups* screen. The *AP Groups* table is displayed below the *Enterprise* summary.
2. Select an AP group from the *AP Groups* table by clicking on the AP group check box.
3. Click *Delete* in the upper-left of the *AP Groups* table. A confirmation dialog appears.
4. Click *OK*. The AP group is deleted successfully.

Editing existing AP groups in FortiWLM MEA

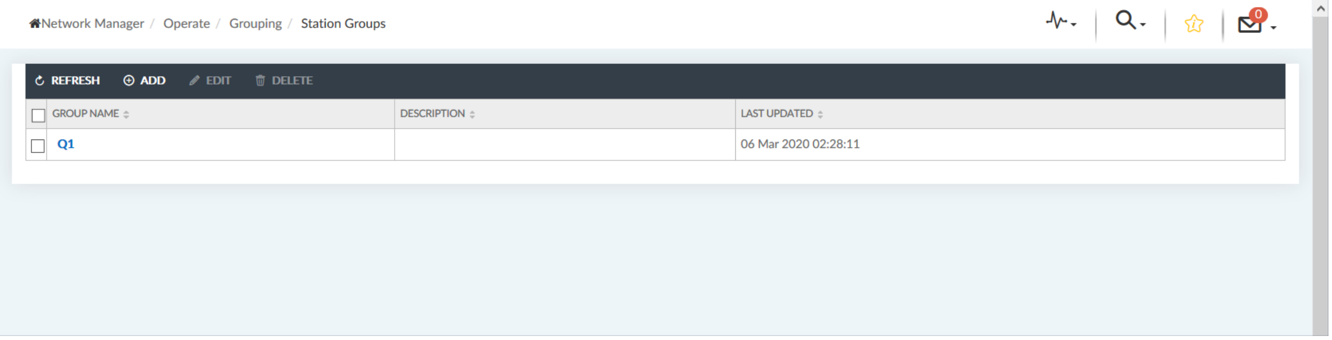
To edit an AP group:

1. Select an AP group to edit.
2. Click *Edit* on the lower-right of the AP group *Summary*. The *Edit AP Group* dialog appears.
3. Change the *Name* and/or *Description* fields.
4. Click *Save*. The AP group is modified/edited successfully.

Station Groups

Stations are logically grouped into station groups based on the *Station MAC Address* or the *Station MAC Prefix* entities.

You can access the *Station Groups* screen through *Operate* > *Grouping* > *Station Groups*.



	GROUP NAME	DESCRIPTION	LAST UPDATED
□	Q1		06 Mar 2020 02:28:11

The Station Group screen displays the various station groups in the system in the form of a table. To *Add*, *Delete*, or *Edit* station groups:

- See Adding Station Groups to FortiWLM MEA on page 64.
- See Deleting Station Groups from FortiWLM MEA on page 65.
- See Editing Station Groups in FortiWLM MEA on page 65.

Adding Station Groups to FortiWLM MEA

To add a station group:

1. Click *Add* on the upper-left of the *Station Groups* table. The *Add Station Groups* dialog appears.
2. Type a name for your station group in the *Group Name* field.
3. Type a description for your station group in the *Description* field. This step is optional.
4. To add stations to the station group:
   a. Click *Add MAC Address*. The *Stations List* dialog appears.
   b. Filter the list of stations as required. The filtered list is displayed in the stations list table.
   c. Select stations from the stations list.
   d. Click *Save*. The selected stations are added to the *Members* stations list on the *Add Station Group* dialog.
   OR
   a. Click *Add MAC Prefix*. The *Add MAC Prefix* dialog appears.
   b. Type in the MAC Prefix.

   c. Click *OK*. The station is added to the *Members* stations list on the *Add Station Group* dialog.

5. If required, select the member stations from the*Members* stations list and click *Delete* to delete the stations added in the previous step.
6. Click *Save*. The station group is created with stations added to it successfully.

Deleting Station Groups from FortiWLM MEA

To delete a station group:

1. Select a station group from the *Station Groups* table by clicking on the station group check box.
2. Click *Delete* in the upper-left of the table. A confirmation dialog appears.
3. Click *OK*. The station group is deleted successfully.

Editing Station Groups in FortiWLM MEA

To edit a station group:

1. Select a station group from the *Station Groups* table by clicking on the station group check box.
2. Click *Edit* on the upper-left of the table. The *Edit Station Group* dialog appears.
3. Change the *Group Name* and/or *Description* fields.
4. Add or delete stations as required.
5. Click *Save*. The station group is modified/edited successfully.

Tools

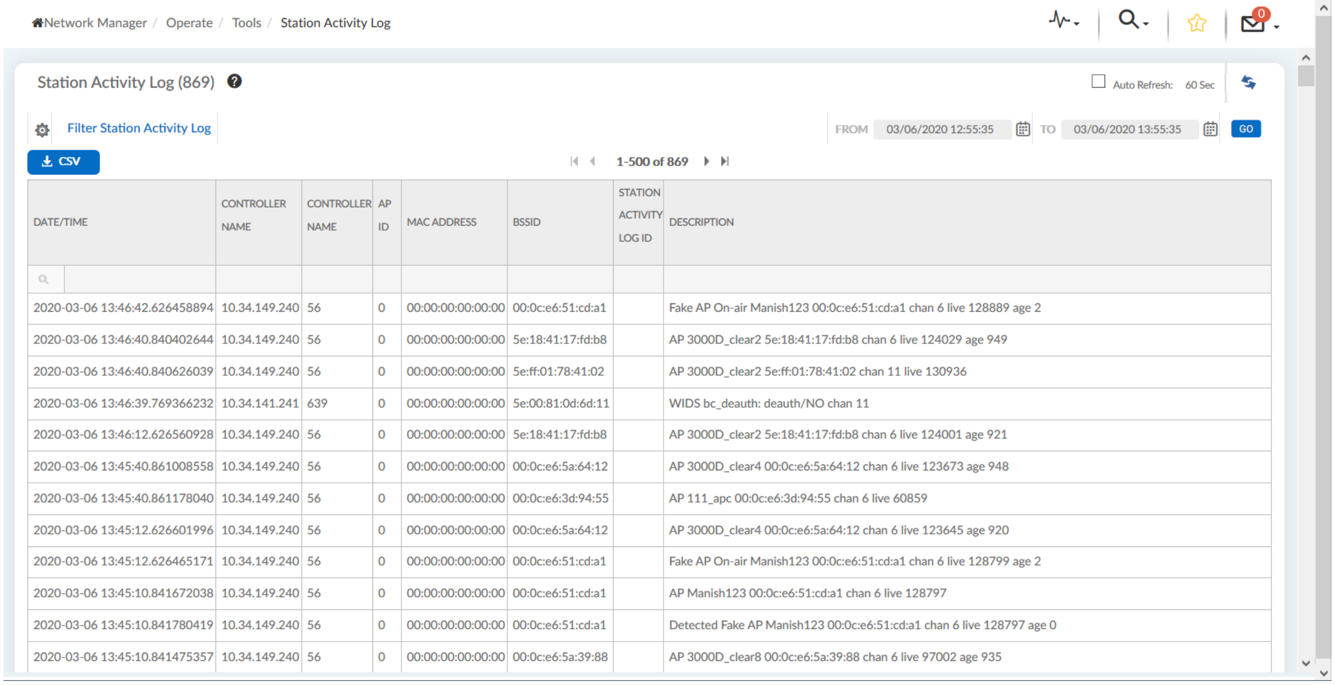
FortiWLM MEA provides various tools to maintain system and devices logs, and generate diagnostics data. It allows you to view the logs and diagnostics data to identify any faults in the system and monitor the wireless network efficiently. The *Tools* branch of the tree menu in the left navigation pane is further branched into:

- Station Activity Log on page 65
- Syslog on page 67
- Diagnostics on page 68

Station Activity Log

Station Activity Log is a log of events for all the stations, for any specified time period. Station events are logged almost immediately after the events occurs.

You can access the *Station Activity Log* screen through *Operate* > *Tools* > *Station Activity Log*.



Network Manager / Operate / Tools / Station Activity Log
Station Activity Log (869)
□ Auto Refresh: 60 Sec
Filter Station Activity Log
FROM 03/06/2020 12:55:35
TO 03/06/2020 13:55:35
GO
CSV
1-500 of 869

DATE/TIME	CONTROLLER NAME	CONTROLLER NAME	AP ID	MAC ADDRESS	BSSID	STATION ACTIVITY LOG ID	DESCRIPTION
2020-03-06 13:46:42.626458894	10.34.149.240	56	0	00:00:00:00:00:00	00:0c:e6:51:cd:a1		Fake AP On-air Manish123 00:0c:e6:51:cd:a1 chan 6 live 128889 age 2
2020-03-06 13:46:40.840402644	10.34.149.240	56	0	00:00:00:00:00:00	5e:18:41:17:fd:b8		AP 3000D_clear2 5e:18:41:17:fd:b8 chan 6 live 124029 age 949
2020-03-06 13:46:40.840626039	10.34.149.240	56	0	00:00:00:00:00:00	5e:ff:01:78:41:02		AP 3000D_clear2 5e:ff:01:78:41:02 chan 11 live 130936
2020-03-06 13:46:39.769366232	10.34.141.241	639	0	00:00:00:00:00:00	5e:00:81:0d:6d:11		WIDS bc_deauth: deauth/NO chan 11
2020-03-06 13:46:12.626560928	10.34.149.240	56	0	00:00:00:00:00:00	5e:18:41:17:fd:b8		AP 3000D_clear2 5e:18:41:17:fd:b8 chan 6 live 124001 age 921
2020-03-06 13:45:40.861008558	10.34.149.240	56	0	00:00:00:00:00:00	00:0c:e6:5a:64:12		AP 3000D_clear4 00:0c:e6:5a:64:12 chan 6 live 123673 age 948
2020-03-06 13:45:40.861178040	10.34.149.240	56	0	00:00:00:00:00:00	00:0c:e6:3d:94:55		AP 111_apc 00:0c:e6:3d:94:55 chan 6 live 60859
2020-03-06 13:45:12.626601996	10.34.149.240	56	0	00:00:00:00:00:00	00:0c:e6:5a:64:12		AP 3000D_clear4 00:0c:e6:5a:64:12 chan 6 live 123645 age 920
2020-03-06 13:45:12.626465171	10.34.149.240	56	0	00:00:00:00:00:00	00:0c:e6:51:cd:a1		Fake AP On-air Manish123 00:0c:e6:51:cd:a1 chan 6 live 128799 age 2
2020-03-06 13:45:10.841672038	10.34.149.240	56	0	00:00:00:00:00:00	00:0c:e6:51:cd:a1		AP Manish123 00:0c:e6:51:cd:a1 chan 6 live 128797
2020-03-06 13:45:10.841780419	10.34.149.240	56	0	00:00:00:00:00:00	00:0c:e6:51:cd:a1		Detected Fake AP Manish123 00:0c:e6:51:cd:a1 chan 6 live 128797 age 0
2020-03-06 13:45:10.841475357	10.34.149.240	56	0	00:00:00:00:00:00	00:0c:e6:5a:39:88		AP 3000D_clear8 00:0c:e6:5a:39:88 chan 6 live 97002 age 935

The *Station Activity Log* screen displays a log of stations activity for the specified time period in the form of a table. The following information is summarized in the table:

Column Name	Description
Date/Time	Displays the date and time at which the log was recorded.
Controller Name	Displays the controller IP address that a station is connected to for which the log was recorded.
AP ID	Displays the ID of the AP the station belongs to.
MAC Address	Displays the MAC Address of the station.
BSSID	Displays the BSSID associated with the AP.
Station Activity Log ID	Displays the event ID. The value can be: IP address discovered, DHCP, station hand-off, 802.11 state, CP user authentication, or 802.1X authentication.
Description	Displays the details such as the diagnostics type, RF statistics, interface ID, severity, and a short description.

Hover over the ⚙ icon in the upper-left of the *Station Activity Log* table and select or deselect the desired fields to control the display of columns in the table. To set the desired time period and view logs from that period, select the *From* and *To* dates and times in the upper-right of the table and click *GO*.

To filter the station activity log displayed on screen:

1. Click *Filter Station Activity Log* in the upper-left of the *Station Activity Log* table. The *Filter Station Activity Log* dialog is displayed.
2. Select an option from the *Search Order* drop-down list.
3. Select an option from the *Number of Rows per page* drop-down list.

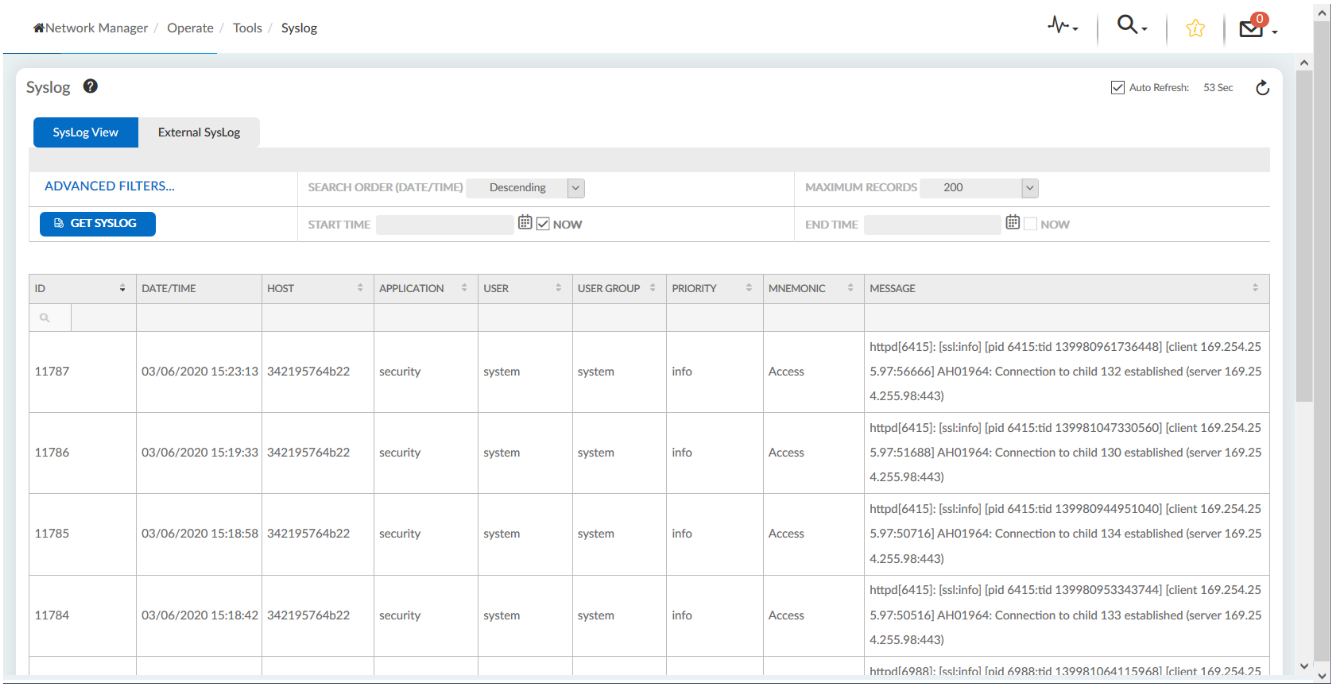
4. Enter controller names in the *Controller* field.
5. Enter station activity log IDs in the *Station Activity Log ID* field.
6. Enter MAC addresses in the *MAC Address* filed.
7. Click *Apply*. The filter is applied and the table is updated accordingly.

To download the logged details, click the *CSV* button. The system downloads a CSV file of the logged data.

Syslog

FortiWLM MEA generates and maintains system logs on the system, or on an external server if required, and displays the logged information on the *Syslog* page.

You can access the *Syslog* screen through *Operate* > *Tools* > *Syslog*.



☑ Auto Refresh: 53 Sec

SEARCH ORDER (DATE/TIME) Descending

MAXIMUM RECORDS 200

START TIME ☑ NOW

END TIME □ NOW

ID	DATE/TIME	HOST	APPLICATION	USER	USER GROUP	PRIORITY	MNEMONIC	MESSAGE
11787	03/06/2020 15:23:13	342195764b22	security	system	system	info	Access	httpd[6415]: [ssl:info] [pid 6415:tid 139980961736448] [client 169.254.255.97:56666] AH01964: Connection to child 132 established (server 169.254.255.98:443)
11786	03/06/2020 15:19:33	342195764b22	security	system	system	info	Access	httpd[6415]: [ssl:info] [pid 6415:tid 139981047330560] [client 169.254.255.97:51688] AH01964: Connection to child 130 established (server 169.254.255.98:443)
11785	03/06/2020 15:18:58	342195764b22	security	system	system	info	Access	httpd[6415]: [ssl:info] [pid 6415:tid 139980944951040] [client 169.254.255.97:50716] AH01964: Connection to child 134 established (server 169.254.255.98:443)
11784	03/06/2020 15:18:42	342195764b22	security	system	system	info	Access	httpd[6415]: [ssl:info] [pid 6415:tid 139980953343744] [client 169.254.255.97:50516] AH01964: Connection to child 133 established (server 169.254.255.98:443)
								httpd[6988]: [ssl:info] [pid 6988:tid 139981064115968] [client 169.254.25

The Syslog page is organized into the following tabs:

- SysLog View on page 67
- External Syslog on page 68

SysLog View

System log data is displayed in the *SysLog View* tab on the *Syslog* page in the form of a table that summarizes the following:

Column Name	Description
ID	Displays the log ID.
Date/Time	Displays the date and time at which the log was recorded. The time is server local time.

Column Name	Description
Host	Displays the host name for which the log was recorded.
Application	Indicates the category to which the log belongs to.
Mnemonic	A code, usually an abbreviation, that identifies the type of error or event.
Priority	Displays the priority level. Currently only information messages are logged.
User	Displays the name of the logged in user at the time of log generation.
User Group	Displays the user group of which the user is a member.
Message	Consolidated description of the configuration changes that contain the objects on which an operation was performed, the type of operation, and the name of the modified profile.

You can filter the displayed system log data by modifying the *Search Order*, *Maximum Records*, *Start Time*, and *End Time* fields. To add advanced filters, click on *Advanced Filters* and add the required filtering parameters. Click the *Get Syslog* button to update the *Syslog* table with the latest system logs.

External Syslog

FortiWLM MEA is capable of maintaining the system log data on an external server. The External Syslog tab provides a way to enable remote system logging.

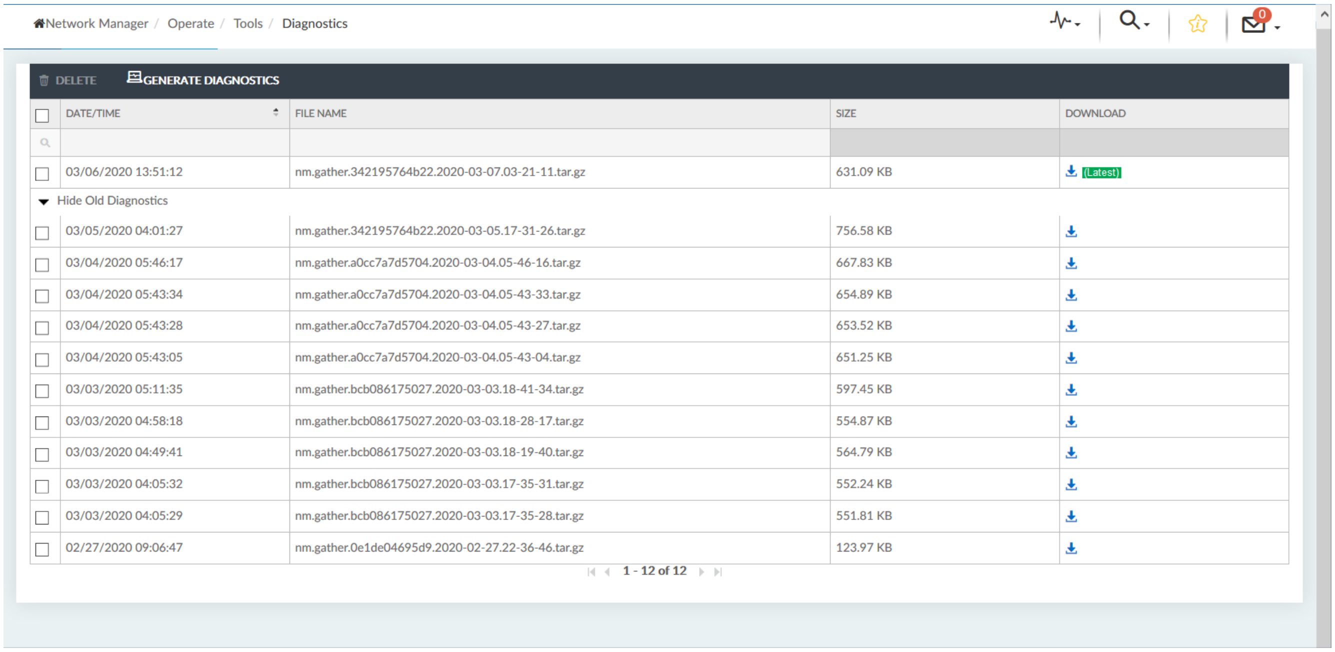
To enable remote system logging:

1. Select the *Enabled* radio button in the *Remote SysLog* field.
2. Enter the server IP address of the remote server in the *Server IP* field.
3. Specify the port number in the *Port* field.
4. Select the desired logging levels for *NMS*, *System*, and *Security* fields each.
5. Click *Save*. External or remote system logging is now enabled.

Diagnostics

FortiWLM MEA allows you to collect system diagnostics data that comprises of system logs and other files. Diagnostics data is particularly helpful in troubleshooting any issues with the system.

You can access the *Diagnostics* screen through *Operate* > *Tools* > *Diagnostics*.



☐	DATE/TIME	FILE NAME	SIZE	DOWNLOAD
☐	03/06/2020 13:51:12	nm.gather.342195764b22.2020-03-07.03-21-11.tar.gz	631.09 KB	⤓ (Latest)
☐	03/05/2020 04:01:27	nm.gather.342195764b22.2020-03-05.17-31-26.tar.gz	756.58 KB	⤓
☐	03/04/2020 05:46:17	nm.gather.a0cc7a7d5704.2020-03-04.05-46-16.tar.gz	667.83 KB	⤓
☐	03/04/2020 05:43:34	nm.gather.a0cc7a7d5704.2020-03-04.05-43-33.tar.gz	654.89 KB	⤓
☐	03/04/2020 05:43:28	nm.gather.a0cc7a7d5704.2020-03-04.05-43-27.tar.gz	653.52 KB	⤓
☐	03/04/2020 05:43:05	nm.gather.a0cc7a7d5704.2020-03-04.05-43-04.tar.gz	651.25 KB	⤓
☐	03/03/2020 05:11:35	nm.gather.bcb086175027.2020-03-03.18-41-34.tar.gz	597.45 KB	⤓
☐	03/03/2020 04:58:18	nm.gather.bcb086175027.2020-03-03.18-28-17.tar.gz	554.87 KB	⤓
☐	03/03/2020 04:49:41	nm.gather.bcb086175027.2020-03-03.18-19-40.tar.gz	564.79 KB	⤓
☐	03/03/2020 04:05:32	nm.gather.bcb086175027.2020-03-03.17-35-31.tar.gz	552.24 KB	⤓
☐	03/03/2020 04:05:29	nm.gather.bcb086175027.2020-03-03.17-35-28.tar.gz	551.81 KB	⤓
☐	02/27/2020 09:06:47	nm.gather.0e1de04695d9.2020-02-27.22-36-46.tar.gz	123.97 KB	⤓

On the *Diagnostics* screen, you can view old and new diagnostics data in the form of a table. The latest system diagnostics data is always the first row in the table and is indicated by a green highlighted `(Latest)` label next to the download button. All other old diagnostics data follows on in subsequent rows. Each row of the table is comprised of the following fields:

Field	Description
Date/Time	Displays the date and time at which the diagnostics data was collected, in MM/DD/YYYY HH:MM:SS format.
File Name	The name of the diagnostics data file.
Size	The size of the diagnostics data file.
Download	Provides a download button to download and save the diagnostics file on your local drive.

To generate new diagnostics data, click the *Generate Diagnostics* button on the upper-left of the diagnostics data table.

To delete a row of diagnostics data from the table, select the row and click *Delete*.

Maps

FortiWLM MEA provides a way to visually track the APs in the network. You can create maps to track the APs visually. Maps are image files that accurately represent the physical layout of a site and are as close to scale as possible.

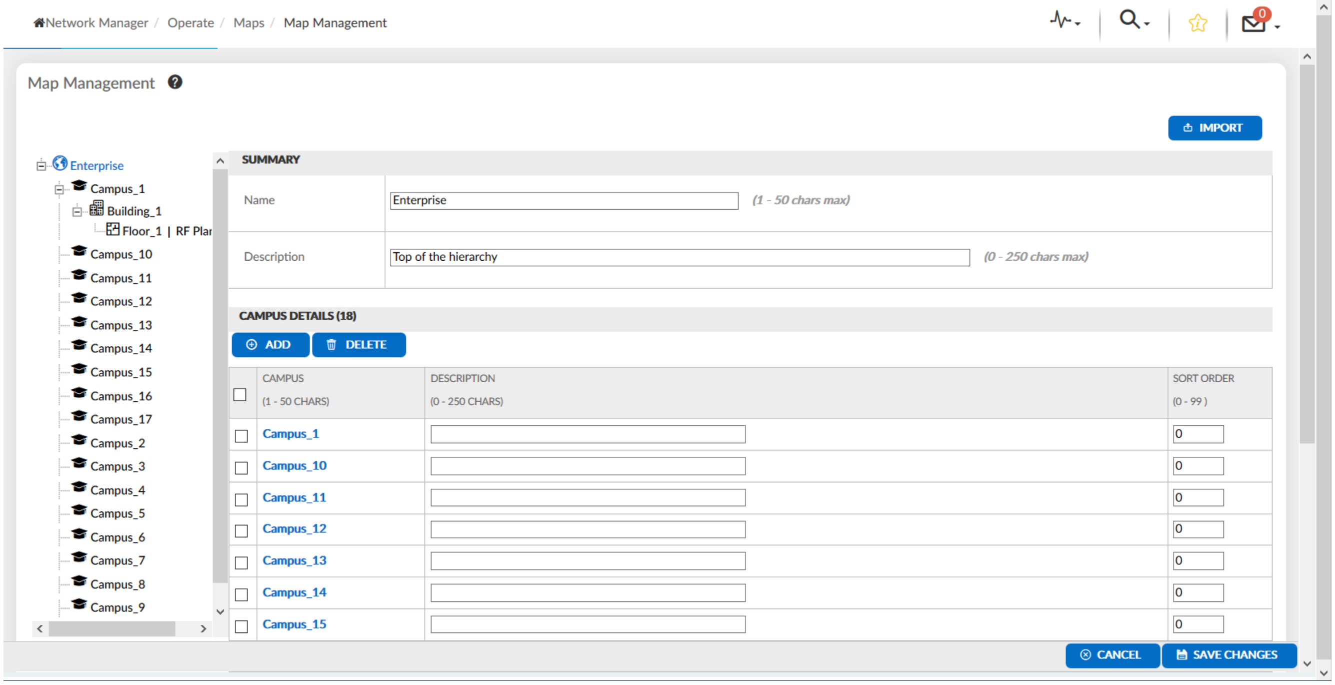
You should use separate maps for separate floors in a multi-floor building. Map images should be based on accurate architectural drawings. The image files should be in a PNG, JPEG, BMP, or GIF file format, and no larger than 2 MB in size.

The *Maps* branch of the tree menu in the left navigation pane is further branched into Map Management on page 70.

Map Management

Map management involves the procedures like importing maps; adding a new campus, building, and floor to the imported map; depicting the wireless network topology by placing icons on the map; viewing, editing, and deleting maps, and so on.

You can access the *Map Management* screen through *Operate* > *Maps* > *Map Management*.



SUMMARY

Name	Enterprise	(1 - 50 chars max)
Description	Top of the hierarchy	(0 - 250 chars max)

CAMPUS DETAILS (18)

☐	CAMPUS (1 - 50 CHARS)	DESCRIPTION (0 - 250 CHARS)	SORT ORDER (0 - 99)
☐	Campus_1		0
☐	Campus_10		0
☐	Campus_11		0
☐	Campus_12		0
☐	Campus_13		0
☐	Campus_14		0
☐	Campus_15		0

The *Map Management* screen displays a tree menu in the left with the *Enterprise* node being the top level node. You can add any number of campuses below the *Enterprise* node. You can add *Buildings* and *Landmarks* in a *Campus*, and add *Floors* to *Buildings*. You can also change the map image associated with a Floor.

For more information on managing maps:

- See Importing a Map Plan on page 70.
- See Managing a Campus Map on page 71.
- See Managing a Floor Map on page 73.
- See RF Planner on page 75.
- See Viewing Maps on page 77.

Importing a Map Plan

FortiWLM MEA provides a way to import a map plan created in and exported from FortiPlanner. FortiPlanner exports the map plan files in a ZIP file format. The exported ZIP file can be imported in FortiWLM MEA.

To import a map plan:

1. Click the *Import* button on the upper-right of the *Map Management* screen. The *Import Map Plan* screen is displayed.
2. Browse for the ZIP file to be imported, which is the map data file exported from FortiPlanner.

3. Click *Next*. A summary of map information is displayed.
4. Map the unassigned APs, and click *Finish*.

   The planner for each of the imported campuses is displayed on the *Map Management* screen, where you can manage buildings, landmarks, floors, APs, map images, and so on.

   You may click *View Latest Import Planner Logs* on the *Import Map Plan* screen to view error logs, if there are any errors in the import process.

Managing a Campus Map

When you are at the *Enterprise* top-level node on the *Map Management* screen, a quick summary of the node is displayed. Below the summary, you can view all the campuses that belong to the top-level node, in the form of a table called *Campus Details*. You may add a new campus, or delete an existing one:

- See Adding a campus on page 71.
- See Deleting a campus on page 71.

After you have added a campus, click on the campus name in the tree menu at the left to view the *Campus Map* screen. On the *Campus Map* screen you may add or delete buildings and landmarks, and change the campus image:

- See Adding buildings to a campus on page 71.
- See Deleting buildings from a campus on page 72.
- See Adding landmarks to a campus on page 72.
- See Deleting landmarks from a campus on page 72.
- See Changing campus images on page 72.

Adding a campus

To add a campus:

1. Click the *Add* button located at the upper-left of the *Campus Details* tables. A new row is added to the table.
2. Type a name for the new campus in the *Campus* field of the new row.
3. Click *Save Changes*. A new campus is added.

Deleting a campus

To delete a campus:

1. Select the campus to be deleted by clicking the campus check box in the *Campus Details* table.
2. Click the *Delete* button located at the upper-left of the *Campus Details* table.
3. Click *OK* in the confirmation dialog.
4. Click *Save Changes*. The campus is deleted.

Adding buildings to a campus

To add a building to a campus:

1. Click the *Buildings* button from the *Campus Map* screen. The *Manage Campus Buildings* dialog appears.
2. Click the *Add* button. A new row is added to the *Building Details* table.
3. Type a name for the new building in the *Building* field of the new row.
4. Click *OK*. The 🏢 icon appears on the icons tray on screen.

5. Click on the 🏢 icon once. The icon is selected.
6. Click on the image map below the icons tray. The building is now placed on the image map.
7. Click *Save Changes*. A new building is added.

Deleting buildings from a campus

To delete a building:

1. Click the *Buildings* button from the *Campus Map* screen. The *Manage Campus Buildings* dialog appears.
2. Select a building to be deleted by clicking the building selection check box in the table.
3. Click the *Delete* button located at the upper-left of the table.
4. Click *OK* in the confirmation dialog.
5. Click *OK* again.
6. Click *Save Changes*. The building is deleted.

Adding landmarks to a campus

To add a landmark to a campus:

1. Click the *Landmarks* button from the *Campus Map* screen. The *Manage Landmarks* dialog appears.
2. Click the *Add* button. A new row is added to the *Campus Landmarks* table.
3. Type a name for the new landmark in the *Landmark Name* field of the new row.
4. Click *OK*. The 📍 icon appears on the icons tray on screen.
5. Click on the 📍 icon once. The icon is selected.
6. Click on the image map below the icons tray. The landmark is now placed on the image map.
7. Click *Save Changes*. A new landmark is added.

Deleting landmarks from a campus

To delete a landmark:

1. Click the *Landmarks* button from the *Campus Map* screen. The *Manage Landmarks* dialog appears.
2. Select a landmark to be deleted by clicking the landmark selection check box in the table.
3. Click the *Delete* button located at the upper-left of the table.
4. Click *OK* in the confirmation dialog.
5. Click *OK* again.
6. Click *Save Changes*. The landmark is deleted.

Changing campus images

To change a campus image:

1. Click the *Change Image* button from the *Campus Map* screen. The *Change Image* dialog appears.
2. Select the type of operation you want to perform from the *Operation* field:
   - a. Select the *Upload* option to upload a new image.
   - b. Browse for an image file and select it.
   - c. Click *Upload*. The image file is uploaded.

   OR

   a. Select the *Delete* option to delete the existing image. The *Image File* field is grayed.
   b. Click *Delete*.
   c. Click *OK* in the confirmation dialog. The image file is deleted.
3. Click *Save Changes*. The campus image is changed.

Managing a Floor Map

Click on a building name in the tree menu at the left to view a summary of the selected building and the floors belonging to that building. The floors are listed in the *Floor Details* table. You may add a new floor, or delete an existing one:

- See Adding floors to a building on page 73.
- See Deleting floors from a building on page 73.

After you have added a floor, click on the floor name in the tree menu at the left to view the *Floor Map* screen. On the *Floor Map* screen you may add or delete APs and landmarks, and change the floor image:

- See Adding APs to a floor on page 73.
- See Deleting APs from a floor on page 74.
- See Adding landmarks to a floor on page 74.
- See Deleting landmarks from a floor on page 74.
- See Changing floor images on page 74.

Adding floors to a building

To add a floor to a building:

1. Click the *Add* button located at the upper-left of the *Floor Details* tables. A new row is added to the table.
2. Type a name for the new floor in the *Floor* field of the new row.
3. Click *Save Changes*. A new floor is added.

Deleting floors from a building

To delete a floor from a building:

1. Select the floor to be deleted by clicking the floor check box in the *Floor Details* table.
2. Click the *Delete* button located at the upper-left of the *Floor Details* table.
3. Click *OK* in the confirmation dialog.
4. Click *Save Changes*. The floor is deleted.

Adding APs to a floor

To add APs to a floor:

1. Click the *Add APs* button from the *Floor Map* screen. The *AP Selection* dialog appears.
2. Select a controller from the *Controller Name* drop-down list. The corresponding *Controller IP* is selected and the APs connected to the selected controller are displayed.
3. Select the APs you want to add on the floor from the list of APs.
4. Click *Save*. The ☎ icon appears on the icons tray on screen.
5. Click on the ☎ icon once. The icon is selected.

6. Click on the image map below the icons tray. The AP is now placed on the image map.
7. Click *Save Changes*. An AP is added.

Deleting APs from a floor

To delete APs from a floor:

1. Click the *Floor APs* button from the *Floor Map* screen. The *Manage Floor APs* dialog appears.
2. Select an AP to be deleted by clicking the AP selection check box in the table.
3. Click the *Delete* button located at the upper-left of the table.
4. Click *OK* in the confirmation dialog.
5. Click *OK* again.
6. Click *Save Changes*. The AP is deleted.

Adding landmarks to a floor

To add landmarks to a floor:

1. Click the *Landmarks* button from the *Floor Map* screen. The *Manage Landmarks* dialog appears.
2. Click the *Add* button. A new row is added to the *Floor Landmarks* table.
3. Type a name for the new landmark in the *Landmark Name* field of the new row.
4. Click *OK*. The 📍 icon appears on the icons tray on screen.
5. Click on the 📍 icon once. The icon is selected.
6. Click on the image map below the icons tray. The landmark is now placed on the image map.
7. Click *Save Changes*. A new landmark is added.

Deleting landmarks from a floor

To delete landmarks from a floor:

1. Click the *Landmarks* button from the *Floor Map* screen. The *Manage Landmarks* dialog appears.
2. Select a landmark to be deleted by clicking the landmark selection check box in the table.
3. Click the *Delete* button located at the upper-left of the table.
4. Click *OK* in the confirmation dialog.
5. Click *OK* again.
6. Click *Save Changes*. The landmark is deleted.

Changing floor images

To change a floor image:

1. Click the *Change Image* button from the *Floor Map* screen. The *Change Image* dialog appears.
2. Select the type of operation you want to perform from the *Operation* field:

    a. Select the *Upload* option to upload a new image.

    b. Browse for an image file and select it.

    c. Click *Upload*. The image file is uploaded.

    OR

   a. Select the *Delete* option to delete the existing image. The *Image File* field is grayed.
   b. Click *Delete*.
   c. Click *OK* in the confirmation dialog. The image file is deleted.
3. Click *Save Changes*. The campus image is changed.

RF Planner

RF Planner facilitates in the planning of addition of new APs and areas with obstacles like walls, columns, and so on, to the *Floor* plan. To access RF planner, click on the *RF Planner* link beside the floor name in the left tree menu, or go to the *Floor Map* screen and click the *RF Planner* button. The *RF Planner* for that floor opens up in a new modal window.

RF Planner may be interacted with in the following two modes:

- Edit mode: It is the default mode. It allows you to add, edit, and delete *APs*, *Walls*, *Columns*, and so on, on the floor map.
- View mode: It displays the *Data Rate*, *Channel*, and *Signal Strength* of APs on the floor map for 2.4 GHz or 5 GHz spectrum.

Adding APs on the floor map

To add an AP on the floor plan:

1. Select an AP from the *Add APs* section at the upper-left of the *RF Planner*. The cursor changes to a crosshair, as you move the cursor onto the floor map.
2. Click on the floor map. The selected AP is added on the floor map.
3. Click and drag the added AP to change its position on the floor map.
4. Click *Save* at the upper-right of the *RF Planner* window to save the configuration.

Deleting APs from the floor map

To delete an APs from the floor plan:

1. Move and point the cursor to an AP on the floor map.
2. Right-click on the AP. A right-click menu with options to choose from appears.
3. Select *Delete* from the menu. The AP is deleted.
4. Click *Save* at the upper-right of the *RF Planner* window to save the configuration.

Editing APs on the floor map

To edit an APs on the floor plan:

1. Move and point the cursor to an AP on the floor map.
2. Right-click on the AP. A right-click menu with options to choose from appears.
3. Select *Edit* from the menu. The *Access Point Configuration* dialog is displayed.
4. Select the required AP from the *Device* drop-down list. You may have one or more *Radios* having different frequencies associated with the selected AP.
5. Choose the required transmission power by sliding the *Transmit Power dBm* slider.
6. Select an appropriate channel for the AP from the *Channel* drop-down list.

7. Select the required orientation from the *Orientation* drop-down list. The graphic below is updated based on the selected option.
8. Set the inclination of the AP in degrees by changing the *Direction* setting.
9. Click *Save*. The AP is configured.
10. Click *Save* at the upper-right of the *RF Planner* window to save the configuration.

Adding walls on the floor map

To add a wall on the floor plan:

1. Click the ⟍ button from the toolbar at the left of the *RF Planner* window. The cursor changes to a crosshair, as you move the cursor onto the floor map.
2. Click once and drag in the direction you want to add the wall on the floor map, and click again to stop drawing. A wall is added on the floor map.
3. Click and drag the added wall to change its position on the floor map.
4. Click *Save* at the upper-right of the *RF Planner* window to save the configuration.

Deleting walls from the floor map

To delete a wall from the floor plan:

1. Move and point the cursor to a wall on the floor map.
2. Right-click on the wall. A right-click menu with options to choose from appears.
3. Select *Delete* from the menu. The wall is deleted.
4. Click *Save* at the upper-right of the *RF Planner* window to save the configuration.

Editing walls on the floor map

To edit a wall on the floor plan:

1. Move and point the cursor to a wall on the floor map.
2. Right-click on the wall. A right-click menu with options to choose from appears.
3. Select *Edit* from the menu. The *Wall Configuration* dialog is displayed.
4. Select the required wall material from the *Material* drop-down list. You may select the material for the wall, window, or door.
5. Click *Save*. The wall is configured.
6. Click *Save* at the upper-right of the *RF Planner* window to save the configuration.

Adding columns on the floor map

To add a column of walls on the floor plan:

1. Click the ⌑ button from the toolbar at the left of the *RF Planner* window. The cursor changes to a crosshair, as you move the cursor onto the floor map.
2. Click once and drag across on the floor map, and click again to stop drawing. A column of four walls is added on the floor map.
3. Click and drag the added walls to change their position individually on the floor map.
4. Click *Save* at the upper-right of the *RF Planner* window to save the configuration.

To edit or delete a column, each of the four walls of a column must be edited or deleted separately.

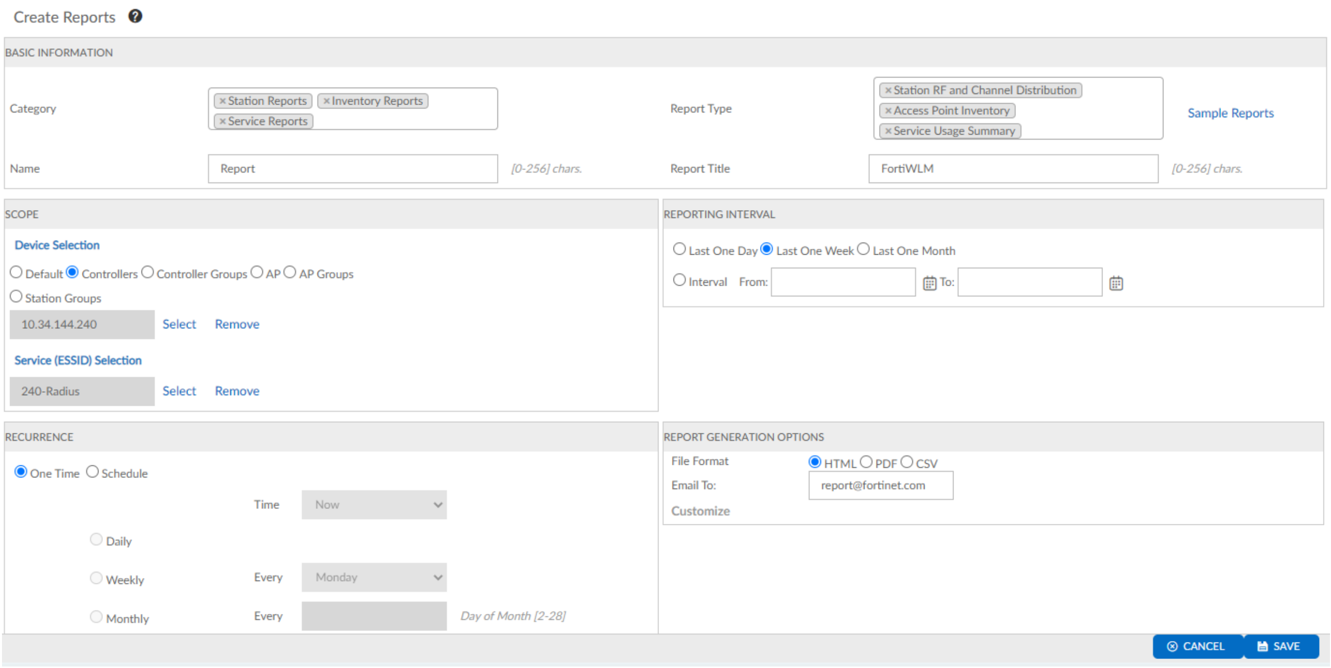
Viewing Maps

FortiWLM MEA provides a visualization feature allowing you to check the coverage and performance of APs in the wireless network. The *Network Heat Maps* dashboard displays actual AP statistics retrieved from the controller, extrapolated into graphic files known as *Heat Maps*. Heat maps can be generated for historical data.

You can access the *Network Heat Maps* dashboard through *Monitor* > *Overview* > *Heat Maps*. For more information on viewing heat maps, see Network Heat Maps on page 42.

Reporting in FortiWLM MEA

The FortiWLM MEA provides standard report types to assist the administrator to generate a report or schedule a report. You can select and combine multiple report categories and the subsequent report types (maximum 5) to generate a single report instead of generating multiple reports for each category. These are saved as *Report Templates* and can be scheduled similar to other reports. Navigate to the *Reports* tab.



Create Reports

BASIC INFORMATION

Category: ×Station Reports ×Inventory Reports ×Service Reports

Report Type: ×Station RF and Channel Distribution ×Access Point Inventory ×Service Usage Summary

Name: Report [0-256] chars.

Report Title: FortiWLM [0-256] chars.

SCOPE

Device Selection

○ Default ● Controllers ○ Controller Groups ○ AP ○ AP Groups
○ Station Groups

10.34.144.240

Service (ESSID) Selection

240-Radius

REPORTING INTERVAL

○ Last One Day ● Last One Week ○ Last One Month

○ Interval From: To:

RECURRENCE

● One Time ○ Schedule

Time: Now

○ Daily

○ Weekly Every: Monday

○ Monthly Every: Day of Month [2-28]

REPORT GENERATION OPTIONS

File Format: ● HTML ○ PDF ○ CSV

Email To: report@fortinet.com

- Basic Information on page 78
- Scope on page 83
- Reporting Interval on page 84
- Recurrence on page 84
- Report Generation Options on page 84
- Managing Reports on page 85

Basic Information

Enter the report *Name* and *Title* and select the report category. The following report categories and associated types are supported.

- Station Reports
- AP Reports on page 80
- Inventory Reports on page 81
- Network Health Reports on page 81
- Service Reports on page 83
- Application Visibility on page 83

Station Reports

The following types of station reports can be generated.

Report Type	Description
Station RF and Channel Distribution	Generates a report based on the statistics accumulated over the reporting interval. The number of stations per channel over the reporting period is displayed. **Graphs** - The following graphs are displayed. • **Station Distribution by RF Type** - This graph displays the station distribution based on the RF Type. • **Station Distribution Across 2.4 GHz and 5GHz Bands** - This graph displays the station distribution based on the 2.4GHz and 5GHz. • **Station Density on each Channel Over Time** - This graph displays the station density on each of the channels over time plotted against the time in weeks. **Station RF and Channel Distribution Details** - This section provides each station's *OUI, Date/Time (GMT), Station Mac, RF Type, AP Name, AP Radio, SSID* and *Channel*.
Station Session Details	Generates the station statistical report (Throughput, Loss, Airtime Utilization and Noise) for a connected station. **Graphs** - The following graphs are displayed. • **Trend On Airtime Utilization** - This graph displays the trend of airtime utilization for the selected station. • **Trend On Loss** - This graph displays the trend of loss for the selected station. • **Trend On Throughput** - This graph displays the trend of throughput for the selected station. **Station Session Details** - This section provides each station s *Date/Time, IP4 Address, IP6 Address, Controller, AP ID, SSID, User, Throughput (Kbps), Loss%, Airtime Utilization%*, and *AP Name*.
Top Stations	Generates reports for the busiest stations based on the Throughput and Airtime Utilization. This report type generates the Top N stations based on the number of bytes transferred and received and total Rx/Tx. The information includes each station s *Station Mac, Controller, AP Id, SSID, Throughput (Kbps)*, and *Date/Time (GMT)*.
EAP-AKA Error	Generates a report with details of EAP-AKA errors associated with specific ESSIDs and on specific stations connected to network within the reporting interval.**User selected Top 5 EAP-AKA Errors** - The top 5 most common EAP-AKA errors with the number of stations the errors were reported on and the number of EAP authentication failures for each station. **User selected Top 5 Station by Errors** - The top 5 stations (MAC addresses) with highest EAP-AKA errors reported and the number of EAP authentication failures for each station.

Report Type	Description
	EAP-AKA Errors - The list of EAP-AKA errors within the reporting interval. The details displayed are, date and time of the error, associated controller, access point, station MAC address, and the ESSID, and the error description/reason.
Unique Stations	This report type generates a report with all the stations connected to network within the reporting interval. The *Unique Station Reports* are available to all groups and list stations connected to network during last 24 hours. • **Summary** - This section provides the total number of unique stations. • **Graphs** - The following graphs are supported. • **Station Distribution** - This graph displays the station distribution based on the RF Type. • **OUI Distribution** - This graph displays the station distribution based on the OUI. • **Finger Print Device Distribution** - This graph displays the station distribution based on the Device Type. • **Finger Print OS Distribution** - This graph displays the station distribution based on the OS Type. • **Unique Station Details** - This section provides the station s OUI, *Date/Time (CST), Station MAC, User, IPv4 Address, IPv6 Address, RF Type, SSID, Device Type, OS Type* and *Floor*.

AP Reports

The following types of AP reports can be generated.

Report Type	Description
Rogue Details	Generates the report on the individual rogue. It displays the rogue mobility trend. The trend is plotted against time and APs detecting the rogue. The data displayed is a maximum of hourly data sample. • **Summary** - This section provides the details of the selected rogue. • **Graph** - The **Rogue Mobility Trend** graph is displayed. Trend is plotted against AP which detects rogues with high strength and its time as samples. • **Rogue Details** - This section provides details about the APs detecting the rogue along with *Date/Time, Controller, AP Detecting Rogue, AP Location, SSID, Channel*, and *RSSI*.
Rogue Summary	Generates the report based on the trend of the number of rogues reported on a per controller basis, per hour. The data is a maximum of hourly data samples. **Summary** - This section provides the details of the total number of rogues. **Graph** - The following graphs are displayed. • **Rogue Trend By Type** - The two types of *Rogue Trend By Type* graphs are displayed. • **Trend On Rogue AP** - This graph displays the trend type based on the number of Rogue APs. • **Trend on Rogue Station** - This graph displays the trend type based on the number of Rogue Stations.

Report Type	Description
	- **Rogue Trend By Controllers** - This graph displays the top 10 controllers with the highest number of Rogues. **New Rogues Detected During Reporting Interval** - This section provides the details of the new rogues detected during reporting interval. The details are *Date/Time, Controller, AP Detecting Rogue, AP Location, Rogue MAC, Rogue Type*, and *Channel RSSI*.
Top Radio	Generates a report displaying all the top radios based on *Station Count, Throughput*, and *High Loss*. The top radio report type displays the *AP Name, Radio, Controller Name, AP Location, Station*, and *Date/Time (GMT)*.

Inventory Reports

The following types of inventory reports can be generated.

Report Type	Description
Access Point Inventory	Generates the AP inventory summary reports for any APs that are accessible to your user group. **Summary** - This section provides the total number of APs. **Graph** - The **AP Model Distribution** graph provides the pictorial representation of the distribution of APs. **AP Inventory Summary** - This section provides the details of the AP inventory. The details are *Name, Mac address, Model, Software Version, IP Address, Controller, Availability State, Connectivity Preference*, and *Floor*.
Controller Inventory	Generates the controller inventory summary reports for any controllers that are accessible to your user group. **Summary** - This section provides the total number of controllers. **Graph** - The following graphs are displayed. - **Controller Model Distribution** - This graph displays the controllers based on the controller model distribution. - **Controller Software Version Distribution** - This graph displays the controllers based on the controller software version distribution. **Controller Inventory Summary** - This section provides the details of controller Inventory. The details are *Hostname, IP Address, Mac address, Node Name, Software Version, Model, Description, Availability State, Management State*, and *Location*.
Device Availability	Generates the report for each controller and AP. It displays the *Device Name, UP Duration, Down Duration time* and *Availability(%)* for the AP and controller.

Network Health Reports

The following types of network health reports can be generated.

Report Type	Description
Alarm	Generates a report on the alarms raised. **Summary** - This section provides the total number of alarms raised. This includes the *Critical Alarms, Major Alarms*, and *Minor Alarms*. **Graph** - The following graphs are displayed. • **Alarm Distribution By Category** - This graph displays the alarm distribution based on Category. • **Top 10 Controller with High Alarms** - This graph displays the alarm distribution based on the controller with high alarms. • **Top 10 Access Points with High Alarms** - This graph displays the alarm distribution based on the APs with high alarms. **Alarm Report table**s - The following types of alarm reports are generated. • **Most Frequent Alarms** - This table provides a statistical output of the top 10 most frequent alarms raised. It displays the alarms *Category, Alarm Type, Severity* and *Number of Occurrence*. • **Longest Duration Alarms** - This table provides a statistical output of the top 10 longest duration alarms raised. It displays the alarms' *Source, Device ID, Category, Alarm Type, Severity, Raise Date/Time (GMT), Clear Date/Time (GMT), Duration* and *Message*. • **List of Standing Alarms** - This table provides a statistical output of the top 10 standing alarms raised. It displays the alarms' *Date/Time (GMT), Source, Device Name, Category, Alarm Type, Severity* and *Message*. • **Devices With High Alarms** - This table provides a statistical output of the devices with high alarms raised. It displays the alarms' *Device* and *Number of Occurrence*.
Network Utilization and Capacity	Generates a report on the overall load of the system. The overall load is the highest overload contributed by of any of the constituent variables. **Graph** - The following graphs are displayed. • **Capacity Utilization for 2.4GHz radios by station count** - This graph displays the capacity utilization for 2.4GHz radios by number of stations. • **Capacity Utilization for 5GHz radios by station count** - This graph displays the capacity utilization for 5GHz radios by number of stations. • **Capacity Utilization for 2.4GHz radios by Throughput** - This graph displays the capacity utilization for 2.4GHz radios by throughput. • **Capacity Utilization for 5GHz radios by Throughput**: This graph displays the capacity utilization for 5GHz radios by throughput. **Network Utilization and Capacity Report** tables - The following types of *Network Utilization and Capacity Reports* are generated. • **List of overloaded APs based on station count** - This table provides a statistical output of the list of overloaded APs based on station count. It displays the station's *Date/Time, Controller, AP Name, AP MAC, AP Location, AP Model, Radio Type* and *No. Of Stations*. • **List of overloaded APs based on Throughput** - This table provides a statistical output of the list of overloaded APs based on throughput. It displays the throughput's *Date/Time, Controller, AP Name, AP MAC, AP Location, AP Model, Radio Type* and *Throughput (Mbps)*.

Report Type	Description
	• **List of overloaded APs based on Air time utilization** - This table provides a statistical output of the list of overloaded APs based on airtime utilization. It displays the air time utilization's *Date/Time, Controller, AP Name, AP MAC, AP Location, AP Model, Radio Type* and *Air time utilization*.

Service Reports

The following types of service reports can be generated.

Report Type	Description
Service Usage Summary	Generates a report displaying all the ESSIDs. **Graph** - The following graphs are displayed. • **Top SSIDs Based on Number Stations** - This graph displays the top SSIDs based on number of stations. • **Top SSIDs Based on Throughput** - This graph displays the top SSIDs based on the throughput. **Network Usage Summary** - Displays the *ESSID, Average Station Count, Max Station Count, Time When Max Station Occurred, Total Unique Stations* and *Maximum Throughput*.
Service Usage Trend	Generates a report for a selected ESSID. **Graphs** - The **Server Usage Trend** graphs are displayed with a trend of maximum, minimum, and average stations connected and stations throughput on hourly basis during reporting interval. This is a graphical report represented with a line chart having two lines, one for maximum and second one for average station count. **Service Usage Trend Details** - The service usage trend report type displays *Date/Time (GMT), Max Stations Connected, Min Stations Connected, Avg Stations Connected*, and *Throughput (Kbps)*.

Application Visibility

Th is report type generates a report displaying all the selected devices.

Report Type	Description
Application Visibility	**Graph** - The following graphs are supported. • **Top 10 applications** - For each application, it provides total number of connected users, ESSIDs and traffic utilization. • **Top 10 users** - For each of the user, it displays the client MAC address, applications connected by the client, ESSIDs and traffic utilization.

Scope

You can select the scope of the report by selecting the devices to generate the report for. Click on *Select* to select a controller, controller group, AP, or AP group and the list of the available devices for the selected type is displayed. Select one or multiple associated SSIDs.

Reporting Interval

Configure the time interval to generate the report. You can specify the interval manually or use the *Calendar* option. Additionally, the following options are also supported.

- **Last one day -** The last one day's report is displayed.
- **Last one week -** The last one week's report is displayed.
- **Last one month -** The last one month's report is displayed.

Recurrence

You can schedule report generation at fixed intervals or make it happen just one time. You can select the *One Time* option to generate the report once or *Schedule* it. Update the following parameters to **schedule** report generation.

Parameter	Description
Daily	Generates the report every day.
Weekly	To generate the weekly reports, select this option and then select the day of the week for report generation.
Monthly	To generate the monthly reports, select this option and specify the day of month between 1 and 31.

Report Generation Options

You can customize and generate the reports in various file formats.

Parameter	Description
File Format	The following report generation formats are supported. • **HTML Report** - Select the HTML option to export and save the report to HTML format. The generated report is saved with the naming convention *<report type>_report_datetime.html.* • **PDF Report** - Select the PDF option to export and save the report to PDF format. The generated report is saved with the naming convention *<report type>_report_datetime.pdf*. • **CSV Report** - Select the CSV option to export and save the report to CSV format. The generated report is saved with the naming convention *<report type>_report_datetime.csv*.
Email To	Provide an email ID to email the report in the selected file format.
Customize Report	You can generate customized reports by selecting the desired attributes to be displayed on the report. Select the *Customize* link and the *Customize Report* wizard is displayed. **Display Summary Graphs** - This graph provides the following options. • Yes: This option displays the graph in the generated report. • No: This option does NOT display the graph in the generated report.

Parameter	Description
	Available Attributes - This column displays a list of available attributes that can be selected for the report generation. **Attributes to be displayed in report** - This column displays a list of selected attributes to be displayed in report.

Managing Reports

You can view, print, and save the generated reports in the *View Reports* window. All generated reports are displayed here. To view scheduled reports that are generated at specific intervals go to **Scheduled Reports**; you can edit or add a new schedule from this page.

FortiWLM MEA can be validated against specific PCI requirement compliance. To run a compliance test, go to **PCI Report** and set *Run PCI tTst* to **Yes**. Now select the tests to validate FortiWLM MEA and click **Run Test**. After the test is executed, an alert box displays the status of the text. The page is refreshed to show the list of PCI requirements that are validated for FortiWLM MEA. The validation results are shown in *green* if they are passed and in *red* if the compliance is not validated or failed. You can download the PCI report in a *.pdf* format.

Administering FortiWLM MEA

FortiWLM MEA administration involves setting user preferences like notification profiles and filters, configuration of system settings like server details, mail server administration, system log policies, the management of licenses, upgrading the system, and so on.

The *Administration* branch from the tree menu in the left navigation pane provides a way to access the various administration tools through the following branches:

- User Preferences on page 86
- System Settings on page 89
- Licensing on page 98
- Upgrade on page 100

User Preferences

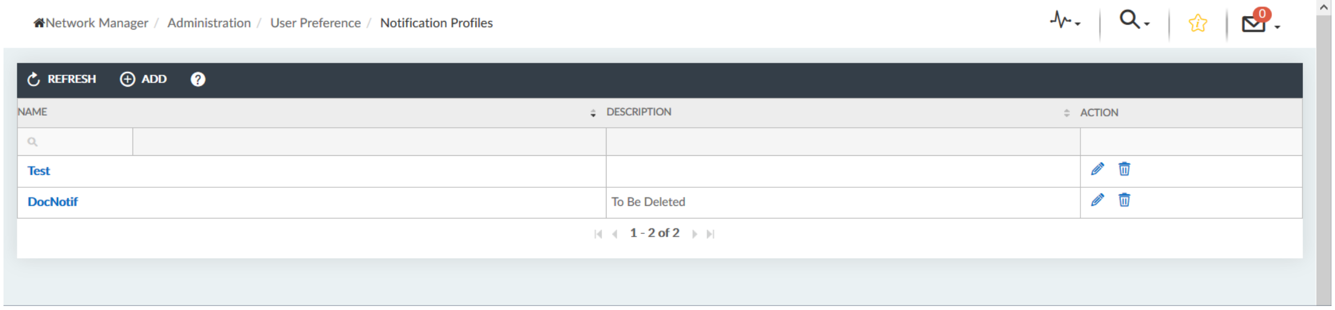
FortiWLM MEA monitors and manages various devices in the wireless network. It facilitates you as a user to get notified if a controller goes down at any time. The notification system involves setting up notification profiles and filters. The *User Preferences* branch of the tree menu in the left navigation pane is further branched into:

- Notification Profiles on page 86
- Notification Filters on page 87

Notification Profiles

Notification Profiles are configured to define an email list of recipients to be notified by the system. Configuring a notification profile alone will not result in any action unless you associate it with a response either by creating a notification filter or by configuring an email server and creating the corresponding users in your email system.

You can access the *Notification Profiles* screen through *Administration* > *User Preferences* > *Notification Profiles*.


Network Manager / Administration / User Preference / Notification Profiles
REFRESH
ADD

NAME	DESCRIPTION	ACTION
Test		
DocNotif	To Be Deleted	

1 - 2 of 2

To view an existing notification profile, click the notification profile name from the *Name* column of the *Notification Profiles* table.

To add, edit, or delete notification profiles:

- See Adding a Notification Profile on page 87.
- See Editing a Notification Profile on page 87.
- See Deleting a Notification Profile on page 87.

Adding a Notification Profile

To add a notification profile:

1. Click the *Add* button on the upper-left of the *Notification Profiles* table. The *Add Notification Profiles* dialog appears.
2. Enter a name for the notification profile in the *Name* field.
3. Enter a description for the notification profile in the *Description* field. It is optional.
4. Enter the list of e-mails of recipients separated by commas in the *E-Mail IDs* field. You must enter at least one e-mail.
5. Click *Save*. A notification profile is created and added to the table.

Editing a Notification Profile

To add a notification profile:

1. Click the ✎ button from the *Actions* column for the notification profile to be edited from the *Notification Profiles* table. The *Edit Notification Profiles* dialog appears.
2. Change the notification profile description in the *Description* field as required.
3. Add or remove email addresses from the *E-Mail IDs* field as required.
4. Click *Save*. The notification profile is edited successfully.

Deleting a Notification Profile

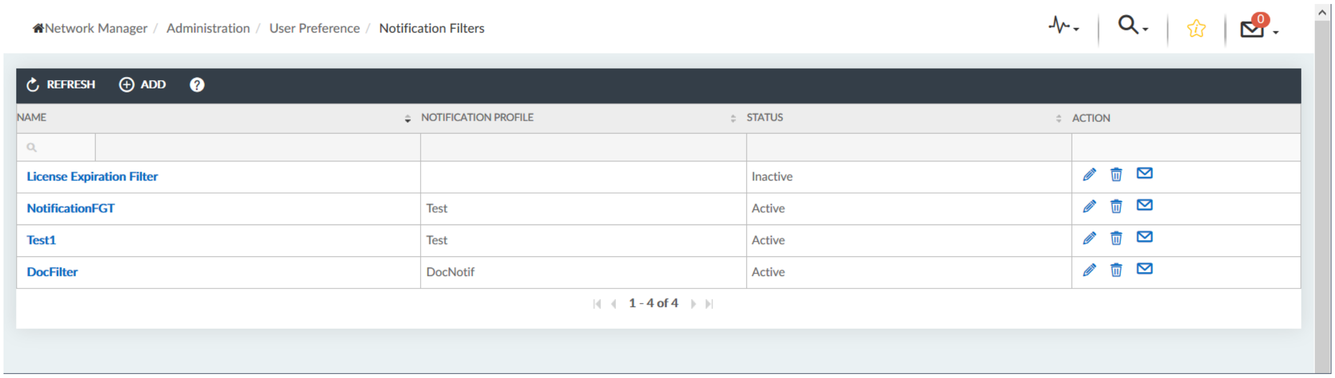
To delete a notification profile:

1. Click the 🗑 button from the *Actions* column for the notification profile to be deleted from the *Notification Profiles* table. A confirmation dialog appears.
2. Click *Yes*. The notification profile is deleted successfully.

Notification Filters

Notification Filters are configured to specify which alarms trigger notifications. For example, if you configure a notification filter with the *Critical* alarm severity selected, only critical alarms will trigger notifications. You may associate a notification profile with a notification filter to notify the users defined in the notification profile. You may also send weekly reports by configuring notification filters.

You can access the *Notification Filters* screen through *Administration* > *User Preferences* > *Notification Filters*.


Network Manager / Administration / User Preference / Notification Filters
REFRESH
ADD
1 - 4 of 4

NAME	NOTIFICATION PROFILE	STATUS	ACTION
License Expiration Filter		Inactive	
NotificationFGT	Test	Active	
Test1	Test	Active	
DocFilter	DocNotif	Active	

To view an existing notification filter, click the notification filter name from the *Name* column of the *Notification Filters* table.

To add, edit, or delete notification filters:

- See Adding a Notification Filter on page 88.
- See Editing a Notification Filter on page 88.
- See Deleting a Notification Filter on page 89.
- See Testing a Notification Filter on page 89.

Adding a Notification Filter

To add a notification filter:

1. Click the *Add* button on the upper-left of the *Notification Filters* table. The *Add Notification Filters* dialog appears.
2. Enter a name for the notification filter in the *Filter Name* field.
3. Select a notification profile from the *Notification Profile* drop-down to associate that notification profile with the notification filter being created.
4. Set the filter status to *Active* or *Inactive* by toggling the *Filter Status* toggle. By default, it is set to *Active*.
5. Enter a MAC/IP address in the *Alarm Device* field. It is optional.
6. Enter an IP address/Hostname in the *Alarm Source* field. It is optional.
7. Enter a description for the notification filter in the *Filter Description* field. It is optional.
8. Enter a message in the *Alarm Message* field. It is optional.
9. Select one or more options in the *Alarm Severity* field. To select multiple options, press the *Ctrl* key on the keyboard and click the options.
10. Select one or more options in the *Include Alarms* field to specify the type of alarms to be included in the notification filter.
11. Select one or more options in the *Exclude Alarms* field to specify the type of alarms to be excluded from the notification filter.
12. Select an AP group from the *AP Group* field.
13. Click *Save*. A notification filter is created and added to the table.

Editing a Notification Filter

To edit a notification filter:

1. Click the ✎ button from the *Actions* column for the notification filter to be edited from the *Notification Filters* table. The *Edit Notification Filters* dialog appears.
2. Change the *Filter Status*, *Alarm Device*, *Alarm Source*, *Filter Description*, *Alarm Message*, *Alarm Severity*, *Include Alarms*, *Exclude Alarms*, or *AP Group* fields as required.
3. Click *Save*. The notification filter is edited successfully.

Deleting a Notification Filter

To delete a notification filter:

1. Click the 🗑 button from the *Actions* column for the notification filter to be deleted from the *Notification Filters* table. A confirmation dialog appears.
2. Click *Yes*. The notification filter is deleted successfully.

Testing a Notification Filter

To verify if the configured primary and secondary mail servers successfully send emails to the recipients configured in the notification profile associated with the notification filter from which the verification was initiated, click the ✉ button from the *Actions* column of the *Notification Filters* table.

The system displays a message on a widget if the email is sent successfully to the intended recipients.

System Settings

FortiWLM MEA allows you to configure various system settings like server details, mail server administration, system log policies, and so on. The *System Settings* branch of the tree menu in the left navigation pane is further branched into:

- Server Details on page 89
- Mail Servers on page 90
- SNMP Administration on page 92
- Maintenance on page 94
- Station Activity Log Archival Policy on page 97

Server Details

The *Server Details* screen displays the server parameters of the FortiWLM MEA service appliance. You can access the *Server Details* screen through *Administration* > *System Settings* > *Server Details*.

The following server parameters are displayed on the *Server Details* screen:

Parameter	Description
Host Name	The FortiWLM MEA service appliance host name assigned by the DNS. Typically, administrators keep the same host name even if the IP address is changed.

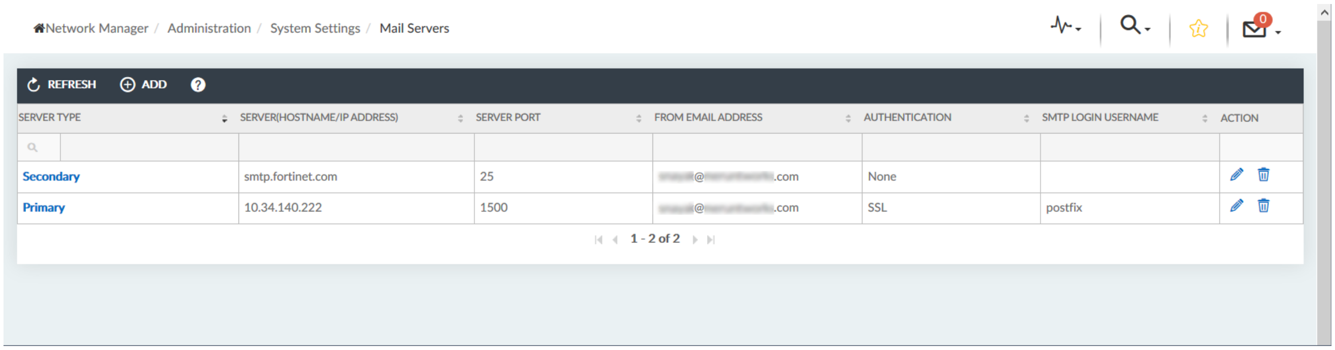
Parameter	Description
Description	A description of the FortiWLM MEA service appliance. It may include the appliance location like the building and floor it belongs to, and so on. You can modify this field.
Architecture	Shows the FortiWLM MEA service appliance system architecture. For example, 64-bit.
Public IP Address	The IP address that is configurable when the FortiWLM MEA server has a public IP address.
IPv4 Address	The IPv4 address used to connect to the FortiWLM MEA GUI of the appliance.
IPv4 Netmask	Subnet mask for the *IPv4 Address*.
IPv4 Default Gateway	The IPv4 gateway for the FortiWLM MEA appliance.
IPv6 Global Address	The global scope IPv6 address used to connect to the FortiWLM MEA GUI of the appliance.
IPv6 Link Local Address	The link-local IPv6 address.
Default IPv6 Gateway	The IPv6 gateway for the FortiWLM MEA appliance.
DHCP Server	If the FortiWLM MEA appliance does not have a static IP address assigned to it, the DHCP server assigns an IP address to it dynamically.
Software Version	The software version of the FortiWLM MEA server.
Server Model	The FortiWLM MEA server model number.
System ID	The FortiWLM MEA server system ID.

If you have modified the *Description* field, click on the *Update* button in the lower-right of the *Server Parameters* screen to update the description.

Mail Servers

The *Mail Servers* screen displays all the configured mail servers in a table. The configured mail servers notify users of alarms and/or send reports to users.

You can access the *Mail Servers* screen through *Administration* > *System Settings* > *Mail Servers*.


Network Manager / Administration / System Settings / Mail Servers
0
REFRESH
ADD
?

SERVER TYPE	SERVER(HOSTNAME/IP ADDRESS)	SERVER PORT	FROM EMAIL ADDRESS	AUTHENTICATION	SMTP LOGIN USERNAME	ACTION
Secondary	smtp.fortinet.com	25	[redacted]@[redacted].com	None		✎ 🗑
Primary	10.34.140.222	1500	[redacted]@[redacted].com	SSL	postfix	✎ 🗑

1 - 2 of 2

Click the *Refresh* button on the upper-left of the table to update the list of configured servers in the table. If the table does not have any rows, no servers are configured. If there are rows in the table, click on a link in the *Server Type* column of the table to view the server configuration details in the *View SMTP Server Configuration* dialog.

The Mail Servers screen allows you to *Add*, *Edit*, and *Delete* mail servers:

- See Adding SMTP Mail Servers on page 91.
- See Editing SMTP Mail Servers on page 91.
- See Deleting SMTP Mail Servers on page 91.

Adding SMTP Mail Servers

To add an SMTP mail server:

1. Click the *Add* button on the upper-left of the *SMTP Mail Servers* table. The *Add SMTP Server Configuration* dialog appears.
2. Select either *Primary* or *Secondary* from the *Server Type* drop-down list. FortiWLM MEA uses the secondary server if the primary server is unavailable.
3. Enter an IPv4 or an IPv6 address in the *Server (HostName/IP Address)* field.
4. Enter a port number in the *Server Port* field. The default server port number is 25.
5. Enter the sender email address in the *From Email Address* field.
6. Select an option from the *Authentication* drop-down list:
   - **a.** Select *None* for no authentication.

   OR
   - **a.** Select *TLS* or *SSL* for authentication.
   - **b.** Enter a username of your choice in the *SMTP Login Username* field.
   - **c.** Enter a password in the *SMTP Login Password* field
   - **d.** Enter the same password in the *Confirm SMTP Login Password* field.
7. Click *Save*. A mail server is added.

Editing SMTP Mail Servers

To edit an SMTP mail server:

1. Click the ✎ button in the *Actions* column for a mail server from the *SMTP Mail Servers* table. The *Edit SMTP Server Configuration* dialog appears.
2. Change the *Server (HostName/IP Address)*, *Server Port*, *From Email Address*, and *Authentication* fields as required.
3. Click *Save*. The mail server is edited.

Deleting SMTP Mail Servers

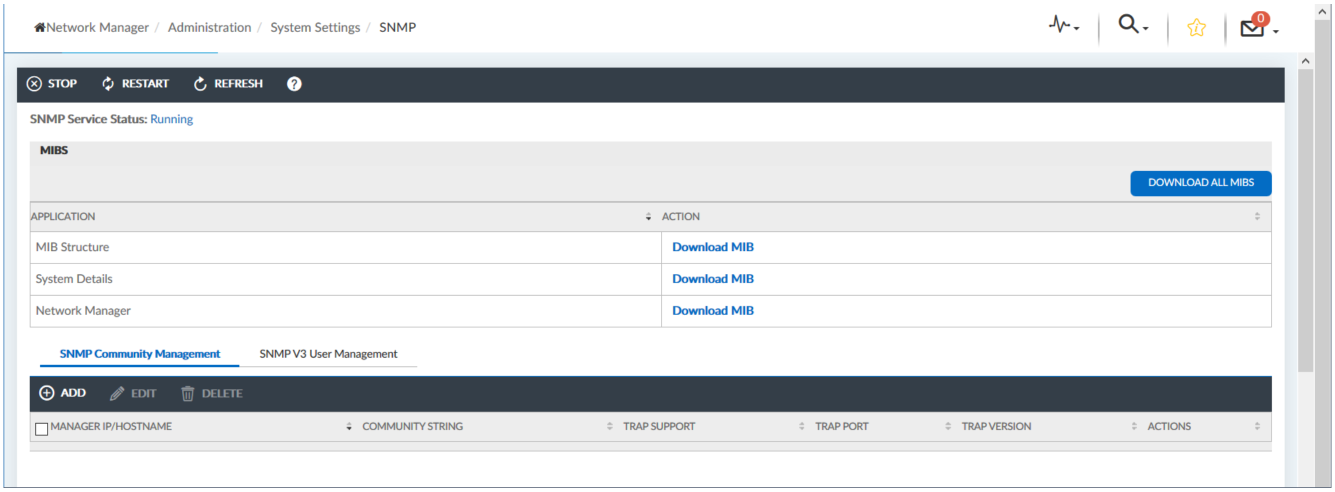
To delete an SMTP mail server:

1. Click the 🗑 button in the *Actions* column for a mail server from the *SMTP Mail Servers* table.
2. Click *Yes* in the confirmation dialog. The mail server is deleted.

SNMP Administration

Simple Network Management Protocol (SNMP) is an Internet-standard protocol for managing devices on IP networks. It uses an extensible design, where the available information is defined by Management Information Bases (MIBs). The MIBs describe the structure of management data using hierarchical namespaces containing object identifiers (OID). Each OID identifies a device attribute that can be read or set via SNMP. FortiWLM MEA provides the SNMP Administration interface that can be used to manage devices in wireless networks.

You can access the *SNMP Administration* screen through *Administration* > *System Settings* > *SNMP* .


Network Manager / Administration / System Settings / SNMP
STOP
RESTART
REFRESH
MIBS
DOWNLOAD ALL MIBS
SNMP Community Management
SNMP V3 User Management
ADD
EDIT
DELETE

SNMP Service Status: Running

APPLICATION	ACTION
MIB Structure	Download MIB
System Details	Download MIB
Network Manager	Download MIB

□ MANAGER IP/HOSTNAME	COMMUNITY STRING	TRAP SUPPORT	TRAP PORT	TRAP VERSION	ACTIONS

The SNMP service runs in the background. Click the *Stop*, *Restart*, or *Refresh* buttons on the upper-left of the screen to stop, restart, or refresh the SNMP service respectively. The *SNMP Service Status* field shows the current status of the SNMP service.

Each of the MIBs defined in the system is listed in a table. To download an application MIB, click on the *Download MIB* link from the *Actions* column for that application. You may download all the MIBs at once by clicking the *Download All MIBs* button on the upper-right of the table.

You can register external SNMP managers with FortiWLM MEA from the *SNMP Administration* screen. SNMP versions v1, v2c, and v3 are supported to receive requests. Versions v1 and v2c both are supported for trap forwarding. The *SNMP Administration* screen provides the following tabs to configure SNMP parameters:

- See SNMP Community Management on page 92.
- See SNMP V3 User Management on page 93.

SNMP Community Management

The *SNMP Community Management* tab displays a table that provides a list of the clients registered with FortiWLM MEA for SNMP services. The table summarizes the following devices parameters:

Parameter	Description
Manager IP/Hostname	The IP address or host name of the third-party SNMP manager device requesting for SNMP services.
Community String	An authentication string in which a registered client must send SNMP service requests.

Parameter	Description
Trap Support	If enabled, the SNMP traps are forwarded to the registered SNMP managers.
Trap Port	The port to which the SNMP service sends the traps.
Trap Version	The trap versions to which the registered SNMP manager wants to receive responses.
Actions	The administrative actions that may be taken on an SNMP manager.

You can add, edit, or delete an SNMP manager device from the *SNMP Community Management* tab:

- See Adding SNMP manager devices on page 93.
- See Editing SNMP manager devices on page 93.
- See Deleting SNMP manager devices on page 93.

Adding SNMP manager devices

To add an SNMP manager:

1. Click the *Add* button on the upper-left of the table. The *Add* dialog appears.
2. Enter the manager IP address or host name in the *Manager IP/Host Name* field.
3. Enter an authentication string in the *Community String* field.
4. Select an option from the *Trap Support* drop-down list.
5. Enter a port number in the *Trap Port* field.
6. Select a trap version from the *Trap Version* drop-down list.
7. Click *Save*. A new SNMP manager is added and listed in the table.

Editing SNMP manager devices

To edit an SNMP manager:

1. Select the SNMP manager to be edited by clicking on the corresponding check box in the table.
2. Click the *Edit* button on the upper-left of the table. The *Edit* dialog appears.
3. Modify the *Community String*, *Trap Support*, *Trap Port*, and *Trap Version* fields as required.
4. Click *Save*. The selected SNMP manager is edited.

Deleting SNMP manager devices

To delete an SNMP manager:

1. Select the SNMP manager to be deleted by clicking on the corresponding check box in the table.
2. Click the *Delete* button on the upper-left of the table.
3. Click *Yes* in the confirmation dialog. The selected SNMP manager is deleted.

SNMP V3 User Management

The *SNMP V3 User Management* tab displays a table that lists the SNMP v3 users enabled to respond to SNMP v3 service requests. The table summarizes the following user parameters:

Parameter	Description
Username	The username of the user.
Authentication Protocol	The protocol type used for authentication.
Privacy Protocol	The protocol type used for data encryption.

You can add or delete an SNMP v3 user, or change the password of an SNMP v3 user:

- See Adding SNMP v3 users on page 94.
- See Deleting SNMP v3 users on page 94.
- See Changing the password for an SNMP v3 users on page 94.

Adding SNMP v3 users

To add an SNMP v3 user:

1. Click the *Add* button on the upper-left of the table. The *Add* dialog appears.
2. Enter a userame in the *Username* field.
3. Select an option from the *Authentication Protocol* drop-down list.
4. Enter a string of characters in the *Authentication String* field.
5. Select an option from the *Privacy Protocol* drop-down list.
6. Enter a string of characters in the *Privacy String* field.
7. Click *Save*. A new SNMP v3 user is added and listed in the table.

Deleting SNMP v3 users

To delete an SNMP v3 user:

1. Select the SNMP v3 user to be deleted by clicking on the corresponding check box in the table.
2. Click the *Delete* button on the upper-left of the table.
3. Click *Yes* in the confirmation dialog. The selected SNMP v3 user is deleted.

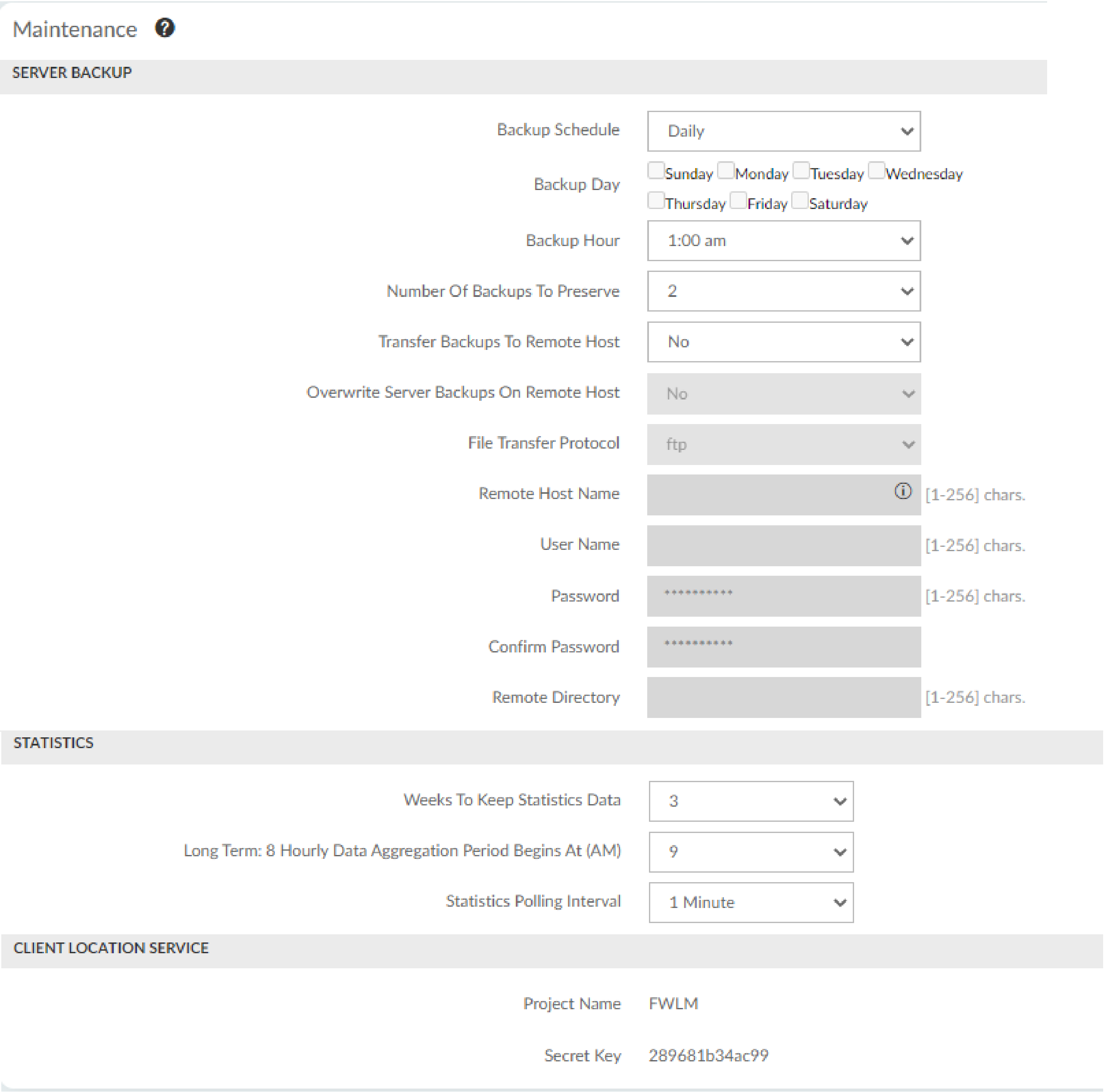
Changing the password for an SNMP v3 users

To change the password for an SNMP v3 user:

1. Select the SNMP v3 user by clicking on the corresponding check box in the table.
2. Click the *Password Reset* button on the upper-left of the table. The *Password Reset* dialog appears.
3. Modify the *Authentication String* and *Privacy String* fields as required.
4. Click *Save*. The password is reset successfully for the selected SNMP v3 user.

Maintenance

The *Maintenance* screen displays the server maintenance parameters of FortiWLM MEA. You can access the *Maintenance* screen through *Administration* > *System Settings* > *Maintenance*.



Maintenance

SERVER BACKUP

Backup Schedule	Daily
Backup Day	□ Sunday □ Monday □ Tuesday □ Wednesday □ Thursday □ Friday □ Saturday
Backup Hour	1:00 am
Number Of Backups To Preserve	2
Transfer Backups To Remote Host	No
Overwrite Server Backups On Remote Host	No
File Transfer Protocol	ftp
Remote Host Name	[1-256] chars.
User Name	[1-256] chars.
Password	********** [1-256] chars.
Confirm Password	**********
Remote Directory	[1-256] chars.

STATISTICS

Weeks To Keep Statistics Data	3
Long Term: 8 Hourly Data Aggregation Period Begins At (AM)	9
Statistics Polling Interval	1 Minute

CLIENT LOCATION SERVICE

Project Name	FWLM
Secret Key	289681b34ac99

You can configure the following parameters for FortiWLM MEA **Server Backup**.

Parameter	Description
Backup Schedule	Select a period to perform the server backup, the backup is *Daily* (default) or *Weekly*.
Backup Day	Select a day to backup the server, the default value is *Sunday*.
Backup Hour	Select a time of the day to perform the backup The *Time* is from 1.00 am. to 12.00 pm. The default backup hour is 1.00 pm.
Number Of Backups To	The number of server backups that can be preserved. The range varies from 1-3.

Parameter	Description
Preserve	The default value is 2.
Transfer Backups To Remote Host	Select to allow transfer the data backup to a remote host. Select from the following options. **Yes** - This option enables automatic transfer of server backup to remote host. By selecting this option, the following parameters related to the remote backup transfer are enabled. • Overwrite Server Backups On Remote Host • File Transfer Protocol • Remote Host Name (IPv4/IPv6) • User Name • Password • Remote Directory **No** - This option disables the automatic transfer of server backup to remote host and the above mentioned parameters related to the remote backup transfer.
Overwrite Server Backups On Remote Host	Select to overwrite the server backup on the remote host.
File Transfer Protocol	Select the protocol that is used for copying the server backup to remote host. The supported protocols are, FTP and SCP.
Remote Host Name	Enter a name for the *Remote Host*.
User Name	Enter a *User Name*.
Password	Enter a *Password* for the *User Name*.
Remote Directory	Enter the name for the *Remote Directory*.

You can configure the following parameters for FortiWLM MEA **Statistics** collection.

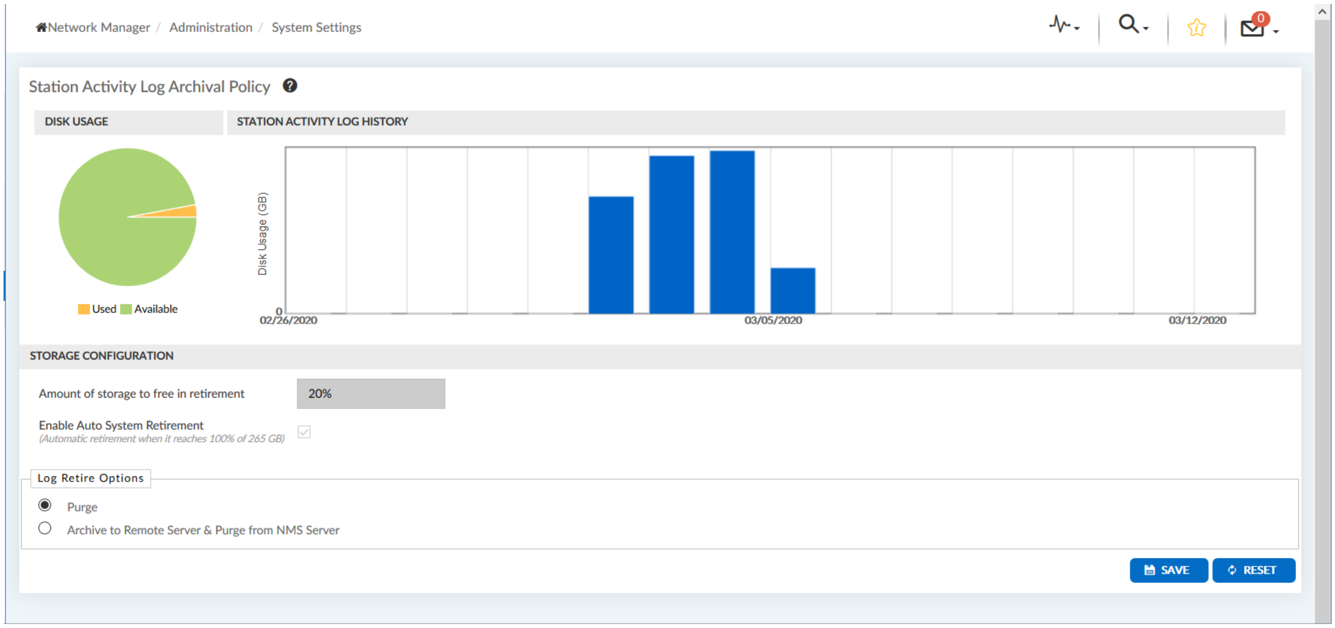
Field	Description
Months to keep statistics data	Set the number of months to preserve the statistics data. The statistics data older than the number of months specified in this field from the current date will be automatically deleted from the server. The statistics data includes, • Global trend • Controller trend • Controller distribution • AP dashboard • Station dashboard -> Statistics • Alarms • Syslog The duration to preserve the statistics is between 1 - 6 months. The default value is 3 months.
Long term: 8 hourly data aggregation period begins at (AM)	Enter the start period for the data aggregation. Enter the time for the data aggregation to begin.

Field	Description
Statistics Polling Interval	The period in minutes at which FortiWLM MEA receives the statistics from controller. The polling interval can be 10 minutes or 1 minute. **Note**: After modifying the polling interval (1 minute to 10 minutes or vice versa), it is recommended NOT to refer to the old data.

Station Activity Log Archival Policy

FortiWLM MEA archives station activity logs in a database based on the *Station Activity Log Archival Policy*. The *Station Activity Log Archival Policy* dashboard allows you to monitor the disk usage, log history, storage configuration, and so on.

You can access the *Station Activity Log Archival Policy* dashboard through *Administration* > *System Settings* > *Station Activity Log Archival Policy*.



Network Manager / Administration / System Settings

Station Activity Log Archival Policy

DISK USAGE

STATION ACTIVITY LOG HISTORY

STORAGE CONFIGURATION

Amount of storage to free in retirement: 20%

Enable Auto System Retirement ☑
(Automatic retirement when it reaches 100% of 265 GB)

Log Retire Options

● Purge
○ Archive to Remote Server & Purge from NMS Server

The *Station Activity Log Archival Policy* dashboard displays the following sections:

- Disk Usage on page 97
- Station Activity Log History on page 97
- Storage Configuration on page 98

Disk Usage

The *Disk Usage* pie chart displays the used and available disk space in percentages.

Station Activity Log History

The Station Activity Log History graph is a plotting of the *Disk Usage (GB)* over time. The bars on the bar chart represent disk usage.

Storage Configuration

The *Storage Configuration* section provides the storage configuration settings based on the *Station Activity Log Retirement Policy*. This policy enforces event archival or deletion based on the utilized disk space.

The *Storage Configuration* section displays the following fields:

- Amount of storage to free in retirement on page 98
- Enable Auto System Retirement on page 98
- Log Retire Options on page 98

Amount of storage to free in retirement

The *Amount of storage to free in retirement* filed displays the amount of storage to be deleted during retirement in percentage. By default, 20% of the events get archived or deleted when the disk usage reaches 100%.

Enable Auto System Retirement

The *Enable auto system retirement* option enables automatic retirement of the system when the storage space reaches 100%.

Log Retire Options

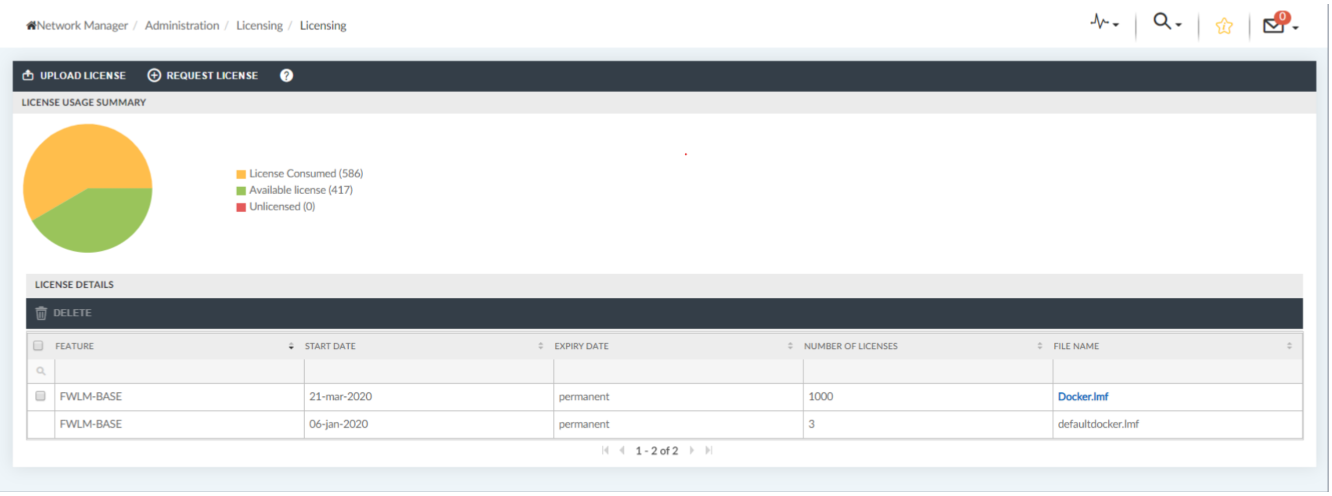
You can select either of the following options to retire logs:

- Purge: This option deletes the records based on the percentage of disk usage as compared to a configurable predefined setting.
- Archive to Remote Server & Purge from NMS Server: This option exports the records in the CSV format, transfers the records to a remote server, and then deletes the records from the FortiWLM MEA server. After you select this option, fill in the required fields manually or you can click the *Copy from Maintenance* link to emulate the remote server details from *Maintenance*, and click *Save*.

Licensing

The *Licensing* screen allows you to manage licenses for WLAN components. You can view a summary of licenses, upload new license files, or request new licenses.

You can access the *Licensing* screen through *Administration* > *Licensing* > *Licensing*.



FEATURE	START DATE	EXPIRY DATE	NUMBER OF LICENSES	FILE NAME
FWLM-BASE	21-mar-2020	permanent	1000	Docker.lmf
FWLM-BASE	06-jan-2020	permanent	3	defaultdocker.lmf

To Licensing screen has the following sections:

- License Usage Summary on page 99
- License Details on page 100

License Usage Summary

The *License Usage Summary* section provides a graphical representation of license usage on FortiWLM MEA. License usage is represented by a pie chart where different pies represent licenses in use, licenses available to use, and unlicensed APs.

By default, three permanent licenses are available.

To upload or request licenses:

- See Uploading Licenses on page 99.
- See Requesting Licenses on page 100.

Uploading Licenses

To upload a license file:

1. Click the *Upload License* button on the upper-left of the *License Usage Summary* section. The *Upload License File* dialog appears.
2. Click *Browse*, navigate to, and select the LMF license file from your local hard drive.
3. Click *Upload*. The license file is uploaded and displayed in the *License Details* section.

You can upload only one license file at a time. To upload multiple license files, repeat the process of uploading a license file multiple times. Each time you upload a license file successfully, the *License Details* section is populated with the uploaded license file details.

Requesting Licenses

To request a license:

1. Click the *Request License* button on the upper-left of the *License Usage Summary* section. The *Request License* dialog appears.
2. Follow the instructions in the *Request License* dialog.

License Details

The *License Details* section summarizes the license files being used in the form of a table. For each license file in use, the table summarizes the following:

Attribute	Description
Feature	The license feature type name.
Start Date	The start date of the license feature type.
Expiry Date	The expiry date of the license feature type.
Number of Licenses	The number of the licenses issued for the license feature type.
File Name	The license file name of the license feature type.

You can also delete license files; see Deleting Licenses on page 100.

Deleting Licenses

To delete a license file:

1. Select a license file by clicking the license file selection check box from the *License Details* table.
2. Click *Delete* on the upper-left of the table.
3. Click *Yes* in the confirmation dialog. The license file is deleted.

Permanent licenses that are available by default cannot be deleted.

Upgrade

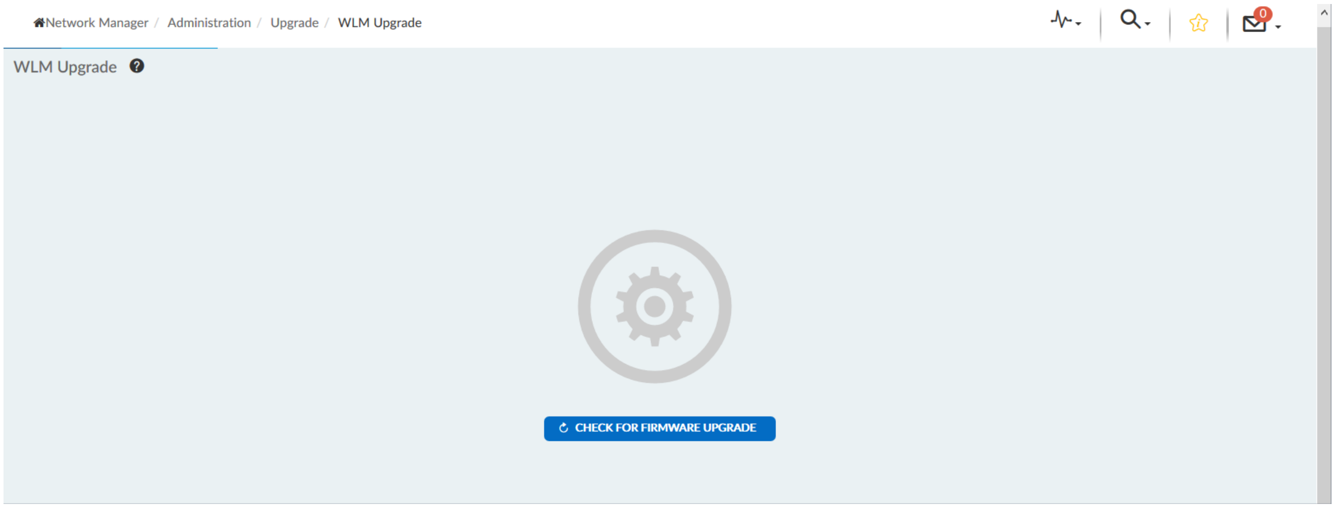
FortiWLM MEA system upgrade involves both the entire system upgrade and patch installation over a released version. The *Upgrade* branch of the tree menu in the left navigation pane is further branched into:

- FortiWLM MEA Upgrade on page 101
- Patch Management on page 101

FortiWLM MEA Upgrade

The *FortiWLM MEA Upgrade* screen allows you to upgrade the system to the latest released version.

You can access the *FortiWLM MEA Upgrade* screen through *Administration > Upgrade > WLM Upgrade*.


Network Manager / Administration / Upgrade / WLM Upgrade
WLM Upgrade
0
CHECK FOR FIRMWARE UPGRADE

To upgrade the system to the latest released version:

1. Click the *Check for Firmware Upgrade* button. The system checks for a newer version of the firmware.

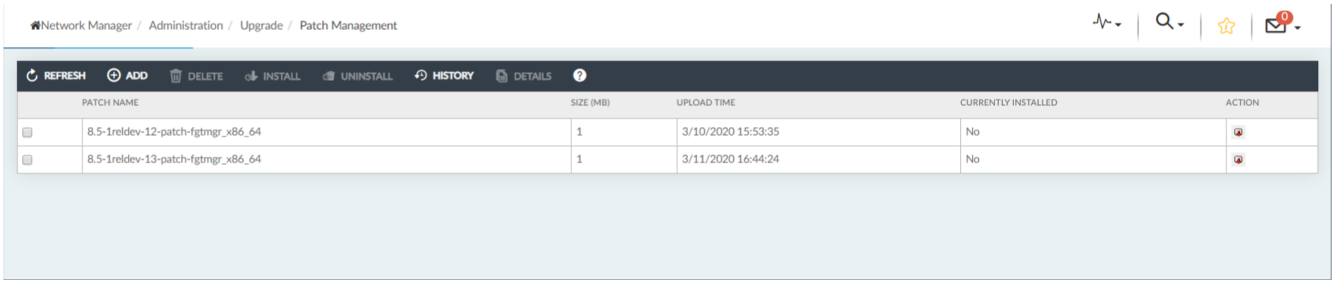
> The system will display a *Firmware Version is up to date* message if your system is the latest released version.

2. Click *Upgrade*. The system automatically upgrades to the latest available firmware.

Patch Management

The *Patch Management* screen allows you to add, delete, install, uninstall, and see details and history of firmware patches.

You can access the *Patch Management* screen through *Administration > Upgrade > Patch Management*.


Network Manager / Administration / Upgrade / Patch Management
0
REFRESH
ADD
DELETE
INSTALL
UNINSTALL
HISTORY
DETAILS

	PATCH NAME	SIZE (MB)	UPLOAD TIME	CURRENTLY INSTALLED	ACTION
□	8.5-1reldev-12-patch-fgtmgr_x86_64	1	3/10/2020 15:53:35	No	
□	8.5-1reldev-13-patch-fgtmgr_x86_64	1	3/11/2020 16:44:24	No	

To manage patches:

- See Adding Patches on page 102.
- See Deleting Patches on page 102.
- See Installing Patches on page 102.

- See Uninstalling Patches on page 102.
- See Patch History on page 102.
- See Patch Details on page 102.

Adding Patches

To add a patch:

1. Click *Add* on the upper-left of the *Patch Management* table. The *Add Patch* dialog appears.
2. Click *Browse*, navigate to, and select the FWLM patch file.
3. Click *Upload*. The patch is uploaded and displayed in the table.

Deleting Patches

To delete a patch:

1. Select a patch by clicking the patch selection check box from the *Patch Management* table.
2. Click *Delete* on the upper-left of the table.
3. Click *Yes* in the confirmation dialog. The selected patch is deleted.

Installing Patches

To install a patch:

1. Select a patch by clicking the patch selection check box from the *Patch Management* table.
2. Click *Install* on the upper-left of the table.
3. Click *Yes* in the confirmation dialog. The selected patch is installed.

Uninstalling Patches

To uninstall a patch:

1. Select a patch by clicking the patch selection check box from the *Patch Management* table.
2. Click *Uninstall* on the upper-left of the table.
3. Click *Yes* in the confirmation dialog. The selected patch is uninstalled.

Patch History

To view a brief patch history such as date of installation, build number, and so on:

1. Select a patch by clicking the patch selection check box from the *Patch Management* table.
2. Click *History* on the upper-left of the table. The patch history is displayed.

Patch Details

To view patch details such as bug resolutions delivered, the patch file md5sum, the available file permissions, and so on:

1. Select a patch by clicking the patch selection check box from the *Patch Management* table.
2. Click *Details* on the upper-left of the table. The patch details are displayed.